Az IT biztonság szabályozása

Az informatika nagyfokú fejlődésével beköszöntött az elektronikus írásbeliség, ami megreformálja a mindennapi kommunikációnkat, az adatok tárolását, és az ügyek intézésének módját is. Ez a reform viszont nem veszélytelen: mind technikai, mind szervezési oldalról sok feladatunk van, hogy ez ne vezessen egy „sötét", írásbeli emlékek nélküli legújabb korhoz. Az új technológiák kihívások elé állítják a használókat, valamint az üzemeltetőket, és egyben új vagy megújult lehetőséget biztosítanak a bűnözők számára is. A jogalkotó szempontjából kiemelkedő jelentőségű a kérdés, hogy hogyan szabályozható ez a terület. A mű a jelenlegi közösségi és magyar IT biztonsági szabályozás elemzése mellett az adatvédelmi jog mintáján mutatja be a jogi és technikai szabályozás közötti különbséget, értelmezési kihívásokat. Ezekre való megoldási javaslatként pedig felállít egy, a jogászok és informatikusok közötti kommunikációt lehetővé tévő módszertant.

Szádeczky Tamás okleveles biztonság- és védelempolitikai szakértő, okleveles mérnökinformatikus és az informatikai jog területén doktorált. CISSP, CISM, CISA és IRCA ISO 27001 lead auditor címekkel rendelkezik. Az információbiztonság területén dolgozik 2003 óta auditorként és tanácsadóként, illetve 2008 óta egyetemi oktató.

978-620-2-48764-1

Globe EDIT

Az IT biztonság szabályozása

Szádeczky Tamás

Globe EDIT

Szádeczky Tamás

Az IT biztonság szabályozása

Szádeczky Tamás

Az IT biztonság szabályozása

Szádeczky Tamás

Az IT biztonság szabályozása

GlobeEdit

Imprint

Cover image: www.ingimage.com

Publisher:
GlobeEdit
is a trademark of
International Book Market Service Ltd., member of OmniScriptum Publishing Group
17 Meldrum Street, Beau Bassin 71504, Mauritius

Printed at: see last page
ISBN: 978-620-2-48764-1

Tartalom

Lektorálta:

Muha Lajos, Ph.D.

1. Bevezetés

Az előző évszázad közepétől hatalmas fejlődés volt tapasztalható a számítástechnika területén. Az első otthoni Commodore 64-esünk és az elszigetelt BBS-ek[1] használata óta eljutottunk az egész életünket átszövő informatikai eszközök és hálózatok garmadájáig: okostelefon, notebook, Internet, amelyek táptalaján egy egész virtuális világ alakult ki. Ebben a virtuális világban a való világban tapasztalható jelenségekhez többé vagy kevésbé hasonló jelenségek tapasztalhatók. Kriminológusok vitatkozhatnak azon, hogy bizonyos bűncselekmények virtuális világban történő végrehajtása eltér-e a való világban történő elkövetéstől. Ami viszont mindenképpen egyedi: a védelem technikai végrehajtásának módja és lehetőségei. Az informatikai biztonság és védelem magába olvaszt elemeket a hagyományos területekből, mint a katonai védelem vagy a vagyonvédelem, viszont azoktól merőben eltérő tulajdonságai is vannak. Az informatikai biztonság különlegességére és fontosságára való rádöbbenés időszaka hazánkban a kilencvenes évekre tehető. Ekkor még minden biztonságról szóló dokumentumban fogalommagyarázatokat kellett feltüntetni és el kellett magyarázni, hogy ez az egész terület miért fontos. Húsz év alatt a biztonsági szakma kiharcolta létjogosultságát, az informatikai biztonságot alkalmazók, azt megfizetők többé-kevésbé tudják, hogy fontos ez a terület. A kérdés a huszonegyedik század elején nem a *miért*, hanem a *hogyan* és a *mennyire*. Az üzleti szférában – a gazdasági világválság idején különösen – nem létezik elég olcsó, nincs olyan kötelező kiadás, amiből ne akarnának még egy kicsit lefaragni. A cél viszont elérendő: az állampolgárok, a shareholderek,[2] a stakeholderek[3] és az állam célja is, hogy mindenhol – úgy az üzleti, a magánéletben és az állami szférában is – megfelelő informatikai biztonsági szint kerüljön kialakításra és fenntartásra. Nap, mint nap tapasztaljuk, hogy a biztonság oltárán való áldozat értéke a költségvetés csökkenésével négyzetesen arányos mértékben csökken. Amíg egy nagy távközlési cég esetében szinte soha nem lehet komoly hiányosságot találni, addig az otthoni számítógépére a felhasználó gyakran még az ingyenes védelmi eszközöket sem telepíti fel. Nyilván ennek rendkívül sok oka lehet: például a szakmai ismeretek,

[1] Bulletin Board System, 1970-1990 között használatos terminálcsatlakozást lehetővé tévő közösségi számítógépek elsősorban fájlmegosztás céljára.
[2] tulajdonos, részvényes
[3] a szervezet működésében érdekelt illetve érintett felek összessége

tapasztalat, információ, pénz, érdeklődés hiánya, de mindemellett a figyelem felhívása sem történik meg a területre, valamint a későbbi felelősségre vonhatóságra. A felelősségre vonhatóság pedig fontos tényező, hiszen a jogalkotó szempontjából nincs teljes megfelelés, mindenen lehet még javítani, az elérendő cél a tökéletesség.

Jelen monográfia tárgya az informatikai biztonság jogi és nem jogi szabályozása. A nem jogi szabályozás elemzésének hangsúlya is elsősorban az állami irányítás eszközrendszerébe illeszthető elemeken van. Az informatikai biztonság a lenti levezetés szerinti fogalmat takarja.

Az adatbiztonság „az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere."[4] Más megfogalmazás szerint „az informatikai rendszerekben az adatok kezelésének megfelelő minőségét jellemző állapot. az adatbiztonság három összetevőre: az integritásra, a titkosságra és a pontosságra bontható."[5]

Az adatbiztonság tágabb értelmezésében az adatok (digitális vagy papíralapú) jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere. Szűkebb értelmezésében technikai adatvédelem, tehát a jogi úton történő magánszféra-védelem műszaki-technikai megvalósítása.

Az információbiztonság „az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése; továbbá, egyéb tulajdonságok, mint a hitelesség, a számon kérhetőség, a letagadhatatlanság és a megbízhatóság, szintén ide tartozhatnak."[6] Az információbiztonság a tágabb értelmezésben használt adatbiztonsággal egy értelmű, viszont az információ szó értelmezett adatot jelent, e szerint az információbiztonság a feldolgozatlan, nem értelmezett adatot nem védené, amely nem felel meg a valóságnak. Használható viszont a szűkebb értelmezésben használt adatbiztonságtól való tartalmi elhatárolásra.

Az informatikai biztonság „olyan előírások, szabványok betartásának eredménye, amelyek az információk elérhetőségét, sérthetetlenségét és bizalmasságát érintik, és amelyeket az informatikai rendszerekben vagy komponenseikben, valamint az informatikai rendszerek vagy komponenseik alkalmazása során biztonsági megelőző

[4] ITB 8. sz. ajánlás, 1994, p. 132.
[5] Szabó J., 1995, adatbiztonság címszó, p. 6.
[6] MSZ ISO/IEC 27001:2006 3.4. p. 22.

intézkedésekkel lehet elérni. […] Informatikai biztonság alatt valamely informatikai rendszer azon állapota értendő, amelyben a kockázatokat, amelyek ezen informatikai rendszer bevezetésekor a fenyegető tényezők alapján adottak, elfogadható intézkedésekkel elviselhető mértékűre csökkentettük."[7]

Ennél rövidebb és pontosabb meghatározás, hogy „az informatikai biztonság az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.[8]

Az informatikai biztonság a tágabb értelemben vett adatbiztonság (amely alapvetően független az adat hordozójától) megvalósítását jelenti az informatikai hálózatok és rendszerek tekintetében. Nem lehet viszont elvonatkoztatni a komplex biztonságfogalomtól, így az informatikai biztonság nem jelentheti kizárólagosan például a kriptográfiai biztonságot, vagy a tűzfalak konfigurációját. Az informatikai biztonság megvalósítása tehát nem korlátozódhat a kibertérre, feltétlenül figyelembe kell vennünk az anyagi világban felmerülő biztonsági igényeket is: az épület nyílászáróinak védelmétől a humánerőforrás biztonságáig.

Az IT biztonság jelentése megegyezik az informatikai biztonsággal, mindemellett az informatika helyett az információtechnológia[9] kifejezés használata jobban hangsúlyozza, hogy a technológiák védelmét tekinti fontosnak. Angolszász nyelvterületen az IT Security kifejezés kizárólagosan használt az informatikai biztonság meghatározásaként, jelentését tekintve is ugyanúgy a komplex biztonság-megközelítés alapján alkalmazzák. Tekintettel arra, hogy az IT idegen rövidítés és a szakmán kívül kevéssé ismert, az alkalmazása az IT-hez hasonlóan kerülendő, bár a szaknyelvben már elfogadott a használata.

Az információvédelem „alapvetően a bizalmasság, a sértetlenség és a hitelesség elvesztése elleni védelmet, a megbízható működés a rendelkezésre állás és a funkcionalitás elvesztése elleni védelmet foglalja magába."[10] Tágabb értelemben tehát a szintén tág értelmében vett adatbiztonsághoz (is) kapcsolódó védelmi intézkedések

[7] ITB 8. sz. ajánlás, 1994, p. 138.
[8] Muha, 2008, p. 145.
[9] A fogalom magyarázata a Forradalmak kora c. fejezetben található
[10] ITB 12. sz. ajánlás, 1996.

összessége. Szűkebb értelemben katonai, nemzetbiztonsági használatban a titokvédelem, a minősített adatok védelme.
A lenti táblázatban összefoglalásra kerültek az alkalmazott legfontosabb fogalmak, a fogalmak tárgya, megjelenési formái és így az összefüggésük.

fogalom	**tárgya**	**formája**	**megjelenése**
adatvédelem	személyes adat	jogi	bármely megjelenés
adatbiztonság (szűk)	személyes adat	műszaki	bármely megjelenés
adatbiztonság (tág), információbiztonság	bármely adat	komplex	bármely megjelenés
információvédelem (szűk), minősített adatok védelme	minősített adat	komplex	bármely megjelenés
információvédelem (tág)	bármely adat	komplex	bármely megjelenés
informatikai biztonság, IT biztonság	bármely adat	komplex	informatikai rendszer, hálózat, adathordozó

A fentiek alapján a kutatás az informatikai biztonság tekintetében elsősorban a számítógépen tárolt és feldolgozott adatok elektronikus védelmével foglalkozik, de ahol szükséges, kitér a biztonság és a védelem más aspektusaira (a fogalom-meghatározásban található informatikai biztonság fogalmának megfelelően). A szabályozás jelen esetben nem a szűken vett jogi szabályozás, hanem a szakterületen alkalmazható bármely szabályzási módszer, így a szabványosítás és a belső szabályozás is. Másrészről viszont első sorban az állam szempontjából kerül megközelítésre a szabályozandó terület, ezért a gyakorlati részben már csak az állam által alkalmazható szabályozások kerülnek kifejtésre.

A témaválasztás aktualitását adja a szakterületre vonatkozó jogalkotási lépések szaporodása: az elektronikus közszolgáltatásokra vonatkozó jogszabályok megalkotása és az informatikai biztonságról szóló törvény tervezetének elkészítése. Közösségi szinten az adatvédelmi szabályozás újragondolási lépései: az adatmegőrzési irányelv és a hírközlési irányelv módosítása, az adatvédelmi irányelv megújításának szándékát mutató lépések a WP 29 részéről. Az időszerűség mellett kiemelendő a fontosság: ezzel a multidiszciplináris kérdéssel tudományos körökben

rendkívül kevesen foglalkoztak, de a szabályozás mindennapi gyakorlati alkalmazása elkerülhetetlen a gazdálkodó szervezetek és az állami szféra számára.

A *miért* kérdés megválaszolására a bevezető első részében leírtak alapján kevéssé van szükség, de az alapvetésben elemzésre kerül mind a veszélyeztetettség, mind a veszélyeztető tényezők összessége.

Fő cél a *hogyan* és a *mennyire* kérdések megválaszolása. A szabályozási módszerek gyakorlati megvalósításának elemzése mellett a kutatási eredményeket egyesítő megfeleltetés készült, amellyel az adatvédelemre vonatkozó jogszabályi követelményekből a szabványok alkalmazásával meghatározásra került az az informatikai biztonsági minimum, ami megkövetelhető, ami a kötelezett részéről is belátható, hogy szükséges, és csökkenti azt a jogbizonytalanságot, amely a jogalkotó esetenként nagyvonalú maximalizmusából fakad.

A tudományos problémát tehát az jelenti, hogy a heterogén informatikai biztonsági szabályozás hazánkban olyan követelményeket támaszt a kötelezettek felé, amelyeket nehéz egyértelműen meghatározni. Ezzel a szabályozás hatékonysága romlik és a jogbizonytalanság is növekszik.

A kutatás célja a jelenlegi szabályozási gyakorlat feltérképezése és az esetlegesen hiányos részek „kipótlása”, tehát a nem megfelelő mértékben szabályozott területeken az alkalmazás megkönnyítése.

2. Írásbeliség a XXI. században

Az emberiség kultúrájának egyik legfontosabb alapja az írás és az írásbeliség, amelynek kifejlődése több rendkívüli hatást kiváltó eseménnyel tűzdelt, amelyeket forradalmak nevezünk. Az írásbeliség fejlődésében az írás feltalálása után három forradalmat különböztethetünk meg.[11] Az első forradalom a fonetikus értéket hordozó alfabetikus írás feltalálása volt a Kr. e. 13. században, amely különválasztotta a szöveget a tartalomtól. A második forradalom a XV. században a Johannes Gensfleisch Gutenberg által feltalált könyvnyomtatás volt, amely lehetővé tette az írott művek elérhetőségét a nagy tömegek számára. A harmadik forradalom – melyet elektronikus írásbeliségnek nevezünk – jelenleg zajlik, és bár történelmi távlat híján nem tudjuk pontosan meghatározni a mibenlétét, azt kijelenthetjük, hogy jelentős mértékben megváltoztatta az írásbeli kommunikáció minden lényeges struktúráját, mindamellett, hogy az ezt megelőző forradalmak által elért vívmányokat is meghagyta.[12] Ez jelenti a kulcsot a digitális kultúrához és az információs társadalomhoz.

Más nézőpontból, a társadalom szerkezetét tekintve pedig szintén forradalmakról beszélhetünk, amelyek nagyfokú szerkezeti átalakulást hoztak a korábbi társadalmi berendezkedésben. A XVIII. század végén a technikai-tudományos eredmények lehetővé tették a gépek által végzett ipari tömegtermelést. Az addigi termelési módszerek megszűnése a társadalmi rétegek szerkezetét is átalakította.[13] Megszületett a vállalkozók és bérmunkások társadalmi csoportja. Az ipari forradalom Angliából indult ki és ott 1848-ra be is fejeződött, főbb műszaki találmányai a repülő vetélő, a vasnyerés koksszal és a gőzgép. A technikai fejlődés nem állt meg. A vegyészet, az elektromosság, az olajipar és az acélipar fejlődése újabb robbanásszerű változást hozott, amelyet második ipari forradalomnak hívunk és 1914 körül ért véget, a tömegtermelésen alapuló ipari társadalom elérésével. A XX. század utolsó évtizedeiben kezdődött meg az ipari társadalom átalakulása információs társadalommá. Mindezt a kommunikációs és informatikai technológiák hihetetlenül gyors fejlődése tette lehetővé és szükségszerűvé.[14] Az információs társadalom – melyben élünk – információs forradalma 3-6-szor gyorsabban zajlott le, mint az ipari

[11] Sebestyén György, 1997
[12] Balogh, 1998. p. 145. alapján, a beszéd, mint első információs forradalom elhagyásával
[13] Kinder – Hilgemann, 1992, p. 321.
[14] Bernek, 2002, p. 152.

társadalmat kialakító ipari forradalom.[15] A számítógép gyors és nagyfokú fejlődése tette alkalmassá azokat az élet sok területén történő felhasználására. Az információfeldolgozás és tárolás, valamint a monoton számítási műveletek elvégzése miatt a közigazgatás, az üzlet és a magánélet területén is, főleg az Internet, mint globális információs hálózat széleskörű és szélessávú hozzáférhetőségével beivódott mindennapjainkba.

A továbbiakban a társadalmi szerkezetváltozással szemben az írásbeliség megváltozásának hatása kerül a vizsgálat előterébe. Az elektronikus írásbeliség fejlődésével teret hódítottak a számítógépek és a számítástechnika a hagyományosan papírhordozót használó alkalmazásokban. A számítástechnika „a tudománynak és a technikának az automatizált adatfeldolgozás elméletével, gyakorlati megvalósításával és eszközrendszerével foglalkozó területe."[16] A számítástechnika fogalma egyesíti magában az elméleti- és az alkalmazott matematika több területét, így különösen a számítástudományt és logikát, valamint a mérnöki tudományok egyes területeit. A számítástechnika tárgya a számítógép, amelynek tervezésétől az üzemeltetésén át az alkalmazásokig lefedi a teljes területét. Az informatika (computer science) „az információ rendszeres és automatikus – elsősorban számítógép segítségével történő – feldolgozásával és továbbításával foglalkozó tudomány,"[17] illetve „adatok, szövegek elektronikus jelekké (információvá) való átalakításával, ezek szerkezetével, tárolásával, rendezésével és feldolgozásával foglalkozó elmélet és ennek gyakorlati alkalmazása."[18]

„Az informatika az a tudományág, amely a tudományos információ struktúráját és tulajdonságait (de nem sajátos tartalmát) vizsgálja, továbbá a tudományos információs tevékenység szabályszerűségeit, elméletét, történetét, módszertanát és szervezetét."[19]

„Az informatika, mint diszciplína meghatározásában kétértelműség figyelhető meg. Az informatikát valaha az információ tudományának tekintették, így az információs technológia és rendszerek, az „informatistics", az „informology" és az „informatilogy" szinonimájának. Az informatikát inkább az információtudományhoz, semmint a számítógép-tudományhoz kötődő kifejezésnek tekintették, mint az információtudomány alkalmazott formáját. Azt is mondják, hogy annak ellenére, hogy

[15] Masuda, 1988, p. 46.
[16] Szabó J., 1995, számítástechnika címszó p. 1241.
[17] Breuer, 1995, p. 13.
[18] Bakos, 1994, informatika címszó
[19] Simpson, 1993, informatics címszó

lehetősége van meghatározó szerepet játszani az információs társadalom technológiai alapja kialakításában, az informatika még mindig formálódóban van. Saját alapvető fogalmainak kifejlesztésével egyre inkább úgy határozzák meg, mint különféle tudományterületek ötvözetét. Az informatika interdiszciplináris területként bontakozik ki, amely az információ és a technológia természetét tanulmányozza arra összpontosítva, az emberek hogyan hozzák össze e kettőt annak érdekében, hogy előállítsák és menedzseljék (kezeljék) az információt és a tudást."[20]

Az informatika a számítástechnikánál annyival tágabb értelmű terület, hogy az információelmélet és a híradástechnika területét is magában foglalja, vagy még inkább csak kiemeli jelentőségüket.

A köznyelvben ma inkább csak divatosabb kifejezés a számítástechnikánál, ezért a korábbi számítástechnika tantárgyat átkeresztelték informatikává, a tematikán pedig nem változtattak. Ez utóbbi néven futó középiskolai tárgyak vagy felsőoktatási kurzusok továbbra sem tartalmaznak hírközléselméletet, vagy a GSM technológia alapjait.

Az információtechnológia (Information Technology, IT) „a számítástechnika, a hírközléstechnika és az információ feldolgozásával foglalkozó összes eszköz, szolgáltatás és ezek alkalmazása együtt."[21]

„Átfogó fogalom, az információszerzés céljából alkalmazott adatfeldolgozási módszerek és eljárások (számítástechnika, adatfeldolgozás, hardver, szoftver, adatbázisok, stb.) együttese."[22]

Az információtechnológia a korábban ismertetett informatika, mint tudomány tárgyát képező technológiák összessége. Angolszász nyelvterületen szinte egyedül alkalmazott kifejezés a gyakorlati informatikára.

Az információs és kommunikációs technológiák (IKT, ICT) fogalma az információtechnológiánál a kommunikációs technológiákkal, tehát hírközlési technológiákkal bővebb fogalom. Megtekintve az információtechnológia címszót, ez elvileg már benne foglalt fogalom. Ezért érdemes ezeket ismét kissé szétválasztani. Mivel a számítástechnika és hírközléstechnika konvergenciája növekvő mértékű (pl. rádiós adatátvitel, WLAN, 3G), ez nehéz feladat, de a kommunikációs technológiák határát talán élesebben látjuk: a nyilvános kapcsolt vonali „vezetékes" telefon (PSTN)

[20] Shaoyi, 2003.
[21] Bakos, 1994, információtechnológia címszó
[22] Szabó J., 1995, információtechnológia címszó p. 590.

egyértelműen kommunikációs technológia, ahogyan a GSM mobil távközlés is az. Viszont a VoIP[23] alapú helyhez kötött telefon szolgáltatáson (pl. UPC telefon vagy T-Home Kábeltelefon) már elgondolkozhatunk: mivel az átviteli közeg a számítógép-hálózatokban alkalmazottakkal megegyező, ezt inkább információtechnológiának tekinthetnénk. Ez a kategorizálás tehát kevéssé tudományos, inkább a hagyományos hírközléstechnika információtechnológiától való megkülönböztetését szolgálja.

Ilyen, fent említett hagyományosan papírhordozót használó alkalmazásnak tekinthetjük az iratkezelést, a számviteli bizonylatolást, valamint általában a köziratok, köz- és magánokiratok készítését. Az ehhez szükséges technikai feltételek már az 1990-es évek óta adottak, mióta a számítógép-technikai és hálózati technológiák mellett kidolgozásra került az aszimmetrikus kulcsú titkosítás technológiája. Ez tette lehetővé az elektronikus aláírás megalkotását, majd a jogi kereteket meghatározó jogszabályok elfogadását. A nemzetközi gyakorlatban, illetve a magyar jogszabályi követelmények alapján a dokumentumok elektronikus hitelesítését elektronikus aláírással oldhatjuk meg.

Az Európai Unióban, illetve a Magyar Köztársaságban a jelenlegi politikai, illetve jogalkotói törekvések az elektronikus írásbeliség (és így az információs társadalom) igen gyors fejlődését tűzték ki célul.

A következő alfejezetekben a követelmények, az elért vívmányok és az ezekből fakadó kockázat kerül nagyító alá. A számítógéprendszerek komplexitásának növekedésével és az ügyvitel egyre nagyobb mértékű számítógépesítésével ugyanis fokozódik az informatikai biztonsági kockázat. A hardver, szoftver és hálózat (hálózati szolgáltatások) komplexitása folyamatosan növekszik, viszont ezzel szemben a biztonsági intézkedések fejlődése lemaradt.[24]

[23] Voice over Internet Protocol, számítástechnikai hálózaton továbbított beszédhang-alapú kapcsolat, a végpontok tekintetében a felhasználó számára hagyományos kapcsolt vonali telefonnak (PSTN) tűnik.
[24] Crume, 2003, p. 249.

2.1. Az elektronikus írásbeliség kialakulásának feltételei

Az elektronikus írásbeliség kialakulásához szükséges műszaki követelmények három részre bonthatók: a számítógépre, a hálózati kapcsolatokra és az írásbeliség követelményeinek gyakorlati megfelelést biztosító adatbiztonsági eljárásokra.

A Zuse Z3-at, az első Turing-teljes digitális számítógépet Konrad Zuse alkotta meg 1941-ben. A tranzisztor megalkotása 1947-ben forradalmasította az addig kezdetleges elektromechanikus számítógépek világát.[25] 1958-ban elkészült az integrált áramkör, az egy lapra szerelt tranzisztorok tömege. Az első személyi számítógép (IBM PC) megjelenésével 1981-ben lehetőség nyílt arra, hogy az emberek otthonába, illetve munkaasztalára kerülhessen az addig csak a számítóközpontokban, illetve azokhoz kapcsolódva elérhető számítási teljesítmény.

A számítógép-hálózatok fejlesztése 1962-ben kezdődött, amikor az Advanced Research Projects Agency (ARPA) Intergalactic Network néven kutatócsoportot állított fel J. C. R. Licklider vezetésével, amely csoport kifejlesztette az időosztásos rendszert, ami lehetővé tette a fent említett mainframe[26] szolgáltatásainak nagyszámú felhasználó közötti megosztását telexhálózaton.[27] 1969-ben szintén az ARPA keretein belül a Leonard Kleinrock vezette amerikai kutatócsoport megalkotta az első csomagkapcsolt számítógépes hálózatot, az ARPANET-et. A hálózat ekkor még csak négy végpontot kapcsolt össze.[28] A hálózat polgári, és főleg szélesebb körű alkalmazása egészen a hetvenes évek végéig váratott magára, ekkor azonban robbanásszerű fejlődésnek indult, majd a katonai eredetet jelző ARPANET név 1998-ban Internetre változott. A World Internet Project 2007-es adatai szerint a magyar háztartásoknak már 49%-ában, tehát közel kétmillió háztartásban van számítógép, valamint harmadában (35%) van internetkapcsolat.[29]

Még egy igen jelentős, de általában kisebb hangsúlyt kapó követelmény merül fel az elektronikus írásbeliség kialakulásával kapcsolatban: a humán erőforrás. Az állampolgárok, ügyfelek részvételi hajlandósága az információs társadalomban való aktív részvételre, hajlandóságuk és képességük az elektronikus írásbeliség

[25] Köpeczi Béla, 1974, p. 206.
[26] Számítóközpontban működő nagy teljesítményű számítógép, amely több felhasználót szolgált ki.
[27] Kita, 2003, p. 65.
[28] University of California, Los Angeles (UCLA), Stanford Research Institute's Augmentation Research Center, University of California, Santa Barbara (UCSB), University of Utah's Computer Science Department
[29] ITTK, 2007, p. 38.

vívmányainak használatára. Ezen és a gazdasági aspektus értékelését a fejezet a mű korlátozott terjedelme miatt nem tartalmazza.
A fejezet további részében műszaki feltételként az adatbiztonsági eljárások és a jogi-politikai feltételek kialakulása kerül ismertetésre, mint a témakör jelen megközelítése szempontjából kiemelt jelentőségű területek.

2.1.1. Adatbiztonsági eljárások

Az elektronikus írásbeliség kialakulásának igen fontos része az írásbeliség követelményeinek megfelelést biztosító adatbiztonsági eljárások kialakulása és nyilvános használata.
Az adat fogalmának meghatározására „tények és elképzelések nem értelmezett, de értelmezhető formában való közlése, formailag befogadható, de szemantikailag nem értelmezett közlés."[30] „Az adatok az információ, különösen a számítógépben feldolgozásra kerülő információ ábrázolására használt jelsorozatok. A feldolgozásra vonatkozó utasítások szintén adatoknak minősülnek. A számítógépben az adatokat rendszerint bináris ábécé reprezentálja."[31]
Adatnak tekintjük mindazon elektronikus rendszerben vagy adathordozón tárolt, papíralapú hordozón tárolt vagy nem tárolt formában létező tényeket és elképzeléseket, amelyek a megjelenési formától, kódolástól, rejtjelzéstől függetlenül folyamatok és rendszerek bemenetét, kimenetét, vagy részeredményét képezik.
Az adat fogalma sok megközelítésben előfordul és gyakran trivialitásként kezelik jelentését ezért szükséges megkülönböztetni az adat-fogalmakat egymástól: elektronikus adat (számítógéprendszerben alapvetően binárisan tárolt adat, tartalmától függetlenül, pl. JPEG kép), papíralapú adat (papírhordozón megjelenő adat, tartalmától függetlenül, pl. nyomtatott könyv), személyes adat (hordozótól függetlenül, tartalmát tekintve természetes személlyel kapcsolatba hozható adat, ld. 2.1.3.), stb.
„Az információ (latinul: informatio, képzés, felvilágosítás, kioktatás) a mindennapi életben tudásnyereséget jelent. Az információelméletben az információ (rövidítése: I) tisztán egy technikai mérték, amelyet az üzenethordozó jelsorozathoz rendelünk. Az

[30] Balogh, 2005, p. 20.
[31] Breuer, 1995, p. 55.

információ szigorú, általános definíciója azonban még nem alakult ki."[32] Az információ az üzenet [adat] hírtartalmát jelenti.[33]

Az információelmélet szerint az információ- vagy hírtartalom jellemzője az entrópia, amely egy valószínűségi változó által reprezentált véletlen kísérlet kimenetelének bizonytalansága. A biztosan bekövetkező esemény kimenetelének bizonytalansága, így egyben az entrópia, tehát az információtartalom nulla. Ilyen például a levegőbe feldobott tárgy leérkezését jellemző valószínűségi változó, míg a lottószámokat jellemző valószínűségi változó meglehetősen nagy entrópiát mutat.

A fentiek alapján az információ fogalom az adat fogalmának valódi részhalmazát képezi, jelentését tekintve az értelmezett adatok tartoznak bele. Ettől függetlenül a köznyelvben és a nem információelméleten alapuló szaknyelvben gyakran nem különböztetik meg az adat fogalmától, így például az adatvédelem és az információvédelem fogalmak közötti különbség nem az entrópiában keresendő.

Az adatok logikai biztonságának eléréséhez szükséges azok bizalmasságának, hitelességének és sértetlenségének igazolása.

„A biztonság ma komplex fogalom és állapot; a politikai, gazdasági, katonai, szociális, humanitárius, környezetvédelmi szférákra, valamint a katasztrófa-elhárításra egyaránt kiterjed. Ez az átfogó, sok ország tapasztalatain alapuló meghatározás azonban Magyarországon még nem vált általánossá. Jelenleg még inkább a szűkebb, a külpolitikára és a katonai szempontokra értelmezett fogalomra szorítkozik. Egy ilyen szűkebb, praktikusabb értelmezés és fogalom célszerű változata (Magyarországra vonatkoztatva) lehet: A Magyar Köztársaság biztonsága komplex fogalom, olyan reális képességeken nyugvó helyzet és állapot, amely magában foglalja: az ország lakosságának, területének, állami érdekeinek, nemzeti értékeinek megóvását és védelmét minden olyan külső és belső potenciális veszélytől, fenyegetéstől, amely az emberi és nemzeti (nemzetiségi, etnikai, vallási) létet, az egyén boldogulását, a progresszív irányú fejlődét hátráltatja és akadályozza."[34]

A biztonságot olyan állapotnak tekinthetjük, amelyben kizárható, vagy megbízhatóan kezelhető az esetlegesen bekövetkező veszély, illetve adottak a veszéllyel szembeni eredményes védekezés feltételei.[35]

[32] Breuer, 1995, p. 33.
[33] Sramó András, 2004, http://nti.btk.pte.hu/main/ictsources/M/infojelm.html
[34] Szabó J., 1995, biztonság címszó p. 144.
[35] Gyuricza Béla értelmezése In: Horváth István – Kiss Jenő, 1997. p. 77.

Tehát a biztonság nem a veszély hiánya, nem egy konstans állapot, hanem a biztonsági kihívások és a biztonsági kihívásokra adott válaszoknak az eredője, dinamikus állapothalmaz. A biztonsággal foglalkozók célja, hogy a biztonsági kihívások és a biztonsági kihívásokra adott válaszok egyensúlyban legyenek.

A hagyományos írásbeliségben a bizalmasságot (biztonságot) borítékkal, a hitelességet sajátkezű aláírással és a sértetlenséget a papír fizikai sértetlenségének szemrevételezés útján történő ellenőrzésével lehetett ellenőrizni. Az elektronikus írásbeliségben ugyanezt matematikai módszerekkel valósítjuk meg, amellyel a kriptográfia (titkosítás) tudománya foglalkozik. Az információ titkosítása gyakorlatilag az írással egyidős, hiszen mióta üzeneteket papírra (vagy agyagtáblára) vetünk, azóta felmerül arra is az igény, hogy ezt mások ne tudják elolvasni. Az ókortól napjainkig négy generációját különböztetjük meg a titkosítást és visszafejtést lehetővé tevő logikai-matematikai eszközrendszereknek, melyeket kriptorendszereknek nevezünk. Három generáció történeti előzménye a mai kriptorendszereknek, amelynek robbanásszerű fejlődését a számítástechnika fent vázolt eredményei tettek lehetővé. Ez a három az egyábécés kriptorendszerek (pl. Caesar-rejtjelzés), a többábécés kriptorendszerek (pl. De Vigenere rejtjelzés) és a rotoros gépek (pl. Enigma) generációi.[36]

Negyedik generációs kriptorendszereknek a XX. század végén kifejlesztett, teljesen matematikai alapú és számítógépet használó titkosítási módszereket nevezzük. Ezeknek két fajtája van: a szimmetrikus és az aszimmetrikus titkosítás. Elsődleges különbség köztük az, hogy szimmetrikus esetén ugyanazt a kulcsot használjuk titkosításra és visszafejtésre is (ezért egy kulcsosnak is nevezik ezt a módszert), míg aszimmetrikus esetén a titkosítási és visszafejtési folyamatot külön kulccsal végezzük.

A szimmetrikus titkosítás az 1970-es években került kifejlesztésre. A titkosításhoz invertálható (visszafordítható) függvényeket alkalmazunk és blokkonként (általában 64-256 bit) keverést és behelyettesítést végzünk az adott nyílt szövegen. Ezek az eljárások megegyeznek az első generációs kriptorendszereknél alkalmazottal, a különbség csak az, hogy ezeket biteken végezzük, másrészt pedig ezt a műveletsort többször megismételjük (iteráljuk). Így a viszonylag egyszerű eljárások kombinálásával, illetve nagyszámú ismétlésével igen jó biztonság szintet lehet elérni. Ezek a blokkok alapesetben nincsenek kapcsolatban egymással (ez az Electronic Code

[36] Virasztó Tamás, 2004, p. 19-38.

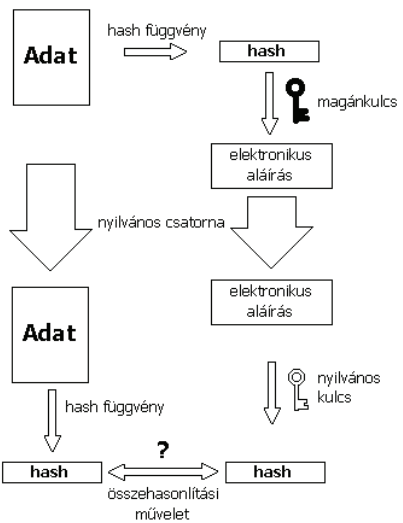
Book), de a biztonság növelése érdekében ezeket a blokkokat különböző módokon kapcsolatba hozhatjuk egymással (ilynek a Cypher Block Chaining, Cipher Feedback és Output Feedback módok).[37] Ilyen népszerű szimmetrikus kriptorendszer a Data Encryption Standard (DES), amelyet ma már a kulcshossz rövidsége miatt (56 bit) nem tartunk biztonságosnak, de még több helyen használják. A DES-re kiírt törési versenyek[38] alapján kijelenthető, hogy megfelelő hardver alkalmazásával akár órák alatt feltörhető bármely titkosított üzenet. Magából a szimmetrikus titkosítás elvéből fakadóan a titkosított szöveg minden esetben feltörhető, csak idő kérdése. A titkosítás biztonságát csak az alkalmazott matematikai algoritmus jósága, illetve a kulcs hossza határozza meg, tehát az algoritmus titkossága nem (ez a Kerchkhoffs-elv).[39] Ettől függetlenül egyes esetekben a biztonság növelése érdekében (DES) vagy szerzői jogi okokból kifolyólag (IDEA) az algoritmus is titkos lehet. A ma már elsősorban alkalmazott módszer a századfordulón kifejlesztett Advanced Encryption Standard (AES), amely 128-256 bit kulcshosszal és az eddigi kísérletek alapján megfelelő algoritmusválasztással (eddig senki nem talált rajta gyenge pontot) a világ összes számítógépével évmilliók alatt lenne feltörhető.[40]

A kriptográfia jelenlegi tudományának teljes felborítását jelentené a kvantumszámítógépek kifejlesztése, amelyekkel igen rövid időn belül visszafejthető lenne a jelenlegi legerősebb szimmetrikus kulccsal titkosított szöveg is.[41]

A modern kriptográfia másik ága a hasonlóan 1970-es években kifejlesztett nyilvános kulcsú vagy aszimmetrikus kulcsú kriptográfia. Itt a matematikai alapokat már más problémák jelentik. Ilyenek többek között a nagy számok prímtényezőkre bontását jelentő faktorizációs probléma (RSA, Rabin, Blum-Goldwasser sémák alapulnak ezen), a diszkrét logaritmus problémája (Diffie-Hellmann és ElGamal kriptorendszerek), valamint a részhalmaz-összeg probléma (Merkle-Hellman knapsack, Chor-Rivest knapsack sémák).[42] Ezen problémák megoldása egy bizonyos titok (magánkulcs) ismeretében egyszerű, míg annak hiányában igen nehéz matematikai probléma. Az aszimmetrikus rendszerek alkalmazásánál általában nagyobb kulcsot kell használni (1024-4096 bit) és több időt vesz igénybe a kódolási és dekódolási folyamat is, de az elért biztonság megegyezik a szimmetrikus

[37] bővebben lásd Horváth László – Lukács György – Tuzson Tibor – Vasvári György, 2001, p. 111.
[38] lásd http://www.rsa.com/rsalabs/node.asp?id=2108 [2010. 05. 10.]
[39] Virasztó Tamás, 2004, p. 9.
[40] Virasztó Tamás, 2004, p. 50.
[41] Schneier, 1996. 7
[42] Menezes–Oorschot–Vanstone, 1996, p. 284.

kriptorendszereknél elérhetővel. Az, amiért ez forradalmasította a kriptográfiát, az a kulcscsere problémáinak kiküszöbölése. Először Diffie, Hellman és Merkle publikálták a biztonságos kulcscsere elméletét. Az elmélet szerint a kommunikáló partnereknek az üzenetváltás előtt nem szükséges titkosított csatornán megosztania a kulcsot. Ezzel, és az aszimmetrikus titkosítási módszerrel vált lehetővé a titkosítás széleskörű publikus alkalmazása az elektronikus aláírás és a nyilvános kulcsú infrastruktúrán (PKI) alapuló rendszerek által. Az aszimmetrikus titkosításhoz egy közös titokból kell matematikai úton két kulcsot (egy kulcspárt) generálni. Ezután a közös titok megsemmisítésre kerül. A kulcspár egyik tagja lesz a kriptográfiai magánkulcs, amely semmilyen körülmények között nem kerülhet ki a tulajdonos ellenőrzéséből. Ha ez mégis megtörténne, azt kompromittációnak nevezzük és a kulcspárt többé nem szabad használni, illetve ha infrastrukturálisan lehetséges, azt vissza kell vonni. A kulcspár másik tagja a nyilvános kulcs, amely közzétehető az Interneten, illetve bármely nem biztonságos csatornán továbbítható. A két kulcs a használat szempontjából ekvivalens, tehát amit az egyik kulccsal titkosítottunk, azt a másik kulccsal lehet visszafejteni. Így lehetővé válik az eltérő irányok alkalmazása (titkosítás és elektronikus aláírás).

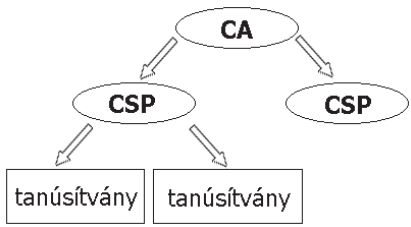


2. ábra: Az elektronikus aláírás folyamata

Az elektronikus aláírás készítésének folyamata a következő: az adatból egy úgynevezett hash függvénnyel ujjlenyomatot képezünk. Ez a függvény egy csapóajtó függvény, amely azt jelenti, hogy a függvény elvégzése az egyik irányba egyszerű, a másik irányba pedig bonyolult matematikai feladat. Ez a függvény tetszőleges mennyiségű adatból egy állandó méretű (128-512 bit) adathalmazt generál. A bemeneti adathalmazban egyetlen bit megváltozása legalább a kimeneti bitek 50 százalékát meg fogja változtatni (ez a lavinahatás). A kimenetként kapott adathalmazt ujjlenyomatnak nevezzük, mivel közel egyedi módon jellemzi a bemeneti adathalmazt. A kimenetből a bemenetet előállítani nem lehet. A gyakorlatban jellemzően az SHA-256, SHA-512, esetleg az SHA-1, RIPEMD-160, Whirlpool, SHA-3 algoritmusokkal találkozhatunk. Az elavult MD5, SHA-1, RIPEMD-160 algoritmusok használata többé elektronikus aláírási célra nem biztonságos.[43] Az aláírandó dokumentumon ezt a folyamatot végrehajtva kapott ujjlenyomatot a kriptográfiai magánkulccsal titkosítjuk. Így megkapjuk az elektronikus aláírást. Az aláírt dokumentumot és az aláírást együtt, egy nyilvános csatornán, például e-mailben elküldhetjük a címzettnek. A címzett az elektronikus aláírást a mi nyilvános kulcsunkkal megfejti, így megkapja azt az ujjlenyomatot, amelyet mi készítettünk. Ezalatt az átküldött dokumentumból ő is elkészíti az ujjlenyomatot, és ezt a kettőt összehasonlítja. Amennyiben ezek megegyeznek, biztosan állíthatjuk, hogy az aláírt dokumentumban nem történt változtatás, valamint hogy egy meghatározott kulccsal történt a dokumentum aláírása. Nem bizonyítja viszont azt, hogy ez ténylegesen a feladónak a magánkulcsa volt, azt, hogy ezt nem vonták vissza, és nem állapítható meg belőle a feladás ideje sem. Ezek bizonyítására más, kiegészítő funkciókat kell alkalmazni. A kulcsok személyhez kötését, a hitelességi problémát kétféle módon oldhatjuk meg: egyrészről a bizalmi háló (*web of trust*) módszerével,[44] amelyet a PGP használ. Ezen módszer szerint az egymásban megbízó személyek egymás kulcsait aláírják, így ha a címzett megbízik a feladó kulcsát aláíró bármelyik személyben, vagy vissza tudja vezetni az aláírásokat egy megbízható személyig, akkor ez biztosítékot jelent számára a feladó megbízhatóságára is. Ennek a módszernek a hátránya, hogy igen nagy bizalmi hálókat követel meg az, hogy két ismeretlen ember közös ismerőssel rendelkezzen. Másik módszerként a nyilvános kulcsú infrastruktúra (Public Key Infrastructure, PKI) használatos. Itt a felek megbízhatóságát egy mindenki által

[43] Sotirov–Stevens–Appelbaum–Lenstra–Molnar–Osvik–Weger, 2008.
[44] bővebben lásd Alfarez Abdul-Rahman, 1997. p. 2.

megbízható harmadik személy tanúsítja. Ez tanúsítvány segítségével történik, amely egy elektronikus adathalmaz és általában tartalmazza a nyilvános kulcsot is. A harmadik személy a megbízhatónak tartott hitelesítés-szolgáltató (Certificate Service Provider, CSP), aki a tanúsítvány kiadása előtt ellenőrzi a kulcsbirtokos és a kulcs összetartozását (például személyigazolvány kérésével). Ezek a hitelesítés-szolgáltatók tanúsítási láncot alkotnak, amelynek a tetején a legmagasabb szintű gyökér hitelesítés-szolgáltató áll. Ezek a CA-k mindenki által elfogadottak és ebből kifolyólag a tanúsítási lánc többi eleme is megbízhatóvá válik. Az aláírás idejének hiteles megállapítása időbélyeg szolgáltató (Time Stamping Authority, TSA) segítségével történik, aki a pontos időt látja el saját elektronikus aláírásával, amit a feladó beépít a dokumentum elektronikus aláírásába. Az időbélyeg igénylése alapvetően Interneten keresztül, on-line történik. A TSA megbízhatóságát a tanúsítványa biztosítja, amely a tanúsítási lánc mentén visszavezethető egy CSP-hez. Az elektronikus aláírások, illetve tanúsítványok használati köre korlátozott. Egy kulcspárt csak elektronikus aláírásra, vagy titkosításra, vagy biztonságos kapcsolat kiépítésére (SSL) lehet használni. Amennyiben ezek közül több funkciót is használni kívánunk, több kulcspárra, illetve tanúsítványra lesz szükségünk.



3. ábra: a tanúsítási lánc

Az ismertetett fejlődési folyamat a bemutatott két évezred során szerves fejlődéssel elért oda, hogy bizonyítottan alkalmas legyen az elektronikus írásbeliség kiszolgálására. Ez a tény persze közel sem elegendő e cél eléréséhez.

2.1.2. Szabályozási háttér és gyakorlat

Az elektronikus aláírás algoritmikus és műszaki infrastrukturális megvalósítása után a tényleges gyakorlati használathoz szükséges volt az, hogy ezt a jogalkotó is elfogadja,

és így ki lehessen váltani a papír alapú aláírást elektronikus aláírással az írásba foglalást megkövetelő minden területen. Az elektronikus aláírás, mint a hagyományos aláírást több jogterületen kiváltó aktus jogi elfogadására Európában először Németországban 1996-ban (Gesetz zur digitalen Signatur), az Egyesült Királyságban 1999-ben (Building Confidence in Electronic Commerce – A Consolidation Document), az Európai Unió szintjén 1999-ben (az elektronikus aláírás közösségi keretéről szóló 1999. december 13-i 1999/93/EK európai parlamenti és tanácsi irányelv), az Egyesült Államokban 2000-ben (Electronic Signatures in Global and National Commerce Act) megszületett jogszabályok teremtettek lehetőséget. A magyar jogalkotásban az első ilyen lépés a 2001. évi XXXV. törvény az elektronikus aláírásról. A törvény alapelveit a Kormány az elektronikus aláírásról szóló törvény szabályozási alapelveiről és az ezzel kapcsolatban szükséges intézkedésekről szóló 1075/2000. (IX. 13.) Korm. határozatban határozta meg. A főbb alapelvek a technológiafüggetlenség, a joghatály meg nem tagadhatósága, a hitelesítés-szolgáltatás szabályozottsága és a szolgáltató felelőssége, a minősített elektronikus aláírással ellátott elektronikus irathoz teljes bizonyító erejű magánokirati, illetve közokirati minőség elrendelése, az alkalmazás önkéntessége, az állami alkalmazás és a külföldi szolgáltatók feltételhez kötött elfogadása.

Az elektronikus kormányzati szolgáltatások részben e törvény alapján indultak el. Az elektronikus adóbevallás a 90-es évek végétől több fázisban vált elérhetővé, melynek 2002 és 2006 voltak a fordulópontjai.[45] 2003-ban indult a TakarNet, a földhivatali elektronikus adatszolgáltató rendszer, 2005-től az Ügyfélkapu, 2006-ban megszülettek az elektronikus iratkezelésre vonatkozó jogszabályi követelmények, elindult az elektronikus közbeszerzés, 2007-ben az elektronikus cégeljárás, 2008-ban indult az Adó- és Pénzügyi Ellenőrzési Hivatal elektronikus árverése, az ügyvédek számára a jogügyletek biztonságának erősítése céljából hozzáférhető adatellenőrzés, valamint megtörtént a számviteli szabályok változtatása az elektronikus számlák tárolásának egyszerűsítése irányában (annak tömeges elterjedése ez után várható).

A magyar elektronikus aláírási törvény az 1999/93/EK irányelvvel megegyezően a műszaki háttértől függetlenül az elvi működést figyelembe véve három szintet különböztet meg. A legalsó szint az „egyszerű" elektronikus aláírás,[46] amely mindennemű biztonsági követelmény nélkül az elektronikus dokumentumokba leírt

[45] Jacsó, 2006. p. 8.

[46] A jogszabályban nem nevesített, de a szakma használja az „egyszerű" előtagot.

nevünket jelenti (például az aláírás az email végén). Ehhez a jogalkotó különös jogkövetkezményt nem fűz, szabad mérlegelés tárgyává teszi ennek elfogadását. Második biztonsági szint a fokozott biztonságú elektronikus aláírás, amellyel szemben követelmény, hogy alkalmas legyen az aláíró azonosítására, egyedül csak az aláíróhoz legyen köthető, olyan eszközökkel kerüljön létrehozásra, amelyek kizárólag az aláíró befolyása alatt állnak, és a dokumentum tartalmához olyan módon kapcsolódjon, hogy minden – az aláírás elhelyezését követően a dokumentumon tett – módosítás érzékelhető legyen.[47] Jogkövetkezményként meghatározott területeket kivéve[48] az írásba foglalás követelményeinek való megfelelést nevesíti a törvény. Az elektronikus aláírások közül a legbiztonságosabb, illetve a legmagasabb követelményeket kielégítő a minősített elektronikus aláírás. A minősített elektronikus aláírás olyan fokozott biztonságú elektronikus aláírás, amelyet az aláíró biztonságos aláírás-létrehozó eszközzel hozott létre, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.[49] Az ezzel szemben kitűzött követelmények igen szigorúak és további jogi szabályozás tárgyát képezik az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 3/2005. (III. 18.) IHM rendeletben foglaltak szerint.[50] A minősített elektronikus aláírással ellátott dokumentum teljes bizonyító erejű magánokirat, ezért annak hitelessége és az aláíróhoz való egyértelmű tartozása annak ellenkezőjének bizonyításáig kétségbe nem vonható. Ez utóbbi két szint esetében mind az előállítás módjára, mind pedig a szolgáltató működésére vonatkozóan tanúsítást, illetve hatósági felügyeletet követel meg a jogszabály. A tanúsítást az informatikáért felelős miniszter által kijelölt, független tanúsító szervezetek[51] (jelenleg a HUNGUARD Számítástechnikai-, Informatikai Kutató-fejlesztő és Általános Szolgáltató Kft. és a MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft.) végzik, míg a hatósági felügyeletet a Nemzeti Média- és Hírközlési Hatóság látja el.[52] Ezekkel az eljárásokkal biztosítható a szolgáltatók és így az elektronikus aláírási rendszer működésének biztonsága és

[47] Eat. 2. § 15.
[48] Eat. 3. § (2)-(3) családjog és bírósági eljárások, kivéve, ha ezt az eljárástípusra vonatkozó jogszabály kifejezetten lehetővé teszi
[49] Eat. 2. § 17.
[50] további részletes iránymutatás található a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről szóló 2/2002. (IV. 26.) MeHVM irányelvben.
[51] 9/2005. (VII. 21.) IHM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról
[52] 45/2005. (III. 11.) Korm. rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól

minősége. A Magyar Köztársaságban hitelesítés-szolgáltatóként jelenleg a NetLock Kft., Microsec Kft., MÁV Informatika Zrt., Magyar Telekom Nyrt. és az EDUCATIO Kht. működnek. A hitelintézetek közötti elszámolás-forgalom lebonyolításának biztosításában vezető szerepet betöltő GIRO Zrt. 2001 óta hitelesítés-szolgáltatóként működött, de érdektelenség miatt 2005 óta nem bocsátott ki tanúsítványokat, majd 2008 áprilisában határozott úgy, hogy megszünteti hitelesítés-szolgáltatói tevékenységét. Nyilvántartásait a NetLock Kft. vette át, ami az első ilyen szolgáltatás-átadási eset volt Magyarországon.

Ma Magyarországon az elektronikus aláírás igénylése és alkalmazása úgy történik, hogy az állampolgár felkeresi a hitelesítés-szolgáltatót, akitől személyazonossága igazolása mellett email címéhez elektronikus aláírást és tanúsítványt igényel. A személyazonosság igazolása történhet a személyazonosság igazolására alkalmas okmány (személyazonosító igazolvány, útlevél, kártya formátumú jogosítvány) illetve a cégkivonat másolatának elküldésével, vagy annak személyes bemutatásával. Ezeket a hitelesítés-szolgáltatók külön biztonsági kategóriába sorolják (például Class C és Class B). Megkülönbözteti ezeket a jogalkotó a közigazgatásban való alkalmazás tekintetében is, ugyanis ahhoz előírt a személyes megjelenés.[53] A minősített aláírások esetében közjegyző általi hitelesítés történik.

A kulcspárt a birtokos a tulajdonában lévő biztonságos aláírást létrehozó eszközzel (BALE, pl. smart card, USB token) vagy szoftveres eszközzel állítja elő, amelynek nyilvános kulcsát a tanúsítvány elkészítéséhez átad a hitelesítés-szolgáltatónak. A tanúsítvány és a kulcsok így valamely biztonságos adathordozón vagy szoftveres kulcstárban kerülnek tárolásra. A megfelelő szoftvereket a számítógépre telepítve kártyaolvasó segítségével alá tudja írni e-mailjeit, illetve bármely egyéb dokumentumot. Különleges alkalmazásokban is lehetőség nyílik az elektronikus aláírás használatára, ilyen például az elektronikus cégeljárás, amely nem sokban különbözik egy dokumentum aláírásától, mindössze formalizáltan és a Cégbíróság által feldolgozhatóan teszi lehetővé azt.

A közigazgatási hatósági eljárásokban használható tanúsítványokra vonatkozó szabályokat a 78/2010. (III. 25.) Korm. rendelet határozta meg, mely alapján az ilyen aláíró tanúsítványokat kibocsátó hitelesítés-szolgáltatói tanúsítványokat legfelsőbb szinten a Közigazgatási Gyökér Hitelesítés-szolgáltató (KGYHSZ) bocsátja ki. Az

[53] Előírja a 78/2010. (III. 25.) Korm. rendelet az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól 9. § (2)

ilyen módon kiépített infrastruktúra ellenére a magyar közigazgatásban több, nem PKI rendszerre alapuló azonosítási rendszert is alkalmaztak, illetve alkalmaznak. Ilyen az Adó- és Pénzügyi Ellenőrzési Hivatal által 2004 óta az elektronikus adóbevallás hitelesítésére használt chipkártyás megoldás. Ezt a megoldást 2006. május 2. óta nem használják, a bevallások hitelességének biztosítására azóta az Ügyfélkapu rendszert alkalmazzák. Másik ilyen megoldás a Nemzeti Fejlesztési Minisztérium Infokommunikációs Államtitkárság[54] által felügyelt, és a Kopint-Datorg Zrt. által üzemeltetett Ügyfélkapu rendszer. A rendszerbe való első bejelentkezés, illetve a személyazonosság igazolása Okmányirodákban történik, ezután egy felhasználó név, jelszó páros alkalmazásával lehet belépni a rendszerbe és ott különböző hatósági eljárásokat illetve egyéb tevékenységeket végezni. A felhasználó azonosítására kétségtelenül gyenge módszer az Ügyfélkapuban alkalmazott, ugyanis nem írja elő valamely biztonságos eszköz birtoklását (például chipkártya) az azonosításhoz, amely lehetőséget biztosítana a kétfaktoros azonosításhoz.[55] Maga a kapcsolat titkosított csatornán (SSL) történik. A rendszer üzemben tartásával kapcsolatos több korábbi esemény is megingatta a felhasználók bizalmát a rendszerben.[56]

A területet 2016. 07. 01-től az eIDAS rendelet és az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény szabályozza.

[54] korábban Miniszterelnöki Hivatal Elektronikuskormányzat-központ, az EKK logo és rövidítés továbbra is használatban van.
[55] Hornák Zoltán, 2005.
[56] Az adatvédelmi biztos sajtóközleménye, 2010. és Az adatvédelmi biztos sajtóközleménye, 2009.

2.2. Az elektronikus írásbeliség problémái

Az elektronikus aláírással hitelesített dokumentumok hosszú távú megőrzése komplex feladat. Egyrészről magát az elektronikus adatot, illetve annak fizikai leképezését is meg kell védeni a megsemmisüléstől. Az elektronikus aláírás hosszú távú bizonyító erejét a tanúsítási lánc tárolásával meg kell oldani, valamint biztosítani kell az adott dokumentum megnyitását lehetővé tevő alkalmazás tetszőleges időben történő elérését.
Az elektronikus adatok épségének hosszú távú megőrzése fizikai, logikai és üzemeltetési biztonsági feladatok összessége. Mindenképpen szükséges hozzá az adattároló rendszer redundanciája és az adattároló eszközök biztonságos hosszú távú tárolása.

2.2.1. Túlzott gyorsaság

A kormányok minden téren igyekeztek az állampolgárok, illetve az egyéb ügyfelek eddigi papír alapú tevékenységeit elektronikus mederbe terelni. Ez a gyakorlatban a kizárólag elektronikus dokumentumok készítését és felhasználását jelenti. Ez a törekvés egyes esetekben túlzottan előremutatónak tűnik.
Gyakorlatilag a jogalkotó nem biztosítja az időt az átállásra a papíralapú folyamatokról az elektronikusra. Így történt például az elektronikus adóbevallás és az elektronikus cégeljárás esetében is. Az elektronikus adóbevallásra való átállásra a gazdasági társaságok többségének kevesebb, mint egy év állt rendelkezésére, a cégeljárás tekintetében pedig fél év átállási időt kapott a kötelezett. Ha ezt tekintjük az elektronikus írásbeliségre való áttérésnek a hagyományos írásbeliségből, amelyet több ezer éve gyakorlunk, ezzel szemben az analfabéták száma Magyarországon eléri a százezer főt,[57] meggondolatlanságnak tűnik egy ilyen léptékű paradigmaváltás megvalósítása pár év távlatában. Más, tőlünk fejlettebb ország, amely már korábban bevezette azokat a lépéseket, amelyeket mi is ebben a pár évben megtettünk, fenntartja a lehetőségét a papíralapú dokumentumok használatára. Konkrét példaként említve Ausztriát, az elektronikus cégeljárást már a nyolcvanas években telefonhálózaton összekötött gépek segítségével lehetővé tették, a kilencvenes években a polgári- illetve büntetőeljárások számottevő részét elektronizálták, ebben

[57] UNESCO, 2008, Education in Hungary

az évtizedben pedig tovább finomítva az igazságszolgáltatásban alkalmazott informatikai lehetőségeket bevezették az elektronikus fizetési meghagyást. Mindezen nagyfokú és folyamatos fejlődés ellenére mindmáig lehetősége van, sőt bizonyára a jövőben is lehetősége lesz az ügyfélnek papíralapú dokumentumok használatára a fenti cselekményekben, amelyet az igazságügyi tárca honlapjáról letölthet.

2.2.2. Formátumok különbözősége

Jelentős nehézségeket okozott eddig is és az elkövetkezendőkben is valószínűleg problémát fog jelenteni a dokumentumok formátumbeli különbözősége és az ebből adódó feldolgozási és alkalmazási különbségek.

Jól ismert és több-kevesebb ideje széleskörűen használt elektronikus dokumentum állományok az egyszerű szövegfájl (plaintext, TXT) a Microsoft Rich Text Format (RTF), és a Portable Document Format (PDF). Korábban Magyarországon az elektronikus ügyintézési eljárásban a TXT, RTF 1.7, PDF 1.3 dokumentumok estek értelmezési kötelezettség alá a közigazgatási szervek által, de 2009 óta megszűnt ez a szűk felsorolás.[58] Ezen formátumok elsődleges hátránya, hogy nem strukturáltak, ezért nehézkesen dolgozhatóak fel automatikus rendszerrel. Ezeknél is szélesebb körűen használt a Microsoft Word dokumentum (DOC), amely viszont még zárt, egyedi formátum is, annak pontos felépítése a Microsoft üzleti titka, ezzel lehetetlenné téve bármely nem-Microsoft szoftver teljes kompatibilitását. Ezen generációs hibák javítására születtek meg mindkét fejlesztői oldalon (Microsoft és OpenDocument Foundation) az XML-re épülő formátumok. A Kiterjeszthető Leíró Nyelv (Extensible Markup Language, XML) általános célú leíró nyelv, speciális célú leíró nyelvek létrehozására. Az 1986-ban ISO által szabványosított SGML nyelv[59] továbbfejlesztése, 1998-ban vált W3C ajánlássá.[60] Az XML célja az adatok strukturálása, licencmentes, platform-független és széleskörűen támogatott. Egy XML dokumentum akkor helyes, ha helyesen formázott, vagyis megfelel az XML nyelv szintaxisának és érvényes, vagyis megfelel a felhasználó által definiált tartalmi szabálynak, amely meghatározza az elfogadott értéktípusokat és értékhelyeket. Ez

[58] 12/2005. (X. 27.) IHM rendelet az elektronikus ügyintézési eljárásban alkalmazható dokumentumok részletes technikai szabályairól (formátum r.) 1. melléklet, hatályon kívül helyezte a 222/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás működtetéséről.
[59] ISO 8879:1986
[60] World Wide Web Consortium: XML Core Working Group Public Page http://www.w3.org/XML/ [2008.11.15.]

utóbbi követelményhez szükséges a szabályok meghatározása, amely Dokumentum Típus Definícióval (Document Type Definition, DTD) vagy XML Séma Definícióval (XML Schema Definition, XSD) történhet.

Ezen a technológiai keretrendszeren alapul az OpenDocument Foundation által kifejlesztett OpenDocument Format (ODF) formátumcsomag[61] és a Microsoft által kifejlesztett Office Open XML (OOXML) fájlformátum.[62] Ezen formátumok képezhetik az alapját a jövőbeni, széles körben alkalmazható dokumentum-formátumoknak. Valamint az ezen a technológián alapuló egyedi, szigorú megkötésekkel rendelkező XSD-jű űrlapok (form-ok) automatikusan feldolgozhatóak.

Szakmailag partikuláris, de a közigazgatási informatikában jelentős kérdés az általános, illetve az iratkezelési metaadat-probléma, miszerint az adatokat leíró adatok (metaadatok) pontosan milyen formában, értékben és egyedekkel állnak elő. E kérdés megoldására született több kezdeményezés, mint a Dublin Core Metadata Initiative (DCMI), a Managing Information Resources for e-Government (MIREG), GovML és a PSI Application Profile.[63]

Külföldi példa a formátumproblémára, hogy a Viking űrszonda 1976-os mágnesszalagon tárolt mérési adatait nem lehetett visszaállítani, mert az ismeretlen formátumban volt tárolva, ezért újra be kellett azokat gépelni mindent a korábban kinyomtatott dokumentumokból.[64]

2.2.3. Online adatbiztonság

Amennyiben valamely működő számítógéprendszerben (online) őrizzük az adatokat, a rendszert a fizikai biztonság tekintetében védeni kell az elemi károktól, mint a tűz, robbanás, vízkár (amely akár a közüzemi ivóvízellátás illetve csatornázás tekintetében is értendő), földrengés, rezgések és az objektum bármely egyéb okból való megsemmisülése. A műszaki követelmények hiányából bekövetkező incidensektől, mint az áramellátás hiánya, áramellátási zavarok, klimatikus körülmények romlása, amely lehet hőmérsékleti illetve páratartalom probléma, informatikai hálózati probléma, az elektromágneses zavaroktól (akár szándékos károkozás esetén is), és a

[61] ISO/IEC 26300:2006 Open Document Format for Office Applications (OpenDocument) v1.0
[62] ISO/IEC 29500:2008, Information technology – Office Open XML formats, valamint ECMA-376 Office Open XML File Formats - 2nd edition (December 2008)
[63] Bountouri–Papatheodorou–Soulikias–Stratis, 2007.
[64] Blakeslee, 1990.

műszaki megbízhatósági problémák ellen (a gyártási hiba, elfáradás, egyéb műszaki hiba). A logikai biztonság felöleli a szoftver elemek megbízhatóságát (operációs rendszer, alkalmazói programok) a szándékos károkozás elleni védelmet (vírusok, férgek, rosszindulatú programok, hálózati támadások, hacker tevékenység), a hálózati protokollok biztonságát és a hozzáférés-menedzsmentet.

2.2.4. Offline adatbiztonság

A digitális adatok tárolása – amennyiben az adat nem változik, illetve ha a költségek szempontjából ez a megoldás mutatkozik előnyösebbnek – valamely optikai, vagy mágneses adathordozón is történhet. Az optikai adathordozón való tárolásnak elsődleges médiuma ma a DVD lemez. A közhiedelemmel ellentétben ez sem örökéletű adattárolási megoldás. A lemez minőségétől függően legfeljebb 10 évig bízhatunk az adatok fennmaradásában, de rosszabb esetben akár 2 év utáni adatvesztés is előfordulhat. Ebből adódóan az optikai adattároló eszköz alkalmazása esetén is feltétlenül szükséges a periodikus regenerálás, amely a gyakorlatban a DVD lemezek lemásolását jelenti. Az optikai adattárolás előnye az elektromágneses terekre való érzéketlenség, de a megfelelő hőmérsékleti, páratartalmi és mechanikai viszonyokat fenn kell tartani tároláskor. A másik mindmáig működő, nagyobb történelmi múltra visszatekintő adattárolási mód mágnesszalagos egységek használata. Ez a videokazettához hasonló igen hosszú, általában végtelenített mágnesszalagos kazettát takar. Ennek tároló kapacitása mindmáig meghaladja az optikai tárolók kapacitását, akár a terabájtos nagyságrendet is elérheti kazettánként.[65]
A szalag tárolási környezetével kapcsolatban az optikai eszközök igényein felül felmerül az elektromágneses terek illetve zavarok elleni védelem szükségessége is. Regenerálás a tárolási eljárás miatt mindenképpen szükséges, ugyanis a mágneses hordozó idővel demagnetizálódik.
Különösen nagy jelentőséggel bír az a követelmény – amelyet egyébként a felhasználók és az üzemeltetők is hajlamosak elfelejteni – hogy az elektronikus dokumentumok megnyitásához szükséges környezetet is biztosítani szükséges.[66] Ez

[65] lásd pl. http://www.ibm.com/systems/storage/tape/ [2009. 10. 04.]
[66] Melléklet a 24/2006. (IV. 29.) BM-IHM-NKÖM együttes rendelethez, 10.1.1. pontja: „Az ISZ-nek képesnek kell lennie az előírt formátumban rendelkezésre álló elektronikus iratok megjelenítésére olyan módon, ami megőrzi az iratokban foglalt információkat.” Ez egyes jogalkalmazói értelmezések szerint a fenti követelményt takarja.

egy rosszabb esetet feltételezve azt is jelentheti, hogy a teljes számítógép architektúra változás ellenére mondjuk 100 év múlva meg kell nyitnunk egy olyan dokumentumot, amelyet egy garázsban működő szoftverfejlesztő cég szövegszerkesztő-alkalmazásával készítettek 1992-ben, a dokumentum formátuma nem követ semmilyen szabványt, de a jogi szabályozás nem teszi lehetővé a dokumentum selejtezését. Ebből a – természetesen erősen sarkított – lehetőségből adódik, hogy el kell tárolnunk az archivált dokumentummal együtt az azt megnyitni képes alkalmazást, az alkalmazást futtatni képes operációs rendszert, esetleg az ezeket futtatni képes teljes hardver konfigurációt. Ennek egyszerűsített formája lehet a megjelenítésre képes rendszer emulációja vagy az emuláció és a migráció együttes megvalósításával működő Univerzális Virtuális Számítógép (UVC).[67] Ez a probléma Magyarországon a rendszerváltás után az állambiztonsági iratok kutatásakor már felmerült, mikor az adatokat tároló mágnesszalag leolvasására csak azért nem volt lehetőség, mert a megfelelő olvasó már nem szerezhető be és nem utángyártható.[68] Az eset kapcsán természetesen kérdésként felmerül, hogy valamely érdekcsoportoknak szándékában áll-e ezen információk titokban tartása.

2.2.5. Elektronikus aláírás hitelessége

Az elektronikus aláírás hitelessége a létrehozásától számított kb. pár órától pár napos időintervallum után bizonyítható. Ennek oka az, hogy a hitelesség ellenőrzéséhez meg kell ismernünk az aláírás létrehozásakor aktuális visszavonási listát (CRL), amelyben az elektronikus aláírási szolgáltató az adott időpillanatban kompromittáltnak minősülő vagy egyéb okból visszavont tanúsítványokat közzéteszi. Ez az idő on-line tanúsítvány állapot ellenőrzés (OCSP) alkalmazásával jelentősen csökkenthető. Az elektronikus aláírás hitelessége ezek után folyamatosan bizonyítható, amennyiben a hozzáférési listák illetve a teljes tanúsítási lánc hozzáférhető marad. Itt kap szerepet az elektronikus archiválási tevékenység, melynek keretében az archiválás pillanatában érvényes hitelesítési adatokat az elektronikus archiválási szolgáltató eltárolja, illetve felülhitelesíti saját kulcsával. Így az elektronikus archiválási szolgáltató által aláírt elektronikus dokumentum hitelessége csak az archiválási szolgáltató létének

[67] Lorie, 2002.
[68] A probléma kezelésére született az állambiztonsági szolgálatok mágnesszalagra rögzített adatbázisaiban található adatok felülvizsgálatáról szóló 102/2010. (IV. 2.) Korm. rendelet, amelyet a 285/2010. (XII. 16.) Korm. rendelet hatályon kívül helyezett.

függvénye és nem befolyásolja a tanúsítási lánc valamely elemének kiesése, például úgy, hogy az adott tanúsítási szolgáltató befejezte tevékenységét, vagy saját kulcsa kompromittálódott. Ez az a pont, melyben az elektronikus archiválási szolgáltató tevékenysége felülemelkedik az egyszerű biztonságos adattárolás kérdésén.

2.2.6. Kockázat és védekezés

Ezekből a sokrétű követelményekből és széles körű problémákból adódik, hogy az elektronikus dokumentumok tárolását és feldolgozását végző szervezet komoly nehézségekkel kell, hogy szembenézzen. Az ismertetett problémákból fakadó kockázat különböző országokban eltérő mértékű. Abban az esetben, ha az elektronikus írásbeliség nagyfokú fejlődést mutat, a problémák kiküszöbölésére kevesebb idő jut, fokozva a probléma későbbi eszkalálódásának esélyét. Ebbe a kategóriába tartozik a Kelet-Közép-Európai országok gyors közigazgatási informatikai fejlesztése. Magyarországon nem történik meg a Nyugat-Európai államok tapasztalatainak kellő mértékű feldolgozása, hogy azzal kikerüljék az eredendő buktatókat. Ezek a problémák a későbbiekben akár komoly állami adatvesztéseket is okozhatnak.

A fenti problémákból közösen fakadó veszélyekkel és az ellenük való védelemmel a digitális megőrzés (digital preservation) foglalkozik. Az ezekből keletkező apokaliptikus végkifejlet a digitális sötét kor (digital dark age), melyben a fentiek miatt elvesznek a XXI. században keletkezett elektronikus dokumentumok, ami miatt erről a századról is – a sötét középkorhoz hasonlóan – kevés írásos emlék marad fenn. Az elmélet főbb képviselői a Getty Research Institute több kutatója,[69] és Kuny, Terry,[70] de a cáfolat is született, miszerint az eddigi tapasztalatok csak az adat-visszaállítás hiányosságaira, nem pedig az adatvesztésre szolgáltak példaként.[71] A műszaki problémák megoldására átfogó jelleggel Open Archival Information System (OAIS) néven ISO referenciamodell készült.[72]

A túlzott gyorsaság problémájára a jobb politikaalkotás, a formátumproblémára és részlegesen az adatbiztonsági problémákra a jobb illetve szigorúbb szabályozás nyújthat védelmet Magyarországon. Az elektronikus aláírási probléma és részlegesen

[69] MacLean–Davis, 2000.
[70] Kuny, 1997.
[71] Harvey, 2008.
[72] Consultative Committee for Space Data Systems, 2002.

az adatbiztonsági probléma hatékony kezelője a piaci alapokon működő elektronikus archiválási szolgáltatók igénybevétele. Bizonyára e problémák bonyolultságából és a piaci igény hiányából kifolyólag nincsen ma Magyarországon jól működő (megfelelő mértékben kihasznált) archiválás szolgáltató. Másrészről viszont az elektronikus dokumentumok megőrzésére kötelezettek igen nagy része úgy gondolja, hogy e kötelezettségének saját infrastruktúrájával illetve humánerőforrásaival képes eleget tenni. Ide tartoznak a 10 fős községi önkormányzatok is, melyekről még nagy jóindulattal sem jelenthetjük ki, hogy ezen feladatuknak képesek lesznek eleget tenni.

2.3. Új technológiák és alkalmazásuk gyakorlata

Az elektronikus írásbeliség alapjain és javuló társadalmi elfogadásán több olyan új technológia került bevezetésre, amely alapvetően befolyásolhatja a komplex biztonságot. A teljességre törekvés igénye nélkül bemutatásra kerül több ilyen technológia és az azzal kapcsolatos szabályozási vetület.

2.3.1. Elektronikus okmányok

Az elektronikus adatkártyák célja az adatok tárolása általános, azonosítási vagy hozzáférési célból. Ezeket az eszközöket tárolási módszer és az eszköz fajtája alapján tipizáljuk. Mind a tároló kapacitás, a biztonság és a felhasználhatóság is ezen eszközök fajtájától függ.

A legrégebbi adatkártya a lyukkártya, amely egy papír alapú hordozón lyukakban illetve a lyukak hiányában testesítette meg az adatot. A kártya leolvasása kontakt villamos (a két egymással szemben lévő érintkező összeér-e vagy sem) illetve optikai (a fény átvilágít-e a lyukon vagy sem) lehet. A kártyán igen kevés adat tárolható, 80-90 bájt, valamint használata is igen lassú és nehézkes. Alapvetően adattárolási eszközként használták a számítástechnika hajnalán, ma már gyakorlati jelentősége nincs. Az elv használható azonosítási célra is, például menzán az étkezési jegy egy műanyag kártya, amelyen az elhelyezett furatok jelölik a sorszámot. A kártyát optikai úton leolvasva, a kártya jogosultsága az adott napszakban való étkezésre megállapítható a pénztári számítógépen lévő adatbázissal való összehasonlítás után. A kártya eredetiségének megállapítása szemrevételezéssel történhet, egyszerűsége miatt felügyelet nélkül nem alkalmas az azonosításra.

A hagyományos, mindenki által jól ismert adatkártya típus a mágneskártya. Itt az adathordozó egy plasztik lapra épített mágnesezhető fémcsík. Ennek leolvasása a szalagos magnóból ismert mágneses olvasófejek segítségével történik, tehát megköveteli a kontaktust a kártya és az olvasó között. A technológiát több szabvány, például az ISO 7811, 7812, 7813 határozzák meg. A tárolható adatmennyiség itt is korlátos, nagyságrendileg 100 bájt. Egy bankkártya esetén például ugyanazok az adatok kerülnek eltárolásra, mint ami a kártyán is látható, kiegészítve pár ellenőrző

adattal.[73] Ennek a használata még mindig folyamatos, egyszerűsége miatt. Azonosításra felügyelet nélkül is alkalmas. PIN kód használatával biztonsága jelentős mértékben növelhető. A hamisítása a mágnes csík leolvasásával és egy üres kártya felmágnesezésével történhet, nem igényel számottevő felkészültséget. Ebből kifolyólag a szemrevételezéssel történő azonosításnak itt is jelentősége van.

Szintén használatos a vonalkódos kártya, amely egy vagy kétdimenziós vonalkódban tárolja az adatot. Az így tárolható adatok mennyisége kisebb, mint a mágneskártyán tárolható, egydimenziós (lineáris) vonalkód esetén pár bájt. Az adat kódolása nemzetközi szabványok alapján történik, széleskörűen az 1978-ban bevezetett EAN 8 vagy EAN 13 kód használatos. A Magyar Köztársaságban az adóigazolványon és a társadalombiztosítási igazolványon is az Adóazonosító jelet illetve Társadalombiztosítási azonosító jelet is egydimenziós vonalkódban tüntették fel a kártyán. A lineáris vonalkód továbbfejlesztéseként jelent meg a négyzetes adatmátrixkód a '90-es évek elején. A fekete-fehér adatmátrixnak az adattároló-kapacitása elérheti a 2335 alfanumerikus karakterszámot.[74] Legismertebb változata a nyomdatechnikailag könnyen előállítható PDF417 kódrendszer, amelyet a belügyi és rendvédelmi szervek szolgálati igazolványain is alkalmaznak. Az igazolvány teljes adattartalmát kétdimenziós vonalkódban is feltüntetik. Az ABEV program a számítógéppel kitöltött adóbevallásokon is használja ezt a kódrendszert. Ehhez hasonló a manapság divatos QR kód is, amely a kialakításának köszönhetően könnyen leolvasható mobil eszközökkel is.

4. ábra: QR kód[75]

[73] Visdómine, 2009.
[74] Eiler, 2008. p. 44.
[75] http://qrcode.kaywa.com/ [2010. 11. 25.]

Ezen módszerek hátránya, hogy a vonalkód fénymásolható, leolvasható, hamisítható. Ennek megelőzésére egy speciális fedőréteggel lehet ellátni a vonalkódot, amelyet így például csak infravörös fény segítségével lehet megjeleníteni. Ezzel a módszerrel nagymértékben nehezíthető a hamisítás.

5. ábra: Letelepedési engedély[76]

Költségessége miatt kevéssé elterjedt módszer a lézerkártya. Ennél a kemény műanyag hordozón a kompakt lemezhez hasonló technikai megoldással 1,6-3,5 cm szélességben lézersugárral kiolvasható adathordozó csík található. Ilyet Magyarországon nem használnak, de a Kanadában, az Amerikai Egyesült Államokban, Costa Ricán és Olaszországban különböző állampolgárságot és Indiában gépjármű-regisztrációt igazoló okmányokon így oldották meg a digitális adat tárolását. A tárolható adat mennyisége az eddigi módszereknél jóval nagyobb, 1.1MB, 1.8 MB vagy 2.8MB.[77]

Az eddig ismertetett kártyák közös jellemzője, hogy adattartalmukat nem, vagy igen nehezen lehet megváltoztatni és nem tartalmaznak aktív elemet, amely lehetővé tenné biztonságosabb felhasználásukat. Amennyiben szükséges a tárolt adatok megváltoztatása, valamely egyéb módszert kell bevezetni. Egyszerű megoldásként említhető a kilencvenes években Olaszországban használt telefonkártyák módszere, ahol a kártyán lévő fehér csíkra (a biztonság miatt szükségszerűen különleges festék alkalmazásával) a letelefonált egységekkel arányosan a telefon fekete téglalapokat nyomtatott. A telefonkártya addig volt használható, amíg volt rajta szabad fehér felület. Ennek ellenőrzése optikai úton történt. A mágneskártyák adattartalma is változtatható, amennyiben elhelyezünk a leolvasóban egy törlőfejet is. Ezeknél komplikáltabb és biztonságosabb megoldás a memória-áramkörök alkalmazása, ahol

[76] http://www.uscis.gov/uscis/images/nativeimages/PRC_Back_Front.JPG [2011. 01. 31.]
A jobboldali kép felső sorában egydimenziós vonalkód, alatta optikai (lézeres) tároló, legalul MRZ kód látható.
[77] LaserCard Corporation: LaserCard® Optical Memory Card.
http://www.lasercard.com/products.php?key=83 [2009. 02. 24.]

is a plasztik kártyába egy elektronikus úton újraprogramozható, nem felejtő memória-áramkört (EEPROM) ültetve azon adatot lehet tárolni illetve módosítani lehet azt. Ilyet alkalmaznak például a magyar telefonkártyákban. A hamisítás kommersz memória-áramkörök használata esetén nem túlzottan nehéz, valamint a csatlakozópontok kivezetésével és számítógéphez való illesztésével a működés emulálására program írható, megtévesztve az olvasó eszközt.

A kártyák felhasználását forradalmasította az aktív kártyák bevezetése, amelyeken nem csak írni-olvasni lehet az adatokat, hanem a kártya képes adatfeldolgozási és más matematikai műveleteket végezni. Az aktív kártyák központi eleme a mikrokontroller. A mikrokontroller gyakorlatilag egy darab áramköri lapkán (chip) megvalósított kvázi komplett számítógép. Egy tokban megtalálható benne a processzor, a nem felejtő memória (ROM, FLASH) és a tetszőleges hozzáférésű memória (RAM), a ki- és bemeneti egységek (I/O) valamint egyéb kiegészítő elemek (például óra, komparátor stb.). Ez, mint aktív elem, lehetővé teszi a negyedik generációs kriptorendszerek[78] implementálását, aktív védelmet biztosítva a tárolt adatoknak illetve a hozzáférésnek. A tárolókapacitása a típustól függően 1-256 kilobájtos nagyságrendű lehet. Mikrokontroller alkalmazásával kialakíthatunk kontakt és nem kontakt (érintés nélküli) adatkártyákat is. Ilyen kontakt adatkártya a smart card (intelligens kártya, chipkártya). Ilyet alkalmaznak Magyarországon a felsőoktatási diákigazolványban valamint az újabb bankkártyákon is. Ez az elsődleges eszköze az elektronikus aláírás magánkulcsa tárolásának is. Több féle nemzetközi szabvány foglalkozik a chipkártyákkal, mind funkcionális, mind biztonsági szempontból.[79] Ilyen funkcionális szabvány például az ISO/IEC 7816. Az adatkártya kiolvasásához közvetlen érintkezés kell a leolvasóval, amely így közvetlen villamos kapcsolatot létesít a mikrokontroller kivezetéseivel. Értelemszerűen ez a leggyorsabb és legbiztonságosabb módja az adatátvitelnek.

A mikrokontrolleres aktív adatkártya nem kontakt megvalósítása a proximity kártya (RFID, rádiós kártya). Az ebben alkalmazott aktív eszköz alapvetően megegyezik a intelligens kártyában alkalmazottal, lényegi különbség az, hogy a leolvasóval való kapcsolata rádiófrekvencián történik. A működési elve az, hogy az adatkártyán egy nagy tekercsantenna található, amely össze van kötve a mikrokontrollerrel. Alap

[78] Szimmetrikus, illetve aszimmetrikus kulcsú számítógépes titkosító-megfejtő algoritmusok, például DES, AES, RSA, stb. ld. 2.2.2. fejezet
[79] bővebben ld. Hassler, 2009.

kiépítés szerint a kártya áramforrást nem tartalmaz, a működéséhez szükséges energiát a leolvasó által gerjesztett elektromágneses térből veszi fel. Tehát a leolvasóhoz közelítve a kártyát, az automatikusan bekapcsol és a teret meghatározott módon modulálni kezdi, például elküldi a kártya azonosítószámát. A leolvasó ellenőrzi, hogy az adatbázisában szerepel-e ez az azonosítószám és ennek függvényében például engedélyezi a belépést. Könnyen felismerhető ennek a rendszernek a hibája, ugyanis az adat kinyeréséhez csak az adott frekvenciájú elektromágneses térre van szükség. Tehát bármilyen leolvasónak „elárulja" a kártya az azonosítószámát, így a rosszindulatú személy által üzemeltetett leolvasónak is. Ő ezt az azonosítót csak lemásolja egy üres kártyára és máris megtörtént a kártya másolása. Ennek megakadályozására a rendszer kombinálható az olvasó azonosításával is. A kártya ekkor az elektromágneses térbe kerülésekor csak jelzést ad a jelenlétéről, ezután az olvasó küldi el az azonosító kódját. Amennyiben ez a kód szerepel a kártya memóriájában tárolt engedélyezett olvasók listáján, akkor fogja csak kiadni a kártya a saját azonosítószámát. Az adatátvitel komplikálható még az adatátvitel titkosításával, például elektronikus aláírás alkalmazásával. A rádiófrekvenciás adatátvitel miatt az átvitel sebessége és ebből kifolyólag a tárolt adat mennyisége is több nagyságrenddel kisebb az intelligens kártyákénál, általában 26-37 bit hosszúságú adatot használnak. Kártyába épített akkumulátor segítségével az alapesetben az olvasótól való néhányszor 10 cm-es legnagyobb távolság akár 10 m-es nagyságrendűvé növelhető (long range proximity). A technológiát az ISO/IEC 14443 szabvány írja le. Ezek az aktív kártyák már elég biztonságosnak alakíthatóak ki arra, hogy hitelesen alkalmazhatóak legyenek közokiratokban egyedüli vagy kiegészítő azonosítási funkciókra.

Az aktív kártyák következő generációja a biometriai biztonsági elemekkel kombinált kártyák alkalmazása. Az emberi kültakaró legjellegzetesebb eleme az arc, mely a Homo Sapiens egyéb érzékeinek (pl. szaglás) fejletlensége miatt a látás útján a szociokommunikációs funkciói mellett a személyek azonosításának elsődleges eszköze. Ennek alkalmazása ösztönös és az emberi faj kezdetektől alkalmazza. Az első nyoma más biometrikus jellemzők alkalmazásának a XIV. századi Kínában ujjlenyomat használata volt a gyermekek azonosítására, amit Joao de Barros felfedező jegyzett le.[80] Európában 1890-ben Alphonse Bertillon párizsi rendőr vezetett be

[80] Osborn, 2005.

testrész-méret alapú azonosítási rendszert bűnözők azonosítására. Módszerét a téves azonosítások tömeges előfordulásáig használták. Az ujjnyomat alapú azonosítást Bertillon munkája alapján Richard Edward Henry vezette be a Scotland Yard-nál. A XX. században Karl Pearson a University College of London alkalmazott matematikusa tett komoly felfedezéseket a biometria területén. Az 1960-as években az aláírás-dinamika elemzés terén történt komoly fejlődés, amely viszont megmaradt a katonai és nemzetbiztonsági alkalmazásban. A terrorveszély fokozódásával az Amerikai Egyesült Államokban és Nyugat-Európa területén a biometrikus azonosítás állami alkalmazása ugrásszerűen megnőtt.

Jelenleg az alábbi biometrikus jellemzőkön alapuló azonosítási rendszerek léteznek:

- ujjlenyomat
- kézfej geometria
- tenyérlenyomat
- vénamintázat
- markolás-dinamika felismerés
- koponya hőkép
- 2D arcvonások
- 3D arcvonások
- írisz[81] felismerés
- retina[82] felismerés
- hangfelismerés
- aláírás dinamikája
- billentyűleütés dinamikája
- DNS
- testtartás felismerése

Ezek többé-kevésbé alkalmazottak a személyek azonosítására. A biometrikus jellemzők matematikai leírásával és annak tárolásával lehetőség van az egyedre jellemző adatok alapján pontosabb azonosítást végezni.

[81] szivárványhártya

[82] Szemfeneket borító ideghártya erezete, erős fénnyel kell megvilágítani hozzá a szemet, amely komoly ellenállást eredményezett az alanyok részéről. Az új, infravörös fénnyel megvilágító technológia kifejlesztésével csökkent az ellenállás és új erőre kaptak a fejlesztések.

Az úti okmányok történetében az adatkártyák, mint kiegészítő elem és a biometria, mint a személyhez kötöttség magasabb foka együttes integrálásával új generáció került megalkotásra, amely az eddiginél szignifikánsan magasabb megbízhatóságot jelent az okmánybiztonság területén.

6. ábra: ePassport[83]

Az Egyesült Államok után az Európai Unióban is elkezdték az elektronikus azonosítással is rendelkező útlevelek (ePassport) bevezetését. Ennek főbb okai az úti okmányok biztonságának növelése, ezzel az EU határbiztonság növelése, valamint az US Visa Waiver programban való bennmaradás, amely a régi EU államok vízummentességét jelenti. A Magyar Köztársaság szempontjából az ePassport bevezetése a programba való bekerülést célozza meg. Az ePassport az előbbiekben ismertetett proximity kártya beépítése az útlevélbe. Először csak az adatok, majd ujjlenyomat tárolásával. A Tanács 2252/2004/EK rendelete alapján az ePassport első bevezetése az Unióban 2005 októberében történt Svédországban. Magyarországon 2006. augusztus 29-e óta az adatoldal teljes tartalma megtalálható az RFID-ben, a fényképpel és az aláírással egyetemben. Az ujjlenyomat tárolását 2008. év folyamán kívánták bevezetni. A Tanács döntése értelmében 2009. június 28-áig az Unió minden államának át kell térnie az ujjlenyomatot is tároló ePassport alkalmazására. Ez természetesen az Unió több államában elismert adatvédelmi szakemberek ellenállásába ütközik, így Péterfalvi Attila és Majtényi László is ellenezték ezt. Az

[83] http://www.bundesdruckerei.de/pics/presse/fotoarchiv/aktuelle_fotos/060330_BMI_epass_ohne.jpg [2011. 02. 01.] Quelle: Bundesministerium des Innern

ePassport első oldalába került integrálásra egy proximity kártya, amely tárolja a szóban forgó adatokat. Az adatok védelmére több biztonsági intézkedést implementáltak. A hagyományos okmánybiztonsági védelmi eljárásokon (alapanyagba integrált fénykép és aláírás, egyedi mintázatok, különleges festékek) kívül az elektronikus tároló egység a fizikai támadás hatására megsemmisíti a tárolt tartalmat.[84] Másrészről a chip aktív hitelesítésre képes, ami az abba integrált PKI magánkulcs segítségével történik, passzív hitelesítésként pedig belekerült az útlevél kiadójának tanúsítványa. A proximity kártyánál ismertetetett módon megtörténik az olvasó hitelesítése is egy ún. Basic Access Control (BAC) módszer segítségével. Ennek működése a következő: az útlevelek adat oldalának alsó részén hasonlóan a személyazonosító igazolványhoz, egy ún. MRZ kód található, amely az okmány és tulajdonosa legfontosabb adatait tartalmazza. Ez az adatok gépi leolvasásának egyszerűsítését szolgálja. Ebből kinyerve az útlevélszámot, a születési időt és az érvényességi időt generál a leolvasó egy hozzáférési kulcsot. Az ePassport ezen hozzáférési kulcs után fogja csak a tárolt adatokat rádiófrekvencián elküldeni a leolvasónak. Ezzel a módszerrel a leolvasó bizonyítja azt az útlevél felé, hogy ténylegesen hozzáfér ahhoz (nem távolról próbálja egy adatkalóz kihalászni a tartalmat). Ez a módszer korlátozott mértékben biztonságos. A kulcs megfejtése bruteforce módszerrel a kb. 50 bites entrópia miatt több mint 35 év, míg az adatok elemzésével (születési idő intervallum megválasztása, útlevélszám kiosztásának követése) 35 bitre csökkenti az entrópiát, így akár 3 óra alatt feltörhető a kód.[85] A kód törése történhet a titkosított adatforgalom lehallgatásával, rögzítésével, majd bruteforce módszerrel való törésével, esetleg közvetlen támadással, amelyhez viszont háttérismeretek szükségesek. Ez a kódolás nem igazán alkalmas az ujjlenyomat titkosítására, erre egy biztonságosabb eljárás került kifejlesztésre, amelyet Extended Access Control-nak (EAC) hívnak.[86] Az EAC nem egységes szabvány alapján történik, alapját az ICAO Doc 9303 fekteti le. Megfontolandó továbbá a tagállamok részére a sorszámozás megváltoztatása nagyobb tartományra illetve a tartományon belüli véletlenszerű kiosztásra. Minden tagállamban az eddig kiadott úti okmányok érvényben maradnak, viszont az újonnan kiadottak minden esetben már az új módszerrel készülnek.

[84] Jóri – Hegedűs – Kerekes, 2010.
[85] Robroch, 2006.
[86] Moses, 2008.

2.3.2. Térfigyelés

A megfigyelési célú kamerarendszerek telepítése körül mindig is komoly szakmai viták alakultak ki. A két szemben álló tábor harca ez, a kamerák telepítését támogatóké: akik a tulajdonosok, haszonélvezők, önkormányzatok, hatóságok és a megfigyelést ellenzők táboráé: a jogvédőké. Az állampolgárok e két tábor körül csoportosulnak valamilyen eloszlásban.

A térfigyelés számos alkotmányos alapjogot érint, így például az emberi méltósághoz való jogot, a személyes adatok védelméhez, a magántitok védelméhez, a magánlakás sérthetetlenségéhez való jogot, a békés gyülekezés jogát, a szabad véleménynyilvánítás jogát, a vallás szabad gyakorlása, és a szabad mozgás jogát. Személyes adat az azonosítható természetes személlyel összefüggésbe hozható információ, függetlenül attól, hogy a kapcsolat milyen nehezen állítható vissza. A felvételek felbontásának minősége fontos, de nem egyedüli kritérium, ugyanis gyengébb felbontás esetén is lehetőség van az azonosításra, például lakás bejárata, szokások alapján. Az Európai Unió adatvédelmi irányelve szerint személyes adatok kezelése a személyes adatokon végzett bármely művelet vagy azok összessége, tehát a személyes adatokba való betekintés is. Így a magyar jogban is a puszta megfigyelés is adatkezelésnek tekintendő. Az Alkotmánybíróság értelmezése szerint a személyes adat kezelése az információs önrendelkezési jog korlátozásának minősül, ezért minden esetben a szükségesség, az arányosság, az alkalmasság és a törvényben szabályozottság elveit kell be tartani. Az adatvédelem elvei a célhoz kötöttség, az adatminimum elve, a tisztességes adatkezelés követelménye, az adatbiztonság követelménye, az átláthatóság követelménye és az érintettek jogainak biztosítása, melyeknek a térfigyelés során is minden esetben érvényesülni kell.

Amennyiben a kamerás megfigyelés magánterületen, vagy magánterület közönség számára nyilvános részén történik, a tevékenységet viszonylag jól szabályozza a 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól (Szvmt.), mely alapján a térfigyelő rendszer tervezését kizárólag a Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamara által kidolgozott szakmai követelményeknek megfelelő, a Kamara által kiadott tervezői névjegyzéken szereplő személy végezheti. A karbantartás, üzemeletetés szintén rendőrségi engedélyhez és kamarai tagsághoz kötött. Az elektronikus

megfigyelőrendszernek kép-, hang-, vagy kép- és hangrögzítést is lehetővé tevő formája az emberi élet, testi épség, személyi szabadság védelme, a veszélyes anyagok őrzése, az üzleti, bank- és értékpapírtitok védelme, valamint vagyonvédelem érdekében alkalmazható. De ezen esetekben is csak akkor, ha a megbízás teljesítése során fennálló körülmények valószínűsítik, hogy a jogsértések észlelése, az elkövető tettenérése, illetve e jogsértő cselekmények megelőzése, azok bizonyítása más módszerrel nem érhető el, továbbá e technikai eszközök alkalmazása elengedhetetlenül szükséges mértékű, és az információs önrendelkezési jog aránytalan korlátozásával nem jár. Az adatvédelmi jogban, amely a természetes személyekre vonatkozó személyes adatok védelmével foglalkozik, komoly jelentősége van az adatkezelés célhoz kötöttségének, mivel a térfigyelés is adatkezelésnek számít. Minél pontosabban meghatározott a cél, annál erősebb a jogalap. A felvételeknek háromféle tárolási időtartama lehet. A maximum 60 nap, amely pénzügyi, biztosítási, postai pénzforgalmi tevékenység esetében lehetséges. 30 napig lehet tárolni nyilvános rendezvény esetén, 2 millió forintot meghaladó értékű pénz, drágakő, stb. őrzése, szállítása esetén. Csupán 3 munkanapig lehetséges a tárolás minden egyéb esetben. Ha nem használták fel a felvételeket, akkor az időtartam lejártakor meg kell semmisíteni azokat.

A közterületi térfigyelés viszont a fentiekkel ellentétben kevésbé jól definiált szabályok alapján történik. Mivel személy- és vagyonvédelem csak a magánterületre korlátozódik, ezért az Szvmt. szabályai a közterületi térfigyelésre egyes jogértelmezések alapján egyáltalán nem vonatkoznak. Ezzel szemben az ORFK gyakorlata szerint a tervezést, kivitelezést az Szvmt. alapján kell végezni és csak az üzemeltetésre nem vonatkoznak az Szvmt. passzusai. Az Adatvédelmi Biztos ajánlása alapján a rendszer bevezetésének indokoltnak, az adatkezelésnek célhoz kötöttnek kell lennie. A célhoz kötöttség feltételének mindössze a „közbiztonság javítása” indok nem elég, a döntés megalapozottságát alá kell támasztani kutatási dokumentumokkal, felmérésekkel. Nagy port kavart, hogy a megfigyelést kik végezhetik: egy korábbi ORFK intézkedés alapján nyugdíjas rendőrök is végezték a közterületi térfigyelő kamerarendszer képének figyelését, amely viszont a Rendőrségi törvény alapján jogellenes, mivel ők már nem tartoznak a rendőrség állományába. Az Adatvédelmi Biztos Hivatala több ellenőrzést végzett megfigyelőhelységekben, amelyek során megfigyelést végző polgárőrökkel is találkoztak, amely szintén jogellenes magatartás. A közterület-felügyeletről szóló 1999. évi LXIII. törvény módosítása alapján viszont

2009. szeptember 1-jétől már a közterület-felügyelet is üzemeltethet térfigyelő rendszert és végezhet megfigyelést. A rendőrségi felvételek készítésének három esete van, a határátkelőhelyről készített felvétel, az általános közterületi térfigyelés, és a rendőrségi intézkedésről készített felvétel. A tárolás időtartama rendre 3 nap, 5 nap, és 30 nap. A rögzített felvétel egy alkalommal 30 napig megtartható, ha szabálysértési vagy büntető eljárásban való felhasználása feltételezhető. Felhasználás hiányában az időtartam lejártakor a felvételt meg kell semmisíteni. A közterület-felügyelet által felvételek készítésének két esete van, az általános közterületi térfigyelés és a felügyelői intézkedésről készített felvétel. A tárolás időtartama 5 munkanap, és 30 nap. A rögzített felvétel ezen időn túl csak akkor tartható meg, ha az eljáró hatóság még nem tudta átvenni a felvételt, és ebben az esetben is a maximum 30 nap. A felvételeken az eljárásban érintett vagy más okból a felvétel hasznosításában jogosan érdekelt személyek érdekében is felhasználható. Minden fenti esetben a kamerát láthatóan kell elhelyezni, valamint a lakosság figyelmét táblával fel kell hívni a térfigyelés tényére. Kiemelendő, hogy a fegyveres biztonsági őrséget, a természetvédelmi őrszolgálatot, mezőőrt, hegyőrt nem jogosítja fel törvény a térfigyelés végzésére.

2008. január 1-jén módosult a rendőrségről szóló törvény, amelyben új elemként jelent meg az önkormányzati jóváhagyás igénye. Az önkormányzati mérlegeléshez kíván támpontot adni így a rendőrség. Érdemi mérlegelés nélkül nem jogszerű a térfigyelésről dönteni.

Az adatvédelmi biztos munkatársai által végzett helyszíni vizsgálatok tapasztalata, hogy a vizsgált térfigyelő rendszert üzemeltetőknél több mint egy hónap alatt nem volt olyan esemény, amelynek kapcsán intézkedni kellett. A helyszíni vizsgálat alatt az adatvédelmi szakértő által is tapasztalt szabálysértésnek nem volt következménye, valamint a térfigyelő helységbe belépők regisztrálása nem történik meg. A rendőrök több esetben nem tudták megfelelően alkalmazni a rendszert.

Számos más buktatója is van a térfigyelő rendszer telepítésének. Például a megrendelő önkormányzatok többször tapasztalták, hogy a kivitelező nem megfelelően végezte el a telepítést. Több településen is előfordult, hogy a kivitelezés nem történt meg a szerződésben meghatározott időpontra, a kamerákat nem a rendőrség által meghatározott helyre telepítették, vagy a kameraképek nem voltak megfelelő minőségűek, így a gépjárművek rendszámát nem lehetett leolvasni, a jogellenes cselekményekről nem készült használható felvétel.

2.3.3. Számítási felhőbe szervezett szolgáltatások

Az informatikai szolgáltatások innovációja a számítógépek és a hálózatok fejlődésével párhuzamos. A kezdetektől, 1962-től elindult bizonyos szolgáltatások kiszervezése: H. Ross Perot megalapította az Electronic Data Systems (EDS) vállalatot az outsourcing üzlet ősét. A cég az informatikai üzemeltetési feladatok ellátására szakosodott, amelyet az ügyfeleik a saját szervezetükön belül nem kívántak ellátni. Ekkor még kevés szakember állt rendelkezésre az amerikai piacon, így a kiszervezés ezt a problémát is megoldotta. Az outsourcing szerződésben ki lehet kötni az irodai munkaállomások egységesítését és a központi szoftvermenedzsmentet. A megrendelő szervereinek üzemeltetését átveheti a megbízott, akár olyan módon is, hogy saját hardverén más megbízók szolgáltatásaival is együtt üzemelteti a szolgáltatásokat. Ekkor garantálja a szolgáltatások biztonságos szétválasztását. A kiszervezési szerződés legfontosabb eleme hogy szolgáltatási szint megállapodás (Service Level Agreement, SLA) készül, amelyben kikötésre kerül minden lényeges körülmény: rendelkezésre állási mutató, hibajavítási idő, válaszidő, kötbér, premizáció stb.

Azóta is komoly üzleti jelentősége van a másodlagos, kiszolgáló feladatok vállalaton kívülre szervezésének. Magyarországon a ’90-es években a MATÁV is kiszervezte az informatikai üzemeltetési tevékenységét az EDS-nek, amelyet ma is – immár Magyar Telekomként – kiszervezetten működteti, csak már a T-csoporton belül.

1990-ben létrejöttek a vezetői információs rendszerek, amelyek a döntéshozók számára a megfelelő formában biztosítják a döntést megalapozó információt. Szintén a döntéstámogatásra 1995-ben kiépülnek az adattárházak és elkezdődik az adatbányászat. Az integrált vállalatirányítási rendszerek a ’90-es évek végén jelentek meg. 2000-ben elterjedtek a CRM (Customer Relationship Management) rendszerek, és kivirágzik az elektronikus kiskereskedelem (Amazon, e-Bay, web áruházak), amelyek az internetes rendelést követően futárral végzik a kiszállítást. Megjelennek a közösségi oldalak: wiw.hu (2002), facebook.com (2004), megjelenik a twitter.com (2006).[87]

Az informatikai szolgáltatások kiszervezési folyamata az olcsó informatikai eszközök és a képzett informatikusok nagy száma miatt a 2000-es évekre lelassult, megakadt. Az utóbbi tíz év viszont ismét rámutatott a kiszervezés lehetséges előnyére: az

[87] Racskó, 2011.

outsourcing tevékenységoptimalizálásra változott, és hatalmas multinacionális informatikai szolgáltatók kezdték el kínálni különböző szolgáltatásaikat, melyek képesek kiváltani a szervezetnél üzemeltetett szolgáltatások nagy részét. Szolgáltatásukat egy számítási felhőből (cloud) nyújtották. Az elnevezés az informatikában alkalmazott rajzjelekből származik, amelyben felhő jelölte azokat a hálózatokat, amelyeknek a belső felépítése lényegtelen, kizárólag az input és output rendelkezik jelentőséggel.

Technikailag a szolgáltatás legfontosabb alapköve a virtualizáció, amely már majdnem egy évtizede a piacon van, de az utóbbi pár évben vált kiemelt jelentőségűvé és igazán széles körben támogatottá. A virtualizáció keretében az egy vagy több fizikai rendszeren (host) egy vagy több virtuális rendszert (guest) futtatunk. A virtuális rendszert futtató hardver nem valódi, de erőforrásait a host rendszerből kapja. A virtualizált rendszerben a host rendszer erőforrásai bárhogy eloszthatóak a guest rendszerek között. A virtuális rendszerek fölötti felügyeletet a hypervisor program látja el. A virtualizáció keretében egész hálózatokat lehet kialakítani, virtualizált hálózati elemekkel. Ilyen módon például három fizikai gépen futhat öt szerver, tűzfalakkal szeparálva egymástól és terhelés függvényében kapnak a szerverek processzoridőt és memóriát. Így tehát azt, hogy egy guest szerver melyik fizikai hoston fut, csak a hypervisor segítségével tudjuk megmondani, de lehet, hogy mind a hármon.

A cloud computing abban különbözik a virtualizációtól, hogy a virtualizált rendszerek fizikailag külön telephelyen kerülnek megvalósításra, üzemeltető személyzettel, magas rendelkezésre állással és magas fokú optimalizációval.

A felhőszolgáltatások több csoportra bonthatóak a nyújtott szolgáltatás jellege alapján, amelyek mindegyikét XaaS – valami, mint szolgáltatás (something as a service) néven illetjük. Így beszélhetünk alapvetően infrastruktúra, mint szolgáltatásról (IaaS), platform, mint szolgáltatásról (platform as a service, PaaS) és szoftver, mint szolgáltatásról (software as a service, SaaS). Ezen fő kategóriák mellett egyéb elemek is előfordulnak, például a Salesforce által használt fejlesztés, mint szolgáltatás (development as a service, DaaS).

Az IaaS keretében a szolgáltató virtuális hardverkörnyezetet biztosít a megrendelő részére. Ebbe beletartozik a virtuális rendszer a tárterülettel és a hálózati infrastruktúra, amelyeket a szolgáltató üzemeltet. Az operációs rendszert, és az alkalmazásokat az ügyfél telepíti és tartja karban. A PaaS esetében a szolgáltató által

felügyelt kör szélesebb: a virtuális rendszer mellett az operációs rendszert, adatbázist, egyes alkalmazásokat, fejlesztő eszközöket biztosít. Az ügyfél feladata az alkalmazások installálása és felügyelete. A SaaS esetében a szolgáltató minden környezeti elemet biztosít, a felhasználó szoftverek funkcionalitásához fér hozzá. A hozzáférés általában vékony kliensen, böngésző segítségével történik. A felhasználó csak az adatokat tölti fel, csak azokért felelős. Meghatározott alkalmazásokat, így szövegszerkesztőt, táblázatkezelőt, egyéb irodai alkalmazásokat, vagy pedig valamilyen különleges szoftvert, CRM rendszert használhat. A használati díjak kialakítása hozzáférések számán alapuló és időalapú is lehet, minden esetben a tényleges használatért fizet az ügyfél.

Egyelőre kevés és szűk körű cloud szolgáltatás érhető el a világon. A Google irodai alkalmazásokat nyújt. Az Amazon, a Rackspace Hosting, a Yahoo és a Microsoft virtuális gépeket kínál, a Salesforce CRM rendszert biztosít, a Zoho pedig mindegyiket.

SaaS szolgáltatást nyújt a Google Google Apps márkanéven.[88] A szolgáltatás keretében céges levelezést hozhatunk létre, amelyben 25 GB lemezterületet, spamszűrőt és 99,9%-os rendelkezésre állást biztosítanak. Lehetőség van közös céges naptárkezelésre, eseményeket lehet ütemezni, a naptárakat egymás között megosztani, valamint a mobil eszközök naptárával szinkronizálni lehet annak tartalmát. Dokumentumkezelő lehetőséget is kapunk, amelybe szövegfájlokat, táblázatokat, prezentációkat lehet feltölteni és azokat szerkeszteni. Céges levelező csoportok hozhatók létre, különböző tartalmakat lehet rajtuk megosztani, archiválni és egyszerűen kereshető a minden tartalom és előzmény. Weblapokat lehet létrehozni a cég saját domain nevével, biztonságos kapcsolat és leválasztott területek alakíthatóak ki, így a vállalati intranetet is helyettesítheti a szolgáltatás. Lehetséges a belső videó megosztás is. A szolgáltatás díja rendkívül kedvező, felhasználói fiókonként évi 50 dollár. Ez egy magyar kkv számára jelentősen olcsóbb, mint ugyanezen infrastruktúra és szolgáltatások fenntartása saját erőből. Ezek mellett segítséget kaphatunk napi 24 órában telefonon és e-mailen. A garantált rendelkezésre állás évi 8 óra kiesést foglal magában. Az ügyfélszolgálat önkiszolgáló módon működik web felületen, amely titkosított SSL csatornán keresztül érhető el. A kéretlen levelek szűrése személyre

[88] ld. Google Apps cégeknek. http://www.google.com/apps/intl/hu/business/index.html [2011. 04. 01.]

szabható. Meghatározható a közös jelszó biztonsági követelménye, az e-mailek átirányíthatóak és a korábbi tartalmak migrációjára is van lehetőség.

A másik, ehhez hasonló szoftver, mint szolgáltatás a Salesforce.[89] Ez vállalatoknak nyújtott különböző alkalmazásokat kínál, így egy értékesítést automatizáló és az ügyfélkapcsolatot támogató szoftvert, ügyfélkiszolgálást és támogatást végző eszközöket. Együttműködést lehetővé tevő eszközöket, fejlesztési eszköztárat, külön adatbázis szervert, valamint a kifejlesztett alkalmazások felhasználók közötti cseréjét teszi lehetővé. A szoftverfejlesztési eszköz (force.com) használata bejelentkezésenként 90 centbe kerül, amely segítségével bármilyen alkalmazást el lehet készíteni, amely a fenti szolgáltatásokat igénybe veszi például adatfeldolgozó, folyamattámogató, üzleti intelligencia alkalmazásokat készíteni. Megkülönböztetésül a cég ezt a szolgáltatását fejlesztés, mint szolgáltatás névvel illette. Ez az alacsony bejelentkezési díj lehetővé teszi, hogy a kisebb szervezetek is magas szintű eszközöket használjanak alkalmazásaik fejlesztéséhez. Gyárilag egyébként több mint 50 ezer beépített alkalmazás áll rendelkezésre. Ilyenek például tartozáskezelés, humán erőforrás nyilvántartások, időmenedzsment, élelmiszer-összetevők kezelése. Az ilyen jellegű árazás nagy előnye, hogy a fejlesztési költségek közvetlenül hozzárendelhetőek a különböző szervezeti egységekhez. Ilyen módon megállapítható, hogy az egyes osztályok mennyit költöttek és milyen mennyiségben lehet további időegységeket hozzájuk rendelni. Ez az ár egyébként jelenleg akciós csak, későbbiekben ez 5 dollárra fog emelkedni. A korlátlan használat pedig havi 50 dollár, felhasználónként. Ezek tehát csak a fejlesztési platform használatát foglalja magában, viszont a többi, pl. CRM rendszer használatát, nem. A harmadik ilyen szolgáltató az Amazon, amely az eddigiekkel szemben viszont nem szolgáltatást, vagy platformot, hanem infrastruktúrát biztosít Amazon Elastic Compute Cloud (EC2) márkanéven.[90] Ez gyakorlatilag azt jelenti, hogy egy virtuális gép használatára van lehetőség, amely a kifizetett díjban foglalt számítási teljesítményt, memóriakapacitást és merevlemez tárterületet foglalja magában. Ezt a környezetet többféle operációs rendszerrel és egyéb rendszerszintű alkalmazásokkal vehetjük igénybe, így adatbázisokkal, alkalmazásfejlesztő eszközökkel, illetve jogosultság kezeléssel. Lehetőség van emellett saját virtualizált környezet feltöltésére. A szolgáltatás díjazása a felhasznált erőforrásokon alapul. Számítási teljesítményt EC2 számítási egységben mérik. A

[89] ld. Salesforce.com http://www.salesforce.com/ [2011. 04. 01.]
[90] ld. Amazon Elastic Compute Cloud. http://aws.amazon.com/ec2/ [2011. 04. 01.]

szolgáltatásnál lehetőség van ingyenes kipróbálásra, egy év időtartamra egy LINUX alapcsomag erejéig. A szolgáltatások ára az óránként 0,095 dollártól a 1,16 dollárig terjed az európai régióban.

A negyedik szolgáltató a Microsoft, amely .NET-es platform, mint szolgáltatás nyújt Windows Azure márkanéven.[91] Ilyen módon bármely Windows-os alkalmazást képes futtatni, gyakorlatilag bármilyen platformon. A vállalt rendelkezésre állás 99,95 százalékos. Az árak alapvetően úgy kerültek kialakításra, hogy az Amazonnál alkalmazott árakkal megegyeznek, viszont egy újabb tényezőt is tartalmaznak, a tártranzakciókat. Ez jelentős mértékben növelheti az összköltséget.

A Microsoft honlapján lehetőség van az Azure-os szolgáltatások teljes bekerülési költségének (TCO) meghatározására három éves intervallumra és annak szembe állításának a hagyományos, a vállalat telephelyén üzemeltett rendszerekkel. A számítások alapján természetesen az Azure jön ki győztesen.

A felhőszolgáltatások törvényei szerint az ilyen közműszerű szolgáltatás összességében akkor is olcsóbb a vállalatnál üzemeltett rendszereknél, ha egyébként magasabb költségekkel jár, ugyanis a számlázás csak a tényleges használatra terjed ki. A dinamikus erőforrás hozzárendelés mindig előnyösebb, mint az előrejelzés alapján történő tervezés, ugyanis hogyha az előrejelzés nem volt pontos, akkor egyszerűen nem vesszük igénybe az erőforrást. Az összes költség a különböző részköltségek összegeként jön ki, szemben a hagyományos rendszerek esetében, ahol meghaladhatja azt. Az erőforrás igények összesítésre kerülnek és így kiegyenlítődik az egyébként változó használati tendencia. A felhőben foglalt nagy számítási teljesítmény miatt a felhő jobban védett a különböző elosztott támadások ellen. A párhuzamos feldolgozás jelentős mértékben meggyorsíthatja az üzleti intelligencia alkalmazásokat. Az, hogy az erőforrások különböző telephelyeken kerültek szétosztásra, növeli a rendszer megbízhatóságát és csökkenti a kiszolgáltatottságát, például a természeti katasztrófáknál, szemben a vállalat adatközpontjával, ami alapvetően a vállalat telephelyén található, a felhő adatközpontjai optimális helyen kerültek kialakításra (energia, hírközlés).

A Gartner, amely az informatikai termékek és szolgáltatások piacán működő tanácsadó cégként többek között előrejelzéseiről híres, minden évben elkészíti a technológiák várható életciklus görbéjét. Ezen a görbén a felhőszolgáltatások 2009 óta

[91] ld. Windows Azure. http://www.microsoft.com/windowsazure/ [2011. 04. 01.]

rendkívül nagy érdeklődésre tartanak számot, 2010-ben majdnem pont a csúcson helyezkedtek el és a beérésüket 2-től 5 éven belül jósolják. A következő hasonló terület a magán felhők (private cloud) kialakítása lesz.[92]

A felhőszolgáltatások előnyei közé tartozik, hogy megosztott erőforrásokkal, hálózati működéssel könnyen konfigurálható és jól skálázható rendszert kapunk, meglehetősen alacsony belépési áron.

A biztonsági kihívást a felhőszolgáltatások tekintetében a felmérések szerint első helyen a szolgáltatóhoz való kötődés jelenti.[93] Ez azt jelenti, hogy a felhőben jelenleg alkalmazott rendszerek és szolgáltatások nem szabványosak, a kis piacon nem teszik lehetővé az átjárhatóságot. Amíg a belépéskori adatbevitel (importálás) egyszerű és a szolgáltató által támogatott, addig a szolgáltatás lemondása után az adatok exportálása rendkívül nehézkes és szándékosan nehezített a szolgáltatók által. Emellett pedig külön probléma, hogy a szoftver, mint szolgáltatás esetében szinte értelmetlen is az adatok exportálása, ugyanis a Salesforce által a CRM adatbázisban tárolt relációk az adatbázison kívül nehezen értelmezhetőek. Ennek az előfordulási valószínűsége magas, a hatása pedig közepes, összességében a kockázat szintje magas. Ez a probléma nemcsak szolgáltató önkéntes váltásakor léphet fel, hanem a szolgáltató csődje esetén is. Ekkor viszont könnyen számolhatunk a teljes adatbázisunk elvesztésével. Ennek a valószínűsége, különböző felmérések alapján kicsi, ugyanis a szolgáltatók az amerikai tőzsdén jegyzett tőkeerős multinacionális cégek.

Kockázat továbbá az irányítás elvesztése a felhőben működő rendszer felett, ami a tisztázatlan szereposztás, nem meghatározott felelősségi rendszer, forráskód elérhetetlensége miatt következhet be. Ennek a valószínűségét nagyon magasnak, hatását IaaS esetén nagyon magasnak, SaaS esetén alacsonynak, az eredő kockázatot magasnak tartják.

A harmadik legnagyobb kockázat a nem-megfelelőségből ered. A rendszerek megfelelőségét a különböző jogszabályi és szabványi megfelelőségek érdekében tanúsítani szükséges, amelyre a felhő nem biztosít lehetőséget. Ennek az az oka hogy a szolgáltató számára jelenleg túlzott költséget jelentene az audit biztosításának lehetősége, és a keresleti piacon nincsen rákényszerítve a nagyobb fokú

[92] Gartner blog. http://blogs.gartner.com/hypecyclebook/2010/09/07/2010-emerging-technologies-hype-cycle-is-here/ [2011. 04. 02.]
[93] Catteddu, 2009.

együttműködésre az ügyféllel. Ennek a valószínűségét nagyon magasnak, hatását nagyon magasnak, az eredő kockázatot magasnak tartják.

Az így nyújtott szolgáltatások rendkívül költséghatékonyak, a nagyvállalatok a kedvezményes áron beszerzett számítógépparkjukat erőművek és transzatlanti adatkábelek mellett telepítik, így az üzemeltetési költség töredéke lehet a vállalatnál üzemeltetett saját szerverénél. Tekintettel arra, hogy a gazdasági recesszió kapcsán a gazdasági társaságok árérzékenysége nagymértében nőtt, a beszerzések elsődleges szempontjává vált a szolgáltatások ára. A saját tulajdonú szerver esetén meg kell fizetni az épületet, a környezeti körülmények (léghőmérséklet, páratartalom) fenntartását, a villamos energiát, a szakszemélyzetet és így tovább. Egy távolról igénybevett szolgáltatás esetén elég megfizetni egy informatikust és a szolgáltatást, amely ráadásul egy jól követhető költségtényező.

Ez az üzlet 2009-ben 17 milliárd dolláros volt, 2013-ra az IDC becslése szerint 45 milliárd dollárra fog nőni. Ez a tendencia a világ más országaiban is, így az Európai Unióban és Magyarországon is hasonlóan fog alakulni, legfeljebb a kialakulás időtartama lesz hosszabb. Mindamellett, hogy a költségeket és környezetszennyezést is ezzel a megoldással minimalizálhatjuk, olyan biztonsági és jogi megfelelőségi kérdéseket vetődnek fel, amelyek Európában egyelőre megoldhatatlannak látszanak. A felhőszolgáltatók számítóközpontjaikat ugyanis a világ különböző pontjain építik fel és mivel az erőforrásokat dinamikusan osztják meg ezek között, ők maguk sem tudják megmondani, hogy az általunk használt szolgáltatás vagy az ügyfeleink adatai éppen a világ melyik részén vannak.[94] A hatályos európai adatvédelmi irányelvek alapján csak oda lehet adatot továbbítani, ahol az európaival megegyező az adatok védelme, így ez a szolgáltatók telephelyeinek túlnyomó részét ki fogja zárni. A szolgáltatókkal nem lehet egyedi szerződést kötni (legalábbis a magyar cégek méretét tekintve nem) és nem vállalják azokat a rendelkezésre állási, megfelelőségi, stb. követelményeket sem, amelyek egy outsourcing szerződés keretében normálisak voltak. Egyelőre ez egy kínálati piac, így a szolgáltatókat egyáltalán nem érdeklik ezek az igények és aggályok, de várhatólag, ha telítetté válik a piac, akkor szofisztikáltabb biztonsági megoldásokat fognak nyújtani. Ilyen lehet például az, hogy az európai személyes adatok kezelését csak Európában lévő felhőszervereken fogják végezni, vagy pont ezért új európai szolgáltató lép a piacra. A piacra lépés egyébként

[94] Spivey, 2009.

hihetetlen költségeket emészt fel, a jelenlegi, piacon lévő szolgáltatók is a korábban más célból kiépített rendszereik erőforrását ajánlják fel a felhőszolgáltatások keretében.

2.4. Támadás az adatok ellen

2.4.1. A túlzottan gyors fejlődés külső veszélyei

A globalizálódó világra jellemző gazdasági, társadalmi, politikai folyamatok, illetve az ezen folyamatoknak való megfelelés kényszere igen nagy intenzitással növeli az egész rendszer komplexitását. Ez a növekvő komplexitás nem lassú, szerves fejlődés része, ahol egyre finomabban kidolgozzák a rendszer részleteit, hanem a túl nagy sebesség miatt – mint a túlhűtött oldatban – nem alakulnak ki a természetes kötések. Ilyen módon az informatikai szolgáltatások kiforratlanul jelentős veszélyforrást rejtenek magukban. A gyakorlatban ez például egy új kormányzati szolgáltatásnál, ahol a szoftverfejlesztés tesztelési fázisát nem végzik el megfelelően a rövid határidők miatt és több ezer állampolgár személyes adataihoz férnek hozzá illetéktelenek, vagy egy kritikus infrastruktúra (pl. energia-ellátás) hirtelen, nem megfelelően bevezetett informatizálása miatti hosszú áramszünetet jelentheti. És akkor még csak a műszaki oldalt vettük figyelembe és nem számoltunk a társadalom felkészültséggel, a jogalkotó szabályozási képességével és hasonló tényezőkkel. A megfelelő biztonság implementálásához idő kell. A biztonság a joghoz hasonlóan utólag képes megfelelően reagálni. Azok a percepciók, amelyeket egy új technológia megjelenése előtt felállítunk (például a kockázatbecslés terén) csak teoretikusak, ugyanúgy, mint ahogy a jogalkotó is csak becsülni tudja egy szabályozandó területbe való beavatkozás joghatását. A megfelelő biztonság csak a tényleges üzemelés eredményéből levont konzekvenciák alapján alakítható ki, és akkor is csak konvergálhatunk a tökéletes védelem célja felé, el sosem érhetjük azt. Eközben is folyamatos visszacsatolásra, értékelésre és önkorrekcióra van szükségünk. Ha a folyamatok nem ebbe az irányba haladnak, akkor az egyébként instabil rendszer csak a stabilitás illúzióját nyújtja. Nyilván csak addig, ameddig valami hatalmas robajjal össze nem dönti ezt a kártyavárat.

És itt lép be a cyberterrorizmus, mint a kvázistabil rendszer esetleges megbontója. Azért esetleges, mert a védelmi tudományokra jellemző módon nem lehet kijelenteni biztosan egy ilyen esemény bekövetkezését, de arra feltétlenül számítani kell. Oliver Cromwell jelszava „Bízz Istenben, és tartsd szárazon a puskaport!”, máig kitart a biztonságpolitikában. Az országvédelem rendszerében szükséges az olyan káros eseményekkel is foglalkozni, amelyek egyébként a széles közvélemény szerint nagy

valószínűséggel nem fognak bekövetkezni (ilyen lehet a külső fegyveres támadás vagy a cyberterrorizmus is), ugyanis egy ilyen esemény váratlan és a Magyar Köztársaságot felkészületlenül érő bekövetkezése sokkal komolyabb károkat okozhat annál, mintha felkészülve történik ugyanez.

2.4.2. Az informatikai bűncselekmények

2.4.2.1. Az informatikai bűncselekmények jellemzői

Kriminológiai definíció alapján a csúcstechnikát[95] alkalmazó (vagy informatikai) bűnözéshez tartozik az arra irányuló kísérlet, hogy a fejlett elektronikus média felhasználásával folytassanak illegális tevékenységeket.[96] A klasszikus bűncselekményekkel szemben az elkövetőnek nem szükséges közvetlen kapcsolatot létesíteni az áldozattal, a bűncselekményt akár a világ másik végéről, a névtelenség (látszólagos) homályába burkolózva követheti el. Az informatikai bűncselekmények elkövetésekor az egyedi számítógépek, a hálózati eszközök, vagy a teljes hálózat is lehet célpontja, megvalósítási illetve elkövetési tárgya illetve környezete, az elkövetés szimbóluma, vagy akár az elkövetés „tanúja", tehát objektív módon rögzítheti az elkövetés egyes lépései vagy akár teljes folyamatát.[97]

A klasszikus bűncselekményekkel szemben az elkövetőnek nem szükséges közvetlen kapcsolatot létesíteni az áldozattal, a bűncselekményt akár a világ másik végéről, a névtelenség (látszólagos) homályába burkolózva követheti el. A bűncselekmény tárgyát képező vagyontárgy nehezen determinálható. Mivel azok általában adatok vagy jó hírnév, ezért nagy kihívás a kárérték meghatározása. Nehezíti a helyzetet, hogy a károsult nem minden esetben veszi észre azonnal, hogy áldozattá vált. A bűncselekmény megvalósítása igen kis anyagi ráfordítást igényel, az esetek nagy többségében csak egy személyi számítógép és hálózati kapcsolat szükséges hozzá, amíg az elkövetéssel járó haszon hatalmas lehet, világviszonylatban 8 milliárd dollárra becslik.[98] A bűncselekmény felderítése több komoly nehézségbe ütközik. Egyik, hogy a bűncselekmény elkövetése nehezen felderíthető nyomokat hagy maga

[95] high-tech-en vagy csúcstechnikán értjük az elektronikus az elektronikus berendezések (számítógép, mobiltelefon, stb.) olyan kifinomult formáit, amelyek ma már mindennapos használatban vannak. Adler–Mueller–Laufer, 2000, p. 401.
[96] Adler–Mueller–Laufer, 2000,. p. 401.
[97] Illési, 2009, p. 164.
[98] A British Banking Association becslése szerint. In: Adler–Mueller– Laufer, 402. p.

után. Szemben például egy emberölés helyszínével, ahol jó esetben sok hagyományos értelemben vett nyom található, ahol a traszológia segítségül hívható, a számítástechnikai bűncselekmény „helyszínén" csak adatokat találhatunk, melyek vizsgálatát csak gyakorlott igazságügyi számítástechnikai szakértő tudja elvégezni (igen magas a bűncselekmény komplexitási foka). Másik a nyomok gyors változása, megsemmisülése, amely a bűncselekmény későn történő felismerése esetén nagy valószínűséggel bekövetkezik. Harmadik probléma, hogy az elkövetés földrajzi helye nagymértékben meghatározza az eljárás végeredményét, ugyanis külföldi elkövető esetén kétes, hogy a bűnvádi eljárás lefolytatható lesz-e.[99] Ennek megoldására az Európa Tanács létrehozta a Számítástechnikai bűnözésről szóló egyezményét,[100] melyet Magyarországon is kihirdettek. Az egyezményt alá nem író államokban még általában a cselekmények büntetendősége sem biztosított, de az aláíró felek között is nehezen működik az európai kölcsönös jogsegély, illetve a nemzetközi jogsegély.[101]

2.4.2.2. Az informatikai bűncselekmények típusai

Több, a Büntető Törvénykönyvben nevesített tényállás van, ami segítségével tipizálhatóak az informatikai bűncselekmények. Ezek a következőek:

Számítógépes hálózatok feltörése

A cselekmény elkövetése három típusra osztható, az egyik a behatolás, amikor nem avatkoznak bele a rendszer működésébe (Btk. 423. § (1)). Ekkor az elkövető (hacker) csak engedély nélkül belép, körülnéz a rendszerben és kilép onnan. Ez elsősorban a sikerélmény megszerzésére irányul. Második esetben nem haszonszerzési célból, viszont beavatkozással (adatok törlése, megváltoztatása, működés akadályozása) párosul a behatolás (Btk. 423. § (2) a, b). Ez is az előző csoportra jellemző, csak a sikerélmény bizonyítékaként a szervezet honlapját is megváltoztatja, adatokat lop. Ilyen lehet továbbá valamely személy, szervezet iránti ellenérzés kimutatása. Az első esetben az elkövető csak vétséget követ el, a többi viszont bűntett. A harmadik esetben haszonszerzési célból elkövetett beavatkozás is bűntett (Btk. 375. §). Ez az elkövetési magatartás erősen közelít az ipari kémkedés kategóriához, általában saját célra történő bevételszerzés vagy megbízásból történő hitelrontást takar. Ez a vétségi

[99] Parti, 2004. 204. p.
[100] Convention on Cybercrime, kihirdette a 2004. évi LXXIX. törvény
[101] Parti, 2008, 241. p.

és bűntetti alakzat közötti felosztás jól tükrözi a valós életbeli viszonyokat, amelyet az elkövetők informatikus társadalombeli differenciálása is mutat.

Ipari kémkedés

Ebben az esetben egy gazdasági szervezet felbérel valakit egy rivális cég informatikai rendszerébe való behatolásra és onnan történő információszerzésre, amely jogtalan gazdasági előnyhöz juttatja a megbízót. Ezt informatikai szempontból a Btk. 375. § szankcionálja.

Szoftverkalózkodás

A szoftverkalózkodás a szerzői jogvédett szoftvertermékek illegális használatát, hamisítását jelenti. Ebbe beletartozik az illegális otthoni másolat használata, a másolatok terjesztése, továbbá a másolt szoftverek dobozos, eredeti szoftverként történő terjesztése, eladása. A másolat megakadályozása érdekében léteznek műszaki megoldások, mint a különböző CD-másolásvédelmek (nem kielégítő biztonságú eljárás) és a hardverkulcsok[102] alkalmazása, valamint a DRM technológiák. Szerzői vagy szerzői joghoz kapcsolódó jogok megsértése, védelmet biztosító műszaki intézkedés kijátszása, vagy jogkezelési adat meghamisítása (Btk. 385-387. §§) merülnek fel ilyen esetben.

Gyermekpornográfia

Az Internet, mint nehezen ellenőrizhető fórum lehetőséget teremt különböző illegális anyagok terjesztésére. Ezekből kiemelkedő figyelmet érdemel a gyermekpornográfia bűntette (Btk. 204. §). Az Interneten még amatőrök számára is könnyen lehet ilyen anyagokat találni, viszont nehéz a terjesztők ellen eljárást indítani. Ennek egyik oka a nemzetközi viszonylatban elkövetett bűncselekményének nehéz felderíthetősége és büntethetősége.

Hitelkártyacsalás

Az Interneten fizetésre alkalmas készpénz-helyettesítő eszközök adatainak ellopása a birtokos vagy a pénzintézet informatikai rendszeréből vagy a hálózati forgalom lehallgatásával. Ennek esélyét növelik az egyre inkább az Internetre áthelyeződő

[102] Igen nagy biztonságú külső pl. USB eszköz, amely csatlakoztatása nélkül a program nem fut. Költséges programok hatásos védelme.

üzleti tranzakciók. Az elkövető a kártya-adatok megszerzése után perceken belül képes felhasználni a tulajdonos egyenlegét, még a kártya letiltása előtt. Ez általában phishing (adathalászat) útján történik, hamis honlap közzétételével. A büntetőjog ezt készpénz-helyettesítő fizetési eszközzel visszaélésnek (Btk. 393. §) minősíti.
Ez a felsorolás koránt sem teljes, csupán azt kívánja szemléltetni, hogy a jogalkotó szankcionálja a leggyakrabban előforduló informatikai jellegű deviáns cselekményeket.

2.4.2.3. Az informatikai bűncselekmények elkövetői

Az informatikai bűncselekmények elkövetőit a köznyelv és a sajtó egyszerűen és összefoglalóan hackernek nevezi. A számítástechnikai bűncselekményekkel kapcsolatos elnevezéseknek és így a hacker szó jelentésének is többféle definíciója van, amely az idővel változott.
„Abban az időben [1980] a hacker szót olyasvalakire használtuk, aki rengeteg időt töltött a hardverek és szoftverek bütykölésével, vagy azért, hogy felesleges lépéseket átugorjon, és a munkát gyorsabban elvégezze."[103]
Ma az informatikai szakzsargon a számítógépes hálózatok „jóindulatú" feltörőit hackereknek vagy white-hat hackereknek, „rosszindulatú" feltörőit crackereknek vagy black-hat hackereknek nevezi. A jó- és rosszindulat közötti különbség az anyagi haszonszerzésben valamint a szándékos károkozásban illetve annak hiányában nyilvánul meg, de a fogalom és az elkövetők jogi megítélése, valamint szociológia jellemzői kapcsán már a '70-es évektől vita gyűrűzött.[104]
Crume szerint a hacker olyan személy, aki illegális úton hozzáfér egy számítógépes rendszer információállományához.[105] Tehát Crume nem különíti el egymástól a jó- és rosszindulatú behatolókat, ugyanis egy számítógépes rendszerbe történő behatolás minden esetben okoz károkat, hiszen nem lehet biztosan tudni, hogy a hacker valóban nem rombolt vagy nem másolt le adatokat. A stakeholderek felé minden esetben presztízsveszteséget jelent egy ilyen esemény, így közvetett kárt vagy elmaradt hasznot eredményezhet.
A hackerek általában olyan, nagyrészt 16-30 év közötti fiúk, akik élvezetüket lelik ebben a tevékenységben, általában nem anyagi haszonszerzési célzatból, csak

[103] Mitnick–Simon, 2003. p. XI.
[104] Black, 1993.
[105] Crume, 2003, p. 15.

kíváncsiságból, vagy rosszindulatból követik el tetteiket, magukat digitális banditáknak tekintve. Általában nem ismerik tetteiknek jogi és gazdasági vonzatait. A nem anyagi haszonszerzésből elkövetett hálózatfeltörés is súlyosan károsítja az áldozattá vált szervezetet, ugyanis a cselekmény kivizsgálása, a helyreállítás költségei továbbá például a szervezet honlapjának megváltoztatása igen jelentős, pénzben mérhető hátrányt okoz annak. A nyilvánosságra hozott informatikai biztonsági incidensek esetenként a tőzsdei részvények áresését is okozhatják.[106] Emiatt a szándéktól függetlenül érdemes lehet Crume fogalmát tekinteni az egyébként magyar köznyelvben is ilyen értelemben használt hacker fogalomnak.

A magánszemélyek nagy része úgy véli, semmi nincs a számítógépén, amit érdemes lenne megvédeni, de egyrészt a magánlevelezésünk, hitelkártyaadatok, stb. nem biztos, hogy jó kezekbe kerülnek, másrészt számítógépünket is felhasználhatják más gépek elleni támadásra,[107] mely esetben a megtámadott gépről csak az látszik, hogy a mi gépünkről intéztek támadást ellene, tehát akár bíróság elé is kerülhetünk elővigyázatlanságunk miatt.

A hackerek sem egyformák, nem mindegyik nagy tudású számítástechnikai szakember, sőt a többségük erősen kezdő. A hackertársadalomban megfigyelhető egy rétegződés, amely egy piramisként ábrázolható.[108] A piramis alján helyezkednek el a kezdő hackerek vagy szkriptbetyárok, akik felhasználói szintű ismeretekkel rendelkeznek és az Internetről letöltött hacker-programokkal követnek el behatolási kísérletet, illetve támadást. Az ő létszámbeli arányuk a legnagyobb, ezért ők okozzák a legnagyobb károkat. A piramis középső rétege a haladó hackerek, akik már tudják, mit csinálnak és jelentős számítástechnikai tudással rendelkeznek. A piramis csúcsán helyezkednek el az elit hackerek. Ők nagyon magas szintű szakmai ismeretekkel rendelkeznek, kevesen vannak és igen zárt közösséget alkotnak. Nem pazarolják energiájukat játszadozásra, nagyobb arányban követnek el bűncselekményeket haszonszerzési célból. Utóbbiak tudásuk, a kezdők pedig létszámuk miatt veszélyesek. Másrészt, ahogy Mitnick[109] is rámutat, hackerkedni nem csak komoly informatikai tudással és a számítógép billentyűzetével lehet, hanem rendkívüli

[106] Campbell – Gordon – Loeband – Zhou, 2003, p. 445.
[107] botnetek, zombigépek hálózatának kialakítása
[108] Crume, Jeff, 2003, p. 15.
[109] Mitnick, Kevin D., 2003, p. 3.

eredményeket lehet elérni a humánerőforrás kihasználásával, az emberek megtévesztésével.[110]

2.4.3. A cyberterrorizmus

A cyberterrorizmus összetett szó, elsősorban alkotóelemei alapján értelmezhető.[111]
A kibertér (cyberspace) a számítógép-kommunikációs hálózatok összessége. Legnagyobb egyedi eleme az Internet, mely több mint 200 országot és közel egymilliárd felhasználót foglal magába. A fogalmat William Gibson alkotta meg és használta először Neuromancer című sci-fi regényében, mely 1984-ben jelent meg. Akkori jelentése többmilliárd ember által érzékelt együttes hallucináció volt. A kibertér kifejezés használata kiemeli a hálózatok közötti szoros kapcsolatot, az ember és a hálózatok, valamint a társadalom és a hálózatok közötti összefüggéseket, szemben a hálózat fogalom elsődlegesen technikai jelentésével.
Terrorcselekményt követ el az, aki abból a célból, hogy állami szervet, más államot, nemzetközi szervezetet arra kényszerítsen, hogy valamit tegyen, ne tegyen vagy eltűrjön, a lakosságot megfélemlítse, más állam alkotmányos, társadalmi vagy gazdasági rendjét megváltoztassa vagy megzavarja, illetőleg nemzetközi szervezet működését megzavarja, személy elleni erőszakos, közveszélyt okozó vagy fegyverrel kapcsolatos bűncselekményt követ el.[112]
Anthony Giddens szerint „a terrorizmust az erőszakkal való politikai célú fenyegetőzéseként vagy az ilyen erőszak alkalmazásaként definiálhatjuk olyan egyének részéről, akiknek nincs formális politikai hatalmuk. Ha így fogjuk fel, a terrorizmus sajátságos jelentőségre tesz szert a modern társadalmakban, éppen azért, mivel a kormányzatok – más nemzetekre irányuló fenyegetésként vagy tényleges háborúk formájában – monopolizálni kívánják a politikai célú erőszak alkalmazásának jogát."[113] Benjamin Netanjahu szerint „a terrorizmus, a polgárokon gyakorolt szándékos, módszeres erőszak, amely az általa kiváltott félelmen keresztül politikai célokat kíván megvalósítani."[114]

[110] a szakmában angol nyelven social engineering
[111] Gorge, 2007, p. 9.
[112] Btk. 261. § (1)
[113] Giddens, 1995. p. 366.
[114] Netanjahu, 1995. p. 20.

A terrorizmus hadtudományi szempontból Kovács Jenő altábornagy besorolása szerint az anyagcentrikus és mozgáscentrikus hadikultúrákkal szemben a gerilla hadikultúrába tartozik, melynek elméletét Mao Ce-Tung alkotta meg. Más besorolások szerint attól a társadalmi támogatottság hiánya miatt különbözik. Jellemzője az aszimmetrikus hadviselés; nem egyenlő hadviselő felek szembenállásáról van szó. Emiatt a hagyományos haderő nem képes hatékonyan felvenni a harcot a terrorizmussal.

A cyberterrorizmus a számítógép-hálózatok felhasználása az emberi élet kioltása céljából, vagy a nemzeti kritikus infrastruktúra szabotálása céljából, amelyet olyan módon követnek el, hogy az emberi életet veszélyeztethet.[115]

A cyberterrorizmus úgy határozható meg, mint az információtechnológia terrorista csoportok és személyek általi használata terveik megvalósításának érdekében. Ez magában foglalhatja az információtechnológia használatát hálózatok, számítógéprendszerek és telekommunikációs infrastruktúrák elleni támadás megszervezésére és végrehajtására vagy információcserére illetve fenyegetés keltésére. Példák a fogalomra a számítógéprendszerekbe történő engedély nélküli behatolás, vírusok bejuttatása sebezhető hálózatokba, weblapok megváltoztatása, szolgáltatás megbénítása vagy terrorfenyegetések elektronikus kommunikáción keresztül.[116]

A cyberterrorizmus tehát felülről történő megközelítésben a „hagyományos" terrorizmus (illetve gerilla hadikultúra) céljainak infokommunikációs eszközökkel való végrehajtása, vagy alulról tekintve az informatikai bűncselekmények tömeges, szervezett végrehajtása. A cyberterrorizmus ellen való védekezés is e két aspektus mentén történhet.

A cyberterrorizmus elleni védekezés a magánszektor szintjén elsősorban az egyedi informatikai támadások, informatikai bűncselekmények elleni védelmet jelenti, a különbség alapvetően a támadások erősségében és intenzitásában valószínűsíthető (alulról való megközelítés).

A felülről történő megközelítés inkább az állami vezetés, katonai, rendvédelmi szervek szempontjából bír jelentőséggel. Ez utóbbi esetben szükséges az ilyen irányú védelmi tervezés, az országvédelem rendszerének ilyen irányú felkészítése, a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről szóló 94/1998. (XII. 29.)

[115] Cohen, 2010. p. 7.
[116] National Conference of State Legislatures, 2007.

OGY határozat, a Magyar Köztársaság nemzeti biztonsági stratégiájáról szóló 2073/2004. (IV. 15.) kormányhatározat, valamint a Magyar Köztársaság Nemzeti Katonai Stratégiájáról szóló 1009/2009. (I. 30.) Korm. határozat bővítése a cyberterrorizmus veszélyként való azonosításával. Szükséges lenne a fenti kiegészítések mellett egy önálló infokommunikációs biztonsági stratégia kialakítása is, amely a nemzeti biztonsági stratégiára épülő ágazati stratégiaként kritikus információs infrastruktúrák elleni támadások hatékony megelőzését, kivédését és kezelését segítené elő.[117]

Ezen kétirányú értelmezés alapján az újdonságot elvileg csak a felülről történő megközelítés nyújtana, hiszen az egyedi támadásokra elvileg felkészültek vagyunk. Természetesen ez nem igaz. Az egyének, a nonprofit, az állami szektor és a gazdasági szektor is erős önfejlesztésre szorulnak az informatikai biztonság területén, elsősorban a biztonság-tudatosság kialakítása lenne szükséges.

Az alábbiakban a cyberterrorizmus elleni védelem formái és szintjei kerülnek bemutatásra,[118] melyek egymással kombinálhatók, illetve azokat kombinálni szükséges. A cyberterrorizmus elleni védelem aktív és passzív formákra bontható. Definíció szerint az aktív védelem komoly kockázatot vagy szankciót hordoz a támadóval szemben. A kockázat vagy szankció lehet azonosítás, felfedés, nyomozás vagy büntetőeljárás, megelőzően vagy utólagosan. Némely jogi illetve más okból kifolyólag az aktív védelmi tevékenység szükségszerűen a kormányzatra hárul. A passzív védelem alapvetően a célpont megerősítése (hardening). Nagyrészt különböző technológiák és termékek alkalmazását jelenti (tűzfalak, titkosítás, behatolás-jelzés), valamint tevékenységeket (belső szabályozás, biztonsági mentés), melyeket a személy vagy szervezet az általa használt IT rendszerek védelmében tesz. A cyberterrorizmus elleni védelem szintjei a megelőzés, a veszteségek korlátozása és a következmény-menedzsment.

2.4.3.1. Megelőzés

Tervezett biztonság

A megelőzési módszerek két fő kérdésre való választ keresik: hogyan lehet egy támadást indítása előtt megállítani, valamint hogy hogyan lehet meghiúsítani egy

[117] Muha, 2009, p. 216.
[118] Goodman– Kirk, J. C.–Kirk, M. H., 2007, p. 193.

támadást, mielőtt az elérné a célpontot. Elsősorban a rendszer biztonságra tervezése a legalapvetőbb megközelítés. Ha a tervezés a biztonságon alapul, a támadások megelőzhetőek, mert hatásuk korlátozottan lesz, vagy nem okoznak kárt. A rendszerek tervezésekor a különböző biztonsági szabványok ezt tekintik a legmagasabb biztonsági szintnek.

Támadások tiltása

A támadások megelőzésének másik általános módja azok jogi eszközökkel való tiltása. Nyilvánvalóan a nemzeti jogalkotás feladata ezen cselekmények kriminalizálása. A hálózatok túlnyomó részének nemzetközisége miatt nemzetközi együttműködés, megállapodások és nemzetközi szabványok, normák kialakítása szükséges. A magyar büntetőjog a cyberterrorizmus több aspektusát kriminalizálja. Aluról való megközelítésben a büntetőjog az információs rendszer felhasználásával elkövetett csalás (Btk. 375. §), az információs rendszer vagy adat megsértése (Btk. 423. §) és az információs rendszer védelmét biztosító technikai intézkedés kijátszása (424. §) törvényi tényállások alapján hivatott szankcionálni a cyberterrorizmus főbb elemeit az Informatikai bűncselekmények típusai című alfejezetben ismertettek alapján. Lehetőség van a felülről történő megközelítésre is, ahol a terrorcselekmény (Btk. 314. §), és a közérdekű üzem működésének megzavarása (Btk. 323. §) törvényi tényállásokat meritheti ki a támadó.

Elrettentés

Az elrettentés történelmileg a hidegháború alatti nukleáris stratégia alapelemét jelenti. Az elrettentés a cybertérben olyan műszaki képességekkel támogatott deklarált irányelvekből áll, melyek nagy valószínűséggel biztosítják a támadás érzékelését, a támadó azonosítását és a megtorlást. Ennek alapjait megfelelő biztonságpolitikai alapelvek lefektetésével lehet elérni, amelyre épülhetnek a későbbiekben a képességek. Ez elsősorban a kormányzati politika feladata, és a fentebb említett biztonság- és védelempolitikai alapelvekben, illetve nemzeti biztonsági stratégiában nyilvánulhat meg.[119]

[119] Az információs hadviselésről ld. Haig – Várhegyi, 2005, p. 133.

Megelőzés vagy elfogás

A megelőzés illetve elfogás különböző formái szintén jellemzőek ezen a területen. A megelőzés jellemzően a támadni készülő ellenfélre mért megelőző csapást jelenti. Az elfogás egy megindított támadás megállítását jelenti. Mindkét megelőzési forma rendkívül gyors cselekvést igényel. Mind a megelőzés, mind az elfogás történhet a kibertérben és fizikailag is.

2.4.3.2. Veszteségek korlátozása

Jelzések és figyelmeztetések

A jelzések és figyelmeztetések célja, hogy a megindított támadásokat jelezzék és figyelmeztessenek. A jelzések és figyelmeztetések adása nehéz feladat, de egyszerűbb, mint a megelőzési feladatok elvégzése. Így a behatolás-érzékelés (intrusion detection) a kutatás-fejlesztés aktív területévé vált. Az érzékelés és a jelentés egy rendszer tekintetében IDS rendszerek üzembe állítását, felügyeletét és a jelzéseket értékelő azokra reagáló csoportot jelent. Országos szinten ezt az aggregált incidensfigyelést a CERT-Hungary Központ (CHK) látja el.[120]

A rendszer megerősítése

A külső behatolás megelőzésére szükséges a rendszer megerősítése mind informatikai, mind fizikai megközelítésből. A legrégebbi és mindmáig széleskörűen alkalmazott informatikai technológia a jelszavak alkalmazása. További technikák a tűzfalak és proxy-szerverek alkalmazása, intelligens kártyás, biometrikus azonosítás, kriptográfia, átviteli csatornák titkosítása. Fizikai oldalról a behatolás elleni védelem, beléptetés, fizikai rendelkezésre állás biztosítása tartozik ebbe a kategóriába.

Csoportokba osztás és feltartóztatás

A rendszer külső támadása esetén a következő védelmi vonal a belső csoportokba osztás és feltartóztatás. Ezek célja a behatolás mértékének és az okozott károknak a korlátozása, a fennmaradó (támadásban nem érintett) információvagyon védelme, valamint a helyreállításhoz és a reagáláshoz szükséges információk gyűjtése. Ez a hálózatok és más erőforrások szegmentálásával érhető el.

[120] http://www.cert-hungary.hu/node/2 [2009. 08.15.]

Leállítás és újraengedélyezés

Másik megközelítés az automatikus teljes vagy részleges leállítása és újraengedélyezése a rendszernek. A rendszer, amely érzékeli, hogy megtámadták, belső sorompókat kezd állítani, amelyek nem elviselhetőek normál üzemben, viszont így izolálhatóak a rendszer kompromittálódott részei. Ez a szegmentált rendszerek szisztematikus leválasztását és kényszerített üzemszünetét jelenti. Vírustámadáskor hatékony eljárás, de jelentős veszteséget jelenthet az alkalmazása.

Biztonsági mentés

A támadás előtti állapot hatékony visszaállításához a lehető legfrissebb támadás előtti mentett állapotra van szükség. Ennek megvalósítása az informatikai rendszerben tárolt információk rendszeres teljes körű biztonsági mentésével történik. Különleges figyelmet kell szentelni a támadás előtti és támadás közbeni adatgyűjtésnek és megőrzésnek, ennek a későbbi nyomozási és bizonyítási eljárásban van szerepe.

Ellenőrzések végrehajtása

Nagyon fontos, hogy a támadás végrehajtása után gyorsan független ellenőrzés kerüljön végrehajtásra. Az audit információkat fog gyűjteni, melyek segíthetnek azonosítani és elfogni a támadót, valamint információt biztosíthat a szervezetnek a hasonló jellegű támadások későbbi elkerülhetősége érdekében. Az ellenőrzéseket – ahhoz, hogy azok eredményét érdemben figyelembe lehessen venni eljárások során – mindenképen a kriminalisztika alapelveinek figyelembe vételével kell lefolytatni.[121]

Biztonsági irányelvek meghatározása

A szervezeteknek nagyobb erőfeszítéseket kell tennie a biztonsági irányelvek és tervek meghatározása terén a támadások elleni védelem érdekében. Az átfogó tervezés a szervezetre kifejezetten veszélyes támadások széles körét lefedheti.

2.4.3.3. Következmény-menedzsment

Helyreállítás

A helyreállítás a védelem passzív formája. Feladata az információs vagyon lehető leggyorsabb helyreállítása, a normális üzemhez legjobban közelítő mértékben. A

[121] Slade, 2004, p. 82.

gondosan kitervelt és végrehajtott támadások a helyreállítás hatékonyságát nagymértékben nehezítik.

Reagálás

A reagálás a helyreállításnál aktívabb formája a védekezésnek. A tettes azonosítása és büntetése, valamint a konzekvenciák levonása által a szervezet védelmének megerősítése a célja. Nehézségei ellenére az incidens utáni nyomozás szükséges a támadás forrásának, indítékának és céljának meghatározása érdekében, valamint a hasonló támadások megelőzésében.

2.5. Összefüggések

A robbanásszerű infokommunikációs, és az ezzel párhuzamosan bekövetkező társadalmi, gazdasági fejlődés – mely az információs társadalom, mint magasabb szintű társadalmi fejlettség felé mutat – eredményeképp egyre kiszolgáltatottabbak vagyunk az informatikának és így az informatikai bűncselekményeknek elkövetőinek is. Az információs társadalomhoz vezető utak legfontosabb ösvénye az elektronikus írásbeliség.

Ezen új típusú írásbeliségnek vannak bizonyos problémái, amelyek várhatólag – akarva, vagy akaratlanul – jelentkezni fognak. Az informatikának való kiszolgáltatottság és az elektronikus írásbeliség már most látható problémái együttesen vezetnek egy biztonsági kockázathoz, amelyben a véletlen események mellett jelentős szerepe van az informatikai bűncselekményeknek elkövetőinek is. Ezek az elkövetők és cselekményeik is jól kategorizálhatók. Ezen informatikai bűncselekmények a cyberterrorizmus építőkövei. A cyberterrorizmus elleni védekezés a terrorizmus és az informatikai bűncselekmények oldaláról is megközelíthető. A cyberterrorizmus a támadás bekövetkezésének valószínűségétől függetlenül – amennyiben az nullától különböző – valós veszélyforrásnak tekintendő, ugyanúgy, mint például egy Magyar Köztársaság elleni fegyveres támadás. Ebből következően az ellene való védekezés legalább tervezési, szervezési szinten szükséges és állami feladat. Az egyedi informatikai támadások oldaláról tekintve a védelem minden üzemeltetőnek és felhasználónak érdeke és kötelessége.

A fenti összetett veszélyforrások elleni védekezés eszközei között kiemelt szerepet foglal el a szabályozás. A jogi szabályozás a támadások tiltásának, az ellenőrzések végrehajtásának és a biztonsági irányelvek meghatározásának elsődleges eszköze, de hatással van a tervezett biztonság, az elrettentés, a rendszer megerősítése, a biztonsági mentés és a reagálás kialakítására is. A szabványosítás a megelőzés vagy elfogás, a jelzések és figyelmeztetések, a rendszer megerősítése, a csoportokba osztás és feltartóztatás, a leállítás és újraengedélyezés, a biztonsági mentés, az ellenőrzések végrehajtása, a biztonsági irányelvek meghatározása és a helyreállítás területén határozza meg a követendő technikai szabályokat.

Önmagában a szabályozási tevékenység nem nyújt megfelelő védelmet, de a védelem alapjainak meghatározásához alkalmazása – így a különböző jogi vagy nem jogi szabályozások elkészítése, hozzáférhetővé tétele és betartása – elengedhetetlen.

3. A szabályozás elmélete

3.1. Jogi szabályozás

A modern normarendszerekre jellemző, hogy a hagyományos, az állampolgárok közösségi magatartását rendező jogágak mellett a XX. században megjelentek a különböző szakmákra és a szervezetekre vonatkozó normák is, így az állam működését meghatározó normák és a technikai normák.[122] A jogfilozófia vitatott területei ezek, nem tisztázott, hogy beletartoznak-e a hagyományos jog fogalmába, egyes jogbölcseleti irányzatok elutasítják ezen területek ius voltát. [123] Az informatikai biztonság szabályozása mindhárom területre kiterjedhet. Az állampolgárok közösségi magatartását szabályozó normák közé tartozhat az egyén saját tulajdonát képező információs technológiának a védelmére tett kötelező intézkedés, vagy a cybertérben való egyes viselkedési normák kriminalizálása. A védelemre kötelezés jogintézménye nem elvetendő terület, hiszen ahogy a rögzítőfékkel nem megállított gépjármű által okozott kárért is felelős a tulajdonos, úgy lehetséges lenne a (jól definiált) elégséges szintet el nem érő hálózati védelem miatt a zombigépként használt számítógéppel okozott kárért is a tulajdonos felelősségét megállapítani. A szakmai-technikai normáknak végtelen listája lehet az informatikai biztonság területén, az elégséges szintű hálózati védelem definiálásától az alkalmazandó kontrollok pontos meghatározásáig. Amellett, hogy egyes jogbölcseleti koncepciók elutasítják ezek ius voltát, már a normaalkotás nehézségei miatt is megfontolandó alkalmazásuk. A szakmai-technikai normák áradata rendkívüli mértékben megnövelné az anyagi jog terjedelmét. A jogszabályok előkészítésétől az elfogadásáig tartó időben is elavulhat az adott norma, de ha nem, akkor is rendszeresen frissíteni kellene az abban lévő információkat, valamint az idejétmúlt jogszabályi rendelkezések hatályos joganyagból való eltávolítását dereguláció útján biztosítani szükséges.[124] Ezért csupán olyan mértékben érdemes ilyen szabályozást alkotni, hogy az abban lévő tételes követelmények ne váljanak anakronisztikussá belátható időn belül. A szervezeti normák alkotásával olyan előírásokat teremtünk, amelyek jogi eljárás útján jogilag érvényesíthetetlenek, valamint ez is, a technikai normákhoz hasonlóan

[122] bővebben ld. Szabó M., 2004.
[123] Samu – Szilágyi, 1998, 113. p.
[124] a dereguláció ról ld. Kiss, 1996.

túlszabályozáshoz vezet.[125] Mi szükség van akkor az informatikai biztonság ius szabályozására, ha az rendkívül nehézkes és egyes esetekben még a jogba tartozónak sem tűnik?

Ami mindenképpen előnyeként tartható számon a jogi szabályozásnak, az az elérhető nagyobb általános biztonsági szint, amely már a normák szélesebb körű ismertségéből is következik. Pozitív gazdasági hatás is várható, egyrészt a biztonsági szektorba való nagyobb befektetés, másrészt az informatikai felhasználásban keletkező kisebb károk miatt a bevételkiesés csökkenése. Nagyobb figyelem fog vetődni erre a területre, ami az önkéntes jogkövetésre is jó hatással van. Egyértelműen a legnagyobb előnye a kötelezés egyetlen lehetősége, hiszen egyedül a jog rendelkezik kötelező erővel a társadalmi viszonyokra. Ezzel szemben hátrányként merül fel a jelentős költségigény, amely a biztonsági szektorba való átáramlás miatt keletkezik. Nagyon nehezen tisztázhatóak azok a kérdések, hogy milyen minimális biztonsági szint kerüljön kötelezően előírásra, valamint hogyan mérjük ennek a teljesülését. Külön problémaként merül fel az erre a szektorra általánosan jellemző határok eltűnése, tehát nem meghatározhatóak, illetve nem betartathatóak a jogszabályok területi hatályai.

Optimális esetben az informatikai biztonság önszabályozó lehetne. A gazdasági szervezetek a működési kockázat csökkentése és az ebből fakadó versenyelőny miatt szükséges és megtérülő befektetésnek tekintené, a non-profit szféra és az állampolgárok belátnák az egyénre és a társadalomra gyakorolt pozitív hatását és egy öngerjesztő folyamatként olyan mértékben szükségessé válna, mint a XX. században a számítógépek üzleti használata. A gazdasági recesszió, és így a kiadások csökkenése, a társadalom tagjainak alacsony szintű informáltsága, valamint az informatikai biztonsági technológiák lassú kullogása az IT általános színvonal-növekedéséhez képest együttesen lecsillapítják ezt az öngerjesztő folyamatot.

A ius szabályozás legfontosabb előnye minden más szabályozási formával szemben a kikényszerítés lehetősége. Amelyre – ha úgy ítéljük meg, hogy a társadalom számára az ebből fakadó előnyök meghaladják a hátrányokat – szükség van.

[125] Samu – Szilágyi, 1998, 113. p.

3.2. Szabványosítás

A szabványosítás nem más, mint az egységesítésre irányuló törekvés. A szabványosítás történelme – ha nem is a mai formában – a régmúltban, az ösztönös szabványosítással kezdődött, amikor kialakultak a nyelvek és számrendszerek, biztosítva az egységes kommunikációt a csoportokon belül. A mértékegységek rendszerének kialakulása volt a tudatos szabványosítás eszköze, a kereskedelem, az adószedés, fegyvergyártás tette ezt szükségessé. A mértékegységek eleinte emberi testrészek voltak, de mivel ezek egyedi biometrikus jellemzői az embernek, a szabvány etalonja az uralkodó volt, az ő testméretei határozták meg a mértékegység tényleges értékét.[126] Így például a hüvelyk (digitus, Zoll, inch) a hüvelykujj szélessége az első ízületnél (kb. 25 mm), a láb (pes, Fuss, foot) a lábfej hosszúsága a sarokcsonttól a nagylábujj végéig (kb. 0,3 m), a kisarasz a kifeszített hüvelyk- és mutatóujj végei között lévő távolság, nagyarasz a kifeszített hüvelyk- és kisujj végei között lévő távolság, a rőf (Reif) a mellkas közepétől számított kartávolság (kb. 0,78 m), és a yard a király orrhegye és kinyújtott karjának hüvelykujjhegye közötti távolság (kb. 0,91 m). Nyilvánvalóan az uralkodóváltások kisebb metrológiai katasztrófát jelenthettek, ezért felmerült az igény az egységesítésre, de erre csak az 1790-es években került sor, Talleyrand francia püspök javaslatára, a méter és prefixumainak meghatározásával (a Párizson áthaladó délkör negyedének tízmilliomod része, amely mérhető és számítható is volt), törvénybe iktatásával és az ősetalon elkészítésével.

A szervezett szabványosítás a nemzeti szabványügyi szervek megalakításával kezdődött a XX. században, amikor is először 1901-ben Londonban megalakították az Engineering Standards Committee-t. Magyarországon két évtizeddel később, 1921-ben alakították meg az ennek megfelelő Magyar Ipari Szabványügyi Intézetet. A szabványosítás legújabb generációja a nemzetközi szabványosítás, amely csak kis késéssel követte a nemzeti szabványosítás szintjét. 1906-ban alakult a Nemzetközi Elektrotechnikai Bizottság (IEC), majd 1928-ban a Nemzeti Szabványügyi Testületek Nemzetközi Szövetsége (ISA).

[126] Pleplár, 2009, p. 1.

A történelmi áttekintés után a modern szabványosítás főbb jellemzőit és kategóriáit érdemes áttekinteni. Először is a szabványosítás fogalma – amelyet természetesen szabvány határoz meg – a következő:

„Szabványosítás: olyan tevékenység, amely általános és ismételten alkalmazható megoldásokat ad fennálló vagy várható problémákra azzal a céllal, hogy a rendező hatás az adott feltételek között a legkedvezőbb legyen."[127]

A szabványosítás feladata a szabványok kidolgozása, kibocsátása, és alkalmazása. A szabványosítás eredménye fokozza a termékek, eljárások, szolgáltatások rendeltetésszerű alkalmasságát, elhárítja a kereskedelem termékekkel, szolgáltatásokkal kapcsolatos technikai akadályait és elősegíti a technológiai együttműködést. Egységesíti például a rajzjeleket, a terminológiát, a vizsgálati módszereket és a betartandó követelményeket.

A szabványosításnak több szintje van, melyek közül a legmagasabb a nemzetközi szabványosítás, ebben bármely ország illetékes szervei részt vehetnek. Nemzetközi szintű szabványügyi szervek a Nemzetközi Szabványügyi Szervezet (International Organization for Standardization, ISO), melynek hazánk 1947 óta tagja, a Nemzetközi Elektrotechnikai Bizottság (International Electrotechnical Commission, IEC) és a Nemzetközi Távközlési Unió (International Telecommunication Union, ITU), amely az ENSZ szakosított szerve.

A regionális szabványosítás olyan szabványosítás, amelyben a világ csak egy meghatározott földrajzi, politikai vagy gazdasági területéhez tartozó országok illetékes testületei vehetnek részt. Regionális szabványügyi szervek például az Európai Szabványügyi Bizottság (Comité Européen de Normalisation, CEN), Európai Elektrotechnikai Szabványügyi Bizottság (Comité Européen de Normalisation Electrotechnique, CENELEC) és az Európai Távközlési Szabványügyi Intézet (European Telecommunications Standards Institute, ETSI).

A nemzeti szabványosítás egy meghatározott ország szintjén folyó szabványosítás. Nemzeti szabványügyi szervek például a Magyar Szabványügyi Testület (MSZT), British Standards Institution (BSI), Deutsches Institut für Normung e.V. (DIN), és az American National Standards Institute (ANSI).

Vállalati szabványosításról beszélhetünk, ha a gazdasági társaság a saját szervezetén belül érvényes, általában kötelező, többnyire termékhez kapcsolódó műszaki előírást

[127] MSZ EN 45020:2007 (ISO/IEC Guide 2:2004)

készít és alkalmaz, biztosítja a nemzeti szabvány vállalati szintű végrehajtását.[128] A vállalati szabványok betartását a beszállítótól is megkövetelhetik.
Látható, hogy a szakmai kompetencia tekintetében a magasabb szinteken egy távközlési, egy elektrotechnikai és egy általános szabványügyi szerv került megalakításra. Az ilyen szervezetekben műszaki bizottságok (Technical Committee, TC) végzik az operatív munkát. Manapság a fent ismertetett hierarchikus rend mellett sok esetben összetettebb a helyzet az informatikai szabványosítás területén és sok olyan szervezet készít de facto szabványokat, amelyek eddig nem végeztek ilyet.[129]
A szabványok jelölésében először a kibocsátói jel(ek)et kell feltüntetni. Ez magyar nemzeti szabvány esetén MSZ, ISO szabvány esetén ISO, brit szabvány esetén BS, német szabvány esetén DIN, és így tovább. A szabvány rendelkezik egy azonosító jelzettel, más néven szabványszámmal, majd egy kettőspont után feltüntetésre kerül a közzététel évszáma. Ilyen módon egységesen és egyértelműen lehet hivatkozni a szabványokra. A közzétételi évszám nélkül hivatkozott szabvány a legújabb kiadást jelenti.

Jelen mű szempontjából nézve a kérdést, a non-ius szabályozási módok közül az egyik legeredményesebb forma a szabványok használata. A szabványosítás definíció szerint olyan tevékenység, amely általános és ismételten alkalmazható megoldásokat ad fennálló vagy várható problémákra azzal a céllal, hogy a rendező hatás az adott feltételek között a legkedvezőbb legyen. Esetünkben az informatikai biztonsági kihívásokra adott válaszok optimalizálása a céljuk. A számítógéprendszerek és hálózatok eredő biztonságát az egyes építőelemek közül a leggyengébbnek a biztonsága határozza meg (leggyengébb láncszem elve). A szabványok alkalmazásának a legnagyobb előnye ezen gyengeségek kiküszöbölése azáltal, hogy minden elemet egyenlő szintre hoz. a szabványok nélküli biztonság-kialakítás lehetséges, de nem megbízható, hiszen nem lehet a szabványosságot, mint formális objektív mércét használni. Az informatikai biztonság megfelelőségének biztosítása más esetekben is szükséges lehet, mint például minőségirányítási rendszer bevezetése, compliance vagy beszállítói audit esetén. Jelen esetben a szabvány fogalmát tágabb értelemben vesszük, a hangsúly a non-ius-on van, nem a szabvány formai követelményein. Formailag ugyanis a de jure szabványokat nemzeti vagy nemzetközi

[128] Forgács, 2004, p. 30.
[129] Jakobs, 2007, p. 3

szabványügyi szervezetek fogadták el és tették közzé. Szabványnak tekintjük ezeken felül a de facto szabványokat is, amelyeket általában széles körűen elismert nemzetközi civil szervezetek vagy kormányzati intézmények, szabványosítási céllal, de a szabvány formai követelményeinek teljesítése nélkül alkotnak. Ez utóbbi esetben általában verziószámozást alkalmaznak a változatok megkülönböztetésére, szemben a de jure szabványoknál alkalmazott kihirdetés évével. Szokásos eljárás, hogy a de facto szabvány egy adott változata de jure szabvánnyá válik. Ebben az esetben is szakmailag célszerűbb a de facto szabvány alkalmazása, ugyanis a de jure változatban általában nem jelennek a verziófrissítések, amelyek esetenként elég gyakoriak. Külön nehézséget okozhat az eredeti nemzetközi szabvánnyal egyébként betűre egyező nemzeti szabvány kiadása és annak változáskövetése. Erre a követésre jelent rossz példát a későbbiekben részletesen bemutatásra kerülő Common Criteria for Information Technology Security Evaluation de facto szabvány, amelynek aktuális verziója a 3.1 Revision 3 (2009. júliusi kiadás), a legfrissebb nemzetközi de jure szabvány egyik tagja az ISO/IEC 15408-2:2008, amely a 2.3-a de facto verzióból készült, a legújabb magyar szabvány pedig az MSZ ISO/IEC 15408-2:2003, ami a régen elavult 2.0 változat magyar fordítása.

A szabványok alkalmazása a magyar jog szerint nem kötelező,[130] de nyilvánvalóan érdemes. Az egyenszilárdságú informatikai biztonság kialakításának ez a legcélszerűbb módja, viszont kötelező erő hiányában a megvalósítás nem várható el. A kérdés az, hogy hogyan lehet a szabványok jó technológiai szint-követését és jól definiáltságát a kötelező erővel rendelkező jogi követelményekkel összemérni.

[130] 1995. évi XXVIII. tv. 6. § (1)

3.3. Belső szabályozás

Az informatikai biztonság helyi szinten történő szabályozása komolyabb múltra tekint vissza, mint a nemzeti szintű informatikai biztonsági tárgyú jogalkotás. Ennek nyilvánvaló oka, hogy az információs technológiák alkalmazása először szigetszerűen kezdődött úgy külföldön, mint Magyarországon is. A mainframe számítógépek beszerzését rendkívüli költségeik miatt csak meghatározott szervezetek engedhették meg maguknak, így a technológia katonai, oktatási, kormányzati és nagyvállalati alkalmazása kezdődött meg. Kiemelendő az a tény, hogy az így biztosított szolgáltatások szűk felhasználói kör számára voltak elérhetőek, a rendszerek eleinte nem voltak kapcsolatban egymással. Az összehangolt működés, a tárolt adatok biztonsága, elérhetősége nem jelent meg állami igényként. Viszont a befektetések védelmében a szervezetnek meg kellett határoznia a rendszerek használatának szabályait, valamint bizonyos mértékben a biztonsági követelményeket a rendszer és a felhasználók adatai, munkája védelmének érdekében. Ekkor az üzemeltetési jellegű szabályzatok domináltak. A gépidőt, mint szűkös erőforrást meghatározott szabályok alapján lehetett igénybe venni, a hozzáférés időpontjának előzetes lefoglalásával.

A rendszerek hálózatba szervezésével, a rendszerek olcsó tömegcikként való elérhetőségével a gépidő szinte korlátlan erőforrássá vált, az üzemeltetés – az asztali alkalmazások tekintetében – vesztett a jelentőségéből. A belső szabályozás súlypontja inkább áttevődött az információra. Általánosságban annak a jelentősége nőtt meg, hogy a rendszerekben tárolt adatokhoz az illetéktelenek (konkurencia, idegenek, arra nem jogosult munkavállalók) ne férhessenek hozzá. Ennek a szabályozásnak tehát a fókuszpontja a vállalati információs vagyon védelme. Manapság mindkét szabályzati típus létezik, külön-külön vagy komplex megvalósításban, elsősorban szervezet mérete és az informatika alkalmazásának mértéke határozza meg, melyik formában.[131]

A védelem viszont csak akkor létezik, ha a szervezet felismeri a saját információs vagyonának értékét és szükségesnek tartja annak megóvását, meg akarja-e védeni saját ügyfelei adatait. A hangsúly tehát a szervezet szándékán van, amely meghatározza azt, megtörténik-e a helyi szabályzatok elkészítése, illetve ezeket a szabályokat be fogják-e tartani és tartatni. A helyi szabályozás magában tehát nem

[131] Dósa – Polyák, 2003, p. 62.

nyújt biztosítékot a biztonság fenntartására, illetve nem érvényesíti társadalom átfogó informatikai biztonsági igényét.

Mindemellett viszont a szervezet belső szabályzatainak betartatására rendkívül hatékony kényszerítő erő és eszközrendszer állhat rendelkezésre, hiszen a munkaadó olyan tárgyalási potenciált képvisel a munkavállalóval szemben, hogy a munka esetleges elvesztésével való fenyegetéssel igen hatékonyan tudja befolyásolni a munkavállalók viselkedését. Ez a lehetőség rendkívül hatékonnyá teheti tehát a belső szabályozási rendszert, viszont a stakeholderek, a szervezet működésében érdekelt külső személyek számára az, hogy a szervezet egyoldalúan kinyilatkoztatja azt, hogy a saját belső szabályai (amelyek megismerésére általában a külső személyek számára nincsen mód) megfelelően szigorúak, valamint az abban foglaltakat betartják, nem nyújt önmagában kellő bizonyosságot. Ezt a bizonyosságot valamely hatóságtól, vagy külső auditor cégtől kaphatják meg.

Komoly előnye a belső szabályozásnak bármely külső szabályhoz képest, hogy jobban képes illeszkedni a szervezet sajátosságaihoz. Minél szűkebb területet fed le a belső szabályozás, annál pontosabban tudja előírni a kötelezettségeket. A szabályozás lehet horizontális vagy vertikális (hierarchikus) szerkezetű. Horizontális szabályzat-kialakítás esetében a szabályzatok mellérendelt viszonyban vannak egymással. Az implementáció során általában egy szabályzat-mintát alkalmaznak az azonos szabályozási területekre. Ez az általában használt szabályzat-struktúra. Hierarchikus elrendezés esetén a szabályzatok fentről lefelé kerülnek kialakításra, és nem tartalmaznak redundáns részeket. Ilyen lehet például a következő struktúra: informatikai biztonsági politika, informatikai biztonsági szabályzat, számlázási rendszerek biztonsági szabályzata, CRM védelmi szabályzat, CRMSVR-1 szerver biztonsági szabályzata. Ebben az esetben sokkal jobban meg kell tervezni a szabályozási struktúrát, viszont egyszerűbbé válik a módosítás, a felső szabályok átültetése a gyakorlatba. A legutolsó szabályzat már csak a konkrét szerverre vonatkozó részletszabályokat rögzíti.

Összességében a belső szabályozás bár rendkívül jól alkalmazható vállalati környezetben, általános kötelező erővel nem rendelkezik, így az állami szabályozás eszköze nem lehet. Viszont tekintettel arra, hogy a testre szabhatóság igényét leginkább ez a szabályozási mód biztosítja, az állami szabályozás (legyen az jogi vagy szabványokon alapuló) helyi végrehajtására ahol lehet, alkalmazni szükséges.

3.4. Az elérendő cél

Mindezen fenti szabályozási lépéseket azért kell megtennünk, hogy az informatikai rendszerek biztonsága megfelelően kialakított legyen. No de mi számít megfelelően kialakítottnak? Milyen jellemzőkkel rendelkezik egy biztonságos rendszer? Ezt a kérdést részben gyakorlati oldalról célszerű megközelíteni, létező és betartható kontrollok bemutatásával, egy magáncélú, hálózatra kötött számítógép és egy komoly informatikai infrastruktúrával rendelkező nagyvállalati rendszer elvárható biztonsági kontrolljainak ismertetésével. A fejezetben ismertetett kialakítás két tipikus eset elméleti bemutatását tűzi ki célul, bemutatva a gyakorlatban megvalósítható kontrollok széles körét és az informatikai biztonság aspektusait.

Egy otthoni felhasználó gépét és adatait viszonylag egyszerű védeni. A szoftvereszközök nagy része ingyenesen elérhető, de emellett kitűnő minőségű. A biztonság kialakításának szűk keresztmetszete leginkább a szakmai ismeretek hiánya szokott lenni. Tehát a hálózat felőli védelem kialakítható egy szoftveres tűzfal alkalmazásával. Az operációs rendszert és minden más szoftvert is szükséges a legújabb biztonsági frissítésekkel felvértezni, vírust és más rosszindulatú szoftvereket kereső alkalmazást, valamint kémprogramot (amely nem minősül rosszindulatú szoftvernek, viszont a tárolt adatokkal való visszaélést valósíthat meg) kereső alkalmazást kell használni és rendszeresen frissíteni. A géphez való hozzáférést szabályozni kell: a felhasználók külön belépési azonosítóval rendelkezzenek, jelszóval védve. A bizalmas adatokra a hozzáférést szabályozni kell a jogosultságok helyes beállításával. A fizikai hozzáférés az elzárva tartással (ajtó zárása, esetleg riasztóberendezés) oldható meg. Amennyiben a tárolt és továbbított adatok bizalmasságához és sértetlenségének biztosításához szükséges, a merevlemez részleges vagy teljes titkosítása illetve az elektronikus levelezés elektronikus aláírással, időbélyeggel való ellátása, üzenetek titkosítása válhat szükségessé.[132]

A jelentős informatikai infrastruktúrával rendelkező szervezeteknek komplex biztonsági kihívásokkal kell szembenézniük. Ez a komplexitás a technikai- és élőerős

[132] Almási–Balázs–Erdősi–Kovács–Rátai–Schvéger, 2010, p. 43.

vagyonvédelem, az információvédelem és a biztonságszervezés területeit foglalja magába.

A biztonság megvalósítása minden esetben a kockázatok és az üzleti igények alapján történik, az arányos védelemre törekedve. Itt egy nagyvállalat informatikai központjának védelmi intézkedései kerülnek áttekintésre, amelyet a kisebb szervezetek saját igényeknek megfelelően tudnak átszabni. A konkrét megvalósításra vonatkozó javaslatot minden esetben gondos mérlegelés után a kockázatelemzés figyelembevételével szakértő terjeszti elő és a menedzsment hagyja jóvá azt.

Az épületek tervezésénél nagy figyelmet kell fordítani az építészeti biztonság kialakítására, úgy, hogy a számítógépterem egy belső épületben lehetőleg földszint alatt helyezkedjen el. Az épület tervezésekor biztonsági szempontból a lehetséges fizikai behatolási pontokat, a természetes illetve mesterséges vizek elleni védekezést, a kinti forgalom által keltett rezgést, valamint az elektromágneses sugárzás elleni árnyékolást kell számításba venni. Egyes esetekben robbanóanyagok, vegyi anyagok elleni védelemről is intézkedni kell.

A cél, hogy maga az objektum körkörösen védhető legyen. Ekkor a megfelelő héjvédelemről és kültéri védelemről mind mechanikai mind elektronikai eszközök útján gondoskodni kell. Az elektromágneses sugárzás elleni védelem felszíni épületrészek esetén Faraday kalitkával történhet.[133] A földszint alatti épületrészek esetében a vasbeton szerkezet önmagában elégségesnek tekinthető.

A gépterem egyik legfontosabb erőforrása a villamos energia, amelynek megfelelő ellátásáról, illetve a szükségellátásról több szinten kell gondoskodni. Az épület betáplálása lehetőleg két, egymástól független alállomásról történjen, megfelelő védelemmel ellátva. Az energiaellátás folyamatos biztosítása érdekében szünetmentes áramforrásokat kell alkalmazni, amelyek a rövidtávú kimaradásokat áthidalják. Hosszabb távra emellett dízelgenerátorok telepíthetők.

A környezeti jellemzők megfelelő szinten tartásának jelentősége nem lebecsülendő ezen a területen. Levegő hőmérséklete és páratartalma légkondicionáló berendezésekkel tartható megfelelő szinten, amelyek kialakításakor a redundanciát és a helyettesíthetőséget is szem előtt kell tartani. A légkondicionáló gépek lehetőleg párosával kerüljenek elhelyezésre, valamint előnyös, ha az egyes egységek kiesése esetén a szomszédos berendezés is el tudja látni a kiesett egység feladatát. A hosszú

[133] Muha – Bodlaki, 2010, p. 120.

távú adattárolásnak a levegő hőmérsékletével és nedvességtartalmával való szoros kapcsolata nemcsak az online, hanem az offline (adathordozóra történő) mentések esetén is bizonyítható.[134]

Az épületnél egyébként szokásos tűzvédelmi berendezések mellett a szervertermekre szigorúbb előírások vonatkoznak a minél gyorsabb oltás és a legkisebb anyagi kár elérésére. Az érzékelés szempontjából ma már bevált technika az aspirációs füstérzékelők telepítése, amely gyorsabban és nagyobb biztonsággal érzékeli a keletkező tüzet. Ez a szerverterembe telepített több szívócsonkból, központi légbeszívásból és egy analizáló berendezésből áll. Mivel ez a megoldás rendkívül költséges, ezért a pontszerű optikai füstérzékelés továbbra is elterjedtebb technika. Az oltásnál ma már alapvető követelmény az automatikus oltórendszer alkalmazása. Az oltás általában valamely inert gáz alkalmazásával történik, de voltak próbálkozások vízköddel oltó berendezés használatára is, amely viszont nem bizonyult megfelelőnek és komoly anyagi károkat okozott. A probléma oka az volt, hogy bár a tiszta víz nem villamos vezető, a szerverterem nem megfelelő tisztasága esetén a szálló por a vízködöt vezetővé változtatta.

A szervertermek őrzése a hagyományos objektumvédelmi feladatokhoz hasonló, viszont nagyobb a jelentősége a védett körletek kialakításának és a belépési jogosultságok szerepkörök alapján történő differenciálásának. Alapvető követelmény a központi jogosultságkezelés kétfaktoros azonosítással, például proximity kártyás és PIN kódos azonosítással. A jogok kiosztása célszerűen egy központi rendszerben történik, az adott munkatárs közvetlen felettesének, az üzleti folyamat felelősének, és a szerver üzemeltetési vagy biztonsági vezetőjének együttes jóváhagyásával. Az így kiosztott jogosultságok felülvizsgálata legalább évente esedékes a kiosztott jogosultságok és az engedélyek automatikus vagy manuális összehasonlításával együtt. Az eltérések okát minden esetben ki kell vizsgálni. A jogosultságok kezelése történhet a személyügyi rendszerrel összekötött identity management (IDM) rendszerrel. Az objektumba történő belépések naplózására a hatályos szabályozás szerint hat hónapig, ideiglenes beléptetés esetén 24 óráig van lehetőség,[135] ezért szükséges az esetleges illegális behatolások, vagy jogosultság-túllépések felderítése ezen időszakon belül. A bizonyítékként felhasználható adatok tovább tárolhatóak a rendőrségi feljelentés vagy a fegyelmi eljárás lefolytatásáig. A biztonsági körletek

[134] Magyar Országos Levéltár: Levéltári állományvédelmi ajánlás. pp. 5-7.
[135] Szvmt. 32. § (3)

kialakításakor érdemes a karbantartók és a logisztika által használt területeket fizikailag elválasztani az informatikai részektől. Célszerű továbbá, ha a szerverpark is több teremben kerül elhelyezésre funkcionális illetve biztonsági szempontok alapján. Szükséges a védett körletek kamerás megfigyelése, kiemelten az átjárók és a munkavégzés során használt területek. Az itt készült felvételek megőrzésére alapvetően három napos megőrzési határidő vonatkozik.[136] A szervertermek lehetőleg ne rendelkezzenek ablakokkal illetve nem védett térbe nyíló ajtókkal. Ha mégis, ezek védelmére kitüntetett figyelmet kell fordítani, biztonsági rácsok, üvegtörés érzékelő és a védett oldalra telepített passzív infravörös érzékelők alkalmazásával.[137]

Magában a védett térben szintén szükséges a passzív infravörös érzékelők használata. Az ajtók biztonsági okokból legyenek zsilip rendszerűek, életvédelmi okból viszont a szerverterem felőli ajtó kilinccsel nyitható legyen, vagy vésznyitó kulcs legyen elhelyezve az ajtó mellett. Ennek célja az oltógázzal történő elárasztás esetén az azonnali menekülés biztosítása. Életvédelmi okból szintén szükséges az oltógáz indítását blokkoló nyomógomb elhelyezése a védett helyiségen belül.

Az informatikai rendszer védelmi igénye szintén összetett. A hálózatot kívülről el kell választani az internettől, amely általában tűzfallal történik. A tűzfalak mellett támadás-észlelő (IDS) illetve támadás-megelőző rendszert is érdemes alkalmazni.[138] Minden külső forgalomnak a tűzfalakon keresztül kell zajlania, titkosított protokollok alkalmazásával (pl. HTTPS, SFTP, SSH). A szervertermen belüli forgalom történhet titkosítás nélkül, amennyiben a hálózatból való kiszivárgás, illetve az illetéktelen hozzáférés kizárható. A szerverekre való belépés a szervertermekbe való belépéshez hasonlóan személyre kiosztott, és több szinten engedélyezett hozzáféréssel történhet. Az azonosítás három faktor útján történhet, a tudás (jelszó), a birtoklás (smart kártya, egyszer használatos jelszó) és a tulajdonság (biometrikus jellemző) alapján.[139] A szerverekre való sikertelen és sikeres belépéseket valamint különösen védendő rendszerek esetén minden tevékenységet naplózni kell, mely naplók védelmére szintén kiemelt figyelmet kell fordítani. A naplókat célszerű központi helyre gyűjteni (naplószerver), amelyhez csak a biztonsági osztály munkatársai férhetnek hozzá. A naplózási tevékenység a bizonyítékként való felhasználás és az illegális cselekmények felderítése kapcsán elengedhetetlen. A naplóállományokat a rendszer szokásos

[136] Szvmt. 31. § (2)
[137] Kerekes – Lukács, 2001, p. 156.
[138] Muha, 2010, 6.4.2.
[139] Horváth–Lukács–Tuzson–Vasvári, 2001, p. 94.

mentéséhez hasonlóan célszerű gyakran, például naponta elvégezni, és amennyiben a szervezetnek erre lehetősége van, a mentéseket másik telephelyen tárolni. Amennyiben a telephelyek közti forgalom elektronikusan történik, akkor az titkosítva illetve az átküldött és fogadott tartalmakat összehasonlítva kell elvégezni, valamint ha a szállítás fizikai módon történik, akkor az értékkíséréskor szokásos biztonsági eljárásokat kell követni.

A katasztrófahelyzetek, amelyek a szervezet infrastruktúráját szignifikáns mértékben károsítják, illetve használhatatlanná teszik, fontos rendszerek esetén kiemelt figyelmet és tervezést igényelnek. A tervezés alappillére a katasztrófaterv vagy katasztrófa helyreállítási terv (Disaster Recovery Plan, DRP), amely a katasztrófahelyzet esetén szükséges szervezési és műszaki feladatokat tartalmazza a helyreállítás részletes leírásával. Ide tartozik a helyreállításra használható rendszerek beszerzésének, konfigurálásának sorrendje, az adatok helyreállításának módszere illetve a megfelelő üzemeltető személyzet rendelkezésre bocsátása is. A katasztrófahelyzetek esetére lehetséges egy telephelyen kívüli, folyamatosan üzemben tartott és az élő rendszerrel megegyező tartalék rendszer használata, szintén telephelyen kívüli, de csak vészhelyzet esetén üzemelő rendszer használata. De akár a hardver forgalmazóval is lehet olyan szerződés kötni, amelyben a forgalmazó vállalja rövid időn belül a megfelelő hardver biztosítását. Gyakran elhanyagolt feladat a katasztrófa tesztek végrehajtása, amely a terv működőképességét és alkalmazhatóságát hivatott ellenőrizni. Ekkor célszerű, de nem feltétlenül szükséges az éles rendszerek kikapcsolása, mivel ez a nem megfelelő tervek és intézkedések esetén szolgáltatás kieséssel járhat. Gyakrabban alkalmazott módszer inkább a terv lépéseinek a munkatársakkal történő begyakorlása a tesztrendszeren. A katasztrófatervezéshez kapcsolódó másik terv az üzletmenet folytonossági terv (Business Continuity Plan, BCP), amely viszont üzleti oldalról közelíti meg a problémát, az üzleti folyamatok működésének biztosítása a célja, a katasztrófában érintett üzleti folyamatok megkerülésével. A működésfolytonosság jellemzői mérhetőek, amelynek eredménye a kockázatelemzésbe illetve a vonatkozó tervekbe beépíthető.[140]

Fontosak továbbá az adminisztratív, szervezési védelmi intézkedések, mint például az informatikai biztonságért felelős szervezeti rendszernek a szervezeti hierarchiában

[140] Beinschróth, 2006.

megfelelően magasan való elhelyezése,[141] vagy éppen az oktatás, a biztonsági tudatosságot növelő tréningek.

A fent leírt eljárások és módszerek iparági legjobb gyakorlatnak tekinthetők, azonban az azokkal szemben elvárt követelmények nagyban függnek az adott terület jellemzőitől.

A fent leírt gyakorlatok két, egymástól nagymértékben különböző élethelyzetet írtak le. A két szint közötti (vagy azok feletti) biztonsági intézkedések mértékét (pl. egy kisvállalat intézkedési körét, vagy a katonai informatikai rendszerek védelmét) sok tényező együttesen határozza meg, így többek között a végzett tevékenység jellege, kezelt adatok köre, rendelkezésre álló erőforrások és a vezetői döntés. Általános receptet adni nehéz, de egyes esetekben szükséges.

[141] Vasvári, 1997, p. 79.

4. A szabályozás gyakorlata

4.1. Jogi szabályozás

A Magyar Köztársaságban jelenleg hatályos jogszabályokban rendkívül heterogén az informatikai biztonságra vonatkozó előírások tartalma és hatálya. Nincsen olyan jogszabály, amely az információbiztonság vagy az informatikai biztonság területén keretszabályozás jelleggel minden területre kiterjedően határozna meg előírásokat. Ezzel szemben a különböző nemzetgazdasági ágakra, adatkezelésekre, egyes szakmák gyakorlására vonatkozó szabályok között gyakran található eltérő mélységű biztonsági szabályozás. A kutatás fókusza az informatikai biztonsági szabályozás volt, de ahol az szükséges volt, az információbiztonsági részek is elemzésre és kiemelésre kerültek. A hatályos magyar szabályozásban a szabályozás mélysége alapján differenciálva négy kategória alkotható: az indirekt szabályozás, az önkéntes-önszabályozott biztonság, a felületesen szabályozott és a részletesen szabályozott területek.[142] A kategorizálás szempontrendszerének kiválasztása azért a szabályozás mélységére jutott, mert ez a kodifikáció mikéntje és a szabályozás minősége szempontjából sokkal átláthatóbb, és jobban mutatja a különbségeket, mintha például a nemzetgazdasági ágak szerint végeznénk a csoportosítást, valamint jobban lehet kezelni olyan keretszabályozási szinten megvalósuló területeket, mint az adatvédelem, vagy az elektronikus közszolgáltatások.

4.1.1. Indirekt szabályozás

Első, talán ide sem tartozó kategória (hiszen az informatikai biztonságot tulajdonképpen nem szabályozza) a büntetőjog és büntetőeljárás-jog indirektnek nevezhető szabályozási kategóriája, amely a jogellenesnek tekintett és ezért pönalizált cselekményeket nevezi meg, valamint a büntetőeljárás kapcsán a bizonyítékszerzés és a bizonyíték-megőrzés eljárási szabályait fekteti le.

[142] A csoportosítás más módon is megoldható. Lehetséges lenne tovább bontani a csoportokat ellenőrzött és nem ellenőrzött területekre, valamint vannak olyan jogterületek, amelyek több csoportba is tartozhatnak. Ezek ellenére a fent ismertetett négyszintű csoportosítás átlátható, viszont nem is jelent túlzott mértékű általánosítást.

Ilyen a 2012. évi C. törvény a Büntető Törvénykönyvről (Btk.) Személyes adattal visszaélés tényállása: Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével jogtalan haszonszerzési célból vagy jelentős érdeksérelmet okozva jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy az adatok biztonságát szolgáló intézkedést elmulasztja, vétséget követ el, és egy évig terjedő szabadságvesztéssel büntetendő.[143]

A tényállást a 2003. évi II. törvény iktatta a régi Btk.-ba,[144] az adatvédelmi biztos 2001. április 25-i ajánlását alapul véve. A normaszövegben alaptényállási elem a jelentős érdeksérelem, amely viszont rendkívül sok értelmezési problémát eredményez. Meglehetősen kevés olyan bírósági ítélet lelhető fel, amelyben kizárólag jelen szakaszra hivatkozva hoztak döntést. Ilyen például az Orosházi Városi Bíróság 4/5-H-BJ-2008-1 sz. ügye, melyben 10.491 természetes személy különleges adatainak a jogellenes kezelése valósult meg. Az ügyben az első fokú elmarasztaló ítélet után a Szegedi Ítélőtábla, mint harmadfokú bíróság Bhar.II.199/2009/13. számon felmentő ítéletet hozott.

Levéltitok megsértése: Aki másnak közlést tartalmazó zárt küldeményét megsemmisíti, a tartalmának megismerése végett felbontja, megszerzi, vagy ilyen célból illetéktelen személynek átadja, illetve elektronikus hírközlő hálózat útján másnak továbbított közleményt kifürkész, ha súlyosabb bűncselekmény nem valósul meg, vétség miatt elzárással büntetendő.[145]

A kifürkészés történhet a PSTN vagy VoIP telefon lehallgatásával, hálózati forgalom figyelésével és rögzítésével (sniffing), a számítógépen rootkit, kémprogram elhelyezésével, vagy bármely más módon. A bűncselekmény kísérlete megállapítható akkor, ha ilyen eszközök telepítésre kerültek a telefonvonalra, hálózati eszközökre vagy számítógépre. Alanya bárki lehet.

Alanya bárki lehet, de titkos információgyűjtés esetében a jogosulatlan titkos információgyűjtés vagy adatszerzés bűntette (Btk. 307. §) valósul meg.

A magántitok megsértése: Aki a foglalkozásánál vagy közmegbízatásánál fogva tudomására jutott magántitkot alapos ok nélkül felfedi, vétség miatt elzárással büntetendő.[146] A tényállás a régi Btk azonos nevű tényállásával szemben már csak a foglalkozás vagy közmegbízatás esetén bünteti az elkövetőt.A Btk. tiltott adatszerzés

[143] Btk. 219. § (1)
[144] 1978. évi IV. tv.
[145] Btk. 224. § (1)
[146] Btk. 223. § (1)

és az információs rendszer elleni bűncselekmények c. XLIII. fejezete határozza meg elsődlegesen az általunk indirekt szabályozásnak hívott terület informatikai biztonsági szabályait.

A tiltott adatszerzés (Btk. 422. §) tényállása szerint aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából más lakását, egyéb helyiségét vagy az azokhoz tartozó bekerített helyet titokban átkutatja, más lakásában, egyéb helyiségében vagy az azokhoz tartozó bekerített helyen történteket technikai eszköz alkalmazásával megfigyeli vagy rögzíti, más közlést tartalmazó zárt küldeményét felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti, elektronikus hírközlő hálózat – ideértve az információs rendszert is – útján másnak továbbított vagy azon tárolt adatot kifürkész, és az észlelteket technikai eszközzel rögzíti, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő. A tiltott adatszerzésre igaz a fent a levéltitok megsértésénél leírt gyakorlati elkövetési módok leírása, kiegészítve azzal, hogy a kamerás vagy lehallgató készülékes megfigyelés is ide tartozik.

Az információs rendszer vagy adat megsértése (Btk. 423. §) tényállása alapján aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad,[147] vétség miatt két évig terjedő szabadságvesztéssel büntetendő. A bűncselekmény tárgya a számítástechnikai rendszerek normális (nem akadályoztatott) működéséhez és a rendszerekben tárolt, feldolgozott, továbbított adatok bizalmasságához, megbízhatóságához, és hitelességéhez fűződő érdek. A törvény három, egymástól elkülönülő esetet sorol be a bűncselekmény elkövetési magatartásai közé. Az első esetben a behatoló, aki – a fogalmi alapvetésben maghatározottak szerint – egy white-hat hacker is lehet, az egyébként létező, a rendszer védelmét szolgáló intézkedést kijátssza, tehát az elkövető a rendszerben nem azonosított felhasználó (unauthenticated user) vagy azonosított felhasználóként a kiosztott jogosultságait lépi túl (authenticated user, unauthorized access). Ezekben az esetekben mindössze a behatolással, illetve a jogosultságok túllépésével tényállásszerűvé válik a cselekmény, de csak abban az esetben, ha további bekezdésekben meghatározott adatmódosítás nem történik meg. A védelmi intézkedés hatékonysága nem képezi szabályozás tárgyát, így bármilyen védelmi

[147] Btk. 423. § (1) a)

intézkedéshez hasonló, szakmailag kifogásolható eljárás alkalmazása esetén megvalósul a cselekmény. Gyakorlati példa a WiFi hálózatok használata és az azzal kapcsolatos szokások. A mai mobil eszközök kiemelten támogatják a védelemmel nem ellátott WiFi hálózatok használatát, amelyek általában ingyenes hozzáférési pontokat jelentenek, de lehet akár olyan otthoni hálózat is, amelyet a tulajdonosa nem titkosított. Ez utóbbi hálózat használata a Btk. 423. szakasza alapján nem büntethető. Negatív példaként említhető az egyébként e tényállás keretében sem pönalizált cselekmény büntetése, amikor a Szegedi Városi Bíróság 2007 novemberében a nem védett WiFi hálózat használatát lopás szabálysértéseként (9 forint kárértékre) büntetni rendelte. Hozzátartozik a WiFi használatával kapcsolatos szokásokhoz, hogy a rádiós routerek[148] gyártói alapértelmezésben bekapcsolt és nem védett WiFi kapcsolattal szállítják termékeiket, hogy a felhasználó minél egyszerűbben használatba tudja azt venni.

Aki az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz, [149] bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

Itt a törvény a b) pontban a rendszer működését, a c) pontban az adatok integritását védi. Ebben az esetben nem tényállási elem a károkozás illetve a jogtalan haszonszerzés, így az alapvetésben meghatározott white hat hackerek által végrehajtott adatmódosítás is büntetendő ez alapján.

A büntetés bűntett miatt egy évtől öt évig terjedő szabadságvesztés, ha az (1) bekezdés b)-c) pontjában meghatározott bűncselekmény jelentős számú információs rendszert érint.[150] A jogalkotó súlyosbító körülményként értékeli, ha mindezt több rendszer ellen követik el.

A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekményt közérdekű üzem ellen követik el.[151] Itt viszont átfedés tapasztalható a közérdekű üzem működésének megzavarása (Btk. 323. §) tényállásával.

Az információs rendszer felhasználásával elkövetett csalás (Btk. 375. §) tényállás szerint aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb

[148] Az otthoni internetmegosztást is biztosító számítógép-hálózati eszközök
[149] Btk. 423. § (1) b)-c)
[150] Btk. 423. § (2)
[151] Btk. 423. § (3)

művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő. Ez utóbbi tényállás hasonlít a régi Btk. 300/C. § (3) tényállásához, még korábban pedig a számítógépes csaláshoz tényállásához. Itt a jogtalan haszonszerzés végett történő végrehajtást rendeli büntetni a törvény. A kár bekövetkezése tényállási elem, viszont nem a számítógéprendszerben okozott kárt, hanem a cselekmény által okozott kárt jelenti.

Az információs rendszer védelmét biztosító technikai intézkedés kijátszása:[152] Aki a 375. vagy a 423. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez, vagy forgalomba hoz, illetve jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja, vétség miatt két évig terjedő szabadságvesztéssel büntetendő. A tényállás hasonló a régi Btk 300/E szakaszában meghatározott tényálláshoz. A 300/E szakaszt a 300/C szakasszal egy időben, a 2001. évi CXXI. törvény iktatta be a Büntető Törvénykönyvbe, a számítástechnikai bűnözésről szóló budapesti egyezmény alapján. A jelen bekezdés esetén az elkövetés tárgya az a hacker-eszköz vagy illegális hozzáférést biztosító jelszó. Az illegális hozzáférést biztosító jelszó (korábban azonosító adat, ami pontosabb kifejezés) alapvetően a külső eszköz (pl. vírus, rootkit) segítségével meggyengített rendszerben létrehozott a behatolás célját szolgáló felhasználói fiók adatait jelenti, de beleértendő a visszaélés céljára átadott jogszerű fiók jelszava is. Az elkövetési magatartás magában foglalja a készítést, megszerzést, forgalomba hozatalt, hozzáférhetővé tételt, illetve a kereskedést. A bűncselekmény a magatartási elemek bármelyike esetén befejezett, nem szükséges az eszközt vagy azonosítót alkalmazni, amely már a 423. §-ban foglaltak szerint büntetendő. A jogalkalmazásban jelentős problémát jelenthet, hogy az ilyen eszközök a saját rendszerünk jogszerű biztonsági vizsgálatára is használhatóak, így az ilyen hacker-eszközök birtoklása – ebben az értelmezésben – pönalizálja a lelkiismeretes rendszergazdát is. Külön nehézséget jelent, hogy „a jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja” pont alapján a vétséget minden informatikai

[152] Btk. 424. §

biztonsági képzést tartó oktató elköveti. A szakasz alkalmazására esetjog nem található.

Egyes esetekben lehet informatikai biztonsági vonzata a (szerzői jogi) védelmet biztosító műszaki intézkedés kijátszása (Btk. 386. §), a (szerzői jogi) jogkezelési adat meghamisítása (Btk. 387. §), a készpénz-helyettesítő fizetési eszköz hamisítása (Btk. 392. §), a készpénz-helyettesítő fizetési eszközzel visszaélés (Btk. 393. §) készpénz-helyettesítő fizetési eszköz hamisításának elősegítése (Btk. 394. §) a közérdekű üzem működésének megzavarása (Btk. 323. §), a terrorcselekmény (Btk. 314. §), a haditechnikai termékkel vagy szolgáltatással visszaélés (Btk. 329. §), és a kettős felhasználású termékkel visszaélés (Btk. 330. §) tényállásoknak is. Viszont ezek informatikai biztonságra közvetlenül gyakorolt hatása minimális, a számítógép az elkövetés eszközeként jelenik meg.

Az indirekt szabályozási kategóriába sorolhatók továbbá a büntető eljárásjog tekintetében a büntetőeljárásról szóló 1998. évi XIX. törvény Számítástechnikai rendszer útján rögzített adatok megőrzésére kötelezés című bekezdésben foglaltak:

A megőrzésre kötelezés a bűncselekmény felderítése és a bizonyítás érdekében a számítástechnikai rendszer útján rögzített adat birtokosának, feldolgozójának, illetőleg kezelőjének a számítástechnikai rendszer útján rögzített meghatározott adat feletti rendelkezési jogának ideiglenes korlátozása.[153]

A megőrzésre kötelezést a bíró, az ügyész vagy a nyomozó hatóság is elrendelheti, határozat formájában. A megőrzésre kötelezett a határozat megismerésétől biztosítani köteles a határozatban meghatározott adatokat változatlanul megőrizni, biztonságosan tárolni. A megőrzés mellett az illetéktelen hozzáférés megakadályozása is feladata a kötelezettnek. Az ilyen módon tárolt adathoz csak a kötelezést elrendelő szerv férhet hozzá, a tárolt adatról még csak tájékoztatást sem adhat a kötelezett harmadik személy számára. Az adatot a kötelezettnek az eredeti helyén és formájában kell tárolnia. Az alapvető szabályoktól való eltérést írásban engedélyezheti az elrendelő. A megőrzésre kötelezett adatot az integritás védelemében a hatóság elláthatja elektronikus aláírással. Az integritás vagy a biztonság sérülését a kötelezettnek haladéktalanul jelentenie kell a hatóság számára. A megőrzésre kötelezés célja, hogy időt biztosítson az adatok átvizsgálására a hatóság számára, amely ez után dönthet az adatok lefoglalásáról. A

[153] Be. 158/A. § (1)

megőrzésre kötelezés legfeljebb három hónapig tart, de mind az adat lefoglalása, mind a büntetőeljárás megszüntetése a kötelezés megszűnését eredményezi a Be. szerint. Gyakorlati nehézséget jelent, hogy a megőrzésre kötelezés nem jelen olyan biztonságot és bizonyítékminőséget, mintha a nyomozóhatóság lefoglalná az adatokat vagy a számítógépet.

A fentiekből egyértelműen látszik, hogy az idézett indirekt informatikai szabályok nem tartalmaznak előírást vagy magyarázatot arra, hogy például mit jelent a „számítástechnikai rendszer védelmét szolgáló intézkedés", tehát ennek jelentését más jogszabályokban kell keresnünk. Másrészről viszont azért tartozik mégis bele az informatikai szabályozásba a terület, mivel a szankcionálás is egy módja a terület szabályozásának.

Vannak továbbá titkok, amelyek jogi védelmet élveznek, de csak a fentiekhez hasonló, indirekt módon: üzleti titok (Ptk. 2:47. §), banktitok (2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról 160. §), értékpapírtitok (2001. évi CXX. törvény 369. §), pénztártitok (1993. évi XCVI. törvény 40/A. §, 1997. évi LXXXII. törvény 78. §), adótitok (2003. évi XCII. törvény 53. §), vámtitok (2003. évi CXXVI. törvény 16. §). Ezek lehetnek informatikai rendszerben vagy bármely egyéb módon tárolt adatok, ezek közül az informatikai rendszerben tároltak esetében tekinthetjük a jogi védelmet indirekt informatikai biztonsági szabálynak.

4.1.2. Önkéntes-önszabályozott biztonság

Másik területként az önkéntes illetve önszabályozott biztonságot nevezhetjük meg, amelybe tartoznak például az informatikai és kommunikációs szektor önszabályozási lépései. Úgy, mint ahogy az élelmiszeripari cégek (legyen az malom vagy kínai gyorsétterem) törekednek az utóbbi időkben a HACCP minősítés megszerzésére, az informatikával vagy távközléssel foglalkozó cégek egy része is törekszik nemzetközi szabványoknak megfelelően üzemeltetni informatikai rendszereit, szolgáltatásit. Ez a vevők részéről felmerülő igény, vagy bizalomnövelő PR-eszköz is lehet. Mindemellett, hogy az ilyen irányú fejlesztéseknek jelentős költségvonzata van a biztonság közgazdasági értelemben pozitív externália, így a ráfordításokat jelentős mértékben meghaladja az a megtakarítás, amit a biztonsági incidensek kiküszöbölése jelent.[154]

[154] Camp -- Wolfram, 2004. 20. p.

Az IKT szektor informatikai biztonsági önszabályozása elsősorban az ISO 27001 szabványnak való megfelelésre törekvés illetve a megfelelés tanúsítása. Emellett az informatikai folyamatokra is vonatkozó ISO 9001 szerinti minőségirányítási rendszer bevezetése, vagy az ITIL követése szintén javíthat az informatikai biztonság szabályozottságán. Az ilyen irányú törekvés általában kinyilvánításra kerül. Tekintettel arra, hogy az ISO 27001 szerint lehetséges tanúsítani, a partnerek felé a megfelelőség bemutatására a legkézenfekvőbb a harmadik fél általi tanúsítás. Ez a jelentős költségvonzata miatt illetve a viszonylag magas követelményekből adódóan a piaci szektor elég kis hányadát fedi le, de ettől függetlenül világviszonylatban is előkelő helyen áll Magyarország a tanúsítások számát tekintve.[155]

A gazdasági szervezetek és állami szervek túlnyomó része rendelkezik informatikai jellegű belső szabályozással (pl. informatikai biztonsági szabályzat, informatikai üzemeltetési szabályzat, adatvédelmi szabályzat), amelyek szintén célszerűen valamely nemzetközi szabvány figyelembevételével készülnek. Már csak azért is, hiszen a szabályzatok teljes körűségéhez leginkább valamely jól bevált normarendszer alkalmazásával közelíthetünk. A témában iránymutatást ad az ITB 8. sz. ajánlásának 4. fejezete: Útmutató az informatikai biztonsági szabályzat (IBSZ) elkészítéséhez.

4.1.3. Felületesen szabályozott biztonság

Következő kategóriaként a felületesen szabályozott területet határolhatjuk el a többitől, ahol a jogi szabályok előírásra kerültek, de azokat a jogalkotó nem részletezte, ebből kifolyólag a jogalkalmazó és a betartásra kötelezett nehezen tudja értelmezni azokat, az önkéntes jogkövetés így nagymértékben megnehezül. Ezt a problémát fokozza az a tény, hogy a jogalkotó polgári jogi terminológiát használva fogalmazta meg a jogszabályban foglalt követelményeket, tehát gyakran használja az „elvárható legjobb", vagy az „elégséges" fordulatokat. A jogszabály kötelezettje az esetek többségében nem rendelkezik – vagy nem is rendelkezhet – azokkal a szakmai ismeretekkel, hogy ezeket a követelményeket közvetlenül értelmezni tudja. Mindemellett pedig a követelményeknek komoly jogi vonzatai vannak, beleértve a büntetőjogi felelősséget és a polgári jogi úton érvényesíthető kártérítést. A

[155] A kérdésről bővebben ld. a szabványalkalmazás gyakorlata c. fejezetet.

következőkben példákkal kerülnek bemutatásra a felületesen szabályozott kategóriába sorolt jogszabályok.

4.1.3.1. Adatvédelem

A felületesen szabályozott területek közül első számú iskolapélda az adatvédelem. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban információs törvény vagy Infotv.) látszólag egy szakaszban foglalkozik az adatvédelem informatikai biztonsági aspektusával, felületesen meghatározva az adatkezelő és az adatfeldolgozó által a tevékenységük során betartani rendelt szabályokat.

A személyes adat „az érintettel (bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy) kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés."[156]

Személyes adat az az adat, amely az adatvédelmi jog tárgyát képezi. A személyes adat az adat fogalmának valódi részhalmaza, független a hordozótól, a megjelenési formától, kódolástól, kizárólag a meghatározott természetes személlyel való kapcsolat határozza meg.

Az adatvédelem „az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok valamilyen szintű, előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségeire vonatkozik"[157]

Az adatvédelem a magánszféra védelmének egyik módja, amely jogi szabályozásban nyilvánul meg.[158] Az adatvédelem, illetve a személyes adatok védelméhez fűződő jog nem akadályozza az adatalanyt a saját személyes adatainak felhasználásában, így az önrendelkezési jog. Az adatvédelem célja az angolszász nyelvterületen használt – a magyar magánszféránál tágabb értelmű privacy védelme. A privacy jelentésébe beletartozik,[159] hogy az adatalany meghatározhatja, hogy mely adataik juthatnak

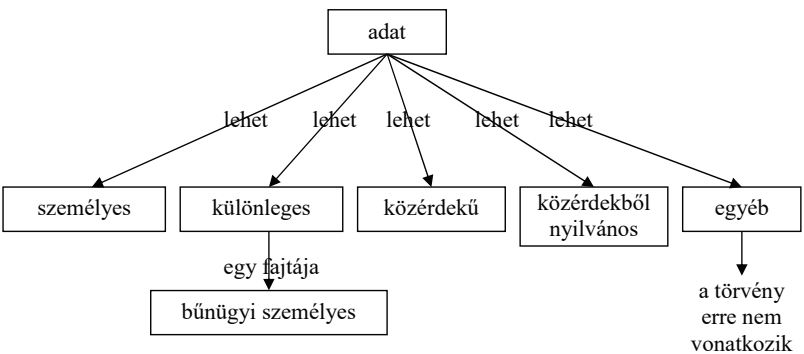
[156] Infotv. 3. §
[157] ITB 8. sz. ajánlás, 1994, p. 132.
[158] Jóri, 2005. p. 11.
[159] Schoemant idézi Jóri, loc. cit.

mások tudomására, meghatározhatja, hogy személyiségének mely jellemzőihez ki férhet hozzá és egyben egy állapotot is jelöl, amelyben az adatalany személyes adataihoz, gondolataihoz és testéhez való hozzáférés korlátozott.

Az adatbiztonság szűkebb értelmezésében technikai adatvédelem, tehát a jogi úton történő magánszféra-védelem műszaki-technikai megvalósítása. Mivel az adatvédelem létrejötte, illetve a jogterület ilyen szintű kifejlődése a technikai fejlettség – az információs és kommunikációs technológiák robbanásszerű fejlődésének – eredménye,[160] ezért az adatbiztonság szerepe az adatvédelemben rendkívül hangsúlyos. Az adatbiztonság nélküli adatvédelem nem rendelkezik több gyakorlati jelentőséggel, mint a jogfilozófia. Annak oka, hogy a technika mégis ennyire[161] eltörpül a jogi kérdések mellett, egyszerűen csak az, hogy az adatvédelmet a szakma alapvetően jogterületnek, nem interdiszciplináris tudományterületnek tekinti.

Az adatbiztonság emellett visszahat az adatvédelemre és technikai úton elősegítheti a személyes adatok védelmét, a privátszférát erősítő technológiák (privacy enhancing technologies, PET) útján.[162]

Az Infotv. fogalmi rendszere szerint az 1. ábrán látható adatfajták határozhatóak meg. Részletes meghatározásuk az Infotv. 3 §-ban, illetve az 1. sz. függelék 4. pontjában található.



1. ábra: Koncepciós térkép az adatokról az Infotv. szerint

[160] Majtényi, 2006. p. 23.
[161] ld. felületes szabályozásról szóló fejezet
[162] bővebben ld. Fischer-Hübner, 2001.

Az információs törvényben az adatbiztonság címszónál a következőket határozta meg a jogalkotó: „Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az e törvény és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét. Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek."[163] Jóri András részletes elemzését[164] felhasználva kijelenthető, hogy az adatbiztonság, és így az informatikai biztonság meghatározott szegmense az adatvédelmi jog szabályozásának tárgyát képezi. Az első bekezdés megerősíti az adatvédelem és az adatbiztonság kapcsolatát, előírja a szűkebb értelemben vett adatvédelmi követelmények informatikai rendszerekben való érvényesülését és így az adatminőséggel és a célhoz kötöttséggel kapcsolatos követelmények alkalmazását. Előírja más jogszabályok, így szektorális adatvédelmi jogszabályok (pl. 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről, 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról) és titokvédelmi jogszabályok (pl. 2009. évi CLV. törvény a minősített adat védelméről, 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól) alkalmazását. Ezek más mélységben is lehetnek szabályozva, mint az adatvédelem területe és egyes területek később kifejtésre is kerülnek.

Az egészségügyi adatok kezelése különösen informatikai rendszerekben új dimenzióját teremtheti meg a visszaéléseknek. Világszerte különös figyelem kíséri ezért ezt a területet, mind a jogalkotás (pl. US Health Insurance Portability and Accountability Act, HIPAA), mind a szabványosítás területén (pl. ISO 27799, ISO 22857).[165] Felismerte ezt a magyar jogalkotó is, ezért is született külön ágazati szabályozás az egészségügyi adatkezelésre (Eüak.), de a gyakorlati megvalósítása a

[163] Infotv. 7. § (1)-(2)
[164] Jóri, 2005, p. 258.
[165] Kokolakis – Lambrinoudakis, 2005, p. 49.

magasabb szintű védelmi igénynek hagy kívánni valót maga után.[166] Az egészségügyi adatkezelés kapcsán az adatvédelmi biztos gyakorlata is bővelkedik a jogesetekben.[167] Az elvárt intézkedések és eljárásrendek nem kerültek meghatározásra. A lehetséges intézkedések és eljárások sem ismertek, de alapvetően helyesen járhat el a kötelezett, ha informatikai biztonsági szabványok alapján alakítja ki a technikai adatvédelmet. Problémát jelenthet viszont, hogy a szabványban meghatározott követelmények túlzottan magas, a veszélyekkel szemben nem arányos mértékű védelmet írnak elő. Célszerű a védelem kialakításakor az arányosságra törekvés, ellenkező esetben a védelmi költségek feleslegesen magasak lesznek. Az Infotv. utal az arányos védelem kialakításának szükségességére: „Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek".[168] Az arányos védelem elérésének a legcélszerűbb módja a formális kockázatelemzés végrehajtása. A konkrét adatkezelési, adatfeldolgozási rendszert illetve folyamatot fenyegető veszélyekről és azok bekövetkezéséről ilyen módon kockázatelemezést célszerű készíteni, ami az információs törvényben nem közvetlen előírás, viszont a részletesen szabályozott területen találkozhatunk vele és a szakmában is elvárhatónak tekinthetjük.

„Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen."[169] Itt a „megfelelő" intézkedés azt emeli ki, hogy az intézkedésnek a potenciális veszély elhárítása szempontjából adekvátnak kell lennie. Így például a logikai hozzáférés-védelem szempontjából nem elégséges a fizikai beléptetést biztosító vagyonőr alkalmazása. A jogalkotó példálózóan sorolja fel a kockázati elemeket, amelyek általánosságban megfelelnek az iparági kockázat-csoportosításoknak. Az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás pedig visszautal a könyvünk elején található elektronikus írásbeliség problémái közül az offline megőrzés, a hosszú távú elérhetőség problémáira. Az adatkezelőnek ilyen módon az Infotv-ben meghatározott kötelessége az elérhetőség biztosítása. A kockázatok új

[166] Alexin, 2010, p. 104.
[167] bővebben lásd Trócsányi, 2007.
[168] Infotv. 7. § (6)
[169] Infotv. 7. § (3)

dimenziója nyílik meg az informatika vívmányainak használata esetén, ahogy az a kockázatokról szóló fejezetben korábban kifejtésre került. A jogalkotó helyesen felismeri ezt és hangsúlyozza ilyen módon, hogy az asztalfiókot és a notebookot fenyegető veszélyek nem azonos mértékűek, de ezen felül mást nem tesz, a vonatkozó szabályokat nem részletezi.

Az új törvény megszűntette az adatvédelmi biztos intézményét és helyette hozzá hasonló jogkörökkel, de bírságoló hatósági jelleggel létrehozta a Nemzeti Adatvédelmi és Információszabadság Hatóságot (NAIH). Az adatvédelmi hatóság a vizsgálata során a vizsgált adatkezelő kezelésében levő, a vizsgált üggyel összefüggésbe hozható összes iratba betekinthet, illetve azokról másolatot kérhet, az adatkezelést megismerheti, az adatkezelés helyszínéül szolgáló helyiségbe beléphet, az adatkezelőtől, és annak munkatársától írásbeli és szóbeli felvilágosítást kérhet, a vizsgált üggyel összefüggésbe hozható bármely szervezettől vagy személytől írásbeli felvilágosítást kérhet, és az adatkezelő hatóság felügyeleti szervének vezetőjét vizsgálat lefolytatására kérheti fel.[170] Az adatvédelmi biztos a vizsgálatai során nem alkalmazott egységesen elvárt követelményrendszert és vizsgálati módszertant, viszont vizsgálta egyes olyan, nyilvánvalóan elvárható követelmények teljesülését, amelyek alapvetően befolyásolják az adatok informatikai biztonságát, ámbár nem teljes körűen. Így vizsgálta a számítástechnikai rendszerekben történő jogosultságkezelést, naplózást,[171] és a fizikai biztonsági intézkedések meglétét megyei ellenőrzések keretében.[172] A NAIH a vizsgálatai során szintén nem alkalmaz formális módszertant.

Az adatvédelmi intézkedések megvalósulásának mértéke ellenőrizhető, aminek módja a német modell szerint (Roßnagel alapján) külső független vállalkozás által, a brit modell szerint belső audit vagy külső vállalkozás vagy a hatóság által történhet.[173] Még az adatvédelem szempontjából kevéssé szabályozott Egyesült Államokban is van piaci kereslet az adatvédelmi auditra.[174] Jelenleg Magyarországon informálisan a külső vállalkozás általi audit végrehajtható lenne, bár ez nem jellemző. Az Infotv. a korábbi adatvédelmi törvénnyel szemben viszont lehetővé teszi az önkéntes külső

[170] Infotv. 54. § (1)
[171] Az adatvédelmi biztos beszámolója 1997. 755/H/1997 és 756/H/1997 ügyek
[172] Az adatvédelmi biztos beszámolója 1999. 194/H/1999, 196/H/1999, 435/H/1999 ügyek
[173] Balogh – Jóri – Polyák, 2002, p. 325.
[174] DeJarnette – Morin, 2010.

hatósági auditot[175]. A hatósági önkéntes audit függetlensége kérdéses, bár a NAIH igyekszik hangsúlyozni a függetlenséget. Az auditnál viszont a törvény előírja[176] a módszertan meghatározását, az a NAIH honlapján 2013.01.02-óta elérhető „Szakmai szempontok az adatvédelmi audit végzéséhez" címmel.[177] A módszertan érdekessége, hogy az adatkezelési gyakorlatot egyáltalán nem vizsgálja, csak a dokumentációt.[178] Visszás az audit szabályozásánál, hogy az audit eredménye nem köti a hatóságot,[179] tehát egy pozitív eredménnyel záruló, akár ötmillió forintba kerülő audit után is következhet egy tízmillió forintos hatósági bírság, valamint az audit során tapasztalt jogellenes adatkezelés esetén köteles a hatóság büntető feljelentést tenni.[180] Mindezek alapján a NAIH audit nem versenyképes egy olyan piaci szolgáltatással, ahol az auditot végző garanciát vállal az auditban foglalt megállapításaiért és vállalja az ebből fakadó anyagi kötelezettségeket is (átvállalja a bírságot).
Mindezek ellenére a fenti szabályozások nem határozzák meg a betartandó informatikai biztonsági kontrollok mértékét, azok betartási módját, vagy eljárásrendjét. A törvényhez végrehajtási rendelet, egyéb ajánlás nem kapcsolódik. Érdemi biztonsági intézkedésre vonatkozó bírósági esetjog nem lelhető fel.

4.1.3.2. Elektronikus hírközlés

Az elektronikus hírközlési iparág szabályozása, így különösen a távközlési szolgáltatók és internet szolgáltatókra vonatkozó informatikai biztonsági követelmények magas szintű meghatározása az elektronikus hírközlésről szóló 2003. évi C. törvény (Eht.) alapján történik. A szolgáltató - szükség szerint más szolgáltatókkal közösen - műszaki és szervezési intézkedésekkel köteles gondoskodni a nyújtott szolgáltatás biztonságának védelméről.[181]A szakasz fókuszpontjában a szolgáltatók közötti javasolt biztonsági célú együttműködés áll. Ez leginkább hozzáférés-védelmi elemeket foglal magában. A műszaki és szervezési intézkedéseknek - figyelembe véve a legjobb gyakorlatot és a meghozandó intézkedések költségeit - a szolgáltatónál, a szolgáltatás nyújtásával kapcsolatban

[175] Infotv. 38. § (4) h)
[176] Infotv. 38. § (4) g)
[177] http://naih.hu/files/AdatvedelmiAuditSzakmaiSzempontokVegleges.pdf [2013.08.12]
[178] ibid. p. 4.
[179] Infotv. 69. § (5)
[180] Infotv. 70. § (1)
[181] Eht. 156. § (1)

jelentkező kockázatoknak megfelelő biztonsági szintet kell nyújtaniuk.[182]Ez a követelmény kockázatbecslést és annak megfelelő biztonsági intézkedéseket javasol. Az IKT terület fontossága és érzékenysége ellenére a követelmények felületesek és általában rendeleti szintűek.

Az elektronikus hírközlési szolgáltatókra vonatkozó informatikai biztonsági tételes követelményeket az elektronikus hírközlési szolgáltatás minőségének az előfizetők és felhasználók védelmével összefüggő követelményeiről, valamint a díjazás hitelességéről szóló 13/2011. (XII. 27.) NMHH rendeletben találjuk meg.

Az adatgyűjtéshez használt eszközöknek és módszereknek a számlázási időszakokra vonatkozóan biztosítaniuk kell hogy forgalommérési adat csak a szolgáltatás igénybevétele esetén keletkezhet, az adatállomány nem lehet utólag szerkeszthető, valamint biztosítani kell, hogy a forgalommérési adatok a feldolgozó rendszerhez történő továbbítás során ne sérülhessenek, és ne lehessen azokhoz jogosulatlanul hozzáférni, függetlenül attól, hogy a forgalommérési adatok informatikai hálózaton vagy egyéb adathordozón kerülnek továbbításra.[183] Biztonsági követelményként fogalmazódik meg, hogy a forgalommérési adat (CDR) a keletkezés helyén (például mobiltelefon bázisállomás) automatikusan kerüljön létrehozásra és azt ne lehessen szerkeszteni, jó esetben technikailag kizárt legyen a szerkesztés lehetősége, rosszabb esetben logikai és adminisztratív védelmi intézkedéseket kell foganatosítani. Biztonsági kérdés az, hogy a forgalommérési adatok hol keletkeznek, és milyen utat járnak be az informatikai rendszerben, illetve ezen a teljes útvonalon milyen módon lehet azokhoz hozzáférni, szerkeszteni azokat. Az adathordozón való továbbítás ma már csak az átviteli utak leállása estén követendő vészforgatókönyvben fordul elő.

A számlázási rendszer és a hálózat védettségére vonatkozó követelmény hogy a feldolgozó helyiségekbe való belépést nyilvántartani és ellenőrizni kell elektronikus beléptetéssel vagy a személyzet által vezetett belépési napló vezetésével valamint egyéb adminisztratív intézkedésekkel a feldolgozás bemenő adataihoz, a feldolgozó folyamathoz és a keletkezett adatokhoz a hozzáférés biztonságát és a hozzáférések nyilvántartását biztosítani kell.[184] Feldolgozó helyiség gyakorlatilag minden olyan terület, ahol hívásadatgyűjtés-, illetve feldolgozás történik, vagy a kész adatokhoz való hozzáférés lehetséges. Ezeknél mindenképpen a fizikai biztonság körébe tartozó

[182] Eht. 156. § (2)
[183] 229/2008. (IX. 12.) Korm. r. 8. § (4)
[184] 229/2008. (IX. 12.) Korm. r. 8. § (6)

hozzáférés-ellenőrzésnek kell működnie. A feldolgozás bemenő adataihoz való hozzáférés nyilvántartását általában az informatikai rendszerben történő naplózás valósítja meg.

Az elektronikus hírközlő hálózat akkor minősül védettnek, ha a szolgáltató fizikai és adminisztratív intézkedésekkel biztosítja, hogy az elektronikus hírközlő hálózathoz, vagy az elektronikus hírközlési szolgáltatáshoz, vagy az előfizető által közölt információhoz jogosulatlanok számára a hozzáférés csak különösen nehéz feltételekkel - így különösen látható rongálással járó, vagy más feltűnő módon, vagy tiltott eszközök, módszerek igénybevételével lehetséges.[185] A fizikai védettség kialakítása az előfizetői hurok esetében a vezetékes telefóniában jelent nagy kihívást. Zárt szerelődobozokat kell alkalmazni, valamint a kábel fizikai védettségét is biztosítani szükséges.

Jelenleg a fenti követelmények teljesülését két módon lehet ellenőrizni: kijelölt tanúsító szervezet által kiadott megfelelőségi tanúsítvánnyal vagy a szervezet által kiállított megfelelőségi nyilatkozattal. Ez utóbbi nem nyújt érdemi biztosítékot az ügyfelek és a hatóság számára és mivel ilyen módon hátrányt jelenthet, kevéssé alkalmazzák. A szabályok be nem tartása hazánkban nehezen szankcionálható, szemben például Németországgal, ahol szabálysértési tényállás valósul meg az adatbiztonsági követelmények be nem tartásakor.[186]

Látható, hogy az elektronikus hírközlési terület szabályozása is csak felületesen szabályozott: a törtvényi szintű szabályozás hasonló az Infotv-hez, a rendeleti szintű pedig elsősorban a szolgáltatás minőségére koncentrál, kevés informatikai biztonsági előírást tartalmaz. Az iparági bevált gyakorlat kikényszerítése a tanúsító és a hatóság feladatává válik. Erre vonatkozó előírás viszont már nincs a joganyagban.

4.1.3.3. Számvitel

A számvitelben, így a társaságok gazdasági nyilvántartásaiban, könyveiben foglalt adatoknak a valóságban megtalálhatónak, bizonyíthatónak kell lennie, szögezi le a valódiság számviteli elve.[187] Magyarországon ebből csak levezethető, nyugatabbra explicite kinyilvánított, hogy az informatikai rendszerekben tárolt adatok biztonsága nélkül ez nem teljesülne. A számviteli információk informatikai biztonságára a

[185] Loc. cit.
[186] Polyák, 2004, p. 15.
[187] 2000. évi C. törvény a számvitelről 15. § (3)

Magyar Nemzeti Könyvvizsgálati Standardok[188] 2017. október 25-i verziójának 315-ös témaszámú „A lényeges hibás állítás kockázatának azonosítása és felmérése a gazdálkodó egység és környezetének megismerésén keresztül" c. standard nem tartalmaz részletes előírásokat, de kijelenti, hogy a könyvvizsgálói ellenőrzésnek a részét képezi az informatikai biztonsági ellenőrzés is.

A könyvvizsgálónak meg kell ismernie, hogy a gazdálkodó hogyan reagált az informatikai kockázatokra. Az informatika alkalmazása befolyásolja azt, hogy az ellenőrzési tevékenységeket hogyan valósítják meg. A könyvvizsgáló fontolóra veszi, hogy a gazdálkodó megfelelően reagált-e az informatikai kockázatokra, hatékony általános informatikai és alkalmazásellenőrzések létrehozásával. A könyvvizsgáló szempontjából az informatikai rendszerek feletti ellenőrzések akkor hatékonyak, ha azok megőrzik a rendszerek által feldolgozott információk sértetlenségét és az adatok biztonságát.

Az általános informatikai ellenőrzések az alábbiak ellenőrzését foglalják magukban:

- adatközpont és hálózati működés
- rendszerszoftverek beszerzése, módosítása és karbantartása
- programváltoztatás
- hozzáférés-biztonság
- alkalmazásrendszerek beszerzése, fejlesztése és karbantartása

Ezeket általában azért valósítják meg, hogy kezeljék a kockázatokat.[189]

A fenti standardok alkalmazása kötelező, ezt a Magyar Könyvvizsgálói Kamaráról, a könyvvizsgálói tevékenységről, valamint a könyvvizsgálói közfelügyeletről szóló 2007. évi LXXV. törvény 23. § írja elő.[190]

Az IT ellenőrzési tevékenységhez tartozó iránymutatásképpen a Magyar Könyvvizsgálói Kamara égisze alatt módszertani útmutató készült az „Informatikai audit a könyvvizsgálatban" címmel,[191] amelyben az ellenőrzést a könyvvizsgáló kompetenciájának tekintik. A könyvvizsgáló, amennyiben a szükséges ismeretekkel és tapasztalattal nem rendelkezik, informatikai szakértőt vehet igénybe a könyvvizsgálatról szóló dokumentumok előkészítéséhez. A dokumentum – ahogy címe is mutatja – csak módszertani útmutató, az elégséges biztonsági szintet semmi

[188] http://www.mkvk.hu/tudastar/standardok [2015. 10. 01.]
[189] Magyar Nemzeti Könyvvizsgálati Standardok 315. standard A96. bek.
[190] A kamarai tag könyvvizsgáló köteles a) feladatait lelkiismeretesen, esküjének megfelelően, a jogszabályok és a 4. § (5) bekezdésének b) pontja szerinti standardok alapján, körültekintően ellátni
[191] Németh–Rácz–Sőtér–Virág–Bakos–Varga, 2008.

nem írja elő. Példaként látható itt a hozzáférés-védelemre vonatkozó módszertani leírás egy részlete:

„A feladatkörök szétválasztását támogató politikák és a munkaköri leírások kialakítása után létre kell hozni ezen politikák betartását biztosító kontrollokat is.

Mind a fizikai, mind a logikai hozzáférés kontrollok egyik fő célja, hogy a feladatkörök szétválasztására vonatkozó szervezeti szabályozásokat biztosítsa. Ezen kontrollok az egyes szervezeti egységek és az egyes személyek munkájához kapcsolódó felelősségi körökhöz kapcsolódnak. Például a logikai hozzáférés kontrollok megakadályozhatják, hogy egy programozó élő alkalmazásokhoz, vagy azok adataihoz férjen hozzá. Hasonló módon a fizikai hozzáférés kontrollok (pl. beléptető-kártya) megakadályozhatják, hogy illetéktelen felhasználók belépjenek a számítógépközpontba."[192]

A fentiek ellenőrzéséhez a módszertani útmutató 9. melléklete hozzáférés kontrollok és ezek ellenőrzése címmel ellenőrzőlistát állít fel, melynek első négy eleme a következő:

„1. Létrehozták-e az osztályozási szisztémát és a hozzá tartozó kritérium rendszert, és ezt az erőforrás tulajdonosok tudomására hozták-e?

2. Az erőforrásokat azok tulajdonosai kockázat értékelés alapján osztályozták?

3. Dokumentált-e az osztályozás, és elfogadta-e a felsőbb vezetés?

4. Felülvizsgálják-e rendszeres időközönként az osztályozást?"[193]

A fentiekből látható, hogy a kérdéslista valóban segíthet az audit végrehajtásában, de nincs meghatározva a mögötte álló előírás vagy bírálati szempontrendszer. Ezzel az informatikai szakellenőrzési feladatokhoz esetleg kevésbé értő könyvvizsgáló nem tud hatékony vizsgálatot végezni. Ez egy viszonylag gyenge kontroll, a gyakorlatban az informatikai biztonsági ellenőrzés kis hangsúlyt kap. Ennek ellenére külföldön, elsősorban az Amerikai Egyesült Államokban ez a legszigorúbb informatikai biztonsági kontroll, amelyet elsősorban a Sarbanes-Oxley Act (SOX) követel meg a befektetők védelmében.[194]

[192] Ibid. 4.2.2.1.3.3.6 pont
[193] Ibid. 9. mell. 1-4.
[194] Damianides, 2005, p. 81.

4.1.4. Részletesen szabályozott biztonság

A részletesen szabályozott kategóriába olyan jogszabályok tartoznak, amelyek részletesen előírt technikai szabályokat tartalmaznak. Emellett rendszeres és mélyreható ellenőrzést is írhatnak elő. Ezekben az esetekben mindig van egy olyan szervezet, amelyet kijelölnek ezekre az ellenőrzésekre és általában minden szükséges eszközzel és kompetenciával rendelkeznek. Ilyen például a pénzügyi szervezetek és a hitelesítés-szolgáltatók szektora.

4.1.4.1. Pénzügyi szolgáltatók

A pénzügyi szektorban több jogszabállyal találkozhatunk, amelyek alapvetően ugyanazokat az informatikai biztonsági szabályokat tartalmazzák, ezek a következők:

- 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról (új Hpt.)
- 1996. évi CXII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról (régi Hpt.)
- 1997. évi LXXXII. törvény a magánnyugdíjról és a magánnyugdíjpénztárakról (Mpt.)
- 1993. évi XCVI. törvény az Önkéntes Kölcsönös Biztosító Pénztárakról (Öpt.)
- 2001. évi CXX. törvény a tőkepiacról (Tpt.)
- 2007. évi CXVII. törvény a foglalkoztatói nyugdíjról és intézményeiről[195]
- 2007. évi CXXXVIII. törvény a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól
- 2014. évi LXXXVIII. törvény a biztosítási tevékenységről (Bit.)

Az előírt szabályok erősen a COBIT de facto szabványon alapulnak. Mindezeket kiegészíti a PSZÁF módszertani útmutatója,[196] amely tovább finomítja az egyébként is részletesnek mondható törvényi szabályozást. Az ellenőrzéssel a Pénzügyi Szervezetek Állami Felügyelete lett megbízva, ahol az informatikai biztonsági ellenőrzést az Informatikai Ellenőrzési Főosztály végzi. A főosztály munkatársai mind rendelkeznek a szükséges nemzetközi vizsgákkal és ellenőrzési gyakorlattal. Az

[195] 18. §-a az Öpt. 40/C. §-ában meghatározott szabályokat írja elő
[196] A Pénzügyi Szervezetek Állami Felügyeletének 1/2007. számú módszertani útmutatója a pénzügyi szervezetek informatikai rendszerének védelméről

ellenőrzések rendszeresek és átfogóak, a pénzügyi szervezeteket egyszerre minden területen vizsgálják. Tekintve hogy a tevékenységük engedélyhez kötött, a szabályok betartása kikényszeríthető.

A régi Hpt. 2004 évi novellája előtt a terület szabályozása hasonló volt az információs törvényhez. A hitelintézetekről és a pénzügyi vállalkozásokról szóló 1996. évi CXII. törvény (régi Hpt.) 13. §-a a biztonság személyi és anyagi követelményeiről csak azt írta elő hogy a pénzügyi szolgáltatási tevékenység csak a tevékenység végzésére alkalmas technikai, informatikai, műszaki, biztonsági felszereltség, helyiség, a működési kockázatok csökkentését szolgáló információs és ellenőrzési rendszer, valamint a rendkívüli helyzetek kezelésére vonatkozó terv megléte esetén kezdhető meg, illetve folytatható.

Sokkal részletesebb és pontosabb követelményeket vezetett be a befektetők és a betétesek fokozott védelmével kapcsolatos egyes törvények módosításáról szóló 2004. évi XXII. törvény. A jogszabály szinte azonos követelményeket épített be a régi Hpt. 13/C §-ba, az Mpt. 77/A §-ba, az Öpt. 40/C §-ba és az Tpt. 101/A §-ba.[197] A biztosítótársaságokról szóló törvény bár hasonló előírásokat tartalmazott, mint a szektor többi régi jogszabálya, az nem került megváltoztatásra. Ennek ellenére a PSZÁF javasolja a többi jogszabályban megfogalmazott szabályok betartását a biztosítótársaságoknak is.[198] A vonatkozó előírásokat a régi Hpt-ben foglaltak szerint tekintjük át.

A régi Hpt. szerint a pénzügyi intézménynek ki kell alakítania a pénzügyi, kiegészítő pénzügyi szolgáltatási tevékenységének ellátásához használt informatikai rendszer biztonságával kapcsolatos szabályozási rendszerét és gondoskodnia kell az informatikai rendszer kockázatokkal arányos védelméről. A szabályozási rendszerben ki kell térni az információtechnológiával szemben támasztott követelményekre, a használatából adódó biztonsági kockázatok felmérésére és kezelésére a tervezés, a beszerzés, az üzemeltetés és az ellenőrzés területén.[199]

A szabályozási rezsim úgy hivatkozik a szabályozási rendszerre, mint informatikai biztonsági politikára, informatikai biztonsági jogszabályokra és IT üzemeltetési szabályokra. Ezek a szabályozások előírandóak és rendszeresen felülvizsgálandóak

[197] Tpt. 101/A §-át később hatályon kívül helyezték.
[198] op. cit. p. 2.
[199] régi Hpt. 13/C. § (1)

(pl. éves rendszerességgel) a felső vezetés által. Minden felhasználónak ismernie kell a vonatkozó szabályozást.

A pénzügyi intézmény köteles az informatikai rendszer biztonsági kockázatelemzését szükség szerint, de legalább kétévente felülvizsgálni és aktualizálni.[200] A szervezetnek be kell vezetnie egy kockázatbecslési eljárást és rendszeresen kell végeznie kockázatbecslést. Abban az esetben, ha a vállalkozás kiszervezett szolgáltatásokkal is rendelkezik, akkor a kockázatbecslésnek a kiszervezett szolgáltatásokra is ki kell terjednie.

Az informatika alkalmazásából fakadó biztonsági kockázatok figyelembevételével meg kell határozni a szervezeti és működési rendeket, a felelősségi, nyilvántartási és tájékoztatási szabályokat, a folyamatba épített ellenőrzési követelményeket és szabályokat.[201] Világosan meg kell határozni a szerepeket, a feladatokat és a felelősségeket, átfedés nélkül. A munkavállalók hatásköre feleljen meg a szerepnek és a felelősségnek. Az informatikai szolgáltatások felelőseként kerüljön kinevezésre külön informatikai igazgató (Chief Information Officer, CIO), vagy ahhoz hasonló. A jogszabályban meghatározott folyamatba integrált, nem pedig attól elkülönülő belső ellenőrzési rendszer elvét más területeken, így folyamatba épített előzetes és utólagos vezetői ellenőrzés (FEUVE) néven a közigazgatásban is alkalmazzák.

A pénzügyi intézménynek ki kell dolgoznia az informatikai rendszerének biztonságos működtetését felügyelő informatikai ellenőrző rendszert és azt folyamatosan működtetnie kell.[202] Ez a követelmény nem számítógép rendszerre vagy alkalmazásra vonatkozik, hanem a belső audit rendszer hatékony eszközrendszerére. Ezt a kontrollrendszert meghatározott gyakorisággal felül kell vizsgálni, tevékenységét és hatékonyságát mérni kell. Ezen kontrollok naprakészen tartását több szabvány is előírja.

A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább a rendszer legfontosabb elemeinek (eszközök, folyamatok, személyek) egyértelmű és visszakereshető azonosításáról.[203] A kockázatbecslés alapján a szervezetnek a konfigurációról legalább jegyzéket kell vezetnie, de jobb esetben teljes konfiguráció-menedzsment is

[200] régi Hpt. 13/C. § (2)
[201] régi Hpt. 13/C. § (3)
[202] régi Hpt. 13/C. § (4)
[203] régi Hpt. 13/C. § (5)

kialakításra kerülhet. Az aktuális állapot és minden korábbi állapot elérhető kell, hogy legyen mindenkor.

Gondoskodni kell az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljeskörűségét biztosító ellenőrzésekről, eljárásokról.[204] Elengedhetetlenül szükséges a megfelelő védelmi eljárások kialakítása és a kialakítás megfelelőségének, hatékonyságának ellenőrzése. Ennek elsődleges módja a belső audit, de szükséges lehet a külső audit kialakítása.

Gondoskadni kell a rendszer szabályozott, ellenőrizhető és rendszeresen ellenőrzött felhasználói adminisztrációjáról (hozzáférési szintek, egyedi jogosultságok, engedélyezésük, felelősségi körök, hozzáférés naplózás, rendkívüli események).[205] Az azonosítási és hozzáférés szabályozási eljárások megalkotása szükséges az adatbázisok felelősségi szabályainak kialakítása mellett. A beosztásban vagy a felelősségben való változtatásnak azonnal meg kell jelennie a hozzáférési szintekben. A feladatra identity management (IDM) rendszer is használható.

Gondoskodni kell olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza és alkalmas e naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, illetve lehetőséget nyújt a nem rendszeres események kezelésére.[206] Naplóelemző alkalmazások használata javasolt, de legalábbis a naplók mentése, biztonságos archiválása és kézi elemzése a legalapvetőbb követelmény. A naplóelemzés kialakításnak két módja az olcsóbb, de pontatlanabb automatikus, tanuló, illetve a költségesebb, de pontos kézileg egyedileg beállított naplóelemző rendszer.

Gondoskodni kell a távadatátvitel bizalmasságáról, sértetlenségéről és hitelességéről.[207] A kommunikációra biztonságos csatornákat vagy protokollokat kell használni, úgymint HTTPS, SSL, SSH, SFTP.[208]

Gondoskodni kell az adathordozók szabályozott és biztonságos kezeléséről.[209] Az adattárolásra használt hordozóeszközöknek, mint a DVD-nek vagy mágnesszalagoknak biztonságos tárolása szükséges. Védeni kell azokat a természeti csapásoktól, a műszaki követelmények hiánya miatt fellépő hibáktól, az

[204] Loc. cit.
[205] Loc. cit.
[206] Loc. cit.
[207] Loc. cit.
[208] Virasztó Tamás, 2004, p. 133.
[209] régi Hpt. 13/C. § (5)

elektromágneses zavaroktól, műszaki megbízhatósági problémáktól és a szándékos károkozástól.

Gondoskodni kell a rendszer biztonsági kockázattal arányos vírusvédelméről.[210] A kártékony programok elleni védelem a szervereken, az asztali számítógépeken és a mobil eszközökön is szükséges.

A pénzügyi intézménynek tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez meg kell valósítania a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket és rendelkeznie kell legalább az informatikai rendszerének működtetésére vonatkozó utasításokkal és előírásokkal, valamint a fejlesztésre vonatkozó tervekkel.[211] Minden rendszer és alkalmazás kötelezendően dokumentálandó. A szolgáltatásokra szolgáltatási szint megállapodást (SLA) kell készíteni.

Az intézménynek rendelkeznie kell minden olyan dokumentációval, amely az üzleti tevékenységet közvetlenül vagy közvetve támogató informatikai rendszerek folyamatos és biztonságos működését - még a szállító, illetőleg a rendszerfejlesztő tevékenységének megszűnése után is – biztosítja.[212] A rendelkezésre állási terv hatókörén belül minden fenti törvényt figyelembe kell venni.

Az intézménynek rendelkeznie kell a szolgáltatások ellátásához szükséges informatikai rendszerrel, valamint a szolgáltatások folytonosságát biztosító tartalék berendezésekkel, illetve e berendezések hiányában az ezeket helyettesítő egyéb – a tevékenységek, illetve szolgáltatások folytonosságát biztosító – megoldásokkal.[213] Ehhez a követelményhez elegendő a katasztrófa-helyreállítási terv (Disaster Recovery Plan, DRP) és az üzletmenet folytonossági terv (Business Continuity Plan, DCP) elkészítése és betartatása.

Az intézménynek rendelkeznie kell olyan informatikai rendszerrel, amely lehetővé teszi az alkalmazási környezet biztonságos elkülönítését a fejlesztési és tesztelési környezettől, valamint a megfelelő változáskövetés és változáskezelés fenntartását.[214] Az éles és a teszt rendszerek elválasztása beleértve a személyzetet is általános iparági igény.[215]

---

[210] régi Hpt. 13/C. § (5)
[211] régi Hpt. 13/C. § (6)
[212] Loc. cit.
[213] Loc. cit.
[214] Loc. cit.
[215]MSZ ISO/IEC 27002:2011 10.1.3. és 10.1.4. p. 60.

Az intézménynek rendelkeznie kell az informatikai rendszer szoftver elemeiről (alkalmazások, adatok, operációs rendszer és környezetük) olyan biztonsági mentésekkel és mentési renddel (mentések típusa, módja, visszatöltési és helyreállítási tesztek, eljárási rend), amelyek az adott rendszer helyreállíthatóságát a rendszer által nyújtott szolgáltatás kritikus helyreállítási idején belül lehetővé teszik. Ezen mentéseket kockázati szempontból elkülönítetten és tűzbiztos módon kell tárolni, valamint gondoskodni kell a mentések forrásrendszerrel azonos szintű hozzáférés védelméről.[216] A rendszer biztonsági mentési funkcióit emellett időszakonként tesztelni is szükséges lenne. A biztonsági mentés lefolytatása általában nem jelent gondot, ha mégis, az nagyobb problémát jelez az üzemeltetők felé. A mentések egy nagy szervezetnél általában el is készülnek. Az igazi nehézséget a visszatöltés jelenti, ez utóbbi szokott gyakran el is maradni, viszont erről nem szól az előírás.

Az intézménynek rendelkeznie kell a jogszabályban meghatározott nyilvántartás ismételt előhívására alkalmas adattároló rendszerrel, amely biztosítja, hogy az archivált anyagokat a jogszabályokban meghatározott ideig, de legalább öt évig, bármikor visszakereshetően, helyreállíthatóan megőrizzék.[217]

Az adatok visszaállítása több esetben feltétlenül szükséges, pl. adózási, terrorellenes és adatvédelmi okokból. Erre egy komplex megoldást kell bevezetni, például megfelelően biztonságos mágnesszalagos tárolási egység és ehhez tartozó eljárásrend bevezetésével.

Az intézménynek rendelkeznie kell a szolgáltatásai folyamatosságát akadályozó rendkívüli események kezelésére szolgáló tervvel.[218] Ehhez a követelményhez a korábban említett katasztrófaterv és üzletmenet-folytonossági terv elegendő.

A pénzügyi intézménynél mindenkor rendelkezésre kell állnia az általa fejlesztett, megrendelésére készített informatikai rendszer felépítésének és működtetésének az ellenőrzéséhez szükséges rendszerleírásoknak és modelleknek és az általa fejlesztett, megrendelésére készített informatikai rendszernél az adatok szintaktikai szabályainak, az adatok tárolási szerkezetének.[219]Jelen esetben a „mindenkor" a pénzügyi szolgáltatás megkezdésétől folyamatosan 24 órában, a hét minden napján értendő. Minden hardver- és szoftver dokumentációnak elérhetőnek és naprakésznek kell lennie. Minden olyan helyen elérhetőnek kell lennie, ahol hibaelhárításhoz vagy más

[216] régi Hpt. 13/C. § (6)
[217] Loc. cit.
[218] Loc. cit.
[219] régi Hpt. 13/C. § (7)

feladathoz a hozzáférés szükséges. A szoftverdokumentációknak, illetve az adatbázisra vonatkozó dokumentációknak adatszerkezet-leírással kell rendelkeznie.

Mindenkor rendelkezésre kell állnia az informatikai rendszer elemei biztonsági osztályokba sorolási rendszerének, az adatokhoz történő hozzáférési rend meghatározásának, és az adatgazda valamint a rendszergazda kijelölését tartalmazó okiratnak.[220] A számítógépeknek, a rendszereknek és hálózatoknak az adatok érzékenysége alapján osztályozásra kell kerülniük. Ezeket a szabályokat dokumentálni kell. A hozzáférés rendjének írott formában elérhetőnek kell lennie. A kijelölési okiratoknak a személyi felelősség megállapíthatóság érdekében rendelkezésre kell állnia.

Mindenkor rendelkezésre kell állnia az alkalmazott szoftver eszközök jogtisztaságát bizonyító szerződéseknek és az informatikai rendszert alkotó ügyviteli, üzleti szoftvereszközök teljes körű és naprakész nyilvántartásának.[221] A szoftver licenceknek és a számláknak adójogi követelmények miatt is rendelkezésre kell állniuk. Úgyszintén szükséges a szoftver leltár elkészítése ami szintén felmerül az adóhatóság részéről is igényként.

A szoftvereknek együttesen alkalmasnak kell lenni legalább a működéshez szükséges és jogszabályban előírt adatok nyilvántartására, valamit a pénz és az értékpapírok biztonságos nyilvántartására.[222] Ez a bekezdés meghatározza a szoftverekre vonatkozó minimum követelményeket. Ahogy a fenti követelmények is előírták, több területen is szükséges a hosszú távú megőrzés. A szoftvernek szintén meg kell felelnie ennek a követelménynek. Tekintettel arra, hogy ma már a pénz nagy része számlapénz formájában létezik (nem jelenik meg fizikai valójában), az értékpapírok pedig dematerializált formában, ezért ezek megbízható rögzítése, nyilvántartása, a visszaélések és a hibák megakadályozása alapvető igény a pénzügyi rendszerek megbízhatósága érdekében.

A szoftvereknek alkalmasnak kell lenni a pénzügyi intézmény tevékenységével összefüggő országos informatikai rendszerekhez történő közvetlen vagy közvetett csatlakozásra, ideértve a pénzforgalmi számlák cégbíróság felé történő bejelentését is.[223]

---

[220] Loc. cit.
[221] Loc. cit.
[222] régi Hpt. 13/C. § (8)
[223] Loc. cit.

A legtöbb B2G[224] igazgatási adat (adóbevallás, statisztikai adatok) számítógéprendszereken keresztül kerül továbbításra. Az ezekhez szükséges interfészek kialakítása és üzemben tartása a szervezet felelőssége.

A szoftvereknek együttesen alkalmasnak kell lenni a tárolt adatok ellenőrzéséhez való felhasználására, a biztonsági kockázattal arányos logikai védelemre és a sérthetetlenség védelmére.[225] Az adat javításához és önjavításához szükséges beépített kontrollok rendkívül jelentősek ilyen nagyméretű adatbázisok esetén. A tárolt adatok értéke és érzékenysége alapján kell meghatározni a szükséges logikai védelem szintjét.

A pénzügyi intézménynek belső szabályzatában meg kell határoznia az egyes munkakörök betöltéséhez szükséges informatikai ismeretet.[226]Más területeken a szükséges informatikai ismeretek szintjét munkaköri leírások tartalmazzák, de pénzügyi szervezetek esetén szabályzatot kell alkotni ezek meghatározására.

A fenti nagy tömegű követelményből látható, hogy a pénzügyi szektorra jóval több törvényi szintű követelmény vonatkozik, mint más üzleti szektorokra. Ennek oka a terület fontossága. Az állampolgárok túlnyomó része megtakarításait ezen szervezetekben tartja. Bármely pénzügyi szervezetben bekövetkező hiba drasztikusan csökkenti a pénzügyi szektorba és a pénzügyi rendszerbe fektetett bizalmat és jelentős anyagi veszteségeket okoz.

Ezzel szemben érdekes változás, hogy a korábbi részletes követelményrendszert az új Hpt.-ben a jogalkotó leváltotta „az általános információbiztonsági zártsági követelmények" teljesítésének és a „jogosulatlan hozzáférést, valamint észrevétlen módosítást" megakadályozó intézkedések bevezetésének igényére.[227] Ezzel ismét jogbizonytalanságot szülve és előírva egy olyan tanúsítást, amelynek a követelményrendszere nem ismert.[228] Ezzel a terület visszalépett a felületesen szabályozott kategóriába.

[224] business-to-government
[225] régi Hpt. 13/C. § (8)
[226] régi Hpt. 13/C. § (9)
[227] új Hpt. 67/A. § (1)
[228] új Hpt. 67/A. § (2)

4.1.4.2. Közigazgatás szervei

Amellett, hogy ebben a kategóriában részletekbe menő szabályozást találhatunk, amelyek esetenként technikai mélységben tartalmaznak az informatikai biztonságra vonatkozó szabályokat, bizonyos esetekben jóval enyhébb mögöttük az ellenőrzési követelmény, az előírás, a kompetencia és a szervezetrendszer, mint például a pénzügyi szervezetek esetében. Ilyenek a közigazgatásra vonatkozó előírások, amelyek a jogfilozófiai szempontból egyébként sem feltétlenül minősülnek jogi normáknak. Ezen jogszabályok számossága növekvő tendenciát mutat az utóbbi öt évben. Jelen fejezetben kronológiai sorrendben mutatjuk be a szakterület szabályozását.

Az elektronikus közszolgáltatásról szóló törvényt megelőzően (2009. június 29-e előtt) a területet érintő informatikai biztonsági kérdést érintő törvényi szintű szabályozás nem volt. Kormányrendeleti szinten a következő jogszabályok vonatkoztak a területre:[229]

- 195/2005. (IX. 22.) Korm. rendelet az elektronikus ügyintézést lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról
- 84/2007. (IV. 25.) Korm. rendelet a Központi Elektronikus Szolgáltató Rendszer és a kapcsolódó rendszerek biztonsági követelményeiről
- 193/2005. (IX. 22.) Korm. rendelet az elektronikus ügyintézés részletes szabályairól
- 194/2005. (IX. 22.) Korm. rendelet a közigazgatási hatósági eljárásban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítésszolgáltatókra vonatkozó követelményekről
- 182/2007. (VII. 10.) Korm. rendelet a központi elektronikus szolgáltató rendszerről

[229] Dedinszky, 2008. p. 4.

2012 áprilisáig a közigazgatási informatikára vonatkozó legfontosabb jogszabály az elektronikus közszolgáltatásról szóló 2009. évi LX. törvény (Ekszt.) volt, amely már alapelvi szinten kiemelte a biztonságot, mint követelményt.

Az elektronikus közszolgáltatást nyújtó szervezetek a szolgáltatás nyújtása során biztosítják a közérdekű, illetve közérdekből nyilvános adatok megismerhetőségét és a személyes, illetve a jogszabályokban védeni rendelt egyéb adatok védelmét.[230]A szolgáltatás nyújtása tekintetében kiemelt figyelmet kell az információs jogok érvényesülésére és a minősített adatok, üzleti tikok és más védendő adatcsoportok védelmére fordítani.

A szolgáltatást nyújtók biztosítják az informatikai biztonságot, ideértve az elektronikus irat sértetlenségének, megváltoztathatatlanságának biztosítását, az erre szolgáló elektronikus aláírási technológia alkalmazhatóságát.[231] A jogalkotó utal az elektronikus aláírási technológia alkalmazásának és a vonatkozó biztonsági követelmények betartásának fontosságára. Az Eat. szerinti elektronikus aláírás alkalmazása nagymértékben segítheti az adatintegritás fenntartását. Diszkrepancia tapasztalható viszont a törvény ezen alapelve az alkalmazási gyakorlat között: elég csak arra gondolnunk, hogy az Ügyfélkapuban mennyi lehetőségünk van elektronikus aláírásunk használatára.

A szolgáltatást nyújtók biztosítják az informatikai rendszerekkel való együttműködés követelményeinek érvényesülését és az üzemeltetés folytonosságát.[232] Az interoperabilitásnak, tehát a különböző rendszerek közötti együttműködésnek különleges jelentősége van a kormányzati informatikában, hiszen a rendszerek szigetszerűen kerültek kifejlesztésre, míg az idők folyamán egyre inkább nőtt az igény az integrációra. A szigetszerű kifejlesztés máig érezteti negatív hatását az együttműködés terén. Az üzemeltetés folytonossága, mint az informatikai biztonság egyik fő követelménye – beleértve a katasztrófa- és üzletmenet-folytonossági tervezést – jelentős szerepet kap a nagy állami adatbázisok esetében, ahol az adatok elvesztése katasztrofális lehet.

A központi rendszeren továbbított adatokból személyi profil (felhasználói szokások elemzése, közvetlen személyes adatokhoz és érdemi ügyadatokhoz való hozzáférés) nem képezhető. Ennek betartását a központi rendszer üzemeltetője technikai

[230] Ekszt. 4. § (1) Az elektronikus közszolgáltatás alapelvei
[231] Loc. cit.
[232] Loc. cit.

megoldással biztosítja.[233]Az utóbbi években az egyik legnagyobb adatvédelmi kihívást jelentő személyiségprofil-készítést az Ekszt. deklaráltan tiltja alapelvei között. A rendszerben ezt technikailag biztosítani kell (pl. Privacy by Design technológiák útján).

Az elektronikus közszolgáltatás részeként igénybe vett távolról történő ügyintézéshez szükséges azonosítás előfeltétele a személyes megjelenéssel, vagy azzal jogszabály szerint egyenértékű módon végzett előzetes regisztráció, és az azonosításra alkalmas adatnak az adat kezelésére feljogosított által történő nyilvántartásba vétele.[234] Tekintettel arra, hogy az elektronikus közszolgáltatások jelentős része közigazgatási eljárás, így a Ket. alapján személyazonosításhoz szükséges kötni azt. A bekezdésben említett személyes megjelenés okmányirodákban történhet, ezzel egyenértékű azonosítás pedig az elektronikus aláírással történő regisztráció.

Az azonosítás történhet: [235]

- az azonosítás alanya által ismert egyedi információ alapján (tudás alapú azonosítás),
- az azonosítás alanya által birtokolt egyedi eszköz, információhordozó alapján (birtoklás alapú azonosítás),
- az azonosítás alanyára kizárólagosan jellemző tulajdonság alapján (tulajdonság alapú azonosítás),
- ezek kombinációjával.

A tudás alapú azonosítás tipikus esete a jelszó, a birtoklás alapúé egy token vagy intelligens kártyán lévő tanúsítvány, míg a tulajdonság alapúé az ujj- vagy tenyérlenyomat. A különböző faktorok együttes alkalmazása biztonságot növelő tényező.

Az azonosítás magas, közepes, vagy alacsony biztonsági szinten történhet. Ezen biztonsági szintek közül az alkalmazandó szintet elektronikus közszolgáltatás esetén jogszabály határozza meg. Ha jogszabály eltérően nem rendelkezik, a távolról történő ügyintézéshez alacsony biztonsági szintű azonosítás szükséges.[236] Az ügyfelek hozzáférése a rendszerhez tehát alacsony biztonsági szinten történik, így kizárólag egyfaktoros, tudás alapú azonosítás (jelszó megadása) szükséges. A követelmény

[233] Ekszt. 4. § (2)
[234] Ekszt. 12. § (1)
[235] Ekszt. 12. § (2)
[236] Ekszt. 12. § (3), (4)

tehát mindamellett, hogy többféle azonosítást lehetővé tesz, csak a legalacsonyabb, – majdhogynem nem is elégséges – szintet teszi kötelezővé az ügyfelek számára.

A magas biztonsági szintű azonosítás legalább két egymástól független azonosítási módszer alkalmazásával történik, amelyek közül egynek tudás alapú azonosításnak kell lennie. A magas biztonsági fokozatú azonosítás során a birtoklás alapú azonosításhoz kizárólag a külön jogszabályban meghatározott feltételeknek megfelelő biztonságos tároló eszköz és a külön jogszabály szerint azon arra feljogosított szolgáltató által elhelyezett és közigazgatási használatra alkalmas azonosítási célú tanúsítvány használható fel.[237]A magas biztonsági szintű azonosítás célszerűen egy biztonságos aláírás-létrehozó eszközre[238] telepített közigazgatási autentikációs tanúsítvánnyal valósítható meg, amely a tudásalapú azonosítással kiegészítve megfelelő biztonságot nyújt.

A közepes biztonsági szintű azonosítás elkülönült azonosítási módszerként az ügyfélkapu jelszó-nyilvántartásán alapuló azonosítással, valamint egy egyszer használatos azonosítóval történő azonosítással történik. Az interneten történő ügyintézéshez rendelkezésre bocsátott egyszer használatos azonosítót az internettől független kommunikációs csatornán kell eljuttatni azonosítás alanyának.[239] Közepes biztonsági szinten az azonosítás jelszóval és mobiltelefonra SMS-ben küldött egyszer használatos jelszóval történhet, amely az internet banking szolgáltatásoknak is elerjedt azonosítási lehetősége.

Alacsony biztonsági fokozatú azonosítás az elektronikus közszolgáltatások körében az ügyfélkapu tudás alapú, jelszót alkalmazó azonosításával történik.[240] Az alacsony biztonsági szint esetén, tehát a fent említettek alapján az interneten keresztüli ügyfélkapcsolatnál csak jelszó alapú azonosítás van kötelezően előírva.

A központi rendszeren keresztül nyújtott elektronikus közszolgáltatás során az elektronikus közszolgáltatást nyújtónak biztosítania kell:[241]

- az alkalmazott informatikai és kommunikációs rendszerek műszaki megfelelőségét és biztonságos működésének feltételeit;
- a szolgáltatás üzemeltetéséhez szükséges eszközrendszer fenntartását, a szolgáltatáshoz való hozzáférés lehetőségét;

[237] Ekszt. 13. § (1)
[238] Eat. 2. § 2.
[239] Ekszt. 14. § (1), (2)
[240] Ekszt. 15. § (1)
[241] Ekszt. 19. § (1)

- az adatok védelmét a jogosulatlan hozzáféréstől, módosítástól, törléstől, megsemmisüléstől;
- a személyes adatok védelméhez fűződő jog érvényesülését

A fent felsoroltakért tehát nem a központi rendszer üzemeltetője, hanem az elektronikus közszolgáltatás nyújtója felelős, beleértve az adatkezelői szerepet és a biztonsági eljárásokért való felelősséget.

A biztonságos és átlátható ügyintézés érdekében a központi rendszer üzemeltetése során kizárólag olyan informatikai és kommunikációs rendszer alkalmazható, amely biztosítja a szolgáltatásokat igénybe vevőkkel való biztonságos kapcsolatot és a központi rendszer folyamatos - előzetesen bejelentett, a legkisebb terhelésű időszakokban megvalósuló karbantartási üzemszünetekkel korlátozható – elérhetőségét. A szolgáltatás nyújtásához kizárólag olyan, a vonatkozó szabványoknak és műszaki előírásoknak megfelelő, megbízható és a külön jogszabály szerint tanúsított informatikai rendszerek és termékek használhatók, amelyek lehetővé teszik a hiteles iratcserét, biztosítják az elektronikus iratok sértetlenségét és védettségét, valamint az informatikai rendszerekben tárolt adatok hiteles archiválását.[242] A központi rendszerhez tehát csak az előírásoknak megfelelő termék illetve rendszer csatlakoztatható, amelynek ellenőrzési és tanúsítási szabályait az elektronikus közszolgáltatás biztonságáról szóló kormányrendelet írja elő.[243] De függetlenül a rendeleti szinten meghatározott szolgáltatás-audittól, ebben a bekezdésben a jogalkotó egyértelműen kinyilvánítja a termékek előzetes tanúsításának követelményét.

A központi rendszerben a továbbított üzenetekről vezetett naplófájlokat úgy kell megőrizni, hogy azokhoz csak a küldő, illetve a címzett írásos megbízásából, valamint az erre törvényben feljogosított szervezeteknek kizárólag olvasási joggal lehessen hozzáférni. A naplófájlokat az üzemeltető öt évig őrzi meg. Folyamatban levő eljárás esetén az eljárás bármely résztvevőjének kérésére a tárolást az ügy lezártáig meg kell hosszabbítani.[244] Az értesítési tárhely forgalmi naplófájljait tehát öt évig illetve az eljárás lezárásig kell tárolni.

A tárhely tartalmához az ügyfélkapu igénybevevője teljes hozzáférési joggal, illetőleg az ügyfélkapu igénybevevőjének engedélye nélkül a törvényben meghatározott

[242] Ekszt. 19. § (2)
[243] 223/2009. (X. 14.) Korm. rendelet 30-32. §§
[244] Ekszt. 19. § (3)

szervek az engedélyhez kötött titkos információgyűjtés, illetve engedélyhez kötött titkos adatszerzés szabályai szerint, írási jog nélkül - az ügyfélkapu működtetőjének közreműködését igénylő módon - férhetnek hozzá.[245]A titkos információgyűjtés lehetőségét a törvény lehetővé teszi, de csak az ügyfélkapu működtetőjének közreműködésével, tehát a hozzáférés jogossága minden esetben tételesen ellenőrizhető.

Az elektronikus közszolgáltatások hitelessége, minősége, üzembiztonsága és a kezelt adatok biztonsága érdekében a központi rendszer részét képező, illetve ahhoz csatlakozó rendszerek külön jogszabályban megállapított egységes biztonsági, valamint a rendszerek együttes működését biztosítani képes szabályok szerint működnek.[246] Itt a törvény az elektronikus közszolgáltatás biztonságáról szóló 223/2009. (X. 14.) Korm. rendeletre utal, amely a 11-32. §§-ban határozza meg a követelményeket és eljárásrendeket.

A törvényben meghatározott követelményeket a következő rendeletek részletezik:

- 223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról
- 224/2009. (X. 14.) Korm. rendelet a központi elektronikus szolgáltató rendszer igénybevevőinek azonosításáról és az azonosítási szolgáltatásról
- 225/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatásról és annak igénybevételéről
- 78/2010. (III. 25.) Korm. rendelet az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól

Nem hatályos és még csak nem is kialakult szabályozásként viszont a területre gyakorolt jelentős befolyása miatt szükséges tárgyalni az informatikai biztonságról szóló törvény 2009-es tervezetét.[247] A tervezet soha nem lett törvény. Maga a jogszabály-tervezet keretszabályozás jellegű, lex specialis. A tervezet gyakorlatilag az élet minden területén alkalmazott informatikai eszközökre tartalmazott előírásokat, a hatálya a Magyar Köztársaságban működő minden IT rendszerre és szolgáltatásra kiterjedt volna. Vonatkozott az üzemeltetőkre és a felhasználókra is. Az informatikai rendszereket 5 egymástól elkülöníthető biztonsági szintre osztotta. A csoportosítás

[245] Ekszt. 19. § (4)
[246] Ekszt. 29. § (1) Az elektronikus közszolgáltatásokkal összefüggő felügyeleti és tanúsítási jogosítványok
[247] MeH: Előterjesztés a Kormánynak az informatikai biztonságról szóló törvényről. 2009.

egyik alapját képezte a személyes adatok tárolásának ténye. A csoportok a következőek voltak:[248]

- az 1. informatikai biztonsági szintbe sorolandók: a lakossági, otthoni, saját célú informatikai hálózat és internethez kapcsolt egyedi számítógép;
- a 2. informatikai biztonsági szintbe sorolandó: minden, munkáltató és munkavállaló közötti jogviszony keretében használt informatikai rendszer, belső informatikai hálózat, korlátozott (belső) hozzáférésű nemnyilvános elektronikus szolgáltatás, illetőleg nyilvános elektronikus szolgáltatás igénybevételére alkalmas belső hálózat vagy egyedi számítógép;
- a 3. informatikai biztonsági szintbe sorolandó: minden olyan nyilvános elektronikus szolgáltatás, amely nem kezel, nem tárol, nem dolgoz fel, illetőleg nem továbbít személyi azonosításra alkalmas adatokat, beleértve a személyes azonosításra alkalmas adatokat nem kötelezően kérő, anonim regisztrációhoz kötött szolgáltatást is;
- a 4. informatikai biztonsági szintbe sorolandó:
    - az elektronikus közszolgáltatást nyújtó szervezet, illetőleg a közszolgáltató vagy közigazgatási szerv részére, vagy annak megbízásából bármilyen jellegű infor-matikai szolgáltatást nyújtó alkalmazásszolgáltató központ informatikai rendszere és nyilvános elektronikus szolgáltatása, abban az esetben is, ha személyi azonosításra alkalmas adatokat nem kezel, tárol, feldolgoz és továbbít;
    - minden olyan nyilvános elektronikus szolgáltatás, amely személyi azonosí-tásra alkalmas adatot kezel, tárol, feldolgoz, illetőleg továbbít;
- az 5. informatikai biztonsági szintbe sorolandók: a kritikus infrastruktúra ágazatok […] informatikai rendszere, zártcélú, és nyilvános elektronikus hálózata, illetőleg szolgáltatása, és informatikai alkalmazása.

Az egyik legérdekesebb kérdés a 4-5. szinten előírt kötelező audit, mint az ellenőrzés eszköze. A szándék szerint az auditot gazdasági társaságok végezték volna, amelyeket a Nemzeti Akkreditációs Testület tanúsítási tevékenységre akkreditált.[249] A jogszabály alkotója nem tudta megmondani, hogy ez irányítási rendszer, vagy termék audit körébe tartozik-e. A leendő törvény társadalmi hatása jelentős lett volna, már csak a hatály szélessége miatt is. A kritikusok részéről kérdésként merült fel, hogy az

[248] ibid. p. 23.
[249] Ez ilyen módon analóg a korábban idézett 223/2009. (X. 14.) Korm. rendelet 30-32. §§-val

1-3. szintig az audit hiánya miatt nincs ellenőrzési kontroll, ezért feleslegessé teszi magát a szabályozást. Ezzel szemben a szabályozás meghatározhatta volna – lex specialis jellege miatt is – a más jogszabályokban előírt biztonsági követelmények szintjét. Például a Btk. 423. §-ában „megfelelő védelem"-nek nevezett, korábban nem tisztázott védelmi szint az új törvénnyel meghatározásra került, tartalma feltöltődött volna. Így az eddig csupán a kötelezett hatáskörébe rendelt „megfelelő védelem" kialakítása konkretizálódott volna, növelve ezzel a jogbiztonságot.

A Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012 (II.21.) kormányhatározat előírja az elektronikus információs rendszerek biztonságának erősítését, a létfontosságú nemzeti információs infrastruktúra védelmének fokozását, továbbá a megfelelő kibervédelem kialakítását. Tovább részletezve a Nemzeti Biztonsági Stratégiában irányelvként megfogalmazottakat, a Kormány elkészítette Magyarország Nemzeti Kiberbiztonsági Stratégiáját is.[250] A jogalkotó úgy vélte, hogy a világban a közelmúltban tapasztalt kiberháborúk indokolják, hogy ennek keretében elkészüljön egy korszerű magyar információbiztonsági törvény is, így 2013. április 25-én hatalmas mérföldkőként a közigazgatási informatika szabályozásában kihirdetésre került az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.). A törvény hatálya a cím és a 2. §-ban meghatározott személyi hatály ellenére jelentősen szélesebb körű, a következő hatály (kiterjesztés) miatt: a jogszabályban meghatározott, a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói és az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek.[251] Ezek a szervek jelentős mértékben bővíthetik (akár gazdasági társaságokkal is) a személyi hatályt, így tipikusan a közüzemi szolgáltatók, elektronikus hírközlési szolgáltatók, pénzügyi szervezetek kerülnek a kötelezett körbe. Tételes lista nem került kihirdetésre. A törvény alapvető információbiztonsági követelményként az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állását írja elő,[252] tehát az információbiztonság területén CIA triádként ismert alapvető elemeket.

[250] 1139/2013. (III.21.) Korm. határozat
[251] Ibtv. 2. § (2) b)-c)
[252] Ibtv. 5. § a)

Az Ibtv. részletes indokolása[253] szerint „az értelmező rendelkezések az elfogadott és általánosan alkalmazott hazai szakkifejezésekre épülnek. Ezek jelentős része a Kormány 3296/1991. (VII. 5.) határozata alapján 1991. november 27-én létrehozott Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága 12. számú ajánlásaként 1996. április 2-án elfogadott Informatikai Rendszerek Biztonsági Követelményei című dokumentumban rögzítésre került. Az itt leírt fogalmak és definíciók az Informatikai Biztonság Kézikönyve (Verlag Dashöfer, Budapest, 2000-2005), illetve a Közigazgatási Informatikai Bizottság 25. és 28. számú ajánlásaiban is megjelentek, a nemzetközi szakirodalmat, szabványokat figyelembe véve, újra feldolgozva korábbi definíciókat." Ezzel a jogalkotó figyelembe vette a '90-es években széles szakmai körben elterjedt ajánlásokat, illetve – mivel a KIB 25. sz. ajánlása az ISO 27001 és 27002 alapján készült – nemzetközileg elfogadott információbiztonsági szabványok is megjelennek benne.

A törvény előírja az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.[254] Fontos, hogy a kockázatokkal arányos védelem és így a kockázatértékelés explicit módon bekerüljön az állami információbiztonsági követelmények közé, ugyanis jellemzően ad hoc módon, a büdzséhez mérten történik a védelem kialakítása.

Annak érdekében, hogy az Ibtv. hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszereket be kell sorolni egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából. A biztonsági osztályba sorolás alkalmával - az érintett elektronikus információs rendszer vagy az általa kezelt adat bizalmasságának, sértetlenségének vagy rendelkezésre állásának kockázata alapján - 1-től 5-ig számozott fokozatot kell alkalmazni, a számozás emelkedésével párhuzamosan szigorodó védelmi előírásokkal együtt.[255] Nehézséget okozhat az alkalmazásnál, hogy az „egy-egy" kifejezésből az adódna, hogy a CIA-faktorok közül mindháromban egy-egy besorolást kell adni, a törvény további szakaszaiból ez nem következik. Bár a biztonsági osztályba sorolás elsősorban az adatok biztonsági besorolásán múlik, a törvény – szemben a bemutatott korábbi törvénytervezettel – nem határozza meg, hogy az adatoknak milyen minimális

[253] http://www.parlament.hu/irom39/10327/10327.pdf [2018.03.11.]
[254] Ibtv. 5. § b)
[255] Ibtv. 7. § (1)-(2)

biztonsági szintje legyen. Ezzel szemben a 9. § (2)-ben a különböző szervezeteknek határoz meg minimális biztonsági besorolást. Ez a közszféra energiaminimumra való törekvése alapján valószínűleg azt fogja eredményezni, hogy az adatok védelmi igényét nem fogják értékelni, csak a lenti listából fognak kiindulni. Mivel a törvény 7. § (5) bek. alapján a szervezet vezetője „kivételes esetben indoklással ellátva alacsonyabb biztonsági osztályt is megállapíthat", az estek jó részében erre fog törekedni a szervezet. Az egyetlen dolog, ami érdemben meg tudja akadályozni ezt a várható lefelé licitálást, a Nemzeti Elektronikus Információbiztonsági Hatóság szigorúsága, amit az Ibtv. 9. § (4) tesz lehetővé és a 14. § (1) hoz létre.

A szervezetenkénti minimális besorolások az Ibtv. 9. § (2) szerint:

- 2. szintűek: Köztársasági Elnöki Hivatal, Országgyűlés Hivatala, Alkotmánybíróság Hivatala, Alapvető Jogok Biztosának Hivatala, helyi és nemzetiségi önkormányzatok képviselő-testületének hivatalai, hatósági igazgatási társulások
- 3. szintűek: központi államigazgatási szervek, Országos Bírósági Hivatal, bíróságok, ügyészségek, Állami Számvevőszék, Magyar Nemzeti Bank, fővárosi és megyei kormányhivatalok
- 4. szintű: Magyar Honvédség
- 5. szintűek (legszigorúbb): a jogszabályban meghatározott, a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói, az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek

A törvény nem határozza meg, hogy ezek a biztonsági szintek mit jelentenek, mi alapján történik a besorolás és melyek a részletes szabályok.

Az Ibtv. 11. § (1) c) alapján a kötelezett szervezet vezetője az elektronikus információs rendszer biztonságáért felelős személyt nevez ki, aki felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért, ami bár egy hagyományos CISO feladatköre a felsorolás[256] alapján, a neve és a feladatkörének definíciója mégis arra utal, hogy a szervezet első számú vezetőjét és a szervezet dolgozóit mentesíti információbiztonsági kötelezettségeik és felelősségeik alól.

[256] Ibtv. 13. § (2)

Az Ibtv. megalkotásakor a Nemzeti Fejlesztési Minisztérium keretében létrehozta a Nemzeti Elektronikus Információbiztonsági Hatóságot és a sérülékenység-vizsgálat és forenzikus logelemzés elvégzéséhez szakhatóságként a Nemzeti Biztonsági Felügyeletet is bevonja a tevékenységébe.[257] Az kormányzati CERT[258] feladatait a megszűnt Puskás Tivadar Közalapítványtól a Nemzetbiztonsági Szakszolgálathoz, létfontosságú rendszerelemek tekintetében pedig a Katasztrófavédelemnél működő Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központjához (LRLIBEK) hez helyezi át.[259]

Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelettel ez a struktúra annyiban változott, hogy a Nemzeti Elektronikus Információbiztonsági Hatóság áthelyezésre került a Belügyminisztérium alá tartozó Nemzetbiztonsági Szakszolgálathoz, ezzel létrehozva a Nemzeti Kibervédelmi Intézetet, ahol a fenti hatáskörök összpontosulnak.

Az Ibtv. 23. § alapján a Nemzeti Közszolgálati Egyetem dolgozza ki az elektronikus információs rendszer biztonságáért felelős személyek és érintett szervezetek munkatársainak képzését, ami azóta is minden félévben induló szakirányú továbbképzési szak, illetve közszolgálati továbbképzés formájában fut.

Összességében az utóbbi évek tendenciája határozottabb jogi szabályozást mutat, részben akár a technikai szabályok jogi normákba ültetésével. A jogszabályok széleskörűsége miatt hosszú távon jelentős társadalmi hatás várható. Valószínűleg a szabványon alapuló rendszerek is szaporodni fognak, tekintettel arra, hogy ha a gazdasági társaság egyébként is betartja az informatikai biztonságra vonatkozó szabályokat, akkor marketing okokból illetve a cég sikeresebb külföldi megjelenése érdekében valamely nemzetközi informatikai biztonsági szabvány alapján is tanúsíttatni fogja rendszerét. A szabályozás nagyobb biztonságot fog eredményezni, hosszabb távon csökkenni fog az informatikai és kommunikációs technológiák területén a nemzeti biztonsági kockázat. Mindezek mellett az Ibtv. bár jó lépés a megfelelő szintű kormányzati információbiztonság irányába, egyelőre túl sok felelőst nevez meg és biztosít kibúvókat a szabályok alkalmazása alól.

[257] Ibtv. 18. §
[258] Computer Emergency Response Team, az informatikai vészhelyzeteket/incidenseket kezelő szervezet
[259] Ibtv. 19. § (6)

4.1.4.3. Elektronikus közbeszerzés

Részletesen szabályozottnak tekinthetjük azokat a területeket, amelyek valamely szabvány előírásainak követését írják elő, függetlenül attól, hogy a szabvány pontjait nem idézik a jogszabály szövegében. Erre példa az elektronikus közbeszerzés területe. A közbeszerzési eljárásokban elektronikusan gyakorolható eljárási cselekmények szabályairól, valamint az elektronikus árlejtés alkalmazásáról szóló 257/2007. (X. 4.) Korm. rendelet 5. § (3) szerint elektronikus közbeszerzési szolgáltatást az nyújthat, aki rendelkezik külső, független rendszervizsgáló által folyamatosan ellenőrzött minőségirányítási és információbiztonsági irányítási rendszerrel és saját honlapján közzéteszi informatikai biztonsági szabályzatát. Ezzel gyakorlatilag kötelezően előírásra került az ISO/IEC 27001 szabvány alkalmazása, amely az ISO/IEC 27002 behivatkozásával részletes szabályokat eredményez.

4.1.4.4. Minősített adatok védelme

Mivel az informatikai biztonság fogalmát a civil alkalmazásokban értelmeztük, a munka hatókörén kívül esik a minősített adatok védelme, valamint a katonai célú adatok védelme. Hasonlóan az indirekt szabályozáshoz ezzel a témával is röviden foglalkozni kell a teljesség kedvéért.

Nemzeti minősített adat „a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést az e törvényben, valamint az e törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről - a megjelenési formájától függetlenül - a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti (a továbbiakban együtt: károsítja), és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza.”[260]

[260] Mavtv. 3. § 1.

A minősített adat a titokvédelem (minősített adatok védelmének) tárgyát képező, nemzetbiztonsági célból védett adat. A minősített adat – hasonlóan a személyes adathoz – nem kötődik kizárólagosan valamely hordozóhoz, megjelenési formához, vagy kódoláshoz. A minősített adat létrejöttének alapvető feltétele a minősítés aktusa, amelynek szabályait a Mavtv. határozza meg. Az aktus útján létrejött minősített adat viszont hordozót, megjelenési formát válthat, de mindaddig megőrzi minősített jellegét, ameddig a minősítése meg nem szűnik. Így az eredetileg papíralapú iratként, vagy hadműveleti térképként minősített adat szóbeli közléssé alakulva is megőrzi minősített jellegét. Tekintettel arra, hogy a minősített adat védelméhez az államnak jelentős érdeke fűződik, külön szervezetrendszert és eljárásrendet működtet annak védelmében, amit titokvédelemnek, információvédelemnek, vagy a jogszabály megfogalmazása szerint minősített adatok védelmének hívunk.

A minősített adatok védelmének szabályozása jelentős mértékben változott 2010 áprilisa óta, amikortól hatályba lépett a minősített adatok védelméről szóló 2009. évi CLV. törvény (Mavtv.).

Minden olyan szervnél, ahol minősített adatot kezelnek, meg kell teremteni a minősített adat védelméhez szükséges, az adat minősítési szintjének megfelelő, e törvényben és a végrehajtására kiadott rendeletekben meghatározott személyi, fizikai, adminisztratív és elektronikus biztonsági feltételeket. Minden olyan helyiséget, épületet, építményt, ahol minősített adatot kezelnek, fizikai biztonsági intézkedésekkel kell védeni az arra nem jogosult személyeknek a minősített adathoz történő hozzáférése ellen. Az adminisztratív biztonsági intézkedésekkel gondoskodni kell a minősített adat nyomon követhetőségéről, bizalmasságáról, sérthetetlenségéről, rendelkezésre állásáról. Elektronikus biztonsági intézkedéseket kell tenni az elektronikus rendszeren kezelt minősített adat és az elektronikus rendszer bizalmassága, sérthetetlensége és rendelkezésre állása érdekében.[261] A hagyományosnak mondható személyi, fizikai, adminisztratív és elektronikus biztonsági intézkedéseknek csak általános, felületes követelménye jelenik meg közvetlenül a törvényben, viszont a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet 10-59. §§, valamint az informatikai rendszerben előírt védelmi tevékenységről a minősített adat elektronikus biztonságának, valamint a

[261] Mavtv. 10. § (4) – (7)

rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendelet 16-40. §§ írják elő. A részletszabályok kormányrendeleti szintű szabályozása a technológiai változásokra való gyorsabb reagálást tesz lehetővé. A kormányrendelet egy esetben szabványra hivatkozik, a biztonsági tároló ellenállási fokozatának meghatározásakor, ahol az EN 14450; MSZ EN 1143-1-A1-A2, EU I-es, EU 00-ás, S 1-es ellenállási fokozatokat sorolja be kategóriákba.[262]

Megemlítendő viszont itt egy olyan terület, amely a civil biztonságvédelemben bár ismert, de ritkán alkalmazott, a TEMPEST védelem. A TEMPEST követelmények abban különböznek a hagyományosan vett elektromágneses kompatibilitási (EMC) védelemtől, hogy az EMC a külső zavarjelek bejutását vagy belső zavarjelek kijutását hivatott megakadályozni, amely a rádiófrekvenciás eszközök természetes működésének velejárója. A TEMPEST viszont a védett rendszerből kijutó elektromágneses sugárzás lehallgatását, és abból adatok visszaállítását hivatott megakadályozni.[263] A jogszabályban meghatározott TEMPEST követelmények a „Bizalmas!" vagy magasabb minősítési szintű adat bizalmasságának védelme érdekében kialakított biztonsági intézkedések - amelyek kiterjednek az elektromos és adatkábelek vonalvezetésére, a rendszer környezetében alkalmazható berendezésekre, árnyékolástechnikai megoldásokra, valamint csökkentett kisugárzású eszközökre - együttese, amelyet a rendszer valamennyi eleme vezetett és elektromágneses kompromittáló kisugárzásának csökkentése érdekében alakítottak ki, [264]

A Mavtv. alapján a Nemzeti Biztonsági Felügyelet látja el a minősített adatot kezelő szervnél a minősített adat kezelésének hatósági felügyeletét, ellenőrzi a minősített adat védelmére vonatkozó jogszabályok, valamint a személyi, fizikai, adminisztratív és elektronikus biztonsági szabályok betartását,[265]viszont a minősített adat védelmi feltételeinek kialakításáért a minősített adatot kezelő szerv vezetője felelős.[266]

A területet szabályozó további fontos jogszabályok:

- 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól

[262] 90/2010. (III. 26.) Korm. rendelet 24. § (1)
[263] Hoad – Jones, 2004, p. 130.
[264] 161/2010. (III. 26.) Korm. rendelet 1. § 21.
[265] Mavtv. 20. § (2)
[266] Mavtv. 23. § (1)

- 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről
- 2000. évi IV. törvény az információ biztonságáról szóló, Brüsszelben, 1997. március 6-án kelt NATO Megállapodás megerősítéséről és kihirdetéséről

4.1.5. Jogi szabályozás külföldön

Jelenleg az informatikai biztonság általános Európai Uniós közösségi szabályozása elsősorban iránymutatásokban merül ki. Több olyan iránymutatást (határozatot, illetve állásfoglalást) találhatunk az Európai Unió részéről, amely célként tűzi ki az információs és kommunikációs technológiák biztonságának hosszú távú javítását, de ezek nem rendelkeznek kötelező erővel. Ilyen például az Európai Parlament és a Tanács 854/2005/EK határozata (2005. május 11.) az Internet és az új online technológiák biztonságosabb használatát elősegítő többéves közösségi program létrehozásáról. Ilyen továbbá a Tanács állásfoglalása (2004. december 9.) az információs és kommunikációs technológiák (IKT) jövőjéről (2005/C 62/01), valamint a Tanács állásfoglalása (2007. március 22.) a biztonságos európai információs társadalomra irányuló stratégiáról (2007/C 68/01).
Konkrétabb szabályozást szakrendszerek esetén találunk, mint például Schengeni Információs Rendszer (SIS) új verziójának bevezetésével kapcsolatos rendeletben (az Európai Parlament és a Tanács 1987/2006/EK rendelete (2006. december 20.) a Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működtetéséről és használatáról).[267] Ezek hatálya viszont nem általános.

Az adatvédelmi jog a Közösségben, – ahogyan a magyar jogban is – iskolapéldája a felületes szabályozás kategóriájának. Az Európai Parlament és a Tanács a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelvébe foglalkozik az adatfeldolgozás biztonságával: A tagállamoknak rendelkezniük kell arról, hogy az adatkezelő végrehajtsa a megfelelő technikai és szervezési intézkedéseket a személyes adatok véletlen vagy jogellenes megsemmisülése, véletlen elvesztése, megváltoztatása, jogosulatlan nyilvánosságra

[267] Regulation (EC) No. 1987/2006; Article 9-14, 15-18

hozatala vagy hozzáférése elleni védelme érdekében, különösen, ha a feldolgozás közben az adatokat hálózaton keresztül továbbítják, továbbá a feldolgozás minden más jogellenes formája ellen.

Tekintettel a technika vívmányaira és alkalmazásuk költségeire, ezen intézkedéseknek olyan szintű biztonságot kell nyújtaniuk, amely megfelel az adatfeldolgozás által jelentett kockázatoknak és a védendő adatok jellegének.[268]

Az első bekezdés második mondata egy informatikai biztonságban ismert fogalmat alkalmaz a kockázatokkal arányos védelmet. Tehát a védelmi szint megállapításának a kockázatelemzés értékelésén kell alapulnia.

A tagállamoknak rendelkezniük kell arról, hogy az adatkezelő – amennyiben az adatfeldolgozás az ő nevében történik – köteles olyan adatfeldolgozót választani, aki a technikai biztonsági intézkedések és az elvégzendő adatfeldolgozásra vonatkozó szervezési intézkedések tekintetében megfelelő garanciákat nyújt, továbbá köteles biztosítani az említett intézkedések teljesítését.[269]

Az adatkezelő feladata tehát az adatfeldolgozó biztonságának kezdeti felmérése (beszállítói audit) és a folyamatos ellenőrzése.

A 2009. év végétől jelentős mértékben megnőtt a személyes adatokat érintő biztonsági incidensek (personal data breach) nyilvánosságával, illetve az incidenskezelés hatósági feladataival kapcsolatos Európai Uniós aktivitás, mind a Parlament és a Tanács, mind az Európai Hálózati- és Információbiztonsági Ügynökség (ENISA) részéről. Az 2009/136/EK irányelv alapján a 2002/58/EK irányelv (elektronikus hírközlési adatvédelmi irányelv) 4. cikke a következőképpen módosult:

(3) A személyes adatok megsértése esetén a nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyújtó illetékes szolgáltató indokolatlan késedelem nélkül bejelenti az illetékes nemzeti hatóságnak a személyes adatok megsértését.

Ha a személyes adatok megsértése várhatóan hátrányosan érinti az előfizető vagy magánszemély személyes adatait vagy magánéletét, akkor a szolgáltató erről az előfizetőt vagy magánszemélyt is indokolatlan késedelem nélkül értesíti.[270]

Az irányelv implementációja folyamatban van. A nemzeti hatóság nem került megjelölésre, az azzal szemben támasztott legfőbb igény a függetlenség. A nemzeti

[268] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) VIII. szakasz 17. cikk (1)
[269] ibid. VIII. szakasz 17. cikk (2)
[270] Az Európai Parlament és a Tanács 2009/136/EK Irányelve (2009. november 25.) 2. cikk 4. c)

hatóság hazánkban lehet a Nemzeti Média- és Hírközlési Hatóság és az Adatvédelmi Biztos Irodája is. Külföldön mind a hírközlési, mind az adatvédelmi hatóság megbízására van példa, egyes országokban (Belgium, Bulgária) vegyes modell működik mindkét hatóság részvételével. A kijelölt hatóság fogadja a bejelentéseket, ellenőrzi a bejelentéseket és megtagadásukat, valamint nem jogszerű megtagadás esetén kötelezi a szolgáltatót az értesítésre.[271]

További bővítést irányoz elő viszont a 2009/136/EK irányelv preambuluma: közösségi szinten kiemelkedő fontosságúnak kell tekinteni a kifejezett, kötelező és minden ágazatra és az információs társadalommal összefüggő szolgáltatások szolgáltatóira kiterjedő tájékoztatási kötelezettség szükségességét is ideértve.[272]

Az ilyen incidensek száma rendkívül nehezen határozható meg, Európában nem is lehet mérvadó adatokat fellelni. A datalossdb.org, ami egy Egyesült Államokban működő magánkezdeményezésű incidensgyűjtő oldal, 2005 óta 3011 incidenst rögzített, amely átlagosan havi 50 incidens-bejelentést jelent. Ezzel szemben a Privacy Rights Clearinghouse 227.052.199 egyedi személyes adat incidensben való érintettségét rögzítette 2005 januárja és 2008 májusa között. Ez utóbbi a magyar lakosságszámra vetítve 2,44 millió adat incidensben való érintettségét jelentené évente, míg az előbbi nyilvántartás esetén évi 19 esetet.

Levonható konzekvencia, hogy bár a személyes adatot érintő incidensek száma hozzávetőlegesen sem ismert, az érintett terület szolgáltatóinak, illetve a szolgáltatóknál incidenskezeléssel foglalkozó személyek nagy száma miatt valószínűleg nagyszámú incidens fordul elő az Unióban és hazánkban is.

Nagy várakozással tekint a szakmai közösség a 2018 május 25-től mindne tagállamban közvetlenül alkalmazandó általános adatvédelmi rendelet (General Data Protection Regulation, GDPR) bevezetésére.[273]

Külföldi kitekintésként az adatvédelem külföldi jogi szabályozását szeretném bemutatni, mivel – ahogy az a műben korábban bemutatásra került – az adatvédelmi jog a magyar jogban is iskolapéldája a felületes szabályozás kategóriájának.

[271] Bíró – Szádeczky – Szőke, 2011.
[272] ibid. Peambulum (59)
[273] 2016/679 EU rendelet

Az Egyesült Királyságban a Data Protection Act 1998[274] szabályozza az adatvédelem területét. Az adatbiztonságra vonatkozóan az adatvédelem elveiről szóló részben a következőket találjuk: „Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."[275]

Ez eddig megfelel az Infotv.-ben foglaltaknak. Az ezen alapelvre vonatkozó értelmező rész a következő: "Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and the nature of the data to be protected."[276]

A jogszabály az irányelvhez hasonlóan figyelembe veszi, hogy az erőforrások nem végtelenek és kockázatarányos védelmet vár el az alkalmazótól. A védelem mértékének megállapításához a két legfőbb mérce a kár mértéke és a védendő adatok köre. Figyelembe veszi továbbá a műszaki fejlettséget is, amely szintén jelentős kérdés az informatikában.

"The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data."[277]

Előírja, hogy az adatkezelőnek meg kell tennie a megfelelő lépéseket, hogy az adatokhoz hozzáférő alkalmazottak megbízhatóságát biztosítsa. Ennek több szintje van, így történhet titoktartási nyilatkozat kitöltésével, háttérellenőrzéssel, vagy nemzetbiztonsági ellenőrzéssel is.

"Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle— choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and take reasonable steps to ensure compliance with those measures."[278]

Ez a követelmény azonos az irányelv 17. cikkének második bekezdésével, tehát az adatkezelőnek kell meggyőződnie az adatbiztonsági intézkedések megfelelőségéről és ellenőriznie azt.

[274] elérhető például: http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/legislation.aspx [2010. 09. 15.]
[275] Data Protection Act 1998 Schedule 1 Part I 7.
[276] ibid. Schedule 1 Part II 9.
[277] ibid. Schedule 1 Part II 10.
[278] ibid. Schedule 1 Part II 11.

"In this section "good practice" means such practice in the processing of personal data as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, and includes (but is not limited to) compliance with the requirements of this Act."[279]

A törvényben megahatározott jó gyakorlatot a biztos határozza meg, amely túlmutathat a törvényi követelményeken, így a tulajdonképpeni követelményeket a törvény és a biztos által kibocsátott helyes gyakorlatok együtt határozzák meg.

"The Commissioner may, with the consent of the data controller, assess any processing of personal data for the following of good practice and shall inform the data controller of the results of the assessment."[280]

A biztos ellenőrzési jogköre gyengébb, mint hazánkban, ugyanis ellenőrzései az adatkezelő beleegyezéséhez is kötöttek.

A következő bemutatásra kerülő szabályozás a szlovén információs törvény. A választás azért esett Szlovéniára, mert Magyarországhoz hasonló helyzetű, az informatikai biztonság nemzetközi szabályozásában követő szerepű ország. Információs törvényéből (Zakon o varstvu osebnih podatkov, ZVOP-1) angol nyelven[281] a következőek vonatkoznak az adatbiztonságra:

"Security of personal data comprises organisational, technical and logical-technical procedures and measures to protect personal data, and to prevent accidental or deliberate unauthorised destruction, modification or loss of data, and unauthorised processing of such data

- by protecting premises, equipment and systems software, including input-output units.
- by protecting software applications used to process personal data;
- by preventing unauthorised access to personal data during transmission thereof, including transmission via telecommunications means and networks;
- by ensuring effective methods of blocking, destruction, deletion or anonymisation of personal data;

[279] ibid. Part IV 51. General duties of Commissioner (9)
[280] ibid. Part IV 51. General duties of Commissioner (7)
[281] Elérhető a szlovén információs biztos honlapjáról: http://www.ip-rs.si/index.php?id=382 [2010. 09. 16.]

- by enabling subsequent determination of when individual personal data were entered into a filing system, used or otherwise processed, and who did so, for the period covered by statutory protection of the rights of an individual due to unauthorised supply or processing of personal data." [282]

A törvény általános felsorolása megegyezik az Infotv.-ben lévővel, de a részletes felsorolás jobban meghatározza a védendő értékeket. Megnevezi a helységeket, a felszereléseket, a rendszerszoftvereket és a be-és kiviteli egységeket (monitor optikai rálátás, adathordozók alkalmazása). A jogszabály külön nevesíti a személyes adatok feldolgozására használt szoftvereket (adatbázis-kezelő, táblázatkezelő, stb.), amelyek védelméről gondoskodni kell. A távközlési rendszereken és hálózatokon továbbított adatok védelme az Infotv.-ben nincs külön hangsúlyozva. Újdonságként merül fel, hogy a szlovén jogalkotó az anonimizálás hatékony eljárásának szükségességét megemlíti informatikai biztonsági igényként, amely valóban sarkalatos probléma, ám kevéssé foglalkozunk ezzel a kérdéssel. Újdonság továbbá, hogy a személyes adatok tárolásra vonatkozó egyes jellemzők (eltárolás ideje, használat, feldolgozás ideje és célja) rögzítését kötelezővé teszi a törvény.

"In cases of processing of personal data accessible over telecommunications means or network, the hardware, systems software and software applications must ensure that the processing of personal data in filing systems is within the limits of authorisations of the data recipient."[283]

Előírásként szerepel, hogy az adatalany felhatalmazásának korlátait az távközlési vagy hálózati úton hozzáférhető személyes adatok feldolgozásakor hardver és szoftver elemekkel biztosítani kell.

"The procedures and measures to protect personal data must be adequate in view of the risk posed by processing and the nature of the specific personal data being processed."[284]

A szlovén törvény előírja a kockázatarányos védelmet, hasonlóan az Infotv.-hez.

"Functionaries, employees and other individuals performing work or tasks at persons that process personal data shall be bound to protect the secrecy of personal data with which they become familiar in performing their functions, work and tasks. The duty to protect the secrecy of personal data shall also be binding on them after termination of

[282] ZVOP-1 Article 24 (1)
[283] ZVOP-1 Article 24 (2)
[284] ZVOP-1 Article 24 (3)

their function, work or tasks, or the performance of contractual processing services."[285]

A személyes adatokat feldolgozó munkatársakat kötelezni kell arra, hogy a munka végzésekor és az alkalmazás megszűnését követően is bizalmasan kezeljék a megismert személyes adatokat.

"Data controllers shall prescribe in their internal acts the procedures and measures for security of personal data and shall define the persons responsible for individual filing systems and the persons who, due to the nature of their work, shall process individual personal data."[286]

A fenti védelmi intézkedéseket mind az adatkezelő, mind az adatfeldolgozó köteles betartani és felelősöket megnevezni, valamint megnevezni minden olyan személyt, aki munkakörénél fogva személyes adatok feldolgozását végzi.

"A fine from EUR 4.170 to 12.510 shall be imposed for a minor offence on a legal person, sole trader or individual independently performing an activity, if he processes personal data in accordance with this Act and fails to ensure security of personal data (Articles 24 and 25).

A fine from EUR 830 to 1.250 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person, sole trader or individual independently performing an activity.

A fine from EUR 830 to 1.250 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community who commits the act from the first paragraph of this Article.

A fine from EUR 200 to 830 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article."[287]

Az adatbiztonsági előírások megszegéséért 1,1-3,5 millió forintnak[288] megfelelő pénzbírságot kell fizetnie a szabályokat megszegő gazdálkodónak, 230-350 ezer forintnak megfelelő pénzbírságot kell fizetnie a szabályokat megszegő gazdálkodó és az állami szerv vagy önkormányzat felelős személyének,[289] 50-230 ezer forintnak megfelelő pénzbírságot kell fizetnie a szabályokat megszegő magánszemélynek.

[285] ZVOP-1 Article 24 (4)
[286] ZVOP-1 Article 25 (2)
[287] ZVOP-1 Article 93 (1) – (4) Violation of the provisions on security of personal data
[288] 1 EUR = 282,3 HUF középárfolyamon, kerekítve
[289] Nem egyértelmű, hogy felelős vezető vagy adatkezelésért felelős személy, de az utóbbi a tételes megnevezési kötelezettség miatt valószínűbb.

A törvényhez nem kapcsolódik végrehajtási rendelet, a szlovén információs biztos nem rendelkezik írásos módszertannal az adatvédelmi-adatbiztonsági auditra, nem találhatóak ennél részletesebb leírások.

Látható, hogy a szabályozás kis mértékben jobban definiált, mint az Infotv.-ben, ám így sem nevezhető részletesnek. Külön elrettentő erő a pénzbírság, viszont ez tovább növeli a jogbizonytalanságot, hiszen jobban kierőszakolható a nem definiált szabályok betartása.

4.2. A szabványalkalmazás gyakorlata

A gyakorlatban az informatikai biztonsági szabványok az informatikai biztonságot szabályozó jogszabályokhoz hasonlóan nem egységesek. Egyrészről azon belül, hogy informatikai biztonsági (vagy azt nagy részben lefedő) szabványok, érdemes kisebb alkalmazási csoportokat alkotnunk, amelyeket olyan módon osztunk fel, hogy elsősorban milyen aspektusra vonatkozik az adott szabvány. Így az alábbi csoportokat tudjuk megalkotni:[290]

- műszaki szabványok és leírások
- termék, rendszer követelményei, azok tesztelése, értékelése és tanúsítása
- ellenintézkedések leírása
- irányítási rendszer, folyamat és tanúsítása

Az ilyen módon, célterület alapján besorolt szabványok nem egy időben jelentek meg, a lista a szabványtípusok tipikus megjelenése szerinti időrendben van. Az időrendiség sem a jelen felsorolás tekintetében, sem általánosságban nem befolyásolja a szabványok alkalmazhatóságát, a jogszabályokkal szemben ugyanis a szabványok bármeddig használhatók, másrészről viszont a visszavont szabványok esetében bizonyos korlátokba lehet ütközni, például, ha tanúsítás a visszavont szabványra már nem adható ki. Sokkal inkább tehát a népszerűség határozza meg, hogy egy szabvány meddig kerül elfogadásra. A lent olvasható történeti áttekintésben említett akár ’80-as évekbeli szabvány is máig használt, de egyes, főképp a műszaki szabványok és leírások kategóriába tartozó szabványok soha nem váltak széleskörűen elfogadottá és még egy tapasztalt szakember sem találkozott minddel.

A számítástechnika őskorában, az 1960-70-es években a korábban említett kötegelt feldolgozású mainframe számítógépek esetében a külön szabványalkotás a jogi szabályozás megalkotásához hasonlóan nem volt szükséges, a hagyományos papíralapú titokvédelmi eljárások megfelelően működtek.[291] A több felhasználós, erőforrásokat megosztó rendszerek támasztottak először új igényeket, amire válaszként 1970-ben szakértői jelentés készült „Security Controls for Computer

[290] Krauth, 2003, p. 6. alapján, módosítással
[291] Krauth, 2007.

Systems: Report of Defense Science Board Task Force on Computer Security" címmel.[292] A dokumentum elemezte az új kockázatokat és javaslatot tett a bevezetendő intézkedésekre. 1972-ben jelent meg az egyik első követelményrendszer Computer Security Technology Planning Study, amelyet az Air Force Systems Command készített.[293] Az informatikai biztonság értékelése egyre inkább előtérbe került, melyre példa az 1979-es Proposed Technical Evaluation Criteria for Trusted Computer Systems.[294]

4.2.1. TCSEC

Az első valóban széles körben elerjedt és mindmáig szórványosan alkalmazott informatikai biztonsági szabvány a Trusted Computer Systems Evaluation Criteria (TCSEC, Orange Book) volt, amelyet az Amerikai Egyesült Államok Védelmi Minisztériuma készített 1983-ban, majd javításra került 1985-ben.[295] A TCSEC célja a hidegháború alatt az Amerikai Egyesült Államok által beszerzett számítógéprendszerek biztonsági szintjeinek meghatározása[296] és egységesítése volt a minősített adatok védelmében. A de facto szabvány négy fő kategóriát nevesít D-től A-ig, azon belül alkategóriákat. A legmagasabb biztonságot az A1 fölötti kategória jelenti. A meghatározott kategóriák és főbb jellemzőik a következők:

- D - Minimal Protection

Olyan rendszer, amely értékelésre került, de nem felelt meg semmilyen magasabb kategóriának.

- C - Discretionary Protection
  - C1 - Discretionary Security Protection

Megvalósul a felhasználók és adatok szétválasztása és a tetszés szerinti hozzáférés-szabályozás (Discretionary Access Control, DAC), amellyel egyedileg meghatározhatóak a hozzáférési jogosultságok.

  - C2 - Controlled Access Protection

[292] Ware, 1970.
[293] Anderson, 1972.
[294] Nibaldi, 1979.
[295] A szabvány történeti jelentősége miatt került itt feltüntetésre.
[296] F. Ható, 2000.

A C1-esnél részletesebb hozzáférés-szabályozás, egyénenkénti elszámoltathatóság a bejelentkeztetés segítségével, audit ösvények (audit trails) és az erőforrások elkülöníthetősége jellemzik.

- B - Mandatory Protection
  - B1 - Labeled Security Protection

Félhivatalos informatikai biztonsági politikát kell létrehozni, az adatokat érzékenységük alapján címkézni kell, ezeket igény szerint exportálni lehessen. Kötelező a hozzáférés-szabályozás (Mandatory Access Control, MAC) meghatározott objektumokon, minden felfedezett biztonsági rést meg kell szüntetni vagy más módon ártalmatlanná kell tenni.

  - B2 - Structured Protection

Formálisan dokumentált, egyértelmű informatikai biztonsági politikát kell létrehozni, a hozzáférést szabályozni kell minden objektumon és védekezni kell az engedély nélküli rejtett tárolók ellen. A rendszerelemeket fel kell osztani védelemkritikus és nem védelemkritikus részekre. Előírás az összetett tervezés és kiépítés, a megerősített azonosítási eljárások, az adminisztrátor és operátor szerepek szétválasztása és szigorú konfiguráció-menedzsment szabályok kialakítása.

  - B3 - Security Domains

A biztonsági politika betartatásához nem szükséges kódot a rendszer ne futtasson. A rendszer összetettségét minimalizálni kell, támogatni kell a biztonsági adminisztrátor munkáját és a biztonsági eseményeket auditálni kell. Automatikus behatolás-érzékelést, értesítési és reagálási módszereket és megbízható rendszer-helyreállítási eljárásokat kell kialakítani. A rejtett időzítési csatornák ellen védekezni kell.

- A - Verified Protection
  - A1 - Verified Design

Funkcionálisan megegyezik a B3 szinttel. Ezen felül formális tervezési és ellenőrzési technikákat és felsőszintű specifikációt, valamint formális menedzsment és osztályozási eljárásokat kell létrehozni.

  - Beyond A1

Az önvédelmi követelmények teljességét demonstráló rendszer-architektúrát jelent. A felső- és alacsony szintű követelményekből automatikusan generált biztonsági tesztelést kell végezni, forráskód szintű ellenőrzést kell végezni lehetőleg formális

eljárásokkal, a tervezési környezetnek biztonságosnak, a személyzetnek megbízhatónak kell lennie.

4.2.2. ITSEC, CTCPEC, FC

A TCSEC európai megfelelőjeként Nagy-Britannia, Franciaország, Hollandia és Németország 1991-ben megalkotta az Information Technology Security Evaluation Criteria (ITSEC) de facto szabványt, amely hasonlóan szintező jellegű volt E0-tól E6-ig, valamint példákat is adott egyes rendszerek elvárható követelményszintjeire.[297] A következő biztonsági szinteket határozza meg az ITSEC:

- Level E0

Nincs megfelelő garancia.

- Level E1

Biztonsági előirányzat (Security Target), valamint a tanúsítás tárgyának (TOE) informális leírása készül. Funkcionális tesztekkel kerül bizonyításra a biztonsági előirányzatnak való megfelelés.

- Level E2

Az E1 szintnél leírtak mellett a részletes terv leírásával is rendelkezni kell. A funkcionális tesztelés bizonyítékait is értékelni kell, valamint konfiguráció-kontroll- és elfogadott disztribúciós eljárást kell kialakítani.

- Level E3

Az E2 szinten felül forráskód illetve tervrajz biztonsági értékelést kell végezni. Ezen biztonsági mechanizmusok tesztelési bizonyítékait is értékelni kell.

- Level E4

Rendelkezni kell a biztonsági előirányzatot támogató biztonsági politika-modellel, valamint félformális stílusban kell meghatározni a biztonsági funkciókat, a magas szintű és alacsony szintű terveket.

- Level E5

A forráskód illetve tervrajz meg kell, hogy feleljen az alacsony szintű terveknek.

- Level E6

Formális stílusban kell meghatározni a biztonsági funkciókat, a magas szintű és alacsony szintű terveket, amelyek megfelelnek a biztonsági politika-modellnek.

[297] Az ITSEC szabvány, valamint a CTCPEC, FC szabványok is csak történeti jelentőségük miatt kerültek itt feltüntetésre, mai használatuk elhanyagolható mértékű.

Az ITSEC-ben meghatározásra került tíz példa funkcionális osztály, melyek rendszer-specifikus követelményeket határoznak meg. Az F-C1, F-C2, F-B1, F-B2, F-B3 példaosztályok a TCSEC osztályok funkcionális követelményeiből kerültek levezetésre. Az F-IN példa funkcionális osztály a magas adat- és program-integritási igényű értékelési tárgyakra vonatkozik, például adatbázis-kezelő rendszerekre. Az F-AV példa funkcionális osztály a magas rendelkezésre állási igényű értékelési tárgyakra vonatkozik, ipari vezérlőkhöz ajánlott. Az F-DI osztály az adatátvitel során magas adatintegritás igénylő alkalmazásokra használható. Az F-DC osztály a legnagyobb bizalmasságot biztosítja adatátvitel során, így például kriptográfiai rendszereknél alkalmazható. Az F-DX osztály magas bizalmasság és integritás igényű hálózatokra alkalmazható, így például bizalmas információ nem biztonságos hálózaton való átvitelére.

Kanadában a TCSEC és az ITSEC alapján a Communications Security Establishment elkészítette saját biztonságértékelési szabványukat, Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) néven. Az Amerikai Egyesült Államok a TCSEC 9 éves tapasztalatán 1992-ben új szabványt tervezett, a Federal Criteria-t, ami viszont soha nem került véglegesítésre.

4.2.3. Common Criteria (ISO/IEC 15408)

A fenti korai informatikai biztonsági termékszabványok után az azokat megalkotó szereplők a TCSEC, ITSEC, CTCPEC bázisán 1996-ban elkészítették a Common Criteria for Information Technology Security Evaluation, rövid nevén Common Criteria (CC) de facto szabványt. A CC az az informatikai biztonsági termékszabvány, amely ma az informatikai biztonság területén etalonnak tekinthető, a világon egyre szélesebb körben elfogadott és folyamatos fejlesztés alatt áll. 1.0-ás változatát az Európai Közösség, az Amerikai Egyesült Államok és Kanada együttesen fogadták el, 2.0-ás verziója ISO/IEC 15408 jelzettel de jure nemzetközi szabvánnyá vált. Az aktuális és a megelőző változat szabadon elérhető a http://www.commoncriteriaportal.org/ oldalról. A CC magyar érdekessége, hogy 2.0-ás változatát az Informatikai Tárcaközi Bizottság 16. számú ajánlásaként magyar nyelven közreadta, majd az MSZ ISO/IEC 15408 jelzetű szabvány is lefordításra került. Problémát jelent, hogy a de jure szabványok verziókövetése esetenként igen

lassú. A CC jelenlegi verziója a 3.1 Release 4 (2012. szeptember), az ISO/IEC szabvány kiadási ideje a kötettől függően 2009 vagy 2008, míg a magyar szabványé 2003 illetve 2002.

A szabványban a funkcionális követelmények, bizonyossági követelmények és értékelési bizonyossági szintek (EAL) mátrixaként határozhatóak meg az alkalmazandó biztonsági követelmények. A követelmények konkretizálása céljából az általános, eszköz fajtájára jellemző védelmi profilok (Protection Profile, PP) alapján biztonsági célkitűzést (Security Target, ST) kell készíteni, amely már az eszköztípusra vonatkozó követelményeket tartalmazza és ez alapján kerül megvalósításra maga a termék, a vizsgálat tárgya (Target of Evaluation, TOE).

A Common Criteria három részből áll:[298]

- Part 1: Introduction and general model (Bevezetés és általános modell[299])
- Part 2: Security functional requirements (A biztonság funkcionális követelményei)
- Part 3: Security assurance requirements (A biztonság garanciális követelményei)

A Common Criteria második kötete tizenegy funkcionális osztályt határoz meg, mely osztályokon belül a funkcionális követelmények részletezésre kerültek. Ezek a következők:[300]

- Class FAU: Security audit (Biztonsági átvilágítás)
- Class FCO: Communication (Kommunikáció)
- Class FCS: Cryptographic support (Kriptográfiai támogatás)
- Class FDP: User data protection (Felhasználói adatvédelem)
- Class FIA: Identification and authentication (Azonosítás és hitelesítés)
- Class FMT: Security management (Biztonságirányítás)
- Class FPR: Privacy (Titoktartás)
- Class FPT: Protection of the TSF (A TSF védelme)
- Class FRU: Resource utilisation (Erőforrás-felhasználás)

[298] Common Criteria for Information Technology Security Evaluation Part 1, 2006, p. 2.
[299] A magyar nyelvű megnevezések a magyar nyelvű MSZ ISO/IEC 15408 jelzetű szabványból származnak.
[300] Common Criteria for Information Technology Security Evaluation Part 2, 2009, p. 4.

- Class FTA: TOE access (TOE-hozzáférés)
- Class FTP: Trusted path/channels (Bizalmi útvonal/csatornák)

Minden osztályban több család van, és családonként több komponens, amelyeket a következő módon jelölünk: FAU_ARP.1 Minden komponens egy adott követelményt fejt ki.

„A garancia az alapja annak a bizalomnak, hogy egy IT termék vagy rendszer kielégíti biztonsági céljait. A garancia származtatható az olyan forrásokra hivatkozásból, mint a meg nem erősített állítások, az idevágó korábbi vagy speciális tapasztalatok. Azonban e szabvány az aktív vizsgálatok révén nyújt garanciát. Az aktív vizsgálat az IT termék vagy rendszer olyan értékelését jelenti, amely meghatározza annak biztonsági tulajdonságait."[301]

A vonatkozó garanciális követelmények a 2.x és a 3.x verziókban jelentős változáson estek át.

A garanciaosztályok a CC 2.1-2.3 változatában a következők:[302]

- Class ACM: Configuration management (A konfigurációmenedzselés)
- Class ADO: Delivery and operation (Kiszállítás és üzemeltetés)
- Class ADV: Development (Fejlesztés)
- Class AGD: Guidance documents (Útmutató dokumentumok)
- Class ALC: Life cycle support (Az életciklus támogatása)
- Class ATE: Tests (Vizsgálatok)
- Class AVA: Vulnerability assessment (A sebezhetőség felmérése)

A garanciaosztályok a CC 3.1 változatában a következők:[303]

- Class APE: Protection Profile evaluation (Védelmi Profil értékelése)
- Class ASE: Security Target evaluation (Biztonsági Előirányzat értékelése)
- Class ADV: Development (Fejlesztés)
- Class AGD: Guidance documents (Útmutató dokumentumok)
- Class ALC: Life cycle support (Az életciklus támogatása)
- Class ATE: Tests (Vizsgálatok)
- Class AVA: Vulnerability assessment (A sebezhetőség felmérése)
- Class ACO: Composition (Összeállítás)

[301] MSZ ISO/IEC 15408-3:2003 1.2.2.3. p. 12.
[302] Common Criteria for Information Technology Security Evaluation Part 3, 2005, p. 5.
[303] Common Criteria for Information Technology Security Evaluation Part 3, 2009, p. 5.

A követelmények teljesülésének bizonyosságát, a garanciaszintet (Evaluation Assurance Level, EAL) az ITSEC E0..E6 szintjeihez hasonlóan a CC is szintezi:[304]

- EAL1 - functionally tested (funkcionálisan vizsgálva)
- EAL2 - structurally tested (strukturálisan vizsgálva)
- EAL3 - methodically tested and checked (módszeresen vizsgálva és ellenőrizve)
- EAL4 - methodically designed, tested, and reviewed (módszeresen tervezve, vizsgálva és átnézve)
- EAL5 - semi formally designed and tested (félformálisan tervezve és vizsgálva)
- EAL6 - semi formally verified design and tested (félformálisan igazolt módon tervezve és vizsgálva)
- EAL7 - formally verified design and tested (formálisan igazolt módon tervezve és vizsgálva)

A Common Criteria szerinti vizsgálatok végrehajtását támogatja a Common Methodology for Information Technology Security Evaluation (CEM), amely részletes módszertani útmutatóként egységes metodológiát határoz meg a vizsgálatokhoz. Ez is megjelent nemzetközi szabványként ISO/IEC 18045:2008 jelzettel.

Jelenleg a terméktanúsítási szabványok közül a Common Criteria a leginkább elterjedt, különösen az európai terméktanúsításban piacvezető Németországban.[305]

[304] Ibid. pp. 5-6.
[305] Spindler, 2007, p. 68.

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

7. ábra: EAL összegzés[306]

4.2.4. ITIL (ISO/IEC 20000)

Az IT Infrastructure Library (ITIL), bár elsősorban informatikai üzemeltetésére és fejlesztésére szolgáló módszertani gyűjtemény, folyamatszabvány és nem biztonsági szabvány, előírásaiban érinti a biztonsági területet. Nemzetközi legjobb gyakorlatként az IT szolgáltatások területén szolgál követelményhalmazként. A 80-as években alkotta az Egyesült Királysági Central Computing and Telecommunications Agency (CCTA), legutóbbi változata a 2011 edition. Jelenleg az AXELOS Ltd. gondozza. Brit nemzeti szabványként BS 15000 jelzettel, majd nemzetközi szabványként ISO/IEC 20000 jelzettel, több kötetben jelent meg, ez azonban nem azonos az ITIL-lel. Amíg az ITIL egy jó gyakorlatokról szóló irányelv (best practice guide), addig az ISO

[306] Common Criteria for Information Technology Security Evaluation Part 3, 2009. p. 31. 1. táblázat

20000 az ezekből levezetett kötelező minimumkövetelmények, amelyek minimálisan elvárhatóak az IT szolgáltatások biztosítása terén. Céljaik és gyökerük viszont azonos, így azokat célszerű együtt kezelni.

Az ITIL célja a jó minőségű, költséghatékony IT szolgáltatások támogatása, a minőségügyben ismert Plan-Do-Check-Act (PDCA) elv alkalmazásával. A biztonsági követelmények elsősorban IT szolgáltatás-folytonossági követelményként kerültek be a keretrendszerbe. A szűken vett információbiztonsági kontrollok tekintetében egy alfejezetben[307] tartalmaz előírásokat, valamint javasolja az ISO/IEC 17799 (ma már ISO/IEC 27002) alkalmazását.

Az ITIL öt kötetből áll, melyek a következők:[308]

- Szolgáltatás-stratégia (Service Strategy): A bevezetendő informatikai szolgáltatások által kiaknázható piaci lehetőségeket lehet kiválasztani a folyamat keretében. A kiválasztás során stratégiai terv készül, amely bemutatja a tervezés, implementáció, üzemeltetés és a folyamatos fejlesztés lépéseit és ezek összefüggéseit. Az új szolgáltatás értéknövelő szerepű. A könyv legfontosabb részei a Szolgáltatás-portfólió kezelése és Pénzügyi menedzsmentje.
- Szolgáltatás-tervezés (Service Design): Az elkészült stratégiában foglaltak megvalósítására projektterv készül a tervezett szolgáltatás gyakorlati megvalósítására. A tervben megtalálható a bevezetés minden lépése, valamint a konkrét bevezetéshez kapcsolódó más átalakítandó folyamatok megnevezése. Legfontosabb fejezetei az Üzemeltetés és üzemvitel biztosítása, Kapacitástervezés valamint az Informatikai- és üzembiztonság. Ezen fejezetek miatt tekintjük a szabványt (részben) informatikai biztonsági jellegűnek.
- Szolgáltatás-létesítés és változtatás (Service Transition): A gyakorlati bevezetés lépéseit tartalmazza, különös tekintettel az előző fejezetben megnevezett módosítandó kapcsolódó és érintett folyamatokra. Lényegi részei a Változás- és verziókezelés, Konfiguráció-menedzsment és Dokumentáció-kezelés.
- Szolgáltatás-üzemeltetés (Service Operation): Az előző kötet alapján létesített rendszer üzemeltetésének folytonosságáról és a hibamentesség biztosításáról szól. Ehhez meghatározott folyamatokat és adminisztratív intézkedéseket kell

[307] ISO/IEC 20000-2:2005, 6.6 Information security management
[308] ITIL edition 2011 Service Strategy 1.2.3

bevezetni. Az elvárt rendelkezésre állási követelményeket szolgáltatási szint-megállapodás (SLA) rögzíti, amelynek betartatása az elődleges célja a kötetnek. Fő fejezetei a Hiba- és igény- és incidenskezelés.

- Állandó szolgáltatás-fejlesztés (Continual Service Improvement): A folyamatos, PDCA-elvet követő minőségjavításról szóló kötet, legfontosabb részei a Szolgáltatási szint mérése, jelentése és menedzsmentje című fejezetek.

Az ISO/IEC 20000 szabvány kötetei a következők:

- ISO/IEC 20000-1:2011 Service management system requirements
- ISO/IEC 20000-2:2012 Guidance on the application of service management systems
- ISO/IEC 20000-3:2012 Guidance on scope definition and applicability of ISO/IEC 20000-1
- ISO/IEC TR 20000-4:2010 Process reference model
- ISO/IEC TR 20000-5:2013 Exemplar implementation plan for ISO/IEC 20000-1
- ISO/IEC 20000-6:2017 Requirements for bodies providing audit and certification of service management systems
- ISO/IEC TR 20000-9:2015 Guidance on the application of ISO/IEC 20000-1 to cloud services
- ISO/IEC TR 20000-10:2013 Concepts and terminology
- ISO/IEC TR 20000-11:2015 Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: ITIL®
- ISO/IEC TR 20000-12:2016 Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: CMMI-SVC

A fentiek közül magyar szabványként az alábbiak jelentek meg:

- MSZ ISO/IEC 20000-1:2013 Informatika. Szolgáltatásirányítás. 1. rész: A szolgáltatásirányítási rendszer követelményei

4.2.5. ISO/IEC 27000 szabványsorozat

Szintén a szigetországból indult egy szabványcsalád, amely mára széles körben ismertté és alkalmazottá vált. 1995-ben a Department of Trade and Industry (DTI) által készített BS 7799 jelzetű szabvány informatikai biztonsági követelményeket foglalt össze, melyek menedzsment szinten alkalmazhatók. Ez nemzetközi szabvánnyá vált ISO/IEC 17799 jelzettel. A BS 7799-2, mint az információbiztonsági irányítási rendszerre vonatkozó szabvány 1999-ben került kifejlesztésre és csatolásra a korábbi BS 7799-hez, amely BS 7799-1-re lett átszámozva, majd ISO/IEC 27001 jelezettel került a nemzetközi porondra, ami után az ISO/IEC 17799-et szintén átszámozták ISO/IEC 27002-re[309] és beindult egy irányítási rendszer szabványcsalád kifejlesztése az ISO 9000-es sorozathoz hasonlóan. A kezdeti szabvány különlegessége volt, hogy fentről-lefelé, az üzleti igényekből határozta meg a biztonsági követelményeket. Az ISO/IEC 27001 abból a célból készült, hogy modellként szolgáljon információbiztonsági irányítási rendszerek (ISMS, IBIR) kialakításához, megvalósításához, működtetéséhez, figyelemmel kíséréséhez, átvizsgálásához, fenntartásához és fejlesztéséhez.[310] A szabvány folyamatközpontú, alkalmazza a Plan-Do-Check-Act (PDCA) modellt és a megvalósított IBIR integrálható a meglévő minőségirányítási (ISO 9001) és a környezetirányítási (ISO 14001) rendszerekkel. A követelmények értelmezése tekintetében célszerű az ISO/IEC 27002 szabvány alkalmazása.

Az ISO/IEC 27000 szabványsorozat publikált és előkészítés alatt álló tagjai:

- ISO/IEC 27000:2016 Information security management systems – Overview and vocabulary: áttekintés és szótár, ismerteti a szabványsorozat főbb elveit és meghatározza a kulcsfogalmakat
- ISO/IEC 27001:2013 Information security management systems – Requirements: a korábban ismertetettek szerint a menedzsment rendszer követelményeit írja le
- ISO/IEC 27002:2013 Code of practice for information security controls: a korábban ismertetettek szerint a gyakorlat követelményeit írja le

[309] A magyar szabvány ezt az átszámozást nem követte, jelenleg is MSZ ISO/IEC 17799:2006 jelzetű, valamint a 27000-es sorozat többi tagja (az MSZ ISO/IEC 27001-en kívül) sem jelent még meg magyar szabványként.
[310] MSZ ISO/IEC 27001:2006 p. 19.

- ISO/IEC 27003:2017 Information security management systems - Guidance: a bevezetésre vonatkozó iránymutatásokat tartalmazza
- ISO/IEC 27004:2016 Information security management – Measurement: a biztonság szintjének mérésével foglalkozik
- ISO/IEC 27005:2011 Information security risk management: a kockázatmenedzsment egy ajánlott keretrendszerétismerteti, az ISO/IEC 13335-3 és az ISO/IEC 13335-4 szabványokból került kifejlesztésre, kompatibilis az ISO 31000:2009 általános kockázatmenedzsment irányelvvel.
- ISO/IEC 27006:2015 Requirements for bodies providing audit and certification of information security management systems: az ISO/IEC 27001 alapján tanúsítást végző szervezetekre vonatkozó követelményeket határozza meg
- ISO/IEC 27007:2017 Guidelines for information security management systems auditing: az auditálás módszertanára vonatkozó iránymutatást tartalmazza
- ISO/IEC TR 27008:2011 Guidelines for auditors on IS controls: az auditoroknak nyújt iránymutatást a helyes ISO/IEC 27002 szerinti kontrollokról
- ISO/IEC 27009:2017 Sector-specific application of ISO/IEC 27001 – Requirements: a különböző gazdasági szerktorokban alkalmazandó spreciális szabályokra vonatkozó követelményeket tartalmazza
- ISO/IEC 27010:2015 Information security management for inter-sector and inter-organizational communications: a szervezetek és a különböző szektorok közötti bizalmas információ-megosztásra ad iránymutatást, különös tekintettel a kritikus infrastruktúrák közötti adatkezelésre.
- ISO/IEC 27011:2016 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002: a hírközlési szolgáltatókra vonatkozó különleges követelményeket tartalmazza
- ISO/IEC 27013:2015 Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001: a szabvány iránymutatást nyújt az ISO/IEC 20000-1 (vö. ITIL) és az ISO/IEC 27001 szerinti IBIR integrált bevezetésére

- ISO/IEC 27014:2013 Governance of information security: Az információbiztonság irányítására vonatkozó irányelveket mutatja be (vö. COBIT)
- ISO/IEC 27015:2012 (Visszavonva!) Information security management guidelines for financial services: Az ISO/IEC 27002:2005 kiegészítése képpen iránymutatást ad a pénzügyi szektorban kialakítandó biztonsági kontrollokra
- ISO/IEC TR 27016:2014 Organizational economics: A szervezetek döntéshozatalára vonatkozó javaslatokat tartalmaz
- ISO/IEC 27018:2014 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors: személyesadat-feldolgozást végző nyilvános felhőszolgáltatásokra fogalmaz meg követelményeket
- ISO/IEC 27019:2017 Information security controls for the energy utility industry: Kiterjeszti a 27000-es sorozat hatókörét a folyamatszabályozásra és automatikára, az energiaszolgáltatók (beleértve a villamosenergia-, gáz- és hőszolgáltatást) digitális rendszereinek (a védelmi reléktől a PLC-ken át a vezérlőközpontokig) védelmében.
- ISO/IEC 27021:2017 Competence requirements for information security management systems professionals: a szakemberekre vonatkozó kompetenciakövetelményeket fogalmazza meg
- ISO/IEC TR 27023:2015 Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002: A szabványváltozások követhetőségét segíti elő
- ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity: Az informatikai és kommunikációs szolgáltatások üzletmenet-folytonossági felkészítésére mutat be keretrendszert és folyamatokat.
- ISO/IEC 27032:2012 Guidelines for cybersecurity: iránymutatásokat fogalmaz meg a kiberbiztonság növelése érdekében, ami magában foglalja az információ- ,hálózat- és internetbiztonságot, valamint a kritikus információs infrastruktúrák védelmét.
- ISO/IEC 27033-1:2015 Network security: Overview and concepts: A szabvány áttekintést nyújt a hálózati biztonságról, valamint ismerteti a tématerülethez kapcsolódó definíciókat

- ISO/IEC 27033-2:2012 Network security: Guidelines for the design and implementation of network security: Iránymutatást nyújt szervezeteknek a hálózati biztonság tervezésére, kivetelezésére és dokumentációjára
- ISO/IEC 27033-3:2010 Network security: Threats, design techniques and control issues: a szabvány bemutatja a veszélyeket, tervezési technikákat és a kontrollokra vonatkozó kérdéseket különféle példákon keresztül
- ISO/IEC 27033-5:2013 Securing communications across networks using Virtual Private Networks (VPNs): a szabvány a virtuális magánhálózatok (VPN) biztonságossá tételéhez nyújt iránymutatásokat
- ISO/IEC 27034-1:2011 Application security. Overview and concepts: Alkalmazásbiztonsági fogalmak, koncepciók, irányelvek. Egy készülőben lévő hétkötetes sorozat első eleme.
- ISO/IEC 27034-2:2015 Application security. Organization normative framework: Szervezeti keretek.
- ISO/IEC 27034-5:2017 Application security Part 5: Protocols and application security controls data structure: Adatstruktúrát határoz meg protokollokhoz és alkalmazásbiztonsági kontrollokhoz
- ISO/IEC 27034-6:2016 Application security Part 6: Case studies: Szoftverek biztonsági követelményeire fogalmaz meg esettanulmányokat
- ISO/IEC 27035-1:2016 Information security incident management – Part 1: Principles of incident management: Irányelv az informatikai biztonsági incidens-menedzsment strukturált és tervezett megvalósítására, elsősorban közepes- és nagyvállalatok számára (ez magyar viszonylatban csak nagyvállalatokra ajánlott).
- ISO/IEC 27035-2:2016 Information security incident management – Part 2: Guidelines to plan and prepare for incident response: Incidenskezelési tervezéshez nyújt iránymutatást
- ISO/IEC 27036-1:2014 Information security for supplier relationships – Part 1: Overview and concepts: A beszállítói kapcsolatok információbiztonsági kérdéseit tekinti át, koncepciót fogalmaz meg
- ISO/IEC 27036-2:2014 Information security for supplier relationships – Part 2: Requirements: A beszállítói kapcsolatok információbiztonsági követelményeit fogalmazza meg

- ISO/IEC 27036-3:2013 Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security: Az IT ellátási láncok biztonságával kapcsolatos ajánlásokat fogalmaz meg
- ISO/IEC 27036-4:2016 Information security for supplier relationships – Part 4: Guidelines for security of cloud services: A felhőszolgáltó, mint beszállítói kapcsolat
- ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence: az igazságügyi informatika (digital forensics) számára nyújt iránymutatást a digitális nyomok azonosítására, rögzítésére és megőrzésére
- ISO/IEC 27038:2014 Specification for digital redaction: A dokumentumok szerkesztésével, anonimizálásával foglalkozó spefikáció
- ISO/IEC 27039:2015 Selection, deployment and operations of intrusion detection and prevention systems (IDPS). Behatolás-jelző (IDS) és behatolás-elhárító (IPS) rendszerek kiválasztása, telepítése, működtetése.
- ISO/IEC 27040:2015 Storage security. Adattárolás, háttértárak biztonsága.
- ISO/IEC 27041:2015 Guidance on assuring suitability and adequacy of incident investigative method: incidensek kivizsgálásának módszertanai
- ISO/IEC 27042:2015 Guidelines for the analysis and interpretation of digital evidence: Digitális bizonyítékok analízise és értelmezése
- ISO/IEC 27043:2015 Incident investigation principles and processes: incidensek kivizsgálásának elve és folyamata
- ISO 27799:2016 Health informatics – Information security management in health using ISO/IEC 27002: az egészségügyi szolgáltatókra vonatkozó különleges követelményeket tartalmazza

A fentiek közül magyar szabványként csak az alábbiak jelentek meg:

- MSZ EN ISO/IEC 27000:2017 Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Áttekintés és szakszótár (ISO/IEC 27000:2016) angol nyelvű szabvány, aminek ebben a formában nem sok értelme van
- MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények

- MSZ ISO/IEC 27002:2017 Informatika. Biztonságtechnika. Gyakorlati útmutató az információbiztonsági kontrollokhoz/intézkedésekhez (ISO/IEC 27002:2013, tartalmazza a 2014. évi 1. és a 2015. évi 2. helyesbítést) angol nyelvű szabvány
- MSZ ISO/IEC 27006:2017 Informatika. Biztonságtechnika. Követelmények információbiztonsági irányítási rendszerek auditját és tanúsítását végző szervezetekre

Az MSZ ISO/IEC 27001:2014 szabvány fejezetei a következők:

0. Bevezetés
1. Alkalmazási terület
2. Rendelkező hivatkozások
3. Szakkifejezések és meghatározásuk
4. A szervezet és környezete
5. Vezetés
6. Tervezés
7. Támogatás
8. Működés
9. Teljesítményértékelés
10. Fejlesztés

A melléklet (előírás): Hivatkozásul szolgáló intézkedési célok és intézkedések

Tekintettel arra, hogy a szabványnak való megfelelőség tanúsítható, az arról szóló tanúsítvány üzleti előnyt jelenthet a cégnek. Mivel a tanúsításokat magáncégek végzik és kötelező regiszter nem létezik, ezért a világszerte vagy akár a Magyarországon tanúsított cégek pontos számának megállapítása szinte lehetetlen. Van azonban egy olyan nemzetközi regiszter, amelybe a legnagyobb tanúsítók (pl. BSI, Bureau Veritas, DNV, KPMG, LRQA, SGS, TÜV) önkéntesen bejelentik a kiadott tanúsítványaikat. Jelenleg a világon e regiszter szerint 6826 db ISO 27001 kiadott tanúsítvány van. Ezek országonkénti bontásban 2010-ben a következők voltak:[311]

[311] International Register of ISMS Certificates. http://www.iso27001certificates.com/ [2010. 10. 17.] Version 201 September 2010

Japan	3632	Philippines	15	Macau	3
India	492	Pakistan	14	Portugal	3
China	483	Vietnam	14	Argentina	2
UK	453	Iceland	13	Belgium	2
Taiwan	371	Saudi Arabia	13	Bosnia Herzegovina	2
Germany	139	Netherlands	12	Cyprus	2
Korea	106	Singapore	12	Isle of Man	2
USA	96	Indonesia	11	Kazakhstan	2
Czech Republic	86	Bulgaria	10	Morocco	2
Hungary	71	Kuwait	10	Ukraine	2
Italy	60	Norway	10	Armenia	1
Poland	56	Russian Federation	10	Bangladesh	1
Spain	54	Sweden	9	Belarus	1
Malaysia	40	Colombia	8	Denmark	1
Ireland	37	Bahrain	7	Dominican Rep.	1
Thailand	36	Iran	7	Jersey	1
Austria	35	Switzerland	7	Kyrgyzstan	1
Hong Kong	32	Canada	6	Lebanon	1
Greece	30	Croatia	6	Luxembourg	1
Romania	30	South Africa	5	Macedonia	1
Australia	29	Sri Lanka	5	Mauritius	1
Mexico	24	Lithuania	4	Moldova	1
Brazil	23	Oman	4	New Zealand	1
Slovakia	21	Peru	4	Sudan	1
Turkey	21	Qatar	4	Uruguay	1
UAE	20	Chile	3	Yemen	1
France	19	Egypt	3		
Slovenia	17	Gibraltar	3		

Sajnos ez az utolsó ismert széles körű gyűjtés, ugyanis 2010 folyamán a hivatkozott honlap megszűnt és azóta sem fellelnető pontos kimutatás.

Ezek a fenti értékek természetesen a fentebb részletezett okok miatt nem megbízhatóak, viszont arányaikban helyesnek tekinthetők. Így a listán a világranglistában tízedik helyünk meglepően jó eredmény.
A kiadott tanúsítványok darabszáma nem egyenlő a tanúsított szervezetek számával. Egy szervezet számára ugyanis több külön tanúsítvány kiadható hatóköri, telephelyi vagy időbeli érvényességi okokból. A tanúsított szervezetek listája szintén lekérdezhető a regiszterből. Ez a lista és a kutatás alapján történő bővítése összesen 98 szervezet 103 tanúsítványát tartalmazza, amely így valós értékhez jobban közelít.

A Hétpecsét Információbiztonsági Egyesület[312] évente információt kér a Magyarországon működő tanúsítóktól a sikeresen lezárt auditok darabszámáról a tanúsított szervezet nevének közlése nélkül. Az adatgyűjtés célja az ISO/IEC 27001 szabvány hazai elterjedtségének vizsgálata. A 13 tanúsító cég nyilatkozatai szerint 2010 januárjáig 138 sikeres auditon átesett magyarországi cég van, ami a 2009. januári 131 céghez képest öt százalékos növekedést jelent. A sikeresebb tanúsítók között a piaci részesedés eloszlása: SGS 35%, CERTOP 14%, DNV 12%.[313] Minden bizonnyal ezen felmérés értékei a legpontosabbak, hátránya viszont, hogy a cégnevek nem ismertek. A cégnevek ismerete azért lenne fontos, mert a tanúsítvány fő értéket maga a tanúsító szervezet adja az adott szektorban. Tehát ha az élelmiszeripari cégek túlnyomó részét egy cég tanúsította, akkor az iparágon belül az a tanúsítvány a leginkább elfogadott. Ha egy új belépő másik céggel tanúsíttatja magát, lehet, hogy az iparágon belül (pl. beszállítók, partnerek) nem fogadják el a tanúsítványát.[314]

Az információbiztonság-irányítási rendszer keretében a kockázatelemzés során meg kell határozni, hogy az egyes fenyegetések mely rendszerelemekre hatnak. Az elemzés során szükséges megbecsülni, hogy az egyes fenyegetések várhatóan milyen gyakorisággal, mekkora valószínűséggel fognak bekövetkezni. Másik fontos szempont, hogy a már bekövetkezett esemény károkozásának forintban kifejezett mértéke várhatóan mekkora lesz. E két szempont egymáshoz való viszonya rajzolja ki a kockázati mátrixot. A konkrét fenyegetések a rendszerelemekre hatnak, így a

[312] http://hetpecset.hu/ [2010. 05. 10.]
[313] Bitport, 2010.
[314] Horváth Zsolt, 2008.

védelmi intézkedésekkel is ezeket kell megcélozni. A védelem teljes körűsége érdekében minden lehetséges rendszerelemet figyelembe kell venni és értékelni kell.

A szabvány alkalmazása önmagában nem elégséges egy teljes kockázatelemzés elvégzéséhez, így egy olyan módszertan alkalmazása szükséges, amely kitölti a szabvány által maghatározott kereteket. Ilyen kockázatelemzési módszertan például az ISO/IEC 27005 szabványon alapuló francia MEHARI,[315] amely egységes veszélyforrás-meghatározásokat, tapasztalati alapon előre kalkulált valószínűségeket és számított kárhatásokat tartalmaz, egységessé és kiszámíthatóvá téve a kockázatelemzési eredményeket. A gyakorlati megvalósítás például a MEHARI-Risk szoftverrel[316] történhet, amely egyszerűsíti az adatbevitelt és megkíméli a kockázatelemzést végző személyt a bonyolult számítások elvégzésétől.
A kárérték-besorolási és kárgyakorisági osztályozások a MEHARI-ban az alábbiak:

A MEHARI hatásszintjei (MEHARI Impact levels)

- Nagyon alacsony hatású (very low impact)
- Alacsony hatású (low impact)
- Közepes hatású (medium impact)
- Magas hatású (high impact)

A MEHARI gyakoriság szintjei (Exposure levels MEHARI)

- Nagyon alacsony gyakoriság (very low exposure)
- Alacsony gyakoriság (low exposure)
- Közepes gyakoriság (medium exposure)
- Magas gyakoriság (high exposure)

A MEHARI-nál a következő, a kalkulációhoz felhasznált bemenő adatok és részeredmények vannak:

Jelleg	MEHARI

[315] http://www.clusif.asso.fr/en/production/mehari/ [2011. 02. 11.]
[316] http://www.mehari-risk.com/ [2011. 02. 11.]

Valószínűségi tényezők	STATUS-EXPO Natural exposure (1..4) Az esemény bekövetkezésének valószínűsége védekezés nélkül.
	STATUS-DISS Effectiveness of dissuasive measures (1..4) Az esemény elleni védekezés eltérítési hatékonysága.
	STATUS-PALL Effectiveness of palliative measures (1..4) Az esemény elleni védekezés tompítási hatékonysága.
	STATUS-PREV Effectiveness of preventive measures (1..4) Az esemény elleni védekezés megelőzési hatékonysága.
	STATUS-PROT Effectiveness of protective measures (1..4) Az esemény elleni védekezés kivédési hatékonysága.
	STATUS-RECUP Effectiveness of recuperative measures (1..4) Az esemény elleni védekezés tompítási hatékonysága. Az esemény elleni védekezés helyrehozási hatékonysága.
	STATUS-P Potentiality of event described by risk scenario (1..4) Az esemény bekövetkezésének valószínűségéből és az esemény elleni védekezések hatékonyságából számított bekövetkezési valószínűség.
Kockázati szint tényezők	Availability (1..4) Rendelkezésre állási szinttel szembeni elvárás mértéke.
	Confidentiality (1..4) Bizalmassági szinttel szembeni elvárás mértéke.
	Integrity (1..4) Sértetlenség, integritás szintjével szembeni elvárás mértéke.
	STATUS-RI Impact reduction (1..4) Hatást csökkentő tényezők.
	STATUS-I Impact (1..4) Eredő hatás: az elvárásokból

	és a hatást csökkentő tényezőkből kerül kiszámításra. Nincs pénzben mért kárérték tényező a MEHARI-ban.
Értékelési eredmény	SERIOUSNESS Risk seriousness for specific scenario (1..4) Az adott esemény súlyossága kockázatok az ellenintézkedésekkel csökkentve, tehát maradványkockázat.

4.2.6. COBIT

Az Information Systems Audit and Control Association (ISACA), mint nemzetközi szinten elismert amerikai IT auditor egyesület és az IT Governance Institute (ITGI) együtt 1992-ben kifejlesztették a Control Objectives for Information and Related Technology (COBIT) de facto informatikai biztonsági szabványt, mint az IT vezetés keretrendszerét. Ebben több információs folyamatra írtak elő követelményeket. A COBIT az ITIL-hez hasonlóan egy bevált gyakorlat-gyűjtemény, tulajdonképpen informatikai auditálási, vezetéstámogatási módszertan, ami üzleti követelményeken alapul. Soha nem vált de jure szabvánnyá, valamint nem is lehet az annak való megfelelést tanúsítani. A COBIT 4.1 verziója 34 magas szintű folyamatot, ezen belül 210 kontroll célkitűzést tartalmaz, amelyek négy szakterület köré csoportosulnak:

- Tervezés és szervezés (Planning and Organization)
- Beszerzés és megvalósítás (Acquisition and Implementation)
- Szolgáltatás és támogatás (Delivery and Support)
- Figyelemmel kísérés és értékelés (Monitoring and Evaluation)

A COBIT 4.1 folyamatok a következők:[317]

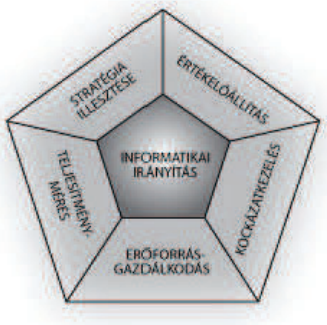
- Tervezés és szervezés (Planning and Organization)
  - PO1 Az informatikai stratégiai terv meghatározása
  - PO2 Az információ-architektúra meghatározása
  - PO3 A technológiai irány kijelölése
  - PO4 Az informatikai folyamatok, szervezet és a kapcsolatok meghatározása
  - PO5 Az informatikai beruházások irányítása
  - PO6 Tájékoztatás a vezetői célokról és irányról

[317] Source: COBIT 4.1. ©1996-2007 ITGI. All rights reserved. Used by permission.

- PO7 Az informatikai humán erőforrások kezelése
- PO8 Minőségirányítás
- PO9 Az informatikai kockázatok felmérése és kezelése
- PO10 A projektek irányítása

- Beszerzés és megvalósítás (Acquisition and Implementation)
  - AI1 Az automatizált megoldások meghatározása
  - AI2 Az alkalmazási szoftverek beszerzése és karbantartása
  - AI3 A technológiai infrastruktúra beszerzése és karbantartása
  - AI4 Az üzemeltetés és a használat támogatása
  - AI5 Az informatikai erőforrások beszerzése
  - AI6 A változtatások kezelése
  - AI7 A megoldások és változtatások üzembe helyezése és bevizsgálása
- Szolgáltatás és támogatás (Delivery and Support)
  - DS1 A szolgáltatási szintek meghatározása és betartása
  - DS2 Külső szolgáltatások igénybevételének irányítása
  - DS3 Teljesítmény- és kapacitáskezelés
  - DS4 A szolgáltatás folyamatosságának biztosítása
  - DS5 A rendszerek biztonságának megvalósítása
  - DS6 A költségek azonosítása és felosztása
  - DS7 A felhasználók oktatása és képzése
  - DS8 A rendkívüli események kezelése és a felhasználói támogatás működtetése
  - DS9 Konfigurációkezelés
  - DS10 Problémakezelés
  - DS11 Az adatok kezelése
  - DS12 A fizikai környezet biztosítása
  - DS13 Az üzemeltetés irányítása
- Figyelemmel kísérés és értékelés (Monitoring and Evaluation)
  - ME1 Az informatika teljesítményének figyelemmel kísérése és értékelése
  - ME2 A belső irányítási és ellenőrzési rendszer figyelemmel kísérése és értékelése
  - ME3 Külső követelményeknek való megfelelőség biztosítása

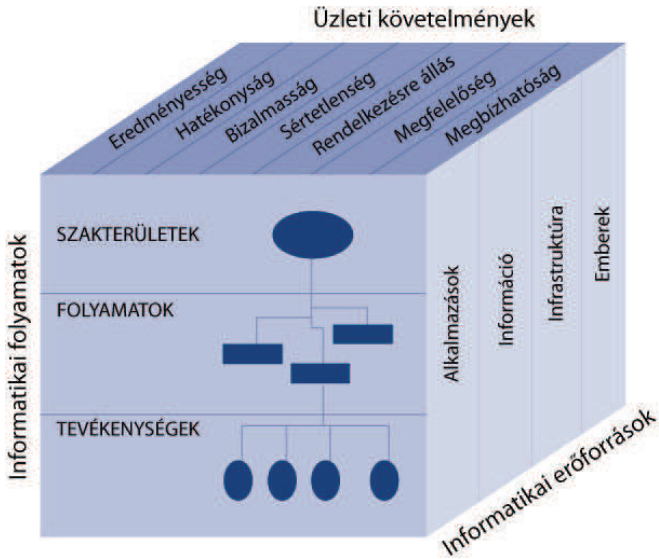
° ME4 Az informatikai irányítás megteremtése

	• A **stratégia illesztése** az üzleti területek, és az informatika terveinek illesztésére; az informatikai érték előállítására vonatkozó ajánlat meghatározására, aktualizálására, és érvényesítésére; valamint az informatikai működés és a vállalati működés illesztésére összpontosít. • **Érték-előállítás** (hasznosság, használati érték): a termelési ciklus során a tervezett többletérték létrehozásával foglalkozik, gondoskodva arról, hogy az informatika a stratégiai tervben meghatározott hasznokat megtermelje, koncentrálva a költségek optimalizálására és arra, hogy az informatika a belső értékét bizonyítsa. • Az **erőforrás-gazdálkodásnak** az a lényege, hogy a létfontosságú informatikai erőforrásokba – alkalmazásokba, információfeldolgozásba, infrastruktúrába és az emberekbe történő befektetés optimális legyen, és azokkal megfelelően gazdálkodjanak. Kulcsfontosságú kérdései a tudás és az infrastruktúra optimalizálásával kapcsolatosak. • A **kockázatkezelés**hez szükség van arra, hogy a szervezet felső vezetői tisztában legyenek a kockázatokkal, hogy egyértelmű legyen a vállalat kockázatvállalási hajlandósága, hogy tisztában legyenek a megfelelőségi követelményekkel, hogy ismertek legyenek a vállalat jelentős kockázatai, és hogy a kockázatkezelési felelősséget beépítsék a szervezetbe. • A **teljesítménymérés** nyomon követi és figyelemmel kíséri a stratégia megvalósítását, a projektek befejezését, az erőforrások felhasználást, a folyamatok teljesítményét és a szolgáltatás biztosítását, felhasználva például a kiegyensúlyozott stratégiai mutatószám rendszert, amely lefordítja a stratégiát tevékenységekre a hagyományos számvitel i mutatókkal nem mérhető célok elérése érdekében.

8. ábra:[318] Az informatikai irányítás központi területei

A COBIT nagy figyelmet fordít az informatikai irányítás elméleti hátterére, így több aspektusból elemzi az informatikai irányítás lényegét és területeit, valamint a különböző követelmények egymásra hatását és összefüggéseit. Példa ezekre az informatikai irányítás központi területeit bemutató 8. ábra, amelyen minden egyes folyamat ismertetésekor kiemelésre kerülnek az érintett területek, valamint a 9. ábrán bemutatott COBIT kocka, amely a COBIT által lefedett három dimenziót, az üzleti követelmények – informatikai folyamatok – informatikai erőforrások dimenzióit és azok elemeit mutatja be.

Annak ellenére, hogy a COBIT-nek nem deklarált célja más szabványokkal való együttműködés, több megfeleltetés készült az ISACA szervezésében, például az ITIL, ISO/IEC 27002 és PMBOK szabványokkal.



9. ábra:[319] COBIT kocka

[318] Source: COBIT 4.1. ©1996-2007 ITGI. All rights reserved. Used by permission.
[319] Source: COBIT 4.1. ©1996-2007 ITGI. All rights reserved. Used by permission.

Mivel a COBIT szerint nincsen lehetőség tanúsításra, ezért elterjedtségének mértékére nincsen hiteles adat. Tény viszont az, hogy a COBIT-ra épülő Certified Information Systems Auditor (CISA) és Certified Information Security Manager (CISM) szakvizsgák világszerte széles körben, valamint az Amerikai Egyesült Államok Védelmi Minisztériuma (DoD) által is elismert[320] informatikai biztonsági szakvizsgák. A COBIT Magyarországon a pénzügyi szektorban elsődlegesen követett szabvány.

A COBIT legújabb, ötödik kiadása magába foglalja a COBIT 4.1-et, a Val IT 2.0-t[321] és a Risk IT keretrendszereket, valamint jelentős mértékben hatással van rá a Business Model for Information Security (BMIS)[322] az Information Technology Assurance Framework (ITAF)[323]. A COBIT 5 szemléletében és a hatókörében is bővült a 4.1-hez képest, ugyanis a korábbi informatikai irányítás (IT Governance) hatókörét az érdekelt csoportok (stakeholtders) igényeivel bővítve már nagyvállalati informatikai irányításról (Governance of Enterprise IT) beszélhetünk. Többek között a folyamatok és a kontroll célkitűzések is bővültek, módosultak.

A COBIT 5 folyamatai:

- Értékelés, irányítás és figyelemmel kísérés (Evaluate, Direct and Monitor, EDM)
- Összehangolás, tervezés és szervezés (Align, Plan and Organise, APO)
- Építés, beszerzés és megvalósítás (Build, Acquire and Implement, BAI)
- Szállítás, szolgáltatás és támogatás (Deliver, Service and Support, DSS)
- Figyelemmel kísérés, értékelés és felmérés (Monitor, Evaluate and Assess, MEA)

4.2.7. Tanúsítás, ellenintézkedések, termékszabványok

A tanúsítási tevékenységre több szabvány vonatkozik, ilyenek például:

[320] Department of Defense Directive 8570
[321] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Val-IT-Framework-2.0.aspx [2013. 07.28.]
[322] http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx [2013. 07.28.]
[323] www.isaca.org/itaf [2013. 07.28.]

- MSZ EN ISO/IEC 17021-1:2016 Megfelelőségértékelés. Irányítási rendszerek auditját és tanúsítását végző testületekre vonatkozó követelmények. 1. rész: Követelmények (ISO/IEC 17021-1:2015)
- MSZ ISO/IEC TS 17021-2:2013 Megfelelőségértékelés. Irányítási rendszerek auditját és tanúsítását végző testületekre vonatkozó követelmények. 2. rész: Kompetenciakövetelmények környezetközpontú irányítási rendszerek auditálásához és tanúsításához
- MSZ ISO/IEC TS 17021-3:2014 Megfelelőségértékelés. Irányítási rendszerek auditját és tanúsítását végző testületekre vonatkozó követelmények. 3. rész: Kompetenciakövetelmények minőségirányítási rendszerek auditálásához és tanúsításához
- MSZ EN ISO 19011:2012 Útmutató irányítási rendszerek auditálásához (ISO 19011:2011)
- MSZ ISO/IEC 27006:2017 Informatika. Biztonságtechnika. Követelmények információbiztonsági irányítási rendszerek auditját és tanúsítását végző szervezetekre
- MSZ EN ISO/IEC 17024:2013 Megfelelőségértékelés. Személyek tanúsítását végző testületek általános követelményei (ISO/IEC 17024:2012)
- MSZ EN ISO/IEC 17025:2005 Vizsgáló- és kalibrálólaboratóriumok felkészültségének általános követelményei (ISO/IEC 17025:2005)
- MSZ EN ISO/IEC 17065:2013 Megfelelőségértékelés. Termékek, folyamatok és szolgáltatások tanúsítását végző szervezetekre vonatkozó követelmények (ISO/IEC 17065:2012)

A megfelelő szabványok alkalmazása a tanúsító szervek számára kötelező, ezek megfelelő alkalmazását értékeli a nemzeti akkreditáló szerv, Magyarországon a Nemzeti Akkreditáló Testület.

Amiből viszont olyan sok van, hogy a felsorolásuk is szinte lehetetlen: a műszaki szabványok és leírások. Ezeknek az alkalmazása konkrét technológiai megvalósításkor, elsősorban termékek tervezésekor, gyártásakor szükséges. Természetesen az ezeknek való megfelelés is ellenőrizhető a tanúsítás során. A teljesség igénye nélkül tehát pár példaként szolgáló szabvány:

- MSZ ISO/IEC 15816:2005 Informatika. Biztonságtechnika. A hozzáférés-ellenőrzés biztonsági információobjektumai
- MSZ ISO/IEC 15945:2002 Informatika. Biztonságtechnika. Ajánlás/nemzetközi szabvány bizalmi harmadik fél (TTP) digitális aláírások alkalmazását támogató szolgáltatásaira
- CEN CWA 14168:2001 Secure Signature-Creation Devices "EAL 4"
- CEN CWA 14169:2004 Secure Signature-Creation Devices "EAL 4+"
- CEN CWA 14170:2004 Security Requirements for Signature Creation Applications
- CEN CWA 14171:2004 General guidelines for electronic signature verification
- ANSI X9.30-1:1997 Public-Key Cryptography for the Financial Services Industry - Part 1: The Digital Signature Algorithm (DSA), American Bankers Association, 1997.
- ANSI X9.30-2:1997 Public Key Cryptography Using Irreversible Algorithms - Part 2: The Secure Hash Algorithm (SHA-1)
- CEN CWA 13987-1:2003 D/E/F, October 2003 Smart Card Systems: Interoperable Citizen Services: Extended User Related Information - Part 1: Definition of User Related Information and Implementation
- ETSI TS 102 176-1 V2.0.0 (2007-11-19) Electronic Signatures and Infrastructures (ESI);
- Algorithms and Parameters for Secure Electronic Signatures;
- Part 1: Hash functions and asymmetric algorithms
- ETSI TS 101 903 V1.4.1 (2009-06-15) XML Advanced Electronic Signatures (XAdES)
- ISO/IEC 10118-3:2004/Amd 1:2006 (2006-02-17) Dedicated Hash-Function 8 (SHA-224)
- ISO/IEC 7816-1:1998 Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics
- ITU X.509 ITU-T Recommendation X.509, Information Technology – Open Systems Interconnection – The directory: authentication framework
- IAS ECC TS 1.0.1 European Card for E-Services and National e-Id Applications

- FIPS[324] PUB 197 Advanced Encryption Standard (AES), 2001
- PKCS[325] #1 V2.1: June 14, 2002 RSA Cryptography Standard
- RFC[326] 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- RFC 5758 Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA

Látható, hogy a szabványok témakörei és a kibocsátó szervek köre nagyon széles körű, az alkalmazandó szabványok kiválasztása a tervezés során komoly szabványismeretet igényel.

4.2.8. Szabványosult ajánlások

Végül, de nem utolsó sorban szükséges foglalkoznunk azokkal a magyar ajánlásokkal, amelyek vagy teljes mértékben magyar szakemberek munkája által, vagy a nemzetközi szabványok felhasználásával készültek és Magyarországon tulajdonképpen szabványként használhatók (másrészről tekinthetőek viszont az állami irányítás egyéb jogi eszközeinek is), tehát például tanúsítható az azoknak való megfelelés is. Ami miatt a szabványok között kerülnek ezek felsorolásra, az a felépítésük és jellegük. Ezek kibocsátói egy szervezet és annak jogutódjai: az Informatikai Tárcaközi Bizottság (ITB), a Kormányzati Informatikai Egyeztető Tárcaközi Bizottság (KIETB), és a Közigazgatási Informatikai Bizottság (KIB).
A téma szempontjából legfontosabb ajánlások a következők:

- Informatikai Tárcaközi Bizottság 8. sz. ajánlása, Informatikai biztonsági módszertani kézikönyv[327]
- Informatikai Tárcaközi Bizottság 12. sz. ajánlása, Informatikai rendszerek biztonsági követelményei[328]
- Közigazgatási Informatikai Bizottság 25. számú ajánlása, Magyar Informatikai Biztonsági Ajánlások (v1.0, 2008. június)

[324] Federal Information Processing Standards, az Egyesült Államok szövetségi kormányának szabványa, nem katonai célú szabvány
[325] public-key cryptography standards, az RSA, az EMC Corporation biztonsági divíziójának, korábban RSA Data Security Inc.-nek a nyilvános kulcsú titkosításra vonatkozó szabványsorozatának része
[326] Request for Comments, az Internet Engineering Task Force (IETF) által kibocsátott Internetes technológiákkal kapcsolatos feljegyzés, de facto szabványnak tekinthető
[327] Az ajánlás már érvényét vesztette, viszont történeti jelentősége miatt szükséges megemlíteni.
[328] Az ajánlás már érvényét vesztette, viszont történeti jelentősége miatt szükséges megemlíteni.

- 25/1 – Magyar Informatikai Biztonság Irányítási Keretrendszer (MIBIK)
  - 25/1-1 – Informatikai Biztonság Irányítási Rendszer (IBIR)
  - 25/1-2 – Informatikai Biztonság Irányítási Követelmények (IBIK)
  - 25/1-3 – Az Informatikai Biztonság Irányításának Vizsgálata (IBIV)
- 25/2 – Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS)
- 25/3 – Informatikai Biztonsági Iránymutató Kis Szervezeteknek (IBIX)

- Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár[329]

A Magyar Informatikai Biztonsági Ajánlások (MIBA) nevet viselő Közigazgatási Informatikai Bizottság 25. számú ajánlássorozata az Informatikai Tárcaközi Bizottság korábbi 8, 12 és 16 számú ajánlásait hivatott kiváltani, mintegy modernizálva, bővítve azokat. Az ajánlások kialakításakor követték a 2008-ban hatályos elektronikus közigazgatásra vonatkozó követelményrendszert (amely azóta nagymértékben megváltozott ld. Ekszt.) és a magyar közszféra realitásait. Az ajánlások alapján meghatározhatóak a szabályok, eljárásrendek, előállíthatóak a szükséges dokumentációk és az értékelés- illetve tanúsítás[330] is elvégezhető azok alapján. Az ajánlás nemzetközi szabványokon alapul, azok fordításával és adaptációjával készült. Felhasználja az ISO/IEC 27001, ISO/IEC 27002, Common Criteria fontosabb elemeit, az informatikai biztonságot irányítási rendszernek tekinti, alkalmazza a PDCA elvet. Sajnos gyakorlati alkalmazásának mértéke elmaradt az elvárttól.

A Közigazgatási Informatikai Bizottság az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytárat 28. számú ajánlásaként adta ki, amely az elektronikus közigazgatás fejlesztéséhez szükséges teljes eszköztárat magában foglalja. Az informatikai biztonsági követelményeken túl funkcionális és módszertani követelményeket is egyesít magában.

[329] A követelménytár elérhető a http://kovetelmenytar.complex.hu/ weblapon [2011. 06. 29.]
[330] ld. Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS)

Látható tehát, hogy a szabványok számossága jelentős mértékben meghaladja a jogi szabályozásokét. Ennek nyilvánvaló oka, hogy az informatikai biztonság alapvetően műszaki terület. Másrészről viszont a korábbiakban ismertetettek szerint a legnagyobb hátránya a szabványosításnak az önkéntesség. Az állami szintű informatikai biztonsági politika kialakításában tehát a szabványok kizárólagos alkalmazása nem lehetséges, viszont műszaki szempontból az alkalmazásuk elkerülhetetlen.

5. Megfeleltetés és tapasztalatok

Jelenleg az informatikai biztonság jogi szabályozása kapcsán szakadék tapasztalható a jogalkotás és jogalkalmazás (jogászok) valamint az intézkedések végrehajtói (informatikusok) között. Ennek oka, hogy a jogi követelmények mögötti technikai tartalom nem ismerhető fel könnyen. A követelmények felületesek, amelynek fő oka a technológiafüggetlenség, de a felületesség a jogalkalmazást rendkívüli módon megnehezíti.[331] Például kérdéses, hogy „az adatkezelő [...] köteles gondoskodni az adatok biztonságáról”[332] kitétel pontosan mit takar? Víruskeresőt, biztonsági mentést DVD-re, offsite backupot, vagy komplex külső auditot az ISO/IEC 27001-nek való megfelelésről? Lehetne erre azt válaszolni, hogy a vonatkozó szabványoknak való megfelelést, no de milyen mértékben? Az informatikus erre józan ésszel próbálja felmérni, hogy mit érdemes bevezetni, de hol van a gondatlanság határa? Egy esetleges káresemény kapcsán hogyan lehet jogi úton kártérítést követelni?

A problémát felismerve és elemezve egy mindkét fél számára támpontot nyújtó megoldás került kidolgozásra. A szabványoknál bemutatott COBIT megfelelő arra, hogy egységes keretrendszerként kerüljön alkalmazásra, amikor az informatikai biztonság és vezetés kérdéskörében valamely átfogó szabályrendszert alkalmazunk. A COBIT-ot már sok más szabályrendszernek is megfeleltették korábban, többek között az ISO/IEC 17799, PMBOK, ITIL, PRINCE2, COSO ERM, NIST FISMA szabványoknak, valamint a Sarbanes-Oxley törvénynek is. A tézis az volt, hogy a COBIT követelményeit valamely informatikai biztonságra vonatkozó anyagi jogi jogszabállyal összerendelve, azokat kölcsönösen megfeleltetve, a COBIT részletesebb leírása alapján implementálni lehet a jogszabályban foglalt követelményeket, mintegy lefordítva azokat az informatika nyelvére. A választás az információs törvényre esett, mert az a felületes szabályozás kategóriájába tartozik, illetve kellően kis számú konkrét informatikai biztonsági követelményt fogalmaz meg. Továbblépve, ha több jogszabály kerül megfeleltetésre, akkor ha egy kötelezettre több megfeleltetett jogszabály vonatkozik, egyszerűen veszi az összes követelményhalmaz unióját, és ha megfelel az ebben foglalt közös szabályoknak, akkor feltehetőleg teljesítette az összes

[331] Reidenberg, 1998, p. 584.
[332] Infotv. 7. § (2)

jogszabály által rá rótt kötelezettséget az informatikai biztonság területén, mintegy informatikai biztonsági legkisebb közös többszörösként.

A második tézis bizonyításaként a fenti megfeleltetésekkel azonos formátumban készült az információs törvény COBIT-nak való megfeleltetése is, amelynek nem rejtett célja az, hogy szakmai körökben használható és az ISACA magyar és nemzetközi vezetősége által is elfogadható, könyv formátumában kiadható dokumentum készülhessen. Ebből következik az a formai és szerkezeti kötöttség, amely meghatározza a függelékben csatolt megfeleltetés keretét. A megfeleltetés oly módon történt, hogy a COBIT minden egyes kontroll célkitűzéséhez (legkisebb követelményegység) – ha az lehetséges volt – párosításra került az információs törvény egy bekezdése. A lefedettség (megfeleltethetőség) mértéke négy szinten került meghatározásra:

- (F) Felülmúlt: az adott kontroll célkitűzést az Infotv. informatikai biztonsági tartalmi szempontból felülmúlja
- (T) Teljes lefedettség: az adott kontroll célkitűzésnek az Infotv. informatikai biztonsági szempontból teljes mértékben megfelel
- (R) Részleges, valamely szempont(ok) lefedve: az adott kontroll célkitűzésnek az Infotv. informatikai biztonsági szempontból részlegesen megfelel, tehát nem a teljes kontroll célkitűzést írja elő a jogszabály
- (N) Nincs lefedve: az adott kontroll célkitűzés teljesülését az Infotv. nem írja elő

A részletes megfeleltetés során látszott, hogy az „F", mint felülmúlt lefedettségi kategória nem fordult elő, az Infotv. minden esetben legfeljebb olyan követelményt állított, mint a COBIT, de a teljes lefedettség is ritka. A törvényi követelmények alapvetően a bizalmasság, sértetlenség és rendelkezésre állás információ-kritériumok köré csoportosulnak. Ez nem meglepő, hiszen a jogi követelmények alkalmazásáról szóló fejezetben is látszik, hogy mind az Infotv., mind az adatvédelmi irányelv, mind pedig a külföldi nemzeti jogszabályok is ezeket tekintik a legfontosabbnak. Ebből következően ahol a COBIT maga ezeket az információ-kritériumokat valamely kontroll célkitűzés tekintetében elsődleges jelentőségűnek tartotta,[333] ott az Infotv. 7. § (2) bekezdése ezen objektív okból kifolyólag megfeleltetésre került.

[333] ld. COBIT 4.1 II. Melléklet - Az informatikai folyamatok leképezése informatikai irányítási központi területekre, a COSO-ra, a COBIT informatikai erőforrásokra és a COBIT információ-kritériumokra. p. 200.

Az Infotv.-ben meghatározott általános követelmények emellett is igen sok kontrollnak megfeleltethetőek voltak, bár kevésbé meghatározott módon. Ezek a megfeleltetések szakmai mérlegelés és egyeztetés útján alakultak ki, tehát tartalmaznak szubjektív elemeket. A széleskörű szakmai vita és a többkörös egyeztetés jelentősége éppen ezeknek a szubjektív elemeknek a bevált gyakorlattá való átformálását szolgálják. Az ilyen jellegű anyagoknak nincs végleges állapota. Ha elfogytak a jelenlegi állapottal kapcsolatos jobbító javaslatok, akkor a jogszabályi és a szabványváltozatok lekövetése miatt szükséges változtatni.

A kidolgozott megfeleltetés mellett – amely csak az informatikai biztonsági követelményekre irányul – lehetőség van más, általános módszertanok alkalmazására is, amely így kibővíti a módszertannal lefedett terület hatókörét. Ez a hatókör-bővítő módszertani kiegészítés szakma-specifikussá teszi a módszertant, így minden megfeleltetni kívánt terület esetében el kell végezni a bővítést. Mivel az a jelenlegi kutatásnak nem része, ezért csak kitekintés formájában kerül bemutatásra ez a lehetőség.

Ilyen bővítési lehetőség a létező audit módszertanok, ajánlások nemzeti adaptációja. A két általam vizsgált módszertan a következő:

- Data Protection Audit Manual [United Kingdom]
- Data Protection Audit Resource. January 2009.Version 1.0 Office of the Data Protection Commissioner [Ireland]

Ezek a jogrendszerbeli eltérések ellenére a harmonizált adatvédelmi irányelv miatt jól használhatóak Magyarországon is.

A szabványosítás területén is találhatóak olyan európai dokumentumok, amelyeket segítségül lehet hívni egy módszertan kialakításához:

- CWA[334] 15262 Inventory of Data Protection Auditing Practices
- CWA 15263 Analysis of Privacy Protection Technologies, Privacy-Enhancing Technologies (PET), Privacy Management Systems (PMS) and Identity Management systems (IMS), the Drivers thereof and the need for standardization
- CWA 15292 Standard form contract to assist compliance with obligations imposed by article 17 of the Data Protection Directive 95/46/EC (and implementation guide)

[334] European Committee for Standardization (CEN) Workshop Agreement

- CWA 15499-1 Personal Data Protection Audit Framework (EU Directive EC 95/46) Part I: Baseline Framework - The protection of Personal Data in the EU
- CWA 15499-2 Personal Data Protection Audit Framework (EU Directive EC 95/46) Part II: Checklists, questionnaires and templates for users of the framework - The protection of Personal Data in the EU

Ezek az Európai Szabványügyi Testület által kidolgozott munkacsoport-megállapodások az adatvédelmi irányelv alapján általános, műszaki jellegű (általában algoritmizálható) leírást illetve követelményrendszert nyújtanak az adatvédelem területén. Így a munkacsoport megállapodás és a nemzeti követelmények alapján kialakítható például egy ellenőrzőlista, amely az adatvédelmi dokumentáció teljes vertikumát lefedi:

- A hatóságoknak[335] megküldött bejelentések másolata.
- A hatóság érkeztetésről szóló értesítései.
- A bejelentési kötelezettségre vonatkozó belső eljárások, utasítások és iránymutatások.
- Az adatvédelemre vonatkozó hirdetmények, levelek, brosúrák.
- Az érintettet tájékoztatási kötelezettségére vonatkozó belső eljárások, utasítások és iránymutatások.
- Az adatkezelés célját és jogalapját meghatározó belső dokumentum.
- Belső eljárások, utasítások és iránymutatások a személyes adatok gyűjtésére, kezelésére, feldolgozására.
- Az adatok megőrzési ideje, az archiválás és a személyes adatok megsemmisítésére vonatkozó belső szabályzatok, eljárások, utasítások vagy egyéb iránymutatások.
- A személyes adatok minőségére (pontosság, a teljesség és naprakész állapot) vonatkozó belső eljárások, utasítások és iránymutatások.
- Az adatalany jogaira vonatkozó tájékoztatás és a jogorvoslat lehetőségeit meghatározó szabályzat, tájékoztató.
- Információbiztonsági politika
- Információbiztonsági tervek (rendszerterv, katasztrófatervek)
- Adminisztratív munkavégzés védelmi követelményei

[335] Értendő alatta az adatvédelmi biztos, illetve bármely felügyeleti szerv, amely felé adatvédelmi, adatbiztonsági tárgyú jelentési kötelezettség áll fenn vagy ilyen irányú felügyeletet gyakorol.

- Adathordozók védelmére és szállítására vonatkozó előírások
- Biztonsági másolatokkal kapcsolatos eljárásrend
- Biztonsági tartalékokra, helyreállításra és üzletmenet-folytonosságra vonatkozó tervek, előírások.
- Mentésre (archiválásra), illetve megsemmisítésre vonatkozó tervek, előírások.
- Szermélyes adatok postán illetve e-mailben történő küldésére és az elektronikus levelezésre vonatkozó szabályok.
- Jogosultság-kiosztási szabályzat
- Bizalmassági előírások, biztonsági incidensek és rendszerhibák kezelése.
- Adatfeldolgozókkal kötött szerződések, beleértve az adatfeldolgozás részletes szabályait.
- A hatályos jogszabályi rendelkezések betartásának időszakos ellenőrzéséről készült dokumentáció (belső ellenőrzés, külső audit, hatósági ellenőrzések).
- Külföldre történő adattovábbításra vonatkozó felhatalmazás, engedély, kötelező érvényű vállalati szabályok (BCR), a harmadik országban történő adattárolás megfelelőségének bizonyítékai, belső eljárások, utasítások és iránymutatások.
- Adatvédelem politika (a személyes adatok védelme céljainak, stratégiájának leírása)
- A személyes adatok gyűjtésére vonatkozó iránymutatások
- A személyes adatok kezelésére vonatkozó iránymutatások
- A személyes adatok nyilvánosságra hozatalára és továbbítására vonatkozó iránymutatások
- A személyes adatok törlésére vonatkozó iránymutatások
- A személyes adatokkal való visszaélések és panaszok kezelésének, bejelentésének rendje
- A belső adatvédelmi szervezet leírása (szervezeti ábra, felelősök)
- A belső adatvédelmi szervezet vezetőjének munkaköri leírása
- Adatvédelemre vonatkozó iratkezelési iránymutatások
- Adatvédelem terv, adatvédelmi kommunikációs terv
- Adatkezelési, adatfeldolgozási műveletek részletes leírása
- Vezetőknek és beosztottaknak szóló adatvédelmi oktatási, figyelemfelkeltő és tájékozató anyagok

- Önértékelési jelentések, belső- és külső auditjelentések
- Iránymutatás az új, megváltozott, vagy megszűntetett adatkezelés esetére
- Adatvédelmet elősegítő technikai intézkedésekre (PET) vonatkozó utasítások
- Az adatkezelésre használt infrastruktúra jellemzőire vonatkozó információ (hardver, adathordozók, szoftver, hálózatok, adatbázisok, kialakításra vonatkozó tervek)

Az ilyen kérdéslisták vagy más módszertani elemek segítségével a kizárólag informatikai biztonsági módszertan jobban az adott szakterületre szabható, viszont megőrzi összehasonlíthatóságát más szakterületek informatikai biztonsági követelményeivel.

Tudományos eredményként értékelhető, hogy a függelékben elhelyezett megfeleltetés biztosítja az információs törvényben meghatározott informatikai biztonsági szabályok értelmezhetőségét. A megfeleltetés a gyakorlatban használható és annak alkalmazása javasolt. A további kutatásoknak is megfelelő kiinduló pontot adnak a jelenlegi kutatási eredmények, a folyamatos tartalmi és elméleti-módszertani fejlesztés lehetősége adott.

6. Összefoglalás

A monográfia témája az informatikai biztonság szabályozása. Ebből az informatikai biztonság tekintetében elsősorban a számítógépen tárolt és feldolgozott adatok elektronikus védelmével foglalkozik, de ahol szükséges, kitér a biztonság és a védelem más aspektusaira (az informatikai biztonság fogalmának megfelelően). A szabályozás jelen esetben nem a szűken vett jogi szabályozás, hanem a szakterületen alkalmazható bármely szabályzási módszer, így a szabványosítás és a belső szabályozás is. Másrészről viszont első sorban az állam szempontjából kerül megközelítésre a szabályozandó terület, ezért a gyakorlati részben már csak az állam által alkalmazható szabályozások kerülnek kifejtésre.

A monográfiában a vonatkozó helyeken meghatározásra kerültek a legfontosabb fogalmak, amelyeket a kutatási téma érint, az informatikai biztonságtól a terrorizmus fogalmáig. A téma alapját képező elektronikus írásbeliség, illetve információs társadalom történelmi felvezetése két szálon történik: az ipari forradalom és az írásbeliség forradalmai útján. Az elektronikus írásbeliség kialakulásához gyakorlati szempontból az adatbiztonsági eljárások és a szabályozási háttér is szükségeltetett. De még ezen háttérrel is tapasztalhatóak problémák, amelyek a fejlődés túlzott gyorsaságából, az adatformátumok különbözőségéből, a működő rendszeren belüli és azon kívüli adatbiztonságból, valamint az elektronikus aláírás – mint az elektronikus írásbeliség hitelességének kulcsa – elveiben rejlő, bizonyítható hitelességet megnehezítő elemeiből erednek. Az elektronikus írásbeliségből táplálkozva több olyan új technológia fejlődött ki, amelynek sajátos jellemzői miatt különleges figyelmet érdemelnek. Ezek közül az elektronikus okmányok, a térfigyelés és a számítási felhők kérdéskörei kerültek elemzésre.

A természetes, rendszer elveiből fakadó kockázatok mellett megjelenik a szándékos támadás lehetősége, amelyet egyedi elkövetés esetén informatikai bűncselekménynek, a tömeges elkövetés különleges esetében pedig cyberterrorizmusnak nevezhetünk. Az egyedi cselekmények elleni műszaki-szervezési védelmet az állampolgárok, szervezetek végzik, és ilyen módon szankcionálható az elkövetés, míg a cyberterrorizmus elleni védelem az állam feladata, és a büntetőjog ebből az irányból is megközelítheti a kérdést.

Az informatikai biztonság – mint a fenti egyedi informatikai bűncselekmények elleni védelem – szabályozása végezhető jogi úton, szabványokkal és a szervezet belső szabályzataival (pl. informatikai biztonsági szabályzat). A szakmában a legjobb gyakorlat alapján körülírható az az elvárt kialakítás, ami megfelel az általános üzleti céloknak.

Az informatikai biztonság jelenlegi magyar szabályozása négy csoportra bontható. Az indirekt szabályozásba sorolhatóak azok a jogszabályok, amelyek csak közvetve írnak elő követelményt a szakterületre, a szabályok megsértését szankcionálják. Az önkéntes –önszabályozott területeken a biztonsági kontrollokat a piaci igények teszik szükségessé. A felületesen szabályozott csoportban kötelezően betartandó előírások vannak, szankciók kilátásba helyezésével, viszont a szabályok a kötelezettek számára pontosan nem ismertek. Ebbe a kategóriába tartozik az információs törvény, amely a szankciórendszer miatt különleges figyelmet igényel. A részletesen szabályozott kategóriában a biztonsági előírások megfelelő mélységben kifejtésre kerültek, függetlenül attól, hogy azok betartása ellenőrzésre került-e.

A felületesen szabályozott területeken lehetséges a jogszabályi követelmények mintegy kiegészítése vagy megfeleltetése valamely informatikai biztonsági témájú szabványban meghatározott követelményrendszernek. A tézis igazolására a gyakorlati megvalósítás a függelékben található, az információs törvény megfeleltetése a COBIT 4.1-nek címmel.

Irodalomjegyzék

Szakirodalom

Hazai irodalom

Adler, Freda – Mueller, Gerhard O. W. – Laufer, William S. (2000): Kriminológia. Osiris, Budapest. ISBN 9789633897935

Alexin Zoltán (2010): Információs törvényünk - kisebb hibákkal, Infokommunikáció és Jog, 38. sz., pp. 104-109. ISSN 1786-0776

Almási János – Balázs László – Erdősi Péter Máté – Kovács Árpád – Rátai Balázs – Schvéger Judit (2010): Elektronikus hitelesség, elektronikus aláírás. OTY StarTel, Budapest. ISBN 9789630687270

Az adatvédelmi biztos beszámolója 1997. Adatvédelmi Biztos Irodája, Budapest, 1998. ISSN 1416-9762

Az adatvédelmi biztos beszámolója 1999. Adatvédelmi Biztos Irodája, Budapest, 2000. ISSN 1416-9762

Az adatvédelmi biztos beszámolója 2008. Adatvédelmi Biztos Irodája, Budapest, 2009. ISSN 1416-9762

Az adatvédelmi biztos sajtóközleménye (2009): Az adatvédelmi biztos az Ügyfélkapu hétvégi hibájáról. Adatvédelmi Biztos Irodája, Budapest, 2009. február 9. http://abiweb.obh.hu/abi/index.php?menu=0/Sajtokozlemenyek&dok=20090209_ABI_1 [2010. 11. 22.]

Az adatvédelmi biztos sajtóközleménye (2010): Vizsgálja az adatvédelmi biztos az Ügyfélkapu üzemzavarát. Adatvédelmi Biztos Irodája, Budapest, 2010. március 11. http://abiweb.obh.hu/abi/index.php?menu=0/Sajtokozlemenyek&dok=20100311_ABI_1 [2010. 11. 22.]

Bakos Ferenc (1994): Idegen szavak és kifejezések szótára. Akadémiai Kiadó, Budapest. ISBN 9789630582056

Balogh Zsolt György (2005): A személyes adatok védelme. Tansegédlet, PTE-ÁJK, Pécs.

Balogh Zsolt György (1998): Jogi informatika. Dialóg Campus Kiadó, Budapest-Pécs. ISBN 9639123196

Balogh Zsolt György – Jóri András – Polyák Gábor (2002): Adatvédelmi „legjobb gyakorlat” kialakítása az elektronikus közigazgatásban. PTE ÁJK IKJK, Pécs.

Beinschróth József (2006): Informatikai rendszerekkel támogatott folyamatok működésfolytonosságának modellezése és mérése, Hadmérnök, I. évf. 2. sz., ISSN 1788-1919

Bernek Ágnes (szerk.) et al. (2002): A globális világ politikai földrajza. Nemzeti Tankönyvkiadó, Budapest. ISBN 9631925269

Bíró János – Szádeczky Tamás – Szőke Gergely László (2011): A hírközlési szolgáltatók értesítési kötelezettsége a személyes adatok megsértése esetén (Data Breach Notification) Infokommunikáció és jog, VIII. évf. 43. sz. ISSN 1786-0776

Bitport (2010): Háttérbe szorul a megfelelőség? Bitport, 2010.01.27. http://www.bitport.hu/biztonsag/hatterbe-szorul-a-megfeleloseg [2010. 04. 10.]

Breuer, Hans (1995): Informatika. (SH Atlasz) Springer-Verlag, Budapest, ISBN 9638455705

Crume, Jeff (2003): Az internetes biztonság belülről …amit a hekkerek titkolnak. Szak Kiadó, Bicske. ISBN 9789639131514

Dedinszky Ferenc (2008): Informatikai biztonsági elvárások, MeH-EKK, Budapest, 2008. július 2.

Dósa Imre – Polyák Gábor (2003): Informatikai jogi kézikönyv. KJK KERSZÖV, Budapest. ISBN 9632246063

Eiler Emil (2008): Kódnyomtatás és nyomtatott vonalkód rendszerek, Magyar Grafika, 2008. 5. sz.

F. Ható Katalin (2000): Adatbiztonság, adatvédelem. Számalk, Budapest. ISBN 9635533535

Forgács László (2004): A magyar szabványosítás jogharmonizációja, Bányászati és Kohászati Lapok – Bányászat, 137. évfolyam, 1. sz., ISSN 0005-5670, pp. 26-32.

Giddens, Anthony (1995): Szociológia. Osiris Kiadó. ISBN 9633790603

Haig Zsolt – Várhegyi István (2005): Hadviselés az információs hadszíntéren. Zrínyi, Budapest. ISBN 9633273919

Hornák Zoltán (2005): Felhasználó-azonosítás. SEARCH-Biztostű.hu. http://www.biztostu.hu/mod/resource/view.php?id=451 [2009. április 29.]

Horváth István – Kiss Jenő (szerk.) (1997): A nemzeti katonai stratégia és integráció. Budapest. ISBN 9637037179

Horváth László – dr. Lukács György – dr. Tuzson Tibor – Vasvári György (2001): Informatikai biztonsági rendszerek. Budapesti Műszaki Főiskola – Ernst & Young, Budapest.

Horváth Zsolt (2008): Miért nem mindegy, hogy kit választok tanúsítónak? Minőségdoktorok.hu.

http://www.minosegdoktorok.hu/cikk/miert_nem_mindegy_hogy_kit_valasztok_tanusitonak [2010. 04. 05.]

Illési Zsolt (2009): Számítógép hálózatok kriminálteчnikai vizsgálata, Hadmérnök, IV. évf. 4. sz., ISSN 1788-1919, pp. 163-175.

Illési Zsolt – Varga Péter (2009): Kritikus infrastruktúrák hatás alapú modellezése, Hadmérnök, IV. évf. 4. sz., ISSN 1788-1919, pp. 390-399.

ITTK (2007): Magyar információs társadalom jelentés 1998–2008. http://www.ittk.hu/images/stories/bme/evkonyv/ittk_mitj_1998-2008.pdf [2010. 11. 01.]

Jacsó Tamás (2006): Az ügyfélkapu és az eBEV használata. Saldo, Budapest. ISBN 9789636381981

Jóri András (2005): Adatvédelmi kézikönyv. Elmélet, történet, kommentár. Osiris, Budapest. ISBN 9633897351

Jóri András – Hegedűs Bulcsú – Kerekes Zsuzsanna (szerk.) et al. (2010): Adatvédelem és információszabadság a gyakorlatban. Complex, Budapest.

Kerekes János – Lukács György (szerk.) et al. (1997): Információ-biztonság. Cedit Információtechnikai, Budapest. ISBN 9638180307

Kinder, Hermann – Hilgemann, Werner (1992): Világtörténelem. (SH Atlasz) Spriger-Verlag, Budapest. ISBN 9637922471

Kiss László (1996): Jogtisztítás – jogszabályrendezés – dereguláció. In: Kiss László-Petrétei József: A törvényhozástan alapvonásai. Pécs.

Köpeczi Béla (szerk.) et al. (1974): Az embergéptől a gépemberig. Minerva, Budapest.

Krauth Péter (2007): Az információbiztonság fejlődése a szabványok tükrében. In: Horváth Zsolt (szerk. et al.): Információbiztonsági rendszermenedzser tanfolyami témaváz. EOQ MNB.

Krauth Péter (2003): Információbiztonsági szabványok fejlődése az elmúlt időszakban, avagy az 17799-es esete a 13335-össel, Magyar Minőség, XII. évf. 7. sz. pp. 6-8. ISSN 1789-5510

Kristóf Csaba (2010): Megcsappant az auditálási kedv, Computerworld, 2010. január 26. http://computerworld.hu/megcsappant-az-auditalasi-kedv.html [2010. 02. 10.] ISSN 0237-7837

Majtényi László (2006): Az információs szabadságok. Adatvédelem és a közérdekű adatok nyilvánossága. Complex, Budapest. ISBN 9632247604

Masuda, Yoneji (1988): Az információs társadalom. OMIKK, Budapest.

Mitnick, Kevin D. – Simon, William L. (2003): A legendás hacker – A megtévesztés művészete. Perfact-Pro Kft., Budapest. ISBN 9632065557

Muha Lajos (2008): Az informatikai biztonság egy lehetséges rendszertana, Bolyai Szemle, XVII. évf. 4. sz. pp. 137-156. ISSN 1416-1443

Muha Lajos (szerk.) et. al. (2010): Az Informatikai Biztonság Kézikönyve. Verlag Dashöfer, Budapest, 2001-2010. ISBN 9639313122

Muha Lajos (2009): Infokommunikációs biztonsági stratégia, Hadmérnök, IV. évf. 1. sz. pp. 214-224., ISSN 1788-1919

Muha Lajos – Bodlaki Ákos (2001): Az informatikai biztonság. PRO-SEC, Budapest. ISBN 9638602260

Netanjahu, Benjamin (1995): Harc a terrorizmus ellen. Alexandra Kiadó. ISBN 9633691906

Parti Katalin (2008): Az eladók már rég hazamentek. A büntetőjog, mint az online pornográfia szabályozásának eszköze. Doktori értekezés, PTE-ÁJK Pécs.

Parti Katalin (2004): Nyomozás az interneten: együttműködés – korlátokkal, Belügyi Szemle, 52. évf. 11-12. sz, ISSN 1789-4689, 204-220. p.

Pleplár Gábor (2009): Bevezetés a fizikába. http://aagk.hu/jegyzetek/9_10_alapfogalmak.doc [2010. 05. 08.]

Polyák Gábor (2004): Az elektronikus szolgáltatások adatvédelme, Jogi Fórum, 2004. június 13.

Racskó Péter (2011): Cloud computing – informatika és kommunikáció a felhőben. OBH-NKI tanfolyam, Budapest, 2011. 03. 21.

Rátai Balázs (2010): Legal compliance audit based on an intermediate model. http://www.carneades.hu/index.php?option=com_content&view=article&id=3&Itemid=6 [2010. 05. 12.]

Samu Mihály – Szilágyi Péter (1998): Jogbölcselet. Rejtjel, Budapest.

Sebestyén György (1997): A Gutenberg-galaxis és a digitális kultúra szintézise: Az elektronikus-virtuális könyvtár. Írás tegnap és holnap, I. évf. 1. sz., ISSN 1417-8206. http://www.oszk.hu/kiadvany/iras/iras_1/11sgy.html [2010. 02. 14.]

Shaoyi, HE (2003): Informatics: a brief survey. (ford.: Papp István), Tudományos és műszaki tájékoztatás, 50. évf. 9-10. sz. ISSN 0041-3917. http://tmt.omikk.bme.hu/show_news.html?id=3391&issue_id=444 [2011.11.14.]

Sramó András (szerk.) et al. (2004): Info-kommunikációs technológiák. PTE-BTK, Pécs. http://nti.btk.pte.hu/main/ictsources/ [2009. 08.11.]

Szabó József (szerk.) et al. (1995): Hadtudományi lexikon. Magyar Hadtudományi Társaság, Budapest. ISBN 9630452278

Szabó Miklós (szerk.) et al. (2004): Regula Iuris. Szabály és/vagy norma a jogelméletben. Prudentia Iuris 22. Bíbor, Miskolc. ISBN 9639466727 ISSN 12198471

Trócsányi Sára (2007): Egészségügyi adatok kezelése a gyakorlatban. Válogatás az adatvédelmi biztos eseteiből, Infokommunikáció és Jog, 19. sz. ISSN 1786-0776

Vasvári György (1997): Biztonsági rendszerek szervezése. Pro-Sec, Budapest. ISBN 9638545372

Vikman László (2009): Az informatikai biztonság szabályozása a magyar jogban, Jogi Fórum, 2009. március 26., http://www.jogiforum.hu/publikaciok/353 [2009. 08. 12.]

Virasztó Tamás (2004): Titkosítás, adatrejtés. NetAcademia, Budapest. ISBN 9632142535

Külföldi irodalom

Alfarez Abdul-Rahman (1997): The PGP Trust Model. EDI-Forum, http://netresearch.ics.uci.edu/Previous_research_projects/agentos/related/security/abdul-rahman-pgp-trust.pdf [2009. 10. 11.]

Anderson, James P. (1972): Computer Security Technology Planning Study Volume I-II, ESD-TR-73-51 Vol. I-II, Electronic Systems Division, Air Force Systems Command, Hanscom Field, Bedford, MA, USA. http://seclab.cs.ucdavis.edu/projects/history/CD/ande72a.pdf [2009. 12. 14.]

Black, Deirdre (1993): The Computer Hacker – Electronic Vandal or Scout of the Networks, Journal of Law and Information Science, Vol. 4, Issue 1, pp. 65-79.

Blakeslee, Sandra (1990): Lost on Earth: Wealth of Data Found in Space, New York Times, 1990. 03. 20.

Bountouri, Lina – Papatheodorou, Christos – Soulikias, Vasilis – Stratis, Mathios (2007): Metadata Interoperability in Public Sector Information, Journal of Information Science, 7. sz. pp. 1–25

Camp, L. Jean – Wolfram, Catherine (2004): Pricing Security in: Camp, L. Jean – Lewis, Stephen: Economics of information security. Springer. ISBN 9781402080890

Campbell, Katherine – Gordon, Lawrence A. – Loeband, Martin P. – Zhou, Lei (2003): The economic cost of publicly announced information security breaches: empirical evidence from the stock market, Journal of Computer Security, 11. sz., ISSN 0926-227X, pp. 431–448

Catteddu, Daniele – Hogben, Giles (eds.) (2009): Cloud Computing. Benefits, risks and recommendations for information security. ENISA, Heraklion, Greece.

Cohen, Aviv (2010): Cyberterrorism: Are we legally ready?, Journal of International Business and Law, Vol. 9. Issue 1. Spring 2010. pp 1-40.

Damianides, Marios (2005): Sarbanes–Oxley and IT Governance: New Guidance on IT Control And Compliance. Information Systems Management, Winter 2005. pp. 77-85.

DeJarnette, Ken – Morin, John (2010): Privacy and Data Protection Audit and Assessment Strategies. Deloitte, San Francisco ISACA Chapter, January 27, 2010

Fischer-Hübner, Simone (2001): IT-Security and Privacy. Design and Use of Privacy-Enhancing Security Mechanisms. Springer, Karlstad. ISBN 3540421424

Goodman, Seymour E. – Kirk, Jessica C. – Kirk, Megan H. (2007): Cyberspace as a medium for terrorists, Technological Forecasting & Social Change, 74. sz., ISSN 0040-1625

Gorge, Mathieu (2007): Cyberterrorism: hype or reality?, Computer Fraud & Security, 2. sz., ISSN 13613723

Harvey, Ross (2008): So where's the black hole in our collective memory? A Provocative Position Paper (PPP). 18th January 2008. http://www.digitalpreservationeurope.eu/publications/position/Ross_Harvey_black_hole_PPP.pdf [2008. 12. 28.]

Hassler, Vesna (2009): IT Security and Smart Card Standards. http://www.infosys.tuwien.ac.at/Staff/vh/papers/std.ps.gz [2010. 01. 11.]

Hoad, Richard – Jones, Andy (2004): Electromagnetic (EM) threats to information security–Applicability of the EMC directive and information security guidelines, Proceedings of the 3rd European Conference on Information Warfare and Security, Royal Holloway, University of London. ISBN 0954709624

Jakobs, Kai (2007): ICT Standardisation – Co-Ordinating the Diversity. http://www.wip.tu-berlin.de/typo3/fileadmin/documents/infraday/2007/papers/paper_jakobs_v02_bv_27.09.2007.pdf [2009. 08. 16.]

Kita, Chigusa Ishikawa (2003): J.C.R. Licklider's Vision for the IPTO, IEEE Annals of the History of Computing, 3. sz., ISSN 1058-6180

Kokolakis, Spyros – Lambrinoudakis, Costas (2005): ICT Security Standards for Healthcare Applications, UPGRADE European Journal for the Informatics Professional, Vol. VI, issue No. 4, ISSN 1684-5285

Kuny, Terry (1997): A Digital Dark Ages? Challenges in the Preservation of Electronic Information. IFLA, Copenhagen.

Lorie, Raymond (2002): The UVC: a Method for Preserving Digital Documents - Proof of Concept. IBM Netherlands, Amsterdam.

MacLean, Margaret - Davis, Ben H. (Eds.) (2000): Time and Bits: Managing Digital Continuity. Getty Publications, Los Angeles. ISBN 9780892365838

Menezes, A. – Oorschot, P. van – Vanstone, S. (1996): Handbook of Applied Cryptography. CRC Press. ISBN 0849385237

Moses, Tim (2008): Protecting Biometric Data with Extended Access Control. http://download.entrust.com/resources/download_page.cfm/23504/WP_ePassport-Biometrics_Aug08.pdf

Nibaldi, Grace H. (1979): Proposed Technical Evaluation Criteria for Trusted Computer Systems, M79-225, The MITRE Corporation, Bedford, MA, USA. http://seclab.cs.ucdavis.edu/projects/history/CD/niba79.pdf [2009. 12. 04.]

Osborn, Alice (2005): Biometrics history. Looking at biometric technologies from the past to the present. http://www.video-surveillance-guide.com/biometrics-history.htm [2009. 01. 15.]

Reidenberg, Joel R. (1998): Lex Informatica: The Formulation of Information Policy Rules Through Technology, Texas Law Review, Vol. 76, No. 3. ISSN 0040-4411

Robroch, Harko (2006): ePassport Privacy Attack. Cards Asia Singapore, April 26. 2006. http://www.riscure.com/fileadmin/images/Docs/200604_CardsAsiaSing_ePassport_Privacy.pdf [2008. 11. 03.]

Schneier, Bruce (1996): Applied Cryptography. John Wiley & Sons, New York. ISBN 0471117099

Simpson, John – Weiner, Edmund (eds.) (1993): The Oxford English Dictionary. Oxford University Press, Oxford. ISBN 0198611862

Slade, Robert M. (2004): Software forensics. Collecting Evidence from the Scene of a Digital Crime. McGraw-Hill, New York. ISBN 9780071428040

Sotirov, Alexander –Stevens, Marc – Appelbaum, Jacob – Lenstra, Arjen – Molnar, David – Osvik, Dag Arne – Weger, Benne de (2008): MD5 considered harmful today. Creating a rogue CA certificate. http://www.win.tue.nl/hashclash/rogue-ca/ [2009. 01. 03.]

Spindler, Gerald (et. al.) (2007): Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären. Studie im Auftrag des BSI durchgeführt von Prof. Dr. Gerald Spindler, Universität Göttingen. Bundesamt für Sicherheit in der Informationstechnik, Bonn.

Spivey, Jeff et al. (2009): Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives. ISACA Rolling Meadows, IL, USA.

UNESCO (2008): UIS Statistics in brief. UNESCO, Párizs. http://stats.uis.unesco.org/ [2009. 10.01.]

Visdómine, Luis Padilla (2009): Track format of magnetic stripe cards. http://www.gae.ucm.es/~padilla/extrawork/tracks.html [2009. 02. 01.]

Ware, Willis H. (ed.) (1970): Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security. Office of the Secretary of Defense, USA. http://cryptome.org/sccs.htm [2009. 12. 04.]

Jogszabályok

Adatvédelem

(röv. Infotv.) 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

(röv. Eüak.) 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről

1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról

(röv. Avtv.) 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról [hatályon kívül 2012. 01. 01-től]

1995. évi CXIX. törvény a kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről

Minősített adatok védelme

(röv. Mavtv.) 2009. évi CLV. törvény a minősített adat védelméről

285/2010. (XII. 16.) Korm. rendelet az állambiztonsági szolgálatok mágnesszalagra rögzített adatbázisaiban található adatok felülvizsgálatáról szóló 102/2010. (IV. 2.) Korm. rendelet hatályon kívül helyezéséről

161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól

102/2010. (IV. 2.) Korm. rendelet az állambiztonsági szolgálatok mágnesszalagra rögzített adatbázisaiban található adatok felülvizsgálatáról

90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről

Hírközlés

(röv. Eht.) 2003. évi C. törvény az elektronikus hírközlésről

100/2004. (IV. 27.) Korm. rendelet az elektronikus hírközlés veszélyhelyzeti és minősített időszaki felkészítésének rendszeréről, az államigazgatási szervek feladatairól, működésük feltételeinek biztosításáról

180/2004. (V. 26.) Korm. rendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről

13/2011. (XII. 27.) NMHH rendelet az elektronikus hírközlési szolgáltatás minőségének az előfizetők és felhasználók védelmével összefüggő követelményeiről, valamint a díjazás hitelességéről

Elektronikus közszolgáltatások, írásbeliség, informatikai biztonság

2017. évi I. törvény a közigazgatási perrendtartásról

2016. évi CL. törvény az általános közigazgatási rendtartásról

2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól

(röv. Ibtv.) 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

(röv. Ekszt.) 2009. évi LX. törvény az elektronikus közszolgáltatásról [hatályon kívül]

2009. évi LII. törvény a hivatalos iratok elektronikus kézbesítéséről és az elektronikus tértivevényről [hatályon kívül]

(röv. Ket.) 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól [hatályon kívül 2018.01.01-től]

2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről

(röv. Eat.) 2001. évi XXXV. törvény az elektronikus aláírásról [hatályon kívül 2016. 07. 01-től]

1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről

466/2017. (XII. 28.) Korm. rendelet az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról

137/2016. (VI. 13.) Korm. rendelet az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről

187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

301/2013. (VII. 29.) Korm. rendelet a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról [hatályon kívül]

85/2012. (IV. 21.) Korm. rendelet az elektronikus ügyintézés részletes szabályairól [hatályon kívül 2017.01.01-től]

84/2012. (IV. 21.) Korm. rendelet egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről.

83/2012. (IV. 21.) Korm. rendelet a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról [hatályon kívül 2017.01.01-től]

78/2010. (III. 25.) Korm. rendelet az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól [hatályon kívül 2016. 07. 01-től]

225/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatásról és annak igénybevételéről [hatályon kívül]

223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról [hatályon kívül]

222/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás működtetéséről [hatályon kívül]

182/2007. (VII. 10.) Korm. rendelet a központi elektronikus szolgáltató rendszerről [hatályon kívül]

84/2007. (IV. 25.) Korm. rendelet a Központi Elektronikus Szolgáltató Rendszer és a kapcsolódó rendszerek biztonsági követelményeiről [hatályon kívül]

207/2006. (X. 16.) Korm. rendelet a számítógépes ingatlan-nyilvántartási rendszerből történő szolgáltatás feltételeit tartalmazó szolgáltatási szerződés kötelező elemeiről

335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről

195/2005. (IX. 22.) Korm. rendelet az elektronikus ügyintézést lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról [hatályon kívül]

194/2005. (IX. 22.) Korm. rendelet a közigazgatási hatósági eljárásban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítésszolgáltatókra vonatkozó követelményekről [hatályon kívül]

193/2005. (IX. 22.) Korm. rendelet az elektronikus ügyintézés részletes szabályairól [hatályon kívül]

45/2005. (III. 11.) Korm. rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól [hatályon kívül 2016. 07. 01-től]

114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól

24/2006. (IV. 29.) BM-IHM-NKÖM együttes rendelet a közfeladatot ellátó szerveknél alkalmazható iratkezelési szoftverekkel szemben támasztott követelményekről [hatályon kívül]

12/2005. (X. 27.) IHM rendelet az elektronikus ügyintézési eljárásban alkalmazható dokumentumok részletes technikai szabályairól [hatályon kívül]

9/2005. (VII. 21.) IHM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról [hatályon kívül]

3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről [hatályon kívül]

7/2002. (IV. 26.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről [hatályon kívül]

2/2002. (IV. 26.) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről

Miniszterelnöki Hivatal: Előterjesztés a Kormánynak az informatikai biztonságról szóló törvényről. 2009. április

Gazdálkodás, pénzügy és számvitel

(röv. Kbt.) 2015. évi CXLIII. törvény a közbeszerzésekről

(röv. Hpt.) 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról

2011. évi CXCV. törvény az államháztartásról

2011. évi CVIII. törvény a közbeszerzésekről [hatályon kívül]

2011. évi LXVI. törvény az Állami Számvevőszékről

2007. évi CXXXVIII. törvény a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól

(röv. ÁFA tv.) 2007. évi CXXVII. törvény az általános forgalmi adóról

2007. évi CXVII. törvény a foglalkoztatói nyugdíjról és intézményeiről

2004. évi XXII. törvény a befektetők és a betétesek fokozott védelmével kapcsolatos egyes törvények módosításáról [hatályon kívül]

(röv. Bit.) 2014. évi LXXXVIII. törvény a biztosítási tevékenységről

(röv. Tpt.) 2001. évi CXX. törvény a tőkepiacról

2000. évi C. törvény a számvitelről

(röv. Mpt.) 1997. évi LXXXII. törvény a magánnyugdíjról és a magánnyugdíjpénztárakról

1996. évi CXII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról [hatályon kívül]

(röv. Öpt.) 1993. évi XCVI. törvény az Önkéntes Kölcsönös Biztosító Pénztárakról

257/2007. (X. 4.) Korm. rendelet a közbeszerzési eljárásokban elektronikusan gyakorolható eljárási cselekmények szabályairól, valamint az elektronikus árlejtés alkalmazásáról

168/2004. (V. 25.) Korm. rendelet a központosított közbeszerzési rendszerről, valamint a központi beszerző szervezet feladat- és hatásköréről

283/2001. (XII. 26.) Korm. rendelet a befektetési és az árutőzsdei szolgáltatási tevékenység, az értékpapír letéti őrzés, az értékpapír letétkezelés, valamint az elszámolóházi tevékenység végzéséhez szükséges személyi, tárgyi, technikai és biztonsági feltételekről [hatályon kívül]

98/1995. (VIII. 24.) Korm. rendelet az egyes értékpapírok előállításának, kezelésének és fizikai megsemmisítésének biztonsági szabályairól [hatályon kívül]

47/2013. (XI. 7.) NGM rendelet az adóügyek állami adóhatóság előtt történő elektronikus intézésének szabályairól és egyéb adózási tárgyú miniszteri rendeletek módosításáról [hatályon kívül]

46/2007. (XII. 29.) PM rendelet az elektronikus számlával kapcsolatos egyes rendelkezésekről [hatályon kívül]

34/2007. (XII. 29.) PM rendelet az adóügyek elektronikus intézésének szabályairól [hatályon kívül]

3/1994. (PK. 13.) BAF rendelkezés az egyes bankbiztonsági követelmények meghatározásáról

Egyéb jogterületek

(röv. Btk.) 2012. évi C. törvény a Büntető Törvénykönyvről

(röv. Szvmt.) 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól

(röv. Ekertv.) 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről

(röv. Be.) 1998. évi XIX. törvény a büntetőeljárásról

1995. évi XXVIII. törvény a nemzeti szabványosításról

(röv. régi Btk.) 1978. évi IV. törvény a Büntető Törvénykönyvről [hatályon kívül]

94/1998. (XII. 29.) OGY határozat a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

1656/2012. (XII.20.) Korm. határozat Magyarország Nemzeti Katonai stratégiájának elfogadásáról

1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

1009/2009. (I. 30.) Korm. határozat a Magyar Köztársaság Nemzeti Katonai Stratégiájáról [hatályon kívül 2012. 12. 21-től]

2073/2004. (IV. 15.) kormányhatározat a Magyar Köztársaság nemzeti biztonsági stratégiájáról [hatályon kívül 2012. 02. 22-től]

Kollégiumvezetők álláspontja a Btk.-t módosító novella (a 2001. évi CXXI. tv.) egyes rendelkezéseinek alkalmazásával kapcsolatos jogértelmezési kérdésekben (2002. május 27.)

Külföldi nemzeti jog

Data Protection Act 1998 (United Kingdom)

Personal Data Protection Act of the Republic of Slovenia (Zakon o varstvu osebnih podatkov, ZVOP-1)

Közösségi jog

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR)

Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS)

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [hatályon kívül]

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Regulation (EC) No. 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)

Szabványok és ajánlások

De jure szabványok

ISO 8879:1986 Information processing – Text and office systems – Standard Generalized Markup Language (SGML)

ISO/IEC 13888-1:2009 Information technology – Security techniques – Non-repudiation – Part 1: General

ISO/IEC 13888-2:1998 Information technology – Security techniques – Non-repudiation – Part 2: Mechanisms using symmetric techniques

ISO/IEC 13888-3:2009 Information technology – Security techniques – Non-repudiation – Part 3: Mechanisms using asymmetric techniques

ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

ISO/IEC 15408-2:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components

ISO/IEC 15408-3:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components

ISO/IEC 18045:2008 Information technology – Security techniques – Methodology for IT security evaluation

ISO/IEC 20000-1:2011 Information technology – Service management – Part 1: Service management system requirements

ISO/IEC 20000-2:2012 Information technology – Service management – Part 2: Guidance on the application of service management systems

ISO/IEC 20000-3:2012 Information technology – Service management – Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1

ISO/IEC TR 20000-4:2010 Information technology – Service management – Part 4: Process reference model

ISO/IEC TR 20000-5:2013 Information technology – Service management – Part 5: Exemplar implementation plan for ISO/IEC 20000-1

ISO/IEC 20000-6:2017 Information technology – Service management – Part 6: Requirements for bodies providing audit and certification of service management systems

ISO/IEC TR 20000-9:2015 Information technology – Service management – Part 9: Guidance on the application of ISO/IEC 20000-1 to cloud services

ISO/IEC TR 20000-10:2015 Information technology – Service management – Part 10: Concepts and terminology

ISO/IEC TR 20000-11:2015 Information technology – Service management – Part 11: Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: ITIL®

ISO/IEC TR 20000-12:2016 Information technology – Service management – Part 12: Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: CMMI-SVC

ISO/IEC 26300:2006 Open Document Format for Office Applications (OpenDocument) v1.0

ISO/IEC 27000:2016 Information security management systems – Overview and vocabulary

ISO/IEC 27001:2013 Information security management systems – Requirements

ISO/IEC 27002:2013 Code of practice for information security controls

ISO/IEC 27003:2017 Information security management systems – Guidance

ISO/IEC 27004:2016 Information security management – Measurement

ISO/IEC 27005:2011 Information security risk management

ISO/IEC 27006:2015 Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27007:2017 Guidelines for information security management systems auditing

ISO/IEC TR 27008:2011 Guidelines for auditors on IS controls

ISO/IEC 27009:2017 Sector-specific application of ISO/IEC 27001 – Requirements

ISO/IEC 27010:2015 Information security management for inter-sector and inter-organizational communications

ISO/IEC 27011:2016 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

ISO/IEC 27013:2015 Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001

ISO/IEC 27014:2013 Governance of information security

ISO/IEC 27015:2012 Information security management guidelines for financial services (Visszavont szabvány)

ISO/IEC TR 27016:2014 Organizational economics

ISO/IEC 27018:2014 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27019:2017 Information security controls for the energy utility industry

ISO/IEC 27021:2017 Competence requirements for information security management systems professionals

ISO/IEC TR 27023:2015 Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002

ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity

ISO/IEC 27032:2012 Guidelines for cybersecurity

ISO/IEC 27033-1:2015 Network security: Overview and concepts

ISO/IEC 27033-2:2012 Network security: Guidelines for the design and implementation of network security

ISO/IEC 27033-3:2010 Network security: Threats, design techniques and control issues

ISO/IEC 27033-5:2013 Securing communications across networks using Virtual Private Networks (VPNs)

ISO/IEC 27034-1:2011 Application security. Overview and concepts

ISO/IEC 27034-2:2015 Application security. Organization normative framework

ISO/IEC 27034-5:2017 Application security Part 5: Protocols and application security controls data structure

ISO/IEC 27034-6:2016 Application security Part 6: Case studies

ISO/IEC 27035-1:2016 Information security incident management – Part 1: Principles of incident management

ISO/IEC 27035-2:2016 Information security incident management – Part 2: Guidelines to plan and prepare for incident response

ISO/IEC 27036-1:2014 Information security for supplier relationships – Part 1: Overview and concepts

ISO/IEC 27036-2:2014 Information security for supplier relationships – Part 2: Requirements

ISO/IEC 27036-3:2013 Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security

ISO/IEC 27036-4:2016 Information security for supplier relationships – Part 4: Guidelines for security of cloud services

ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence

ISO/IEC 27038:2014 Specification for digital redaction

ISO/IEC 27039:2015 Selection, deployment and operations of intrusion detection and prevention systems (IDPS)

ISO/IEC 27040:2015 Storage security

ISO/IEC 27041:2015 Guidance on assuring suitability and adequacy of incident investigative method

ISO/IEC 27042:2015 Guidelines for the analysis and interpretation of digital evidence

ISO/IEC 27043:2015 Incident investigation principles and processes

ISO 27799:2016 Health informatics – Information security management in health using ISO/IEC 27002

ISO/TR 13569:2005 Financial services – Information security guidelines

MSZ EN 1143-1:2013 Biztonságos értéktárolók. A betörésállóság követelményei, osztályozása és vizsgálati módszerei. 1. rész: Páncélszekrények, ATM-páncélszekrények, értéktároló helyiségek ajtói és értéktároló helyiségek

MSZ EN 45020:2007 A szabványosítás és az azzal kapcsolatos tevékenységek. Általános szakszótár (ISO/IEC Guide 2:2004)

MSZ EN ISO 27799:2017 Egészségügyi informatika. Az információbiztonság irányítása az egészségügyben az ISO/IEC 27002 alkalmazásával (ISO 27799:2016)

MSZ ISO/IEC 13335-1:2005 Informatika. Biztonságtechnika. Az informatikai és távközlési biztonság menedzselése. 1. rész: Az informatikai és távközlési biztonság menedzselésének fogalmai és modelljei

MSZ ISO/IEC TR 13335-3:2004 Informatika. Az informatikai biztonság menedzselésének irányelvei. 3. rész: Az informatikai biztonság menedzselésének technikái

MSZ ISO/IEC TR 13335-4:2004 Informatika. Az informatikai biztonság menedzselésének irányelvei. 4. rész: A biztonsági ellenintézkedések megválasztása

MSZ ISO/IEC TR 13335-5:2004 Informatika. Az informatikai biztonság menedzselésének irányelvei. 5. rész: A hálózatbiztonság menedzselési útmutatója

MSZ ISO/IEC 15408-1:2002 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 1. rész: Bevezetés és általános modell (Visszavont szabvány)

MSZ ISO/IEC 15408-2:2003 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 2. rész: A biztonság funkcionális követelményei (Visszavont szabvány)

MSZ ISO/IEC 15408-3:2003 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 3. rész: A biztonság garanciális követelményei (Visszavont szabvány)

MSZ ISO/IEC 18028-4:2005 Informatika. Biztonságtechnika. IT-hálózatbiztonság. 4. rész: Biztonságos távoli hozzáférés (Visszavont szabvány)

MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények

MSZ EN ISO/IEC 27002:2017 Informatika. Biztonságtechnika. Gyakorlati útmutató az információbiztonsági kontrollokhoz/intézkedésekhez (ISO/IEC 27002:2013, tartalmazza a 2014. évi 1. és a 2015. évi 2. helyesbítést)

MSZ ISO/IEC 27006:2017 Informatika. Biztonságtechnika. Követelmények információbiztonsági irányítási rendszerek auditját és tanúsítását végző szervezetekre

De facto szabványok, ajánlások, módszertanok

A Pénzügyi Szervezetek Állami Felügyeletének 1/2007. számú módszertani útmutatója a pénzügyi szervezetek informatikai rendszerének védelméről

ARTICLE 29 Data Protection Working Party: Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules. Adopted on April 14th, 2005

Belső ellenőrzési kézikönyv. Pénzügyminisztérium, 2004.

Committee of Sponsoring Organisations of the Treadway Commission (COSO)

Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017.

Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1 Revision 5, April 2017.

Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1 Revision 5, April 2017.

Consultative Committee for Space Data Systems: Reference Model for an Open Archival Information System (OAIS). CCSDS Secretariat, Washington, DC, 2002.

COBIT 5, ISACA

Control Objectives for Information and related Technology (COBIT) 4.1, ISACA

CWA 15262 Inventory of Data Protection Auditing Practices

CWA 15263 Analysis of Privacy Protection Technologies, Privacy-Enhancing Technologies (PET), Privacy Management Systems (PMS) and Identity Management systems (IMS), the Drivers thereof and the need for standardization

CWA 15292 Standard form contract to assist compliance with obligations imposed by article 17 of the Data Protection Directive 95/46/EC (and implementation guide)

CWA 15499-1 Personal Data Protection Audit Framework (EU Directive EC 95/46) Part I: Baseline Framework - The protection of Personal Data in the EU

CWA 15499-2 Personal Data Protection Audit Framework (EU Directive EC 95/46) Part II: Checklists, questionnaires and templates for users of the framework - The protection of Personal Data in the EU

Data Protection Audit Manual [United Kingdom]

Data Protection Audit Resource. January 2009.Version 1.0 Office of the Data Protection Commissioner [Ireland]

Department of Defense Directive 8570 (DoD 8570)

Fülöp Istvánné – Borsos Ferenc – Weltherné Szolnoki Dóra – Szabó Balázs: Módszertan az informatikai rendszerek kontrolljainak ellenőrzéséhez (Állami Számvevőszék)

Information Technology Security Evaluation Criteria (ITSEC)

IT Infrastructure Library (ITIL)

(röv. ITB 8. sz. ajánlás) Informatikai Tárcaközi Bizottság ajánlásai. Informatikai biztonsági módszertani kézikönyv 8. sz. ajánlás. Budapest, 1994.

(röv. ITB 12. sz. ajánlás) Informatikai Tárcaközi Bizottság ajánlásai. Informatikai rendszerek biztonsági követelményei 12. sz. ajánlás. Budapest, 1996.

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/1. kötet: Magyar Informatikai Biztonsági Keretrendszer (MIBIK) 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/1-1. kötet: Informatikai Biztonsági Irányítási Rendszer (IBIR) 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/1-2. kötet: Informatikai Biztonság Irányítási Követelmények (IBIK) 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/1-3. kötet: Az Informatikai Biztonság Irányításának Vizsgálata (IBIV) 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/2. kötet: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS) 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/2-1. segédlet: MIBÉTS - Modell és Folyamatok 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/2-2. segédlet: MIBÉTS – Útmutató a Megbízók számára 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/2-3. segédlet: MIBÉTS – Útmutató a Fejlesztők számára 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/2-4. segédlet: MIBÉTS – Útmutató Értékelőknek 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/2-5. segédlet: MIBÉTS – Értékelési módszertan 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/3. kötet: Informatikai Biztonsági Iránymutató Kis Szervezeteknek (IBIX) 1.0 verzió

A Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár http://kovetelmenytar.complex.hu/

Magyar Nemzeti Könyvvizsgálati Standardok, 315. Témaszámú standard: Gazdálkodó és környezetének megismerése valamint a lényeges hibás állítás kockázatának felismerése

Magyar Nemzeti Könyvvizsgálati Standardok, 620. témaszámú standard szakértő munkájának felhasználása

Magyar Nemzeti Könyvvizsgálati Standardok, 1005. témaszámú állásfoglalás a kisvállalkozások könyvvizsgálatának specialitásai

Magyar Országos Levéltár: Levéltári állományvédelmi ajánlás. MOL, Budapest, 2005.

National Conference of State Legislatures: Cyberterrorism http://www.ncsl.org/programs/lis/cip/cyberterrorism.htm [2007. 03. 27.]

Németh Tibor – Rácz Judit – Sőtér Mártonné – Virág Anikó – Bakos Rózsa – Varga Eszter: Informatikai audit a könyvvizsgálatban. Módszertani útmutató. 2008. [2009. 11. 14.] http://www.mkvk.hu/tudastar/utmutatok/informatikaiaudit

Neumann, Peter G. – Robinson, L. – Levitt, Karl N. – Boyer, R. S. – Saxena, A. R.: A Provably Secure Operating System, Stanford Research Institute, Menlo Park, CA, USA, 1975. http://seclab.cs.ucdavis.edu/projects/history/CD/neum75.pdf [2009. 12. 04.]

OECD Guidelines for the Security of Information Systems (26–27 November 1992)

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (25 July 2002)

Project Management Book of Knowledge (PMBOK), PMI

Trusted Computer Systems Evaluation Criteria (TCSEC)

1. sz. függelék: COBIT-Infotv. megfeleltetés[336]

1. A dokumentum célja

1996-ban az Information Systems Audit and Control Foundation® (ISACF®) megalkotta az Információra és a kapcsolatos technológiára vonatkozó kontroll célkitűzéseket (COBIT®). A második kiadás, amelyet javítottak és tartalmilag bővítettek, 1998-ban jelent meg. 1998-ban megalakult az IT Governance Institute (ITGI™) a növekvő fontosságú IT vezetés kutatásának céljából, különös figyelemmel a COBIT keretrendszerre, a folyamatokra, a kontroll célkitűzésekre és az érettségi modellekre. Idővel az ISACF és az ITGI egy szervezetté vált és kibocsátotta a COBIT harmadik kiadását 2000-ben, majd a negyediket 2005-ben. Az 5. verzió 2012-ben kiadásra került, de a különböző mapping-ek nem kerültek még frissítésre, ezért a továbbiakban a 4.1 verziót alkalmazzuk.

A COBIT keretrendszer lehetővé teszi az információrendszer-vezetőknek (CIO), az IT funkció menedzsereknek és azoknak, akik felelősek az informatikáért, hogy segítsenek az érdekelteknek megérteni az informatikai folyamatokat és szolgáltatásokat és könnyen egyesíthetővé váljanak a különböző szabványok. Az érdekeltek eszközként használhatják a COBIT-et, hogy irányítsák az IT által biztosított információt az üzleti folyamatok támogatásának szolgálatába.

A COBIT nem légüres térben működik. Ma számos más szabvány és legjobb gyakorlat gyűjtemény hozzáférhető, ami előírja, hogyan kell a szervezeti informatika funkcióit sajátos aspektusokból irányítani. Ilyen útmutatásokat nemzetközi szabványügyi szervezetek, valamint számos magán- és részben magánszervezet tett közzé. Ennek ellenére még nem készült közös keretrendszer ezen különböző útmutatások összehasonlításáról. Ezen publikáció keretet ad az összehasonlításhoz és ennek eredményeképp következetesen irányítható a folyamatok megfelelősége és fejlesztése. Ahol részletes összehasonlítást lehetett végezni, ott az IT funkciók kezelését hangsúlyoztuk, melynek következményeképp jobb döntéseket lehet hozni.

Ismert tény a vállalatokon belül az IT fontossága és az irányítást, vezetést és ellenőrzést segítő útmutatások bősége. Világos, hogy szükség van egy ajánlásra, amely választ ad például a következő kérdésekre:

- Mit kell leírni?
- Milyen részletesen?
- Mit kell mérni?
- Mit kell automatizálni?
- Mi a jó gyakorlat?
- Van-e lehetőség tanúsításra?

Az ISACA több, ehhez a dokumentumhoz hasonló ajánlást bocsátott ki a COBIT különböző iránymutatásoknak való megfeleltetésére, például:
COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT®, 2nd Edition

[336] A COBIT vonatkozó részeinek felhasználását az ITGI engedélyezte. Illési Zsolt a szerzői jogairól lemondott a szerzőtárs javára.

COBIT® Mapping: Mapping of SEI's CMM for Software With COBIT® 4.0
COBIT® Mapping: Mapping of PMBOK® With COBIT® 4.0
COBIT® Mapping: Mapping of CMMI for Development v1.2 With COBIT® 4.0
COBIT® Mapping: Mapping of ITIL With COBIT® 4.0
COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0
COBIT® Mapping: Mapping of TOGAF With COBIT® 4.0
COBIT® Mapping: Mapping of COSO ERM With COBIT® 4.1
COBIT® Mapping: Mapping of IT Baseline Protection Manual With COBIT® 4.1
COBIT® Mapping: Mapping of NIST FISMA With COBIT® 4.1

Bár ezek szabványok, történt már megfeleltetés egy jogszabályi követelménynek: IT Control Objectives for Sarbanes-Oxley, amely egy Amerikai Egyesült Államokban hatályos szövetségi törvényt, a Sarbanes-Oxley Act-et felelteti meg a COBIT-nak. Ez alapján teszünk kísérletet ebben az ajánlásban egy magyar jogszabály COBIT-nak való megfeleltetésének.

Ismert jogalkalmazói probléma a jogszabályban egy bizonyos szakterületre háruló feladatok kinyerése és konkretizálása, az adott szakterület „nyelvére" lefordítani azt. Ebben a dokumentum kísérletet teszünk arra, hogy az információs törvény minden egyes, informatikára háruló szabályát a széles körben elfogadott COBIT követelményeinek feleltessünk meg, lehetővé téve, hogy a jogalkalmazó megtehesse a személyes adatok védelmének és a közérdekű adatok nyilvánosságának érdekében a megfelelő lépéseket.

A következőkben az egymásnak megfeleltetett iránymutatások kerülnek bemutatásra pár mondatban.

COBIT: Eredetileg IT folyamat és kontroll keretrendszerként került kiadásra, amely összekapcsolja az IT és az üzleti követelményeket. A Vezetői útmutató hozzáadásával 1998-ban mára gyakrabban használják az IT irányítás keretrendszereként, amely vezetői eszközöket biztosít, mint a mérés és az érettségi modellek a kontroll keretrendszer kiegészítéseképpen. Legutolsó kiadása a 2007-ben megjelent 4.1-es verzió.

Információs törvény (Infotv.): Az információs törvény a Magyarország területén folytatott minden olyan adatkezelésre és adatfeldolgozásra kiterjed, amely természetes személy adataira vonatkozik, valamint amely közérdekű adatot vagy közérdekből nyilvános adatot tartalmaz. Alkalmazása ezért rendkívül széles körű.

2. A megfeleltetés módszertana

A megfeleltetés két rétegben került végrehajtásra. A magas szintű megfeleltetés összehasonlítja az információs törvény jogszabályszöveg alapján értelmezett céljait a COBIT IT folyamataival.
A részletes megfeleltetés az alábbiak alapján történt.

Lépés	Leírás
1.	Az információs törvény bekezdésekre lett bontva. Azok a bekezdések, amelyek tartalmaztak az informatikai rendszerre értelmezhető követelményeket, megfeleltetésre kerültek egy vagy több COBIT kontroll célkitűzéshez. Ezeket a bekezdéseket információs követelményeknek

	nevezzük.
2.	Az információs követelmények megfeleltetésre kerültek a COBIT kontroll célkitűzésekhez az alábbiak alapján: a) Egy az egyhez megfeleltetés történt, ha az információs követelmény egy kontroll célkitűzéshez illeszkedett. b) Egy az többhöz megfeleltetés történt, ha az információs követelmény egynél több kontroll célkitűzéshez illeszkedett. c) Ha az információs követelmény lefedett egy teljes kontroll célkitűzést, akkor megfeleltetésre került az adott követelményhez.
3.	Az információs követelmények a COBIT keretrendszerben meghatározottak alapján szétválogatásra kerültek.

3. COBIT áttekintés

A dokumentum osztályozása

A COBIT egy dokumentumgyűjtemény, amelyet általánosan elfogatott legjobb gyakorlatnak tekinthetünk az informatikai irányítás, kontroll és a bizonyosság nyújtásának területén.

Kibocsátó

A COBIT első kiadását az ISACF bocsátotta ki 1996-ban. 1998-ban a második kiadás további kontroll célkitűzésekkel és Implementációs Eszköztárral egészült ki. A harmadik kiadást az ITGI bocsátotta ki 2000-ben, amely már tartalmazta a vezetői útmutatót és több, most már részletezett kontroll célkitűzést. 2005-ben az ITGI teljesen átdolgozta a COBIT tartalmát és 4.0 verzióval publikálta azt. 2007-ben készült el a jelenlegi, kisebb javításokat tartalmazó 4.1-es változat.

A kiadvány célja

Egy irányadó, naprakész, nemzetközileg elfogadott informatikai irányítási kontroll keretrendszer kutatása, kidolgozása, közzététele és népszerűsítése annak érdekében, hogy a vállalatok átvegyék, és hogy az üzleti vezetők, az informatikai szakemberek, és a bizonyosság nyújtást végző szakemberek munkájuk során rendszeresen használják.

Üzleti hajtóerő a megvalósításhoz

A COBIT informatikai irányítási keretrendszerként való megvalósításának előnyei közé tartoznak az alábbiak:

- Az informatika és a szervezeti célok jobb illeszkedése, az üzleti célokból kiindulva;
- Egy, a vezetőség számára érthető áttekinthetés biztosítása arra vonatkozóan, hogy mit csinál az informatika,

- Egyértelmű felelősök és kötelezettségek, a folyamat orientált megközelítésre építve,
- A külső felek és a szabályozó hatóságok számára általánosan elfogadottság,
- Az összes érdekelt fél számára közös értelmezés, egy közös nyelv alapján,
- Az informatikai kontroll környezetre vonatkozó COSO követelmények teljesítése

A megvalósítás hiányából fakadó veszélyek

A COBIT bevezetése elmaradásának veszélyei lehetnek:

- rosszul összeálló IT szolgáltatások
- a széttartás miatt az üzleti célok gyenge támogatottsága
- elpazarolt lehetőségek
- az IT fekete doboz marad
- elmaradás a vezetőség által elvárt és a mért a mért eredmények között
- túlzott IT és általános költségek
- hibás befektetési döntések és elvárások
- az üzleti felhasználók elégedetlensége az IT szolgáltatásokkal
- szabályozások megsértése, pénzbüntetés, engedély visszavonása
- nem teljesített információs kritériumok
- belső ellenőrzési rendszer problémái

Célközönség

Minden szervezet, állami szervezetek és gazdasági társaságok, külső bizonyosságot nyújtó és tanácsadó szervezetek. A szervezeteken belül három szintet céloz meg: a vezetést, az IT felhasználókat és szakembereket, valamit a bizonyosságot nyújtó szakembereket.

Időszerűség

A COBIT alapvető fontosságú tartalmi részei 2005-ben frissítése kerültek, ez került kiadásra 4.0 verziószámmal. A frissítést megalapozó kutatás a kontroll célkitűzéseket a vezetői útmutatót célozta meg. A dokumentum újabb frissítése 2007-ben történt, 4.1 verziószámmal. A megcélzott sajátságos területek a következők voltak:

- COBIT-Informatikai irányítás alulról-felfelé és felülről-lefelé illesztése
- Részletes megfeleltetés a COBIT és az ITIL, CMM, COSO, PMBOK, ISF's Standard of Good szabványoknak

A jelen összerendelés elkészítésekor megjelent a COBIT új kiadása 5-ös verzióval, de magyar nyelvű változata még várat magára. Mivel az összerendelés nyelve magyar, ezért a meglévő magyar nyelvű 4.1-es verzió kerül felhasználásra, viszont a 4.1 és 5 verziók közötti megfeleltetés[337] alapján az 5-ös verzió kontroll célkitűzésének azonosítóját is feltüntetjük.

Az informatikai biztonság és az ISO/IEC 27002 lehetővé teszi a szabványok nyelvezetének, definícióinak és koncepcióinak az összeegyeztetését:

[337] COBIT 5 „A" mellékelt, 14. ábra

- KGI[338]-KPI[339] okozati kapcsolatok elemzése
- A KGI-k/KPI-k/CSF[340]-k minőségének felülvizsgálata – A KPI/KGI oksági kapcsolat elemzés alapján, felosztva a CSF-eket azokra az elemekre „amire másoktól van szükség", illetve „amit saját magunknak kell elvegezni". CSF-ek folyamat inputokkal lettek helyettesítve (a sikertényezők egyéb szerepet töltenek be) és tevékenység célokkal, amelyeket a folyamatgazdának kell foglalkoznia.
- A metrikákkal kapcsolatos fogalmak részletes elemzése – A metrikákkal foglalkozó szakértőkkel végzett részletes fejlesztés, melynek az a célja, hogy bővítse a metrikákkal kapcsolatos fogalmakat, kiépítsen egy „folyamat-informatikai-üzleti tevékenység" egymásra épülő metrika rendszert, és hogy meghatározza a metrikák minőségügyi kritériumait
- Az üzleti célok, az informatikai célok és az informatikai folyamatok összekapcsolása – részletes kutatás végeztek nyolc különböző iparag területén, melynek eredménye az, hogy részletesebben át lehet látni, hogy a COBIT folyamatok hogyan támogatják a konkrét informatikai célok elérését, és áttételesen az üzleti célok elérését; ezt követően sor került az eredmények általánosítására
- Az érettségi modellek tartalmi felülvizsgálata – A folyamatok között és a folyamatokon belül biztosította az érettségi szintek ellentmondásmentes alkalmazását és minőségét, beleértve az érettségi modell jellemzők jobb meghatározásait

Tanúsítási lehetőség

Az audit irányelvek alapján lehetőség van a kontroll célkitűzéseknek való megfelelés ellenőrzésére önértékelés útján, de nincsen a szervezetek számára tanúsítási lehetőség. Azonban a COBIT keretrendszert gyakran alkalmazzák könyvvizsgálók és könyvelők az audit irányelveknek vagy a SOX-nak való megfelelés bizonyítására.
Az egyének képesítésére a COBIT Foundation Course™ alkalmas, vagy nem COBIT képesítésként az ISACA Certified Information Systems Auditor™ (CISA®) és Certified Information Security Manager® (CISM®) képesítései alkalmazhatók.

Terjesztés

A COBIT-ot világszerte használják. Az angol nyelvű mellett francia, német, magyar, olasz, japán, koreai, portugál és spanyol fordításai is megjelentek.

Teljesség

A COBIT az informatikai vezetés feladatainak széles spektrumával foglalkozik. Ez magában foglalja a legfontosabb feladatokat, azokat is, melyekkel más szabványok is foglalkoznak. Habár technikai részleteket nem tartalmaz, a kontroll célkitűzéseknek való megfelelést biztosító feladatok önmagukért beszélnek. Emiatt magas szintűnek osztályozzák, ami általános teljes körű, nem specifikus.

[338] Key Goal Indicator: kulcs célindikátor
[339] Key Performance Indicator: kulcs teljesítményindikátor
[340] Critical Success Factor: kritikus sikertényező

Hozzáférhetőség

A COBIT 4.1 egy keretrendszer, amely ingyenesen hozzáférhető és letölthető az ITGI és az ISACA weboldalairól (www.itgi.org vagy www.isaca.org/cobit). A COBIT Online® megvásárolható az www.isaca.org/cobitonline oldalon. A COBIT Online lehetővé teszi a COBIT testre szabását, ami megfelel a saját vállalta igényének, melyet tárolni és megváltoztatni is lehet. On-line valósidejű közvélemény-kutatást és teljesítményértékelést tesz lehetővé. Az aktuális Ellenőrzési Kézikönyv az ISACA tagjainak ingyenesen hozzáférhető. Emellett a COBIT nyomtatott verziója megvásárolható az ISACA könyvesboltjából a www.isaca.org/bookstore címen.

Megcélozott COBIT folyamatok

COBIT 4.1 folyamatok													
	1	2	3	4	5	6	7	8	9	10	11	12	13
Tervezés és Szervezés (PO)	+	+	+	+	+	+	+	+	+	+			
Beszerzés és megvalósítás (AI)	+	+	+	+	+	+	+						
Szolgáltatás és támogatás (DS)	+	+	+	+	+	+	+	+	+	+	+	+	+
Figyelemmel kísérés és értékelés (ME)	+	+	+	+									

Megjegyzés: A grafikon nem összehasonlítás, hanem a COBIT maga.

Megcélozott információ-kritériumok

Információ-kritériumok	
+	Eredményesség
+	Hatékonyság
+	Bizalmasság
+	Sértetlenség
+	Rendelkezésre állás
+	Megfelelőség
+	Megbízhatóság

(+) Gyakran célzott
(o) Közepesen célzott
(-) Nem, vagy ritkán célzott

Érintett IT erőforrások

IT erőforrások	
+	Alkalmazások
+	Információ
+	Infrastruktúra
+	Emberek

(+) Gyakran célzott
(o) Közepesen célzott

(-) Nem, vagy ritkán célzott

Dokumentum leírása és tartalma

A vállalatirányítás (az a rendszer, amely segítségével a vállalatokat irányítják és kontrollálják) és az informatikai irányítás (az a rendszer, amellyel a szervezeti informatikai szolgáltatásokat irányítják és kontrollálják) a COBIT szempontjából szoros kapcsolatban állnak egymással. A vállalatirányítás és az informatikai irányítás kölcsönösen nem megfelelőek. Az informatikai szolgáltatások kiterjeszthetik és befolyásolhatják a szervezet teljesítményét, de megfelelően kell azokat irányítani. Másrészről az üzleti folyamatok az informatikai folyamatokból nyerik az információt, és ezt a kölcsönhatást szintén irányítani kell.
E témakörben a tervezés-cselekvés-ellenőrzés-korrekció (plan-do-check-act, PDCA) életciklus ciklus nyilvánvalóvá vált. A PDCA életciklus koncepciót általában strukturált probléma megoldási és javítási folyamatokban használják. A PDCA ciklust, Deming cikluskénti, vagy Deming kerékként ismerik a folyamatos javítási folyamatokban. Az információ szükségletet (vállalatirányítás) és az információszolgáltatást (informatikai irányítás) mérhető és konstruktív indikátorokkal kell megtervezni (tervezés). Az információt és az informatikai rendszereket ki kell fejleszteni, szolgáltatni és felhasználni (cselekvés). A szolgáltatott és felhasznált információkat összehasonlítják az tervezés során meghatározott indikátorokkal (ellenőrzés). A tervtől való eltéréseket kivizsgálják, és javító intézkedéseket tesznek (korrekció).
A függőségek figyelembevételével nyilvánvalóvá válik, hogy az informatikai folyamatok nem öncélúak, hanem az üzleti és menedzsment folyamatokba szervesen integrált célra vezető eszközök.
Az ITGI az informatikai irányítást a következőképp definiálta:
Az informatikai irányítás a felső vezetés és az igazgatótanács felelőssége. Az informatikai irányítás a vállalatirányítás szerves része és tartalmazza a vezetési és szervezeti struktúrákat, folyamatokat és biztosítják, hogy a szervezeti informatika fenntartsa és kiterjessze a szervezeti stratégiákat és célokat.

Informatikai irányítás a COBIT segítségével

Az informatikai irányítás a felső vezetés és az igazgatótanács felelőssége, és tartalmazza a vezetési és szervezeti struktúrákat, folyamatokat és biztosítják, hogy a szervezeti informatika fenntartsa és kiterjessze a szervezeti stratégiákat és célokat.

A COBIT támogatja az informatikai irányítást azáltal, hogy egy keretrendszert nyújt, mely biztosítja, hogy:

- az informatika illeszkedjen az üzleti tevékenységhez,
- az informatika lehetővé tegye az üzleti tevékenységek végrehajtását és maximalizálja az előnyöket,
- az informatikai erőforrásokat felelősen használják fel,
- az informatikai kockázatok kezelése megfelelő legyen.

Az informatikai irányításnak nélkülözhetetlen eleme a teljesítmény mérése. A teljesítmény mérését támogatja a COBIT, és ez a támogatás kiterjed a mérhető célkitűzések meghatározására, és figyelemmel kísérésére, az informatikai folyamatok

által leszállítandó eredményre (folyamat eredmény) és annak leszállítási módjára (folyamat képesség és teljesítmény) vonatkozóan.

COBIT folyamatok

A COBIT az informatikai tevékenységeket négy szakterületbe csoportosítja (ME, PO, AI, DS területek). Az informatikai szolgáltatások által nyújtott bármilyen szolgáltatás az informatikai szolgáltatási életciklus része.

A már elfogadott terveket és a szervezeti struktúrákat alkalmazni lehet a szolgáltatások számára nyújtott fontosság szerint, és nem szükséges valamennyi informatikai szolgáltatáshoz új terveket kidolgozni. A már elfogadott terveket és a szervezeti struktúrákat alkalmazni lehet a szolgáltatások számára nyújtott fontosság szerint, és nem szükséges valamennyi informatikai szolgáltatáshoz új terveket kidolgozni.

Az ezt követően kidolgozott szolgáltatásoknál figyelemmel kell lenni a bevezetés és ellenőrzés módjára a már működő szolgáltatásoknál. a már működő szolgáltatásoknál. Az egyedi szolgáltatások informatikai irányítási szempontból nem lényegesek.

A tervezés központjában a korábban említett PDCA ciklust kell tartani az informatika által nyújtott szolgáltatások egészére. A tervezés központjában a korábban említett PDCA ciklust kell tartani az informatika által nyújtott szolgáltatások egészére.

Valamennyi folyamat leírása a következő információkat tartalmazza:

- a folyamat leírását,
- a kontrol irányelveket,
- a folyamat által érintett információ-kritériumokat
- a folyamat által érintett informatikai erőforrásokat,
- az informatikai irányítás fókusz területeit
- a folyamat bemeneteit és kimeneteit
- tevékenység-felelős hozzárendelési (RACI) ábráját
- a célokat és a metrikát

Információ-követelmény

Az üzleti célkitűzések elérése érdekében az információknak ki kell elégíteniük bizonyos kontroll kritériumokat, amelyeket a COBIT információkra vonatkozó üzleti követelményeknek nevez.
A szélesebb körű minőségi, pénzügyi megbízhatósági, és biztonsági követelmények alapján az alábbi hét megkülönböztethető, egymást minden bizonnyal átfedő információ-kritérium került meghatározásra:

- Eredményesség –azzal foglalkozik, hogy az információk az üzleti folyamat szempontjából jelentőséggel bírnak, és hogy az információkat időben, helyes, ellentmondásmentes és használható módon biztosítják.
- Hatékonyság – arra vonatkozik, hogy az információk az erőforrások optimális (legtermelékenyebb és leggazdaságosabb) felhasználásán keresztül kerüljenek biztosításra.
- Bizalmasság – arra vonatkozik, hogy megakadályozza, a bizalmas információk engedély nélküli nyilvánosságra hozatalát.

- Sértetlenség – az információknak a vállalati értékek és elvárások szerinti pontosságára, és teljességére, valamint az információk érvényességére vonatkozik.
- Rendelkezésre állás – azzal foglalkozik, hogy az információk akkor álljanak rendelkezésre, amikor azokra az üzleti folyamatnak szüksége van most, és a jövőben. A szükséges erőforrások, és az erőforrások szolgáltatási képességeinek védelmére is vonatkozik.
- Megfelelőség – azon törvények, jogszabályok, szabályozások és szerződéses megállapodások – azaz kívülről előírt üzleti követelmények és belső irányelvek – betartásával kapcsolatos, amelyeknek az üzleti folyamat a tárgyát képezi.
- Megbízhatóság – a szükséges információk vezetés számára történő biztosítására vonatkozik, a vállalkozás működtetése és a pénzügyi megbízhatósági, és irányítási kötelezettségek teljesítése érdekében.

Informatikai erőforrások

A COBIT-ban azonosított informatikai erőforrások az alábbiak szerint határozhatók meg:

- Az alkalmazások automatizált felhasználói rendszerek és manuális eljárások, amelyek feldolgozzák az információkat.
- Az információk azok az adatok, összes formájukban, amelyeket az információrendszerek, mint bemeneti, feldolgozott és kimeneti adatot kezelnek, bármilyen formában használja is az t fel az üzleti tevékenység.
- Az infrastruktúra az a technológia és azok az eszközök (azaz hardver, operációs rendszerek, adatbázis-kezelő rendszerek, hálózatok, multimédia, és az azokat befogadó és támogatást biztosító környezet), amelyek lehetővé teszik az alkalmazások működését.
- Az emberek az információrendszerek és szolgáltatások tervezéséhez, szervezéséhez, beszerzéséhez, megvalósításához, szolgáltatásához, támogatásához, figyelemmel kíséréséhez és értékeléséhez szükséges munkatársak. Lehetnek belső, kiszervezet, illetve szerződéses személyek, az igényeknek megfelelően.

Érettségi modell

Az érettségi modell az informatikai folyamatok feletti irányítást és kontrolt szolgáló érettségi modellezés a szervezet értékelésének egyik módszerére épül, melynek alapján az érettség osztályozható a COBIT 34 folyamatának mindegyikére egy nem létező (1) érettségi szint és az optimalizált (5) szint között. A COBIT 34 folyamatának mindegyikére kidolgozott érettségi modellek segítségével a vezetés be tudja azonosítani az alábbiakat:

- A vállalkozás tényleges teljesítménye – Hol tart a vállalkozás ma
- Az ipar jelenlegi állapota – Az összehasonlítás
- A vállalat folyamatfejlesztési célja – Hol akar lenni a vállalat

Az érettségi attribútum táblázat felsorolja az informatikai folyamatok irányítási módjának jellemzőit és leírja, hogy hogyan alakíthatók ki a nem létező állapotból egy optimalizált folyamattá. Az attribútumok felhasználhatók átfogóbb értékeléshez,

eltéréselemzéshez, és a folyamatjavítás tervezéséhez. Az érettségi attribútumok a következők:

- Tudatosság és tájékoztatás
- Irányelvek, tervek és eljárások
- Eszközök és automatizálás
- Szaktudás és tapasztalat
- Felelősség és elszámoltathatóság
- A célok kitűzése és mérése

COBIT kocka

A korábban említett komponensek (informatikai folyamatok, üzleti információ-kritériumok és erőforrások) három dimenzióban illusztrálják az informatika szerepét. Ezeket a dimenziókat a COBIT kocka tartalmazza. A COBIT kocka megtalálható a COBIT 4.1 „COBIT Keretrendszer" című fejezetében.

Az informatikai folyamatok és kontroll célkitűzéseket, tevékenység célokat, kulcs teljesítmény indikátorokat, kulcs célindikátorokat és érettségi modelleket a COBIT tartalmazza.
További információkért ld. a COBIT Keretrendszert és Mellékleteit.

További hivatkozások

Internet	
ISACA	www.isaca.org/cobit
ITGI	www.itgi.org
ISACA HuC	www.isaca.hu

4. Az információs törvény áttekintése

A dokumentum osztályozása

A 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (információs törvény, Infotv.) egy jogszabály.

Kibocsátó

A törvényeket Magyarország Alaptörvénye és a jogalkotásról szóló 2010. évi CXXX. törvény alapján a Magyarország Országgyűlése alkotja.
Az információs törvény 2011. július 26-án került kihirdetésre.
Az Európai Unió jogának való megfelelés miatt az információs törvény megfelel a 95/46/EK számú irányelvben foglaltaknak.

A kiadvány célja

Az információs törvény célja annak biztosítása, hogy - ha a törvényben meghatározott jogszabály kivételt nem tesz - személyes adatával mindenki maga rendelkezzen, és a közérdekű adatokat mindenki megismerhesse.
A törvényben foglaltaktól eltérni csak akkor lehet, ha azt e törvény kifejezetten megengedi.
A törvény szerint megengedett kivételt csak meghatározott adatfajtára és adatkezelőre együttesen lehet megállapítani.

Üzleti hajtóerő a megvalósításhoz

Az adatvédelmi szabályok betartása növeli a szervezet iránti bizalmat az ügyfelek, vevők részéről és a stakeholderek részéről, így versenyelőnyt jelenthet, kifejezetten az információ-intenzív tevékenységek körében.

A megvalósítás hiányából fakadó veszélyek

Az adatvédelmi szabályok betartása törvényi kötelezettség. Büntető-, polgári-, vagy a Nemzeti Adatvédelmi és Információszabadság Hatóság eljárásában komoly anyagi és erkölcsi veszteséget jelenthet azok meg nem tartása.

Célközönség

Az információs törvény hatálya a Magyarország területén folytatott minden olyan adatkezelésre és adatfeldolgozásra kiterjed, amely természetes személy adataira vonatkozik, valamint amely közérdekű adatot vagy közérdekből nyilvános adatot tartalmaz.
A törvényt a teljesen vagy részben automatizált eszközzel, valamint a manuális módon végzett adatkezelésre és adatfeldolgozásra egyaránt alkalmazni kell.
Nem kell alkalmaznia a törvény rendelkezéseit a természetes személynek a kizárólag saját személyes céljait szolgáló adatkezeléseire.

Időszerűség

Az információs törvény 2011. július 26-én került kihirdetésre, majd 2012. január 1-jétől lépett hatályba. A jelenleg aktuális változat 2013. 07. 01-től hatályos.

Tanúsítási lehetőség

Jelenleg nincsen hivatalosan elfogadott tanúsítási lehetőség. Magyarországon adatvédelmi hatóság működik (Nemzeti Adatvédelmi és Információszabadság Hatóság) és végez adatvédelmi auditot, de ez nem jelent tanúsítást és nincsen jogi kötő ereje.
Lehetőség van továbbá adatvédelmi audit lefolytatására az intézmény keretein belül, illetve üzleti alapon, megállapodás szerinti felelősségvállalással, akár tanúsítási lehetőséggel.
Személyek tanúsítására nincs hivatalosan elfogadott lehetőség, de léteznek belső adatvédelmi felelős képzések.

Terjesztés

Az információs törvényt Magyarországon alkalmazzák és hivatalosan csak magyar nyelven érhető el.

Teljesség

Az információs törvény adatvédelmi jogi szempontból alapvetően megfelel a szakmai követelményeknek.
Az informatikai követelmények szempontjából az információs törvény nem törekszik teljes körűségre.

Hozzáférhetőség

Az információs törvény hivatalosan a Magyar Közlönyben, Magyarország hivatalos lapjában és a www.magyarorszag.hu kormányzati portálon érhető el.

Megcélozott COBIT folyamatok

COBIT 4.1 folyamatok													
	1	2	3	4	5	6	7	8	9	10	11	12	13
Tervezés és Szervezés (PO)	-	+	-	+	-	-	-	-	+	-			
Beszerzés és megvalósítás (AI)	-	-	-	-	-	-	-						
Szolgáltatás és támogatás (DS)	-	-	-	+	+	-	-	+	-	-	+	-	-
Figyelemmel kísérés és értékelés (ME)	-	-	-	-									

Megcélozott információ-kritériumok

Információ-kritériumok	
-	Eredményesség[341]
-	Hatékonyság[342]
+	Bizalmasság[343]
+	Sértetlenség
+	Rendelkezésre állás[344]
-	Megfelelőség
-	Megbízhatóság

[341] Bár a hivatkozott COBIT kontrollok alapján közepesen célzott információ-kritérium az eredményesség, a jogszabályban nem érintett terület

[342] Bár a hivatkozott COBIT kontrollok alapján közepesen célzott információ-kritérium a hatékonyság, a jogszabályban nem érintett terület

[343] A bizalmasság kritériuma csak a személyes adatok tekintetében merül fel.

[344] A rendelkezésre állás kritériuma elsősorban a közérdekű adatok tekintetében, másodsorban a személyes adatok tekintetében merül fel.

(+) Gyakran célzott
(o) Közepesen célzott
(-) Nem, vagy ritkán célzott

Érintett IT erőforrások

	IT erőforrások
-	Alkalmazások[345]
+	Információ*
o	Infrastruktúra
o	Emberek[346]

(+) Gyakran célzott
(o) Közepesen célzott
(-) Nem, vagy ritkán célzott

*Csak az információ zárt körére vonatkozik, amelyek a következőek:

- **személyes adat:** az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;

- **különleges adat:**
  a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,
  b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

- **bűnügyi személyes adat:** a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat

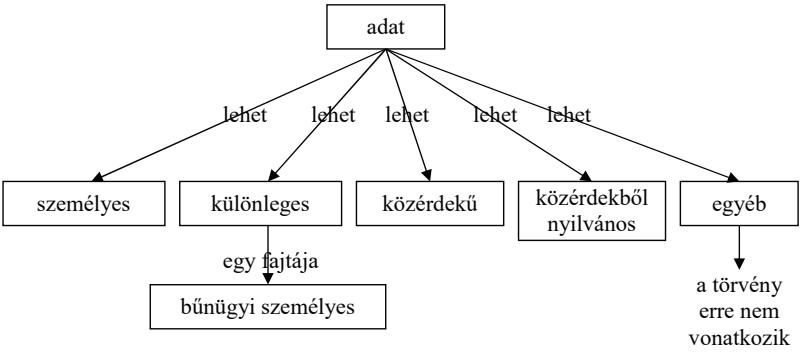
- **közérdekű adat:** az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai

345 A jogszabályban közvetlenül nem érintett IT erőforrások az alkalmazások, de több esetben értelmezhetőek a követelmények az alkalmazásokra is. A részletes megfeleltetésben egy teljes követelmény-csoport, az alkalmazás-kontrollok (AC) fedik le a területet.

346 Az emberek, mint IT erőforrás csak a belső adatvédelmi felelős és a Nemzeti Adatvédelmi és Információszabadság Hatóság esetében érintettek.

tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat

- **közérdekből nyilvános adat:** a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli



1. ábra: Koncepciós térkép az adatokról az Infotv. szerint

Dokumentum leírása és tartalma

Az Infotv. a személyes adatok védelmére és a közérdekű adatok nyilvánosságára vonatkozó általános követelményeket fogalmazza meg, amelyeket a törvényben meghatározott kivételektől (pl. magánszemély magáncélú adatkezelése) eltekintve minden esetben alkalmazni kell. Egyes területekre (pl. egészségügy, direkt marketing) szektoriális szabályok is vonatkoznak, amelyeket külön törvény határoz meg.
Az Infotv. tartalmazza az érintettek jogait és kötelezettségeit és az adatkezelésre vonatkozó általános szabályokat. Az Infotv. kevés direkt utalást tartalmaz az informatikai rendszerekre vonatkozó kontrollok tekintetében.

További hivatkozások

Internet	
adatvédelmi hatóság	http://www.naih.hu/
Országgyűlés	http://www.parlament.hu/
Kormányzati portál	http://www.magyarorszag.hu/

5. Magas szintű megfeleltetés

Áttekintés

Ez a fejezet tartalmazza az Infotv.-ben meghatározott jogszabályi követelményeknek (bekezdéseknek) a COBIT kontroll-célkitűzéseivel való megfeleltetésének az eredményét. Az eredmény összefoglalása tátható a 2. ábrán.

COBIT 4.1 folyamatok													
	1	2	3	4	5	6	7	8	9	10	11	12	13
Tervezés és Szervezés (PO)	o	o	o	+	-	o	o	-	o	-			
Beszerzés és megvalósítás (AI)	o	o	-	-	-	o	o						
Szolgáltatás és támogatás (DS)	o	-	o	o	o	-	-	+	-	o	+	o	o
Figyelemmel kísérés és értékelés (ME)	o	-	o	-									

2. ábra: A lefedettség kvalitatív áttekintése

Jelmagyarázat:
(+) Jelentős egyezés (legalább 5 bekezdés került társításra COBIT folyamatokhoz)
(o) Kisebb mértékű egyezés (1-4 bekezdés került társításra)
(-) Nem kapcsolódó (nem került bekezdés társításra)
Satírozott rubrika: nincs ilyen folyamat

Tervezés és Szervezés

PO1 Az informatikai stratégiai terv meghatározása
Egy jogszabályi követelmény (7. § (1)) volt ennek a COBIT folyamatnak megfeleltethető.

PO2 Az információ-architektúra meghatározása
Három jogszabályi követelmény (3. §, 7. § (2), 7. § (4)) volt ennek a COBIT folyamatnak megfeleltethető.

PO3 A technológiai irány kijelölése
Egy jogszabályi követelmény (7. § (2)) volt ennek a COBIT folyamatnak megfeleltethető.

PO4 Az informatikai folyamatok, szervezet és a kapcsolatok meghatározása
Hat jogszabályi követelmény (7. § (2), 10. § (1), 10. § (3), 10. § (4), 24. § (1), 24. § (2)) volt ennek a COBIT folyamatnak megfeleltethető.

PO5 Az informatikai beruházások irányítása
Nem volt olyan jogszabályi követelmény, amely ennek a COBIT folyamatnak megfeleltethető lett volna.

PO6 Tájékoztatás a vezetői célokról és irányról
Egy jogszabályi követelmény (24. § (2)) volt ennek a COBIT folyamatnak megfeleltethető.

PO7 Az informatikai humán erőforrások kezelése
Egy jogszabályi követelmény (24. § (2)) volt ennek a COBIT folyamatnak megfeleltethető.

PO8 Minőségirányítás
Nem volt olyan jogszabályi követelmény, amely ennek a COBIT folyamatnak megfeleltethető lett volna.

PO9 Az informatikai kockázatok felmérése és kezelése
Két jogszabályi követelmény (7. § (2), 7. § (6)) volt ennek a COBIT folyamatnak megfeleltethető.

PO10 A projektek irányítása
Nem volt olyan jogszabályi követelmény, amely ennek a COBIT folyamatnak megfeleltethető lett volna.

Beszerzés és megvalósítás

AI1 Az automatizált megoldások meghatározása
Egy jogszabályi követelmény (11. § (1)) volt ennek a COBIT folyamatnak megfeleltethető.

AI2 Az alkalmazási szoftverek beszerzése és karbantartása
Egy jogszabályi követelmény (7. § (2)) volt ennek a COBIT folyamatnak megfeleltethető.

AI3 A technológiai infrastruktúra beszerzése és karbantartása
Nem volt olyan jogszabályi követelmény, amely ennek a COBIT folyamatnak megfeleltethető lett volna.

AI4 Az üzemeltetés és a használat támogatása
Nem volt olyan jogszabályi követelmény, amely ennek a COBIT folyamatnak megfeleltethető lett volna.

AI5 Az informatikai erőforrások beszerzése
Nem volt olyan jogszabályi követelmény, amely ennek a COBIT folyamatnak megfeleltethető lett volna.

AI6 A változtatások kezelése
Egy jogszabályi követelmény (7. § (2)) volt ennek a COBIT folyamatnak megfeleltethető.

AI7 A megoldások és változtatások üzembe helyezése és bevizsgálása
Egy jogszabályi követelmény (7. § (3)) volt ennek a COBIT folyamatnak megfeleltethető.

Szolgáltatás és támogatás

DS1 A szolgáltatási szintek meghatározása és betartása

Egy jogszabályi követelmény (10. § (4)) volt ennek a COBIT folyamatnak megfeleltethető.

DS2 Külső szolgáltatások igénybevételének irányítása
Nem volt olyan jogszabályi követelmény, amely ennek a COBIT folyamatnak megfeleltethető lett volna.

DS3 Teljesítmény- és kapacitáskezelés
Egy jogszabályi követelmény (37. § (2)) volt ennek a COBIT folyamatnak megfeleltethető.

DS4 A szolgáltatás folyamatosságának biztosítása
Két jogszabályi követelmény (7. § (2), 7. § (3)) volt ennek a COBIT folyamatnak megfeleltethető.

DS5 A rendszerek biztonságának megvalósítása
Két jogszabályi követelmény (7. § (2), 7. § (3)) volt ennek a COBIT folyamatnak megfeleltethető.

DS6 A költségek azonosítása és felosztása
Nem volt olyan jogszabályi követelmény, amely ennek a COBIT folyamatnak megfeleltethető lett volna.

DS7 A felhasználók oktatása és képzése
Nem volt olyan jogszabályi követelmény, amely ennek a COBIT folyamatnak megfeleltethető lett volna.

DS8 A rendkívüli események kezelése és a felhasználói támogatás működtetése
Nyolc jogszabályi követelmény (7. § (5), 11. § (2), 14. §, 15. § (1), 15. § (4), 16. § (2), 16. § (3), 18. § (1)) volt ennek a COBIT folyamatnak megfeleltethető.

DS9 Konfigurációkezelés
Nem volt olyan jogszabályi követelmény, amely ennek a COBIT folyamatnak megfeleltethető lett volna.

DS10 Problémakezelés
Egy jogszabályi követelmény (10. § (1)) volt ennek a COBIT folyamatnak megfeleltethető.

DS11 Az adatok kezelése
Hét jogszabályi követelmény (4. § (4), 7. § (2), 7. § (3), 10. § (1), 17. § (1), 17. § (2), 33. § (1)) volt ennek a COBIT folyamatnak megfeleltethető.

DS12 A fizikai környezet biztosítása
Két jogszabályi követelmény (7. § (2), 7. § (3)) volt ennek a COBIT folyamatnak megfeleltethető.

DS13 Az üzemeltetés irányítása
Egy jogszabályi követelmény (10. § (1)) volt ennek a COBIT folyamatnak megfeleltethető.

Figyelemmel kísérés és értékelés

ME1 Az informatika teljesítményének figyelemmel kísérése és értékelése
Egy jogszabályi követelmény (10. § (1)) volt ennek a COBIT folyamatnak megfeleltethető.

ME2 A belső irányítási és ellenőrzési rendszer figyelemmel kísérése és értékelése
Nem volt olyan jogszabályi követelmény, amely ennek a COBIT folyamatnak megfeleltethető lett volna.

ME3 Külső követelményeknek való megfelelőség biztosítása
Két jogszabályi követelmény (7. § (2), 11. § (1)) volt ennek a COBIT folyamatnak megfeleltethető.

ME4 Az informatikai irányítás megteremtése
Nem volt olyan jogszabályi követelmény, amely ennek a COBIT folyamatnak megfeleltethető lett volna.

IT rendszerekkel szemben támasztott általános követelmények (AC)

Két jogszabályi követelmény (4. § (4), 7. § (5)) volt ennek a COBIT folyamatnak megfeleltethető.

Folyamatokkal szemben támasztott általános követelmények (PC)

Két jogszabályi követelmény (4. § (1), 10. § (1)) volt ennek a COBIT folyamatnak megfeleltethető.

6. Részletes megfeleltetés

(F) Felülmúlt
(T) Teljes lefedettség
(R) Részleges, valamely szempont(ok) lefedve
(N) Nincs lefedve

Kontroll célkitűzésenkénti különös követelmények

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
PO1	**Az informatikai stratégiai terv meghatározása**			
PO1.1	Az informatikai érték menedzsment Együtt kell működni az üzleti területekkel annak biztosítása érdekében, hogy a vállalat informatikával támogatott beruházásaiból álló portfolióban levő programok szilárd alapon álló üzleti tervekre épüljenek. Fel kell ismerni azt, hogy léteznek kötelező, stratégiát közvetlenül alátámasztó és lehetőség szerint megvalósítható befektetések, amelyek eltérőek összetettségüket és a források elosztásának szabadságfokát illetően. Az informatikai folyamatoknak eredményesen és hatékonyan kell biztosítaniuk a programok megvalósításához szükséges informatikai elemeket, és korán figyelmeztetniük kell a tervtől történő bárminemű olyan eltérés esetén, beleértve a költséget, ütemtervet, illetve funkcionalitást, amely hatást gyakorolhat a programok elvárt eredményeire. Az informatikai szolgáltatásokat méltányos, és érvényesíthető szolgáltatási szint megállapodások szerint kell megvalósítani. Egyértelműen kell kijelölni az előnyök sikeres megvalósításának és a költség kontrollálásának a felelősét és a tevékenységét figyelemmel kell kísérni. A megtérülés elemzések részrehajlás mentes, átlátható, ismételhető és összehasonlítható értékelését kell megteremteni, beleértve a pénzben kifejezett értéket, az adott képesség le nem szállításának kockázatát, és az elvárt előnyök meg nem valósításának a kockázatát.	EDM02	N	
PO1.2	Az üzleti tevékenység és az informatika illesztése Kétirányú folyamatokat kell megteremteni, az oktatás és a stratégiai tervezésben történő kölcsönös részvétel folyamatainak létrehozása, az üzleti területek és az informatika illesztésének és integrálásának érdekében. Az üzlet és az informatika kényszerfeltételei közti egyeztetést kell tartani a prioritásokban történő közös megállapodás érdekében.	APO02.01	N	
PO1.3	Jelenlegi szolgáltatási képesség és teljesítmény értékelése A megoldás és szolgáltatásnyújtás jelenlegi képességét és teljesítményét értékelni kell egy olyan alapszint meghatározása érdekében, amelyhez a jövőbeli követelmények viszonyíthatók. A teljesítményt meg kell határozni abból a szempontból, hogy az informatika mennyiben járul hozzá az üzleti célkitűzésekhez, funkcionalitásokhoz, stabilitásokhoz,	APO02.02	N	

[347] Source: COBIT 4.1. ©1996-2007 ITGI. All rights reserved. Used by permission.
A felhasználást a jogtulajdonos ITGI 2010. augusztus 5-én kelt felhasználási engedélyében lehetővé tette.

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	összetettséghez, költségekhez, erősségekhez és gyengeségekhez.			
PO1.4	Informatikai stratégiai terv Egy olyan stratégiai tervet kell létrehozni, amely meghatározza az érintett érdekelt felekkel együttműködve, hogy az informatikai célok hogyan fognak hozzájárulni a vállalat stratégia célkitűzéseihez, és a mik a vonatkozó költségek és kockázatok. Tartalmaznia kell, hogy az informatika hogyan fogja támogatni az informatika által támogatott beruházási programokat, informatikai szolgáltatásokat és informatikai eszközöket. Az informatikának meg kell határoznia a célkitűzések teljesülésének módját, az alkalmazandó méréseket, valamint az érintett felek formális jóváhagyásának megszerzésére vonatkozó eljárásokat. Az informatikai stratégiai tervnek le kell fednie a beruházási / működtetési költségvetést, a finanszírozási forrásokat, a forrásbiztosítási stratégiát, a beszerzési stratégiát, és a jogi és szabályozási követelményeket. A stratégiai tervnek kellőképpen részletesnek kell lennie ahhoz, hogy lehetővé tegye az informatikai taktikai tervek meghatározását.	APO02.03-05	N	
PO1.5	Informatikai taktikai tervek Az informatikai stratégiai terv alapján informatikai taktikai tervek portfolióját kell kialakítani. A taktikai terveknek ki kell térniük az informatika által támogatott beruházási programokra, informatikai szolgáltatásokra és az informatikai eszközökre. A taktikai terveknek be kell mutatniuk a szükséges informatikai kezdeményezéseket, az erőforrás követelményeket, és azt, hogy az erőforrások felhasználása és az előnyök megvalósítása hogyan lesz figyelemmel kísérve és menedzselve. A taktikai terveknek kellőképpen részletesnek kell lenniük ahhoz, hogy lehetővé tegyék a projekt tervek meghatározását. A projekt és a szolgáltatás portfoliók elemzésével tevékenyen kell menedzselni az informatikai taktikai terveket és kezdeményezéseket.	APO02.05	R	**7. §** (1) Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az e törvény és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét.
PO1.6	Informatikai portfolió menedzsment Az üzleti területekkel együtt tevékenyen kell menedzselni a konkrét stratégiai üzleti célkitűzések eléréséhez szükséges, informatikával támogatott beruházási programok portfolióját, a programok beazonosítása, meghatározása, értékelése, rangsorolása, kiválasztása, kezdeményezése, menedzselése és kontrolálása révén. Ennek ki kell terjednie a kívánt üzleti eredmények tisztázására, annak biztosítására, hogy a program célkitűzései támogatják az eredmények elérését, az eredmények eléréséhez szükséges erőfeszítések teljes terjedelmének megértésére, a támogató intézkedésekért való felelősség egyértelmű kijelölésére, a programon	APO05.05	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	belül a projektek meghatározására, az erőforrások és a finanszírozás elkülönítésére, a hatáskör átruházására és a program indításakor a program elkezdéséhez szükséges projektek indítása.			
PO2	**Az információ-architektúra meghatározása**			
PO2.1	Vállalati információ-architektúra modell Egy vállalati információmodellt kell bevezetni és naprakészen tartani a PO1-ben ismertetett informatikai tervekkel konzisztens módon történő alkalmazásfejlesztés és döntéstámogatás lehetővé tétele érdekében. A modellnek oly módon kell elősegítenie az információknak az üzleti területek általi optimális létrehozatalát, felhasználását és megosztását, hogy az megőrizze a sértetlenséget, és rugalmas, működő, gazdaságos, időszerű, biztonságos és a hibáknak ellenálló legyen.	APO03.02	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
PO2.2	Vállalati adatszótár és adatszintaktikai szabályok Egy olyan vállalati adatszótárt kell naprakészen tartani, amely tartalmazza a szervezet adatszintaktikára vonatkozó szabályait. Ennek a szótárnak lehetővé kell tennie az adatelemek alkalmazások és rendszerek közti megosztását, elő kell segítenie az informatikai és az üzleti felhasználók között az adatok közös értelmezését, és meg kell előznie az ezzel összeegyeztethetetlen adatelemek létrehozását.	APO03.02	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.*** **7. §** (4) A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				tárolt adatok - kivéve ha azt törvény lehetővé teszi - közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.
PO2.3	Adatosztályozási rendszer Egy olyan a szervezet egészére vonatkozó osztályozási sémát kell létrehozni, mely a vállalati adatok kritikus jelentőségén és bizalmas jellegén alapul (például nyilvános, bizalmas, szigorúan titkos). Ennek a sémának tartalmaznia kell az adatokért való felelősségre vonatkozó részleteket; a megfelelő biztonsági szintek és védelmi intézkedések meghatározását és az adat megőrzési és megsemmisítési követelmények, a kritikus jelentőség és bizalmasság rövid ismertetését. Ezt kell felhasználni az olyan kontrollok alkalmazásának alapjául, mint például a hozzáférési jogosultságok ellenőrzése, az archiválás, illetve a titkosítás.	APO03.02	T	**3. §** E törvény alkalmazása során: 2. személyes adat: az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés; 3. különleges adat: a) a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat; 4. bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat; 5. közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				6. közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli; **7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
PO2.4	Adatok sértetlenségének biztosítása Olyan eljárásokat kell meghatározni és megvalósítani, amelyek biztosítják az elektronikus formában tárolt összes adat, úgymint az adatbázisok, adattárházak és adatarchívumok sértetlenségét és konzisztenciáját.	APO01.06	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
PO3	**A technológiai irány kijelölése**			
PO3.1	Technológiai irány tervezése	APO02.03	R	**7. §** (2) Az

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	A létező és a kialakulóban levő technológiákat elemezni kell és azt megtervezni, hogy mely technológiai irány megfelelő az informatikai stratégia és az üzleti rendszerek architektúrájának megvalósításához. Továbbá a tervben azt is azonosítani kell, hogy mely technológiák rendelkeznek azzal a potenciállal, hogy üzleti lehetőségeket teremtsenek. A tervnek foglalkoznia kell a rendszerek architektúrájával, a technológiai iránnyal, a migrációs stratégiákkal és az infrastruktúra elemekkel kapcsolatos rendkívüli helyzet kezelésének kérdéseivel.	APO04.03		adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
PO3.2	Műszaki infrastruktúra terv Az informatikai, stratégiai és taktikai terveknek megfelelő technológiai infrastruktúra tervet kell létrehozni és naprakészen tartani. A tervnek a technológiai irányon kell alapulniuk, és tartalmaznia kell a rendkívüli helyzetekre vonatkozó megoldásokat, és iránymutatást a technológiai erőforrások beszerzésére vonatkozóan. Figyelembe kell vennie a versenykörnyezet változásait, az információrendszerekhez szükséges személyzet és beruházások méretgazdaságosságát, és a platformok és alkalmazások javított együttműködését.	APO02.03-05 APO04.03-05	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
PO3.3	Jövőbeli trendek és jogszabályváltozások figyelemmel kísérése Folyamatot kell működtetni az üzleti szektor, az iparág, a technológia, az infrastruktúra, a jogi és szabályozási környezeti trendek figyelemmel kísérése céljából. Ezen trendek következményeit be kell építeni az informatikai technológiai infrastruktúra terv kidolgozása során.	EDM01.01 APO04.03	N	
PO3.4	Műszaki szabványok A vállalat minden része számára következetes, eredményes és biztonságos technológiai megoldások nyújtása érdekében egy technológiai fórumot kell létrehozni, mely technológiai útmutatásokat, infrastruktúra termékekkel kapcsolatos tanácsadást, a technológia kiválasztásával kapcsolatos útmutatást, valamint ezen szabványok, és útmutatások betartásának	APO03.05	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	mérését biztosítja. Ennek a fórumnak kell meghatároznia a technológiai szabványokat és gyakorlatot az üzleti jelentőségük, a kockázatok és a külső követelményeknek való megfelelőség alapján.			megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
PO3.5	Informatikai architektúra bizottság Egy informatikai architektúra bizottságot kell létrehozni az architektúra útmutatások, és az alkalmazásukra vonatkozó tanácsadás és a megfelelőség ellenőrzésének biztosítása céljából. Ennek a szervezetnek kell irányítania az informatikai architektúra tervezését, biztosítva azt, hogy az lehetővé teszi az üzleti stratégia megvalósítását, és a szabályozási megfelelőségi és a működésfolyamatossági követelmények figyelembe vételét. Ez összefüggésben van / kapcsolódik a PO2 "Az információ-architektúra meghatározása" folyamathoz.	APO01.01	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
PO4	**Az informatikai folyamatok, szervezet és a kapcsolatok meghatározása**			
PO4.1	Informatikai folyamat keretrendszer Informatikai folyamat keretrendszert kell meghatározni az informatikai stratégiai terv végrehajtása céljából. E keretrendszernek tartalmaznia kell egy informatikai folyamat struktúrát és kapcsolatokat (például a folyamat hiányosságok és az átfedések kezelése céljából), a felelősséget, az érettséget, a teljesítménymérést, a javítást, a megfelelőséget, a minőségügyi célokat és az azok eléréshez szükséges terveket. Biztosítania kell az integrációt az olyan folyamatok között, amelyek konkrétan az informatikával, a vállalati portfolió kezelésével, az üzleti folyamatokkal és az üzleti tevékenység változtatási folyamataival kapcsolatosak. Az informatikai folyamat keretrendszernek integrálva kell lennie egy minőségirányítási rendszerbe (QMS) és a belső irányítási és ellenőrzési keretrendszerbe.	APO01.03 APO04.03	N	
PO4.2	Informatikai stratégiai bizottság Igazgatótanácsi szinten létre kell hozni egy informatikai stratégiai bizottságot. Ennek a bizottságnak kell gondoskodnia arról, hogy a	APO01.01	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	vállalatirányítás részeként az informatika irányításával megfelelően foglalkoznak; tanácsot kell adnia a stratégiai irányt illetően; és felül kell vizsgálnia a jelentősebb beruházásokat a teljes igazgatótanács nevében.			
PO4.3	Informatikai irányító bizottság Egy informatikai irányító bizottságot (illetve egy azzal egyenértékű bizottság) kell létrehozni, amely a felső vezetés, és az üzleti és az informatikai vezetés képviselőiből áll az alábbiak érdekében: ▪ Az informatikával támogatott beruházási programok fontossági sorrendjének meghatározása a vállalkozás üzleti stratégiájával és prioritásaival összhangban ▪ A projektek állapotának nyomon követése, és az erőforrás konfliktusok feloldása ▪ A szolgáltatási szintek és a szolgáltatásfejlesztések figyelemmel kísérése	APO01.01	N	
PO4.4	Az informatikai funkció szervezeten belüli elhelyezése Az informatikai funkciót általános szervezeti struktúrában egy olyan üzleti modell szerint kell elhelyezni, hogy az az informatikának a vállalaton belül betöltött jelentőségének megfeleljen, különösen annak megfelelően, hogy mennyire kritikus jelentőséggel bír az üzleti stratégia szempontjából, és hogy a működés mennyire függ az informatikától. Az informatikai igazgató alárendeltségének összhangban kell lennie az informatika szervezeten belüli jelentőségével.	APO01.05	N	
PO4.5	Az informatikai szervezet felépítése Egy olyan belső és külső informatikai szervezeti struktúrát kell létrehozni, amely tükrözi az üzleti igényeket. Ezen kívül egy folyamatot kell bevezetni az informatikai szervezeti struktúra időszakonkénti felülvizsgálatára annak érdekében, hogy a személyzeti követelmények, és az erőforrás stratégiák a várható üzleti célkitűzéseknek, és a változó körülményeknek megfeleljenek.	APO01.01	N	
PO4.6	Szerepkörök és felelősségek kialakítása Az informatikai munkatársak és a végfelhasználók szerepköreit és felelősségeit oly módon kell kialakítani és ismertetni, hogy az informatikai munkatársak és a felhasználók között el legyen különítve a hatáskör, a felelősségek és a szervezet igényeinek kielégítéséért való felelősség tekintetében.	APO01.02	R	**24.** § (1) Az adatkezelő, illetve az adatfeldolgozó szervezetén belül, közvetlenül a szerv vezetőjének felügyelete alá tartozó - jogi, közigazgatási, informatikai vagy ezeknek megfelelő, felsőfokú végzettséggel rendelkező - belső adatvédelmi felelőst kell kinevezni vagy megbízni

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				a) az országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelő, illetve feldolgozó adatkezelőnél és adatfeldolgozónál; *b)* a pénzügyi szervezetnél; *c)* az elektronikus hírközlési és közüzemi szolgáltatónál.
PO4.7	Informatikai minőségbiztosítási felelősség A minőségbiztosítási (QA) funkció teljesítményéért való felelősség ki kell jelölni, és a minőségbiztosítási munkacsoportot el kell látni a megfelelő minőségbiztosítási rendszerekkel, ellenőrzési és tájékoztatási szaktudással. Gondoskodni kell arról, hogy a minőségbiztosítási csoport szervezeti helye és felelősségei, valamint mérete megfeleljen a szervezet követelményeinek.	APO11.01	N	
PO4.8	Kockázatokért, biztonságért és a megfelelőségért való felelősség Az informatikával kapcsolatos kockázatok tulajdonosi szerepét és felelősségét a szervezetben a megfelelő felsővezetői szintjébe kell beilleszteni. Meg kell határozni, és ki kell jelölni az informatikai kockázatok kezelése szempontjából kritikus jelentőségű szerepköröket, úgymint az információbiztonságért, a fizikai biztonságért és a megfelelőségért való konkrét felelősséget. Vállalati szinten kell meghatározni a kockázatkezelési és biztonságirányítási felelősséget a szervezeti egységeken átívelő kérdések kezelése érdekében. További biztonságirányítási felelősségek kijelölése válhat szükségessé rendszer specifikus szinten, az adott rendszerre vonatkozó biztonsági kérdések rendezése érdekében. Meg kell szerezni a felső vezetés iránymutatását az informatikai kockázatvállalási hajlandóság mértékéről, és az informatikai maradványkockázatokat jóvá kell hagyatni velük.	-	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek. **24. §** (2) A belső adatvédelmi felelős a) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában; b) ellenőrzi e törvény és az

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását; c) kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót; d) elkészíti a belső adatvédelmi és adatbiztonsági szabályzatot; e) vezeti a belső adatvédelmi nyilvántartást; f) gondoskodik az adatvédelmi ismeretek oktatásáról.
PO4.9	Adat- és rendszer felelősség Az üzleti területeket el kell látni olyan eljárásokkal és eszközökkel, melyek lehetővé teszik számukra, hogy rendezhessék az adat- és információrendszer felelősséggel kapcsolatos kötelezettségeiket. A felelősöknek döntéseket kell hozniuk az információk és a rendszerek osztályozására, valamint azoknak az osztályozással összhangban történő védelmére vonatkozóan.	APO01.06	T	**10. §** (1) Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit e törvény, valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. Az általa adott utasítások jogszerűségéért az adatkezelő felel. **24. §** (1) Az adatkezelő, illetve az adatfeldolgozó szervezetén belül, közvetlenül a szerv vezetőjének felügyelete alá tartozó - jogi, közigazgatási,

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				informatikai vagy ezeknek megfelelő, felsőfokú végzettséggel rendelkező - belső adatvédelmi felelőst kell kinevezni vagy megbízni *a)* az országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelő, illetve feldolgozó adatkezelőnél és adatfeldolgozónál; *b)* a pénzügyi szervezetnél; *c)* az elektronikus hírközlési és közüzemi szolgáltatónál.
PO4.10	Felügyelet Megfelelő eljárásokat kell megvalósítani a felügyeltre vonatkozóan az informatikai funkción belül annak biztosítása érdekében, hogy a szerepköröket és felelősségeket szabályosan gyakorolják, valamint annak felmérése érdekében, hogy az összes munkatárs rendelkezik-e a szerepeik és felelősségi köreik teljesítéséhez szükséges megfelelő hatáskörrel és erőforrásokkal, valamint általában a kulcsfontosságú teljesítmény indikátorok (Key Performance Indicator, KPI) szemmel tartása végett.	APO01.02	R	**24. §** (2) A belső adatvédelmi felelős a) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában; b) ellenőrzi e törvény és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását; c) kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót; d) elkészíti a belső adatvédelmi és

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				adatbiztonsági szabályzatot; e) vezeti a belső adatvédelmi nyilvántartást; f) gondoskodik az adatvédelmi ismeretek oktatásáról.
PO4.11	Feladatkörök elkülönítése A szerepköröket és felelősségeket oly módon kell megosztani, amely csökkenti annak lehetőségét, hogy egyetlen egyén veszélyeztethessen egy kritikus fontosságú folyamatot. Gondoskodni kell arról, hogy a munkatársak csak a munkakörüknek és beosztásuknak megfelelő, engedélyezett feladatokat hajtsanak végre.	APO01.02	R	**10. §** (3) Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni.
PO4.12	Informatikai személyzet A személyzeti állományra vonatkozó követelményeket rendszeresen, illetve az üzleti, működési, vagy az informatikai környezetben bekövetkező jelentős változtatások esetén ki kell értékelni annak biztosítása érdekében, hogy az informatikai funkció megfelelő erőforrásokkal rendelkezzék ahhoz, hogy megfelelően és szabályosan támogassa az üzleti célokat és célkitűzéseket.	APO07.01	N	
PO4.13	Kulcsfontosságú informatikai munkatársak A kulcsfontosságú informatikai munkatársakat meg kell határozni és be kell azonosítani (például a helyettesítő / tartalék munkatársak), és az egyetlen személy által végzett kritikus fontosságú tevékenységektől való függés mértékét minimalizálni kell.	APO07.02	N	
PO4.14	Szerződéses munkatársakra vonatkozó irányelvek és eljárások Gondoskodni kell arról, hogy az informatikai funkciót támogató tanácsadók, és szerződéses munkatársak ismerjék és betartsák a szervezetnek a szervezet információvagyonának védelmére vonatkozó irányelveket oly módon, hogy betartják a szerződésben rögzített követelményeket.	APO07.06	R	**10. §** (4) Az adatfeldolgozásra vonatkozó szerződést írásba kell foglalni. Az adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				érdekelt.
PO4.15	Kapcsolatok Létre kell hozni és fenn kell tartani egy optimális koordinációs, kommunikációs és kapcsolattartást szolgáló struktúrát az informatikai funkció, és a különböző egyéb olyan, az informatikai funkción belüli és kívüli érdekelt felek között, mint például az igazgatótanács, a felső vezetés, a szervezeti egységek, az egyéni felhasználók, a beszállítók, a biztonsági vezetők, a kockázatkezelők, a vállalati megfelelőségi csoport, a kiszervezett tevékenységet végzők és a telephelyen kívüli vezetők.	APO01.01	N	
PO5	**Az informatikai beruházások irányítása**			
PO5.1	Pénzügyi gazdálkodási keretrendszer Létre kell hozni egy pénzügyi keretrendszert és naprakészen tartani annak érdekében, hogy menedzselni lehessen az informatikai szolgáltatásokba és informatikai eszközökbe történő beruházásokat, és az informatikai költségeket, az informatika által támogatott beruházások portfolióján, az üzleti terveken és az informatikai költségvetési terveken keresztül.	APO06.01	N	
PO5.2	Rangsorolás az informatikai költségvetésen belül Az üzemeltetés, a projektek és a karbantartás informatikai erőforrásai elosztásának rangsorolására szolgáló döntéshozatali folyamatot kell megvalósítani annak érdekében, hogy maximalizálva legyen az informatika hozzájárulása a vállalat informatikával támogatott beruházási program portfoliójának, és a vállalat egyéb informatikai szolgáltatásainak és eszközei a megtérülésének az optimalizálásához.	APO06.02	N	
PO5.3	Informatikai költségvetés elkészítése Eljárásokat kell kidolgozni és megvalósítani egy olyan költségvetés elkészítése érdekében, amely tükrözi a vállalat informatikával támogatott beruházási program portfoliójában megállapított rangsorolást, és amely tartalmazza a jelenlegi infrastruktúra üzemeltetésének és fenntartásának folyamatos költségeit. Az eljárásoknak támogatniuk kell az általános informatikai költségvetés kidolgozását, valamint az egyedi programok költségvetéseinek kialakítását, külön hangsúlyt fektetve ezen programok informatikai elemeire. Az eljárásoknak lehetővé kell tenniük az általános költségvetés és az egyedi programok költségvetéseinek folyamatos felülvizsgálatát, finomítását és jóváhagyását.	APO06.03	N	
PO5.4	Költség-gazdálkodás A tényleges költségeket a költségvetési tervekkel összehasonlító költség-gazdálkodási folyamatot kell megvalósítani. A költségeket figyelemmel kell kísérni, és jelenteni kell. Eltérések esetén azokat időben be kell azonosítani, és fel kell mérni ezen eltérések programokra gyakorolt hatását. Ezen programok üzleti finanszírozóival együtt megfelelő helyreigazító lépéseket kell	APO06.04-05	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	tenni, és amennyiben szükséges, a program megtérülés elemzését aktualizálni kell.			
PO5.5	Informatikai szolgáltatások előnyeinek menedzsmentje A megfelelő informatikai képességek szolgáltatásából és fenntartásából származó előnyöket figyelemmel kísérő folyamat megvalósítása. Az informatikának az üzleti tevékenységhez történő hozzájárulását – vagy az informatikával támogatott beruházási programok egyik elemeként, vagy a napi vállalati működés támogatása részeként – be kell azonosítani, és dokumentálni kell egy üzleti tervben, azt jóvá kell hagyni, figyelemmel kell kísérni, és jelenteni kell. A jelentéseket felül kell vizsgálni, és ahol lehetőségek vannak az informatika hozzájárulásának javítására, ott a megfelelő intézkedéseket meg kell határozni és meg kell tenni. Amikor az informatika hozzájárulásának változásai hatással vannak a programra, illetve amikor az egyéb kapcsolatos projektek változással vannak a programra, akkor aktualizálni kell a program megtérülés elemzését.	APO05.06	N	
PO6	**Tájékoztatás a vezetői célokról és irányról**			
PO6.1	Informatikai szabályozási és kontroll környezet Meg kell határozni az informatika kontroll környezet elemeit, összhangban a vállalat vezetési filozófiájával és működési stílusával. Ezen elemek között szerepelnie kell az informatikai beruházások által előállított értéknek, a kockázatvállalási hajlandóságnak, az integritásnak, az erkölcsi értékeknek, a személyzet alkalmasságának, az elszámoltathatósággal és felelősséggel kapcsolatos elvárásoknak / követelményeknek. A kontroll környezetnek egy olyan kultúrára kell épülnie, amely támogatja az értékek előállítását, amellett, hogy kezeli a jelentős kockázatokat, támogatja a részlegek közti együttműködést, és csapatmunkát, elősegíti a megfelelőséget, és a folyamatos folyamatjavítást, és kezeli a folyamat eltéréseket is (beleértve a hibás működést is).	APO01.03	N	
PO6.2	Vállalati informatikai kockázati és kontroll keretrendszer Ki kell dolgozni és naprakészen kell tartani a vállalat informatikai kockázatokra és kontrollra vonatkozó általános módszerét meghatározó keretrendszert összhangban az informatikai irányelvekkel, a kontroll környezettel, valamint a vállalati kockázat és kontroll keretrendszerrel.	EDM03.02 APO01.03	N	
PO6.3	Informatikai irányelvek kezelése Ki kell dolgozni és naprakészen kell tartani az informatikai stratégiát támogató irányelveket. Ezen irányelveknek tartalmazniuk kell az irányelv szándékát; a szerepköröket és felelősségeket; a kivételkezelés folyamatát; a megfelelőséget biztosító módszert; valamint az eljárásokra, szabványokra és útmutatásokra vonatkozó	APO01.03 APO01.08	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	hivatkozások. Érvényességüket rendszeresen meg kell erősíteni, és jóvá kell hagyni.			
PO6.4	Irányelvek, szabványok és eljárások bevezetése Az informatikai irányelveket teljes körűen be kell vezetni és érvényesíteni kell az összes érintett munkatárs esetében oly módon, hogy azok beépüljenek a vállalat működésébe és annak szerves részét képezzék.	APO01.03 APO01.08	R	**24. §** (2) A belső adatvédelmi felelős d) elkészíti a belső adatvédelmi és adatbiztonsági szabályzatot;
PO6.5	Tájékoztatás az informatikai célkitűzésekről és irányról Vállalat szerte a megfelelő érdekelt felek és felhasználók számára ismertetni kell az üzleti és az informatikai célkitűzések és irány tudatosságát és megértését.	APO01.04	N	
PO7	**Az informatikai humán erőforrások kezelése**			
PO7.1	A dolgozók felvétele és megtartása Az informatikai munkatársak toborzási folyamatait szinkronban kell tartani a szervezet általános személyügyi irányelveivel és eljárásaival (például felvétel, pozitív munkakörnyezet, eligazítás). Olyan folyamatokat kell megvalósítani, amelyek gondoskodnak arról, hogy a szervezet megfelelően hadrendbe állított informatikai munkaerővel bírjon, amely rendelkezik a szervezeti célok eléréshez szükséges szaktudással.	APO07.01 APO07.05	N	
PO7.2	A dolgozók szaktudása Rendszeresen ellenőrizni kell a végzettségük, képzettségük és/vagy tapasztalatuk alapján azt, hogy a dolgozók rendelkeznek a szerepköreik betöltéséhez szükséges szaktudással. Az alapvető informatikai szaktudás követelményeket kell meghatározni, és ahol lehet, ott minősítési és tanúsítási programokat kell felhasználni annak ellenőrzéséhez, hogy azokat naprakészen tartják.	APO07.03	N	
PO7.3	Szerepek felosztása A dolgozókra vonatkozó szerepköröket, felelősségeket és kompenzációs keretrendszereket meg kell határozni, figyelemmel kell kísérni és felügyelni kell, beleértve azt a követelményt, hogy be kell tartani a vezetési irányelveket, és eljárásokat, az etikai kódexet és a szakmai eljárásokat. A felügyelet szintjének összhangban kell lennie a beosztás bizalmasságával, és az átruházott felelősségek mértékével.	APO01.02 APO07.01	N	
PO7.4	A dolgozók képzése Az informatikai alkalmazottak számára megfelelő eligazítást kell adni felvételükkor, és folyamatos képzést kell nyújtani tudásuk, szakértelmük, képességeik, belső kontroll- és biztonságtudatosságuk a szervezet céljainak eléréséhez szükséges szinten történő fenntartása érdekében.	APO07.03	R	**24. §** (2) A belső adatvédelmi felelős f) gondoskodik az adatvédelmi ismeretek oktatásáról.
PO7.5	Kulcsemberektől való függés A kulcsfontosságú személyektől történő kritikus függésnek való kitettséget minimalizálni kell, a tudást dokumentálni és megosztani kell, az utódlást meg kell tervezni, és helyettesítő	APO07.02	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	személyzetet kell biztosítani.			
PO7.6	A dolgozók átvilágításának eljárásai Biztonsági átvilágítást kell beépíteni az informatikai toborzási folyamatba. Az ezen ellenőrzések időszakos felülvizsgálatának mértéke és gyakorisága a funkció bizalmasságától, és/vagy kritikus jellegétől kell függjön, és azokat alkalmazni kell az alkalmazottakra, az alvállalkozókra, és a szállítókra.	APO07.01 APO07.06	N	
PO7.7	A dolgozók teljesítményének értékelése Szükség van a szervezet céljaiból származtatott egyedi célkitűzések, bevezetett szabványok és konkrét munkaköri felelősségek alapján időben, és rendszeresen történő értékelés végrehajtására. Az alkalmazottakat a teljesítményük és munkavégzésük javítása érdekében mentori (Coaching) segítséget kell nyújtani akkor, amikor arra szükség van.	APO07.04	N	
PO7.8	A munkakörök változtatása és megszűntetése Megfelelő intézkedéseket kell alkalmazni a munkakörváltozások, és különösen a felmondások esetén. A tudás átadását meg kell szervezni, a felelősségeket át kell ruházni, és a hozzáférési jogokat törölni kell oly módon, hogy a kockázatokat minimalizálják, és a funkció folyamatosságát garantálják.	APO07.01	N	
PO8	**Minőségirányítás**			
PO8.1	Minőségirányítási rendszer Olyan minőségirányítási rendszert (Quality Management System, QMS) kell bevezetni és fenntartani, amely szabványos, formális és folyamatos módszert biztosít az üzleti követelményekkel összhangban levő minőségirányításhoz. A QMS-nek be kell azonosítania a minőségügyi követelményeket és kritériumokat, a kulcsfontosságú informatikai folyamatokat és azok sorrendjét és interakcióit; valamint az irányelveket, kritériumokat és módszereket a nem megfelelőség meghatározása, felismerése, korrigálása és megelőzése érdekében. A QMS-nek meg kell határoznia a minőségirányítás szervezeti struktúráját, tartalmaznia kell a szerepköröket, feladatokat és felelősségeket. Az összes kulcsfontosságú területnek ki kell dolgoznia saját minőségügyi terveit, összhangban a kritériumokkal és irányelvekkel, és rögzítenie kell a minőségügyi adatokat. A QMS eredményességét és elfogadottságát figyelemmel kísérni és mérni kell, és szükség esetén azon javítani kell.	APO11.01	N	
PO8.2	Informatikai szabványok és minőségügyi eljárások A kulcsfontosságú informatikai folyamatok szabványait, módszereit és eljárásait be kell azonosítani és naprakészen kell tartani útmutatást biztosítva a szervezetnek ahhoz, hogy a QMS szándékának megfeleljen. Az iparági bevált gyakorlatokat hivatkozásként fel kell használni a	APO11.02	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	szervezet minőségügyi eljárásainak javítása és testre szabása esetén.			
PO8.3	Fejlesztési és beszerzési szabványok Az összes olyan fejlesztésre és beszerzésre vonatkozó szabványt át kell venni és naprakészen kell tartani, amely a végtermékként leszállítandó termék életciklusát átfogja, beleértve a kulcsfontosságú mérföldköveknél a sikeres átvétel jóváhagyását, amelyet az előre megállapított jóváhagyási szempontok alapján hajtottak végre. Figyelembe kell venni a szoftverprogramozási szabványokat; az elnevezési konvenciókat; az állomány formátumokat; az adatséma és adatszótár tervezésre vonatkozó szabványokat; a felhasználói felületre vonatkozó szabványokat; az együttműködési képességet; a rendszer teljesítmény hatékonyságát; a méretezhetőséget; a fejlesztés és tesztelés szabványait; a követelményeknek való megfelelőség igazolását; a teszterveket; és a rendszeregység, a regressziós és az integrációs tesztelést.	APO11.02 APO11.05	N	
PO8.4	Ügyfél-centrikusság A minőségirányításnak az ügyfelekre kell koncentrálnia azáltal, hogy meghatározza a követelményeiket, és összhangba hozza azokat az informatikai szabványokkal és gyakorlatokkal. Szerepköröket és felelősségeket kell meghatározni a felhasználó / ügyfél és az informatikai szervezet közti konfliktus feloldása érdekében.	APO11.03	N	
PO8.5	Folyamatos fejlesztés A folyamatos javítást elősegítő általános minőségügyi tervet kell naprakészen tartani és rendszeresen ismertetni.	APO11.06	N	
PO8.6	Minőség mérése, figyelemmel kísérése és felülvizsgálata Méréseket meg kell határozni, tervezni és megvalósítani kell a QMS-nek történő folyamatos megfelelőség, valamint a QMS által szolgáltatott érték figyelemmel kísérése érdekében. A folyamatfelelősnek használnia kell az információ mérését, figyelemmel kísérését és rögzítését annak érdekében, hogy megfelelő helyesbítő és megelőző intézkedéseket tudjon tenni.	APO11.04	N	
PO9	**Az informatikai kockázatok felmérése és kezelése**			
PO9.1	Informatikai kockázatkezelési keretrendszer A szervezet (vállalat) kockázatkezelési keretrendszerével összhangban levő informatikai kockázat kezelési keretrendszert kell működtetni.	EDM03.02 APO01.03	R	**7.** § (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.*** **7. §** (6) Az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek.
PO9.2	Kockázatok környezetének meghatározása A megfelelő eredmények elérése érdekében meg kell határozni azt a környezetet, amelyben a kockázat felmérési keretrendszert alkalmazzák. Ennek tartalmaznia kell minden egyes kockázatfelmérés belső és külső környezetének meghatározását, a felmérés célját és a kockázatok értékeléséhez felhasznált kritériumokat.	APO12.03	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
PO9.3	Események azonosítása Azonosítani kell azon eseményeket (olyan fontos reális fenyegetések, amelyek egy jelentős, létező sebezhetőséget aknáznak ki), melyek	APO12.01 APO12.03	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	potenciálisan negatívan befolyásolhatják a vállalat céljait, vagy működését, beleértve az üzleti, a szabályozási, a jogi, a technológiai, illetve a kereskedelmi partnerekre, a humán erőforrásokra és az üzemeltetésre vonatkozó szempontokat. Meg kell határozni a hatásuk jellegét és ezen információkat naprakészen kell tartani. A vonatkozó kockázatokat egy kockázat nyilvántartásban kell nyilvántartani és naprakészen tartani.			adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
PO9.4	Kockázat felmérés Időszakonként fel kell mérni az összes azonosított kockázat valószínűségét és hatását, kvalitatív és kvantitatív módszerek alkalmazásával. A belső és a maradványkockázatokkal kapcsolatos valószínűséget és hatást kategóriánként külön-külön kell meghatározni, portfolió alapon.	APO12.02 APO12.04	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
PO9.5	Kockázatra adott válasz Egy olyan kockázatra reagáló folyamatot kell kidolgozni és naprakészen tartani, melynek az a célja, hogy folyamatosan gondoskodjon a kockázatoknak való kitettség gazdaságos kontrollokkal való enyhítéséről. A kockázatra reagáló folyamatnak be kell azonosítania az olyan kockázatkezelési stratégiákat, mint például a kockázat elkerülése, csökkentése, megosztása, illetve elfogadása; meg kell határozni a kapcsolatos felelősségeket; és figyelembe kell vennie a kockázati tűrőképességi szinteket.	APO12.06	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				szükségesek.
PO9.6	A kockázati cselekvési terv naprakészen tartása és figyelemmel kísérése A kontroll tevékenységeket rangsorolni kell és meg kell tervezni a szervezet minden szintjén annak érdekében, hogy a szükségesként azonosított kockázat kezelési reakciók megvalósításra kerüljenek, beleértve a költségek, az előnyök és a végrehajtási felelősség azonosítását. Az ajánlott intézkedéseket jóvá kell hagyatni, és az esetleges fennmaradó kockázatokat el kell fogadtatni, és gondoskodni kell arról, hogy az érintett folyamatfelelősök végrehajtsák a jóváhagyott intézkedéseket. A tervek végrehajtását figyelemmel kell kísérni és az esetleges eltéréseket jelentani a felsővezetés felé.	APO12.04-05	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
PO10	**A projektek irányítása**			
PO10.1	Program menedzsment keretrendszer Az informatikával támogatott beruházási programok portfoliójának részét alkotó projektek programját naprakészen kell tartani, a projektek azonosítása, meghatározása, kiértékelése, rangsorolása, kiválasztása, indítása, menedzselése és kontrollálása révén. Gondoskodni kell arról, hogy a projektek támogassák a program célkitűzéseit. A tevékenységek és a több projekt közti függőségeket koordinálni kell, a programba tartozó összes projekt elvárt eredményekhez történő hozzájárulását menedzselni kell, valamint az erőforrás követelményeket és konfliktusokat rendezni kell.	BAI01.01	N	
PO10.2	Projekt menedzsment keretrendszer A projektmenedzsment keretrendszert kell működtetni és naprakészen tartani, amely meghatározza a projekt menedzsment terjedelmét és határait, valamint az egyes projektek működtetése során követendő és alkalmazandó módszereket. A keretrendszert és a támogató módszereket integrálni kell a program menedzsment folyamatokba.	BAI01.01	N	
PO10.3	Projekt menedzsment módszer Egy olyan projektmenedzselési módszert kell működtetni, amely szinkronban van az egyes projektek méretével, összetettségével és szabályozási követelményeivel. A projektirányítási struktúra tartalmazhatja a programfinanszírozó, a projektfinanszírozó, az irányítóbizottság, a projekt iroda és a projekt menedzser szerepköreit, felelősségeit és elszámoltathatóságát, valamint azokat a mechanizmusokat, amelyen keresztül meg tudnak felelni ezen felelősségeknek (például jelentések	BAI01.01	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	készítése és a fázisok felülvizsgálatai). Gondoskodni kell arról, hogy az összes informatikai projektnek megfelelő hatáskörrel rendelkező finanszírozói legyenek ahhoz, hogy a projekt végrehajtásának gazdái lehessenek az általános stratégiai programon belül.			
PO10.4	Érdekelt felek elkötelezettsége Az érintett érdekelt felek elkötelezettségét és részvételét meg kell szerezni, a projektnek az általános informatikával támogatott beruházási programon belüli megalapítását és végrehajtását illetően.	BAI01.03	N	
PO10.5	A projekt terjedelmének meghatározása A projekt jellegét és terjedelmét meg kell határozni és dokumentálni, annak érdekében, hogy kialakuljon, és megerősödjön a projekt terjedelmének az érdekelt felek által történő közös értelmezése és az, hogy hogyan viszonyul a projekt a többi projekthez az általános, informatikával támogatott beruházási programon belül. A meghatározást a program és projekt finanszírozóknak formálisan jóvá kell hagyniuk a projekt elindítása előtt.	BAI01.07	N	
PO10.6	A projekt fázisainak indítása Minden egyes jelentős projekt fázis indítását jóvá kell hagyni és ismertetni kell az összes érdekelt fél számára. A kezdeti fázis jóváhagyását a programirányítási döntésekre kell építeni. Az azt követő fázisok jóváhagyását az előző fázis termékeinek minőségi szemléjére és elfogadására, valamint a program következő jelentős felülvizsgálata során egy aktualizált projekt üzleti terv jóváhagyására kell alapozni. A projekt fázisok átfedése esetén a program és a projekt finanszírozóknak egy jóváhagyási pontot kell meghatározniuk a projekt folytatásának engedélyezése céljából.	BAI01.07	N	
PO10.7	Felső szintű projektterv Egy formális, jóváhagyott felső szintű projekttervet kell kialakítani (amely lefedi az üzleti és az információrendszerek erőforrásait), a projekt végrehajtásának és ellenőrzésének a projekt teljes élettartama alatt történő irányítása céljából. Az egy programon belüli tevékenységeket és függőségeket meg kell érteni, és dokumentálni kell. A projekttervet karban kell tartani a projekt teljes élettartama alatt. A projekttervet és annak változásait jóvá kell hagyatni a program és a projektirányítási keretrendszerrel összhangban.	BAI01.08	N	
PO10.8	A projekt erőforrásai A projekt munkacsoport tagok felelősségeinek, kapcsolatainak, hatásköreinek és teljesítmény kritériumait meg kell határozni, és a hozzáértő munkatársak, és/vagy alvállalkozók projekt számára való megszerzésének, és delegálásának módját meg kell határozni. Az egyes projektekhez szükséges termékek és szolgáltatások beszerzését	BAI01.08	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	a szervezet beszerzési eljárásainak felhasználásával kell megtervezni és menedzselni a projekt célkitűzéseinek elérése érdekében.			
PO10.9	Projekt kockázatkezelés Az egyes projektekkel kapcsolatos konkrét kockázatok ki kell iktatni, illetve minimalizálni egy olyan szisztematikus eljárás keretében, amely azon területekre, illetve eseményekre – amelyek potenciálisan nem kívánatos változást okozhatnak – vonatkozó tervezés, azonosítás, elemzés, kezelés figyelemmel kísérés, ellenőrzés, és az általuk kiváltott reakciókkal foglalkozik. A projektmenedzsment folyamatot és a projekt termékeit érintő kockázatokat meg kell állapítani, és azokat központilag nyilván kell tartani.	BAI01.10	N	
PO10.10	A projekt minőségügyi terve El kell készíteni egy olyan minőségirányítási tervet, amely leírja a projekt minőségügyi rendszerét, és annak megvalósítási módját. A tervet az összes érintett félnek formálisan felül kell vizsgálnia, és azzal egyet kell értenie, majd azt követően a tervet be kell építeni a felső szintű projekttervbe.	BAI01.09	N	
PO10.11	Projekt változtatás engedélyezési eljárás Minden egyes projekt esetében egy változtatás engedélyezési rendszert kell bevezetni annak érdekében, hogy a projekt alapfeltételeire (például költség, ütemterv, terjedelem, minőség) vonatkozó összes változtatást megfelelően felülvizsgálják, jóváhagyják, és beépítsék a felső szintű, integrált projekttervbe, a program és a projektirányítási keretrendszerrel összhangban.	BAI01.11	N	
PO10.12	A projekttel kapcsolatos bizonyosság nyújtási módszerek tervezése Azonosítani kell projekttervezés során azon bizonyosság nyújtási feladatokat, amelyekre szükség van az új, illetve módosított rendszerek bevizsgálásának támogatásához, és ezeket a feladatokat be kell építeni a felső szintű, integrált projekttervbe. Ezen feladatoknak bizonyosságot kell adniuk arról, hogy a projekt belső irányítási és ellenőrzési rendszere, valamint a biztonsági jellemzők kielégítik a megszabott követelményeket.	BAI01.08	N	
PO10.13	Projekt teljesítmény mérése, jelentések készítése és figyelemmel kísérése A projekt teljesítményét mérni kell a kulcsfontosságú projekt teljesítményét jelző paraméterekhez képest, nevezetesen a terjedelem, ütemterv, minőség, költségek és a kockázati tényezők. A tervtől való eltéréseket azonosítani kell. Az eltéréseknek a projektre és az általános programra gyakorolt hatását értékelni kell, és az eredményeket jelenteni a kulcsfontosságú érdekelt felek felé. Szükség esetén helyesbítési intézkedések ajánlása, megvalósítása és figyelemmel kísérése szükséges a program- és projektirányítási keretrendszerrel összhangban.	BAI01.06 BAI01.11	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
PO10.14	A projekt lezárása Szükség van arra, hogy minden egyes projekt végén a projekt érdekelt felei meggyőződjenek arról, hogy a projekt előállította-e a tervezett eredményeket és hasznokat. Be kell azonosítani, és ismertetni kell az esetleges olyan kiemelkedő tevékenységeket, amelyre szükség volt a projekt tervezett eredményeinek eléréséhez és a program hasznosságához, valamint a jövőbeli projektekben és programokban történő felhasználás céljából azonosítani, és dokumentálni kell a tanulságokat.	BAI01.13	N	
AI1	**Az automatizált megoldások meghatározása**			
AI1.1	Az üzleti funkcionális és műszaki követelmények meghatározása és naprakészen tartása Az informatikával támogatott beruházási programok elvárt eredményeinek valóra váltásához szükséges összes informatikai kezdeményezés teljes terjedelmét lefedő üzleti funkcionális és műszaki követelményeket azonosítani, rangsorolni, specifikálni, és egyeztetni kell.	BAI02.01	R	**11. §** (1) Kizárólag automatizált adatfeldolgozással az érintett személyes jellemzőinek értékelésén alapuló döntés meghozatalára csak akkor kerülhet sor, ha a döntést a) valamely szerződés megkötése vagy teljesítése során hozták, feltéve hogy azt az érintett kezdeményezte, vagy b) olyan törvény teszi lehetővé, amely az érintett jogos érdekeit biztosító intézkedéseket is megállapítja.
AI1.2	Kockázatelemzési jelentés Az üzleti követelményekkel és a megoldás tervével kapcsolatos kockázatokat, a szervezet követelmény kidolgozási folyamatának részeként, azonosítani, dokumentálni és elemezni kell.	BAI02.03	N	
AI1.3	Megvalósíthatósági tanulmány és az alternatív megoldások kidolgozása A követelmények megvalósítási lehetőségeit vizsgáló megvalósíthatósági tanulmányt kell kidolgozni. Az informatikai funkció által támogatott üzleti területek vezetőinek kell értékelnie a megvalósíthatóságot, és az alternatív megoldásokat, és ajánlást kell tennie az üzleti finanszírozónak.	BAI02.02	N	
AI1.4	A követelményekre és a megvalósíthatóságra vonatkozó döntés és vezetői jóváhagyás Ellenőrizni kell, hogy a folyamatban megkövetelik-e az üzleti finanszírozóktól az előre meghatározott kulcsfontosságú szakaszoknál az üzleti funkcionális és műszaki követelmények, és a megvalósíthatósági tanulmány előrehaladási jelentések elfogadását, és jóváhagyását. Az üzleti finanszírozóknak kell meghoznia a végső döntést	BAI02.04	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	a megoldás jellegéről, és a beszerzés módjáról.			
AI2	**Az alkalmazási szoftverek beszerzése és karbantartása**			
AI2.1	Magas szintű terv Az üzleti követelmények szoftver beszerzése céljából le kell fordítani magas szintű szoftver specifikációra, figyelembe véve a szervezet technológiai irányvonalát és információ-architektúráját. A vezetés részéről a szoftver specifikációt jóvá kell hagyni a követelményeknek való megfelelőség biztosítása érdekében. Ha jelentős műszaki, illetve logikai eltérések merülnek fel a fejlesztés, illetve karbantartás alatt, akkor a helyzetet újra kell értékelni.	BAI03.01	N	
AI2.2	Részletes terv El kell készíteni a részletes műszaki tervet és a műszaki alkalmazási szoftver követelményeket. Meg kell határozni a követelmények elfogadási kritériumait. Jóvá kell hagyatni a követelményeket annak biztosítása érdekében, hogy azok megfeleljenek a magas szintű tervnek. Ha jelentős műszaki, illetve logikai eltérések merülnek fel a fejlesztés, illetve karbantartás alatt, akkor a felmérést újra el kell végezni.	BAI03.02	N	
AI2.3	Alkalmazás kontroll és auditálhatóság Üzleti kontrollokat, ahol az értelmes, automatizált alkalmazási kontrollok formájában kell megvalósítani, oly módon, hogy az adatfeldolgozás pontos, teljes, időszerű, engedélyezett és auditálható legyen.	BAI03.05	N	
AI2.4	Alkalmazás biztonság és rendelkezésre állás Az alkalmazás biztonsági és rendelkezésre állási követelmények et az azonosított kockázatoknak megfelelően kell rendezni, összhangban a szervezeti adatok osztályozásával, információ-architektúrájával, információbiztonsági architektúrájával és kockázattűrő képességével.	BAI03.01-03 BAI03.05	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
AI2.5	A beszerzett alkalmazási szoftver beállítása és bevezetése A beszerzett alkalmazási szoftvereket az üzleti célkitűzések teljesítése érdekében kell konfigurálni és bevezetni.	BAI03.03 BAI03.05	N	
AI2.6	A meglevő rendszerek jelentősebb bővítései	BAI03.10	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	Abban az esetben, ha a jelenlegi rendszereket jelentősen megváltoztatják, mely eredményeként a jelenlegi megjelenés, és/vagy funkcionalitás jelentősen megváltozik, akkor az új rendszerek fejlesztéséhez hasonló fejlesztési folyamatot kell követni.			
AI2.7	Alkalmazási szoftver fejlesztés Gondoskodni kell arról, hogy az automatizált funkcionalitás a tervezési specifikációknak, a fejlesztési és dokumentálási szabványoknak, a minőségbiztosítási követelményeknek, és az átadás-átvételi eljárás szabványainak megfelelően kerüljön kifejlesztésre. Gondoskodni kell arról, hogy az összes jogi és szerződéses szempont beazonosításra, és rendezésre kerüljön a harmadik felek által kifejlesztett alkalmazási szoftverek esetében.	BAI03.03-04	N	
AI2.8	Szoftver minőségbiztosítás Szoftver minőségbiztosítási tervet kell kifejleszteni, erőforrásokkal ellátni és végrehajtani azért, hogy a követelmény meghatározásban, és a szervezet minőségügyi irányelveiben és eljárásaiban előírt minőségi színvonalat elérjék.	BAI03.06	N	
AI2.9	Alkalmazások követelményeinek kezelése Az egyedi követelmények (beleértve az összes elutasított követelményt) állapotát nyomon kell követni a tervezés, fejlesztés és a megvalósítás során, továbbá a követelmények megváltoztatását el kell fogadtatni egy bevezetett változtatáskezelési folyamaton keresztül.	BAI03.09	N	
AI2.10	Alkalmazási szoftverek karbantartása Az alkalmazás szoftverek karbantartására stratégiát és tervet kell kidolgozni.	BAI03.10	N	
AI3	**A technológiai infrastruktúra beszerzése és karbantartása**			
AI3.1	Technológiai infrastruktúra beszerzési terv A kialakított üzleti funkcionális és műszaki követelményeknek, és a szervezet technológiai irányvonalának megfelelő tervet kell készíteni a technológiai infrastruktúra beszerzésére, megvalósítására és karbantartására.	BAI03.04	N	
AI3.2	Infrastruktúra erőforrás védelem és rendelkezésre állás A hardverek és az infrastruktúra szoftverek konfigurálása, integrálása és karbantartása során a belső irányítási és ellenőrzési rendszert, a biztonságot és az auditálhatóságot biztosító intézkedéseket meg kell valósítani az erőforrások védelme, és a rendelkezésre állás és a sértetlenség biztosítása érdekében. A bizalmas infrastruktúra elemek használatával kapcsolatos felelősségeket egyértelműen meg kell határozni, és azzal tisztában kell lenniük azoknak, akik az infrastruktúra elemeket fejlesztik és integrálják. Használatukat figyelemmel kísérni és értékelni kell.	BAI03.03 DSS02.03	N	
AI3.3	Infrastruktúra karbantartás Stratégia és tervet kell kidolgozni az infrastruktúra	BAI03.10	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	karbantartására, és annak biztosítására, hogy a változtatások a szervezet változáskezelési eljárásával összhangban, kontrollált módon történjenek. Az üzleti igények szerinti időszakos felülvizsgálatokat, a szoftver javítócsomagok kezelését, a stratégiák frissítését, a kockázatokat, a sebezhetőségek felmérését és a biztonsági követelményeket be kell építeni.			
AI3.4	Megvalósíthatósági teszt környezet Fejlesztési és tesztkörnyezeteket kell kialakítani az infrastruktúra elemek eredményes és hatékony megvalósíthatósági és integrációs tesztelésének támogatása érdekében.	BAI03.07-08	N	
AI4	**Az üzemeltetés és a használat támogatása**			
AI4.1	Megoldások használhatóságának és üzemeltethetőségének tervezése Az összes műszaki, üzemeltetési és használattal kapcsolatos szempont azonosítása és dokumentálása céljából egy olyan tervet kell kidolgozni, mely szerint az összes olyan személy végre tudja hajtani a feladatát, aki üzemeltetni, használni és karban tartani fogja az automatizált megoldásokat.	BAI05.05	N	
AI4.2	Tudás átadása az üzleti vezetőknek A tudást át kell adni az üzleti vezetés számára azért, hogy az érintett egyének felvállalhassák a rendszerek és az adatok tulajdonosi szerepét, és a szolgáltatások nyújtásával és minőségével, a belső irányítási és ellenőrzési rendszerrel és az alkalmazás adminisztrációval kapcsolatos felelősségüket gyakorolhassák.	BAI08.01-04	N	
AI4.3	Tudás átadása a végfelhasználóknak A tudást és a szakértelmet át kell adni annak érdekében, hogy a végfelhasználók az üzleti folyamatok támogatása érdekében képesek legyenek eredményesen és hatékonyan használni a rendszert.	BAI08.01-04	N	
AI4.4	Tudás átadása az üzemeltetési és támogató munkatársaknak A tudást és a szakértelmet át kell adni annak érdekében, hogy az üzemeltetési és műszaki támogató munkatársak képesek legyenek eredményesen és hatékonyan biztosítani, támogatni és karbantartani a rendszert és a kapcsolódó infrastruktúrát.	BAI08.01-04	N	
AI5	**Az informatikai erőforrások beszerzése**			
AI5.1	A beszerzés kontrollja Egy olyan eljáráshalmazt és szabványokat kell kidolgozni és követnie, amelyek összhangban vannak a vállalkozás általános beszerzési folyamatával, és beszerzési stratégiájával, a vállalkozás számára szükséges informatikával kapcsolatos infrastruktúra, létesítmények, hardverek, szoftverek és szolgáltatások beszerzése céljából.	BAI03.04	N	
AI5.2	Beszállítói szerződés menedzsment Egy eljárást kell kidolgozni az összes beszállítói szerződés megkötésére, módosítására és	APO10.01 APO10.03	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	lezárására. Minimumként az eljárásnak ki kell terjednie a jogi, pénzügyi, szervezeti, dokumentációs, teljesítményi, biztonsági, szellemi tulajdonjogi és felmondási felelősségekkel és kötelezettségekkel (beleértve a kötbérezési záradékokat). Az összes szerződést, és szerződésváltoztatást jogászokkal kell felülvizsgálni.			
AI5.3	Szállító kiválasztás A beszállítókat igazságos, és szabályozott gyakorlat szerint kell kiválasztani annak biztosítása érdekében, hogy a specifikált követelményeknek legjobban megfelelő megoldás kerüljön kiválasztásra. A követelményeket a potenciális beszállítóktól származó vélemények alapján kell optimalizálni.	APO10.02	N	
AI5.4	Informatikai erőforrások beszerzése Minden beszerzést érintő szerződéses megállapodás esetén a szervezet érdekeit meg kell védeni és érvényesíteni kell, beleértve minden fél szerződéses feltételek szerinti jogait és kötelezettségeit, a szoftverek, a fejlesztési erőforrások, az infrastruktúra és a szolgáltatások beszerzése tekintetében.	APO10.03	N	
AI6	**A változtatások kezelése**			
AI6.1	Változtatási szabványok és eljárások Formális változtatáskezelő eljárásokat kell felállítani a változtatási kérelmeket (beleértve a karbantartási és a szoftverjavítási kérelmeket) szabványos módon kell kezelni, az összes alkalmazási rendszerre, eljárásra, folyamatra, rendszerre és szolgáltatási paraméterre, és az alattuk működő informatikai platformokra.	BAI06.01-04	R	**7.** § (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
AI6.2	Hatásfelmérés, rangsorolás és engedélyezés Az összes változtatási kérelmet strukturált módon kell értékelni azért, hogy a működő rendszerre és annak funkcionalitására gyakorolt hatást meghatározzák. Gondoskodni kell arról, hogy a változtatások osztályozása, rangsorolása és engedélyezése megtörténjen.	BAI06.01	R	**7.** § (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
AI6.3	Rendkívüli változtatások Meg kell valósítani egy folyamatot az olyan rendkívüli változtatások meghatározására, felvetésére, tesztelésére, dokumentálására, felmérésére és engedélyezésére vonatkozóan, amelyek eltérnek a bevezetett változtatási folyamattól.	BAI06.02	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
AI6.4	Változtatások állapotának nyomon követése és lejelentése Egy nyomon követő és jelentéskészítő rendszert kell kialakítani az elutasított változtatások dokumentálására, a jóváhagyott és a folyamatban levő változtatások állapotáról történő tájékoztatásra, és a változtatások lezárása céljából. Meg kell győződni arról, hogy a jóváhagyott változtatásokat a tervek szerint hajtották végre.	BAI06.03	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
AI6.5	Változtatások lezárása és dokumentálása Minden olyan esetben, amikor változtatások megvalósítására kerül sor, a kapcsolódó rendszer és felhasználói dokumentációt és az eljárásokat értelemszerűen frissíteni kell.	BAI06.04	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
AI7	**A megoldások és változtatások üzembe helyezése és bevizsgálása**			
AI7.1	Képzés Minden egyes információrendszer-fejlesztési, megvalósítási, illetve módosítási projekt részeként ki kell képezni az érintett felhasználói részlegek és az informatikai funkció üzemeltetési csoportjának munkatársait a meghatározott képzési és megvalósítási terv, és a kapcsolódó anyagok szerint.	BAI05.05	N	
AI7.2	Tesztelési terv Olyan tesztterv kell kialakítani, amely a szervezetszintű szabványokra épül, és amely meghatározza a szerepköröket, a felelősségeket, és a tesztindítási és befejezési kritériumokat. Gondoskodni kell arról, hogy a tervet elfogadják az érintett felek.	BAI07.01 BAI07.03	N	
AI7.3	Megvalósítási terv Egy megvalósítási és visszatérési/visszalépési tervet kell kidolgozni. Az érintett felek jóváhagyását meg kell szerezni.	BAI07.01	N	
AI7.4	Tesztkörnyezet A tervezett üzemeltetési környezetnek megfelelő biztonsági teszt környezetet kell előírni és felállítani, a biztonságra, a belső kontrollokra és ellenőrzési eljárásokra, az üzemeltetési eljárásokra, az adatok minőségére és a személyi adatokra vonatkozó követelményekre, valamint a munkaterhelésekre tekintettel.	BAI07.04	N	
AI7.5	Rendszer- és adatkonverzió Az adatkonverziót és az infrastruktúra migrálását a szervezet fejlesztési módszereinek részeként kell megtervezni, beleértve az ellenőrizhetőségi, auditálhatósági naplókat, a visszagörgetési és visszaállítási lehetőségeket.	BAI07.02	R	**7. §** (3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.
AI7.6	Változtatások tesztelése A változtatásokat függetlenül kell tesztelni a meghatározott teszttervnek megfelelően az üzemeltetési környezetbe történő migrációt megelőzően. Gondoskodni kell arról, hogy a terv figyelembe vegye a biztonsági és teljesítményi szempontokat.	BAI07.05	N	
AI7.7	Végső elfogadási teszt Gondoskodni kell arról, hogy az üzleti folyamat felelősök és az informatika érdekelt felei kiértékeljék a tesztelési folyamat eredményeit a teszttervben meghatározottaknak megfelelően. A tesztelési folyamat során beazonosított jelentős hibák kiküszöbölése, a teszttervben előírt tesztsorozat és az esetlegesen szükséges regresszió tesztek befejezését követően. Az értékelés után az éles üzembe állítás jóváhagyása.	BAI07.05	N	
AI7.8	Éles üzembe állítás A tesztelés után, a módosított rendszer üzemeltetésnek történő átadását ellenőrizni kell, hogy vajon a megvalósítási tervvel összhangban van-e. Az olyan kulcsfontosságú érdekelt felek jóváhagyását meg kell szerezni, mint például a felhasználók, a rendszer felelőse, és az informatikai működtetés vezetése. Ahol célszerű, a rendszert a régi rendszerrel egy ideig párhuzamosan kell futtatni, és a rendszer viselkedését és az eredményeket össze kell hasonlítani.	BAI07.06	N	
AI7.9	Megvalósítást követő felülvizsgálat Eljárásokat kell kidolgozni a szervezeti változáskezelési szabványoknak megfelelően azért, hogy a megvalósítási tervben rögzítettek alapján a megvalósítást követő felülvizsgálatot végrehajtsák.	BAI07.08	N	
DS1	**A szolgáltatási szintek meghatározása és betartása**			
DS1.1	A szolgáltatási szint megállapodásokra vonatkozó keretrendszer Olyan keretrendszert kell meghatározni, amely az ügyfél és a szolgáltató között egy formalizált szolgáltatási szint menedzsment folyamatot biztosít. A keretrendszernek az üzleti követelmények és prioritások között folyamatosan fenn kell tartania az összhangot, és elő kell segítenie az ügyfél és a szolgáltató(k) közötti közös nyelv kialakulását. A keretrendszernek tartalmaznia kell folyamatokat a szolgáltatási követelmények, a szolgáltatás meghatározások, a szolgáltatási szint megállapodások, az üzemeltetési szint megállapodások és a finanszírozási források létrehozásához. Ezen attribútumokat egy szolgáltatási katalógusba kell	APO09.01-05	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	szervezni. A keretrendszernek meg kell határoznia a szolgáltatási szint kezelés szervezeti struktúráját, lefedve a belső és külső szolgáltatók és az ügyfelek szerepköreit, feladatait és felelősségeit.			
DS1.2	Szolgáltatások meghatározása Az informatikai szolgáltatások meghatározásait a szolgáltatások jellemzőire és üzleti követelményekre kell alapozni. Gondoskodni kell egy szolgáltatási katalógus portfolió megvalósítása révén a szolgáltatás leírások központi szervezéséről és tárolásáról.	APO09.01-02	N	
DS1.3	Szolgáltatási szint megállapodások Elő kell írni és jóvá kell hagyatni az összes kritikus informatikai szolgáltatásra vonatkozóan a szolgáltatási szint megállapodásokat az ügyfél követelmények és az informatikai képességek alapján. Ennek ki kell terjednie az ügyfél oldali kötelezettségekre; a szolgáltatástámogatási követelményekre; az érdekelt felek által jóváhagyott szolgáltatás mérésének mennyiségi és minőségi metrikáira; ha szükséges a finanszírozási és kereskedelmi konstrukciókra; szerepkörökre és felelősségekre, beleértve a szolgáltatási szint megállapodások felügyeletét. Figyelembe kell venni az olyan elemeket, mint például a rendelkezésre állást, a megbízhatóságot, a teljesítményt, a bővítési lehetőséget, a támogatás szintjeit, a működésfolyamatosság tervezését, a biztonsággal és a szolgáltatások iránti kereslettel kapcsolatos korlátokat.	APO09.03	R	**10. §** (4) Az adatfeldolgozásra vonatkozó szerződést írásba kell foglalni. Az adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt.
DS1.4	Üzemeltetési szint megállapodások Üzemeltetési szint megállapodások meghatározása annak részletezésére, hogy a szolgáltatási szint megállapodások optimális teljesítése érdekében a szolgáltatásokat milyen műszaki feltételek szerint kell biztosítani. Az üzemeltetési szint megállapodásoknak specifikálniuk kell a műszaki folyamatokat a szolgáltató számára értelmezhető módon, és több szolgáltatási szint megállapodást is támogathatnak.	APO09.03	N	
DS1.5	A szolgáltatási szintek figyelemmel kísérése és lejelentése Az előírt szolgáltatási szint teljesítmény kritériumokat folyamatosan figyelemmel kell kísérni. A szolgáltatási szintek elérésére vonatkozó jelentéseket olyan formátumban kell biztosítani, amelyet megértenek az érdekelt felek. A nyomon követés statisztikáit elemezni kell, és azok alapján kell cselekedni azért, hogy az egyes szolgáltatásokkal, valamint az összes szolgáltatással kapcsolatos negatív és pozitív trendeket felismerjék.	APO09.04	N	
DS1.6	A szolgáltatási szint megállapodások és szerződések felülvizsgálata Rendszeresen felül kell vizsgálni a szolgáltatási szint megállapodásokat, és a belső és külső	APO09.05	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	szolgáltatókkal kötött, azokat alátámasztó szerződéseket annak biztosítása érdekében, hogy azok eredményesek és naprakészek legyenek, és hogy a követelmények változtatásait figyelembe vegyék.			
DS2	**Külső szolgáltatások igénybevételének irányítása**			
DS2.1	Az összes szállítói kapcsolat azonosítása Az összes szállítói szolgáltatást be kell azonosítani, és szállítói típus, fontosság és kritikusság szempontjából besorolni. A műszaki és a szervezeti kapcsolatok hivatalos dokumentációját naprakészen kell tartani, beleértve a szerepköröket és felelősségeket, a célokat, az elvárt termékeket, valamint ezen szállítók képviselőinek megbízóleveleit.	APO10.01	N	
DS2.2	Szállítói kapcsolatok kezelése A szállítói kapcsolatok kezelése folyamatot formalizálni kell minden szállító esetében. A kapcsolattartási felelősöknek az ügyfél és a szállító közötti problémák esetén kapcsolatba kell lépniük, és gondoskodnunk kell arról, hogy a kapcsolat minősége bizalomra és átláthatóságra épüljön (például szolgáltatási szint megállapodásokon keresztül).	APO10.03	N	
DS2.3	Szállítói kockázatok kezelése A szállítók biztonságos és hatékony módon, állandó jelleggel való eredményes szolgáltatás nyújtásának a képességére vonatkozó kockázatokat azonosítani és enyhíteni kell. Gondoskodni kell arról, hogy a szerződések megfelelnek az általános üzleti szokásoknak, összhangban a jogi és a szabályozási követelményekkel. Továbbá a kockázatkezelésnek foglalkoznia kell a titoktartási nyilatkozatokkal, a letéti szerződésekkel, a folytonos szállítói életképességgel, a biztonsági követelményeknek való megfelelőséggel, az alternatív szállítókkal, a kötbérekkel és a szolgáltatási díjakkal, stb.	APO10.04	N	
DS2.4	Szállítói teljesítmény figyelemmel kísérése Szolgáltatás nyújtását figyelemmel kísérő folyamatot kell létrehozni azért, hogy biztosíthassuk, hogy a szállítók megfeleljenek az aktuális üzleti követelményeknek, és folyamatosan betartsák a szerződéses megállapodásokat és a szolgáltatási szint megállapodásokat, és hogy a teljesítményük versenyképes legyen az alternatív szállítókkal és a piaci feltételekkel.	APO10.05	N	
DS3	**Teljesítmény- és kapacitáskezelés**			
DS3.1	Teljesítmény- és kapacitástervezés Az informatikai erőforrások teljesítményének és kapacitásának felülvizsgálását szolgáló tervezési folyamat bevezetése annak biztosítása érdekében, hogy költségek szempontjából igazolható kapacitás és teljesítmény álljon rendelkezésre a szolgáltatási szint megállapodásokban meghatározottaknak megfelelő, jóváhagyott	BAI04.03	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	munkaterhelések kiszolgálására. A kapacitási és teljesítmény terveknek ki kell használniuk a megfelelő modellező módszereket az informatikai erőforrások jelenlegi és előre jelzett teljesítményre, kapacitásra és tranzakció áteresztőképességre vonatkozómodelljének előállításához.			
DS3.2	Jelenlegi teljesítmény és kapacitás Az informatikai erőforrások jelenlegi teljesítményének és kapacitását fel kell mérni annak meghatározása érdekében, hogy rendelkezésre áll-e elegendő kapacitás és teljesítmény a jóváhagyott szolgáltatási szintek szerint szolgáltatáshoz.	BAI04.01-02	N	
DS3.3	Jövőbeli teljesítmény és kapacitás Az informatikai erőforrások teljesítmény és kapacitás előrejelzését rendszeres időközönkénti el kell végezni az elégtelen kapacitás, illetve teljesítmény csökkenés miatt bekövetkező szolgáltatási üzemszünetek kockázatának minimalizálása, és a többlet kapacitások lehetséges ismételt hasznosítás céljából történő beazonosítása érdekében. A munkaterhelési trendeket be kell azonosítani és a teljesítmény és kapacitási tervekhez bemenetként szolgáló előrejelzéseket meg kell határozni.	BAI04.01	N	
DS3.4	Informatikai erőforrások rendelkezésre állása A szükséges kapacitás és teljesítményt biztosítani kell, figyelembe véve az olyan szempontokat, mint például a szokásos munkaterhelés, a rendkívüli helyzetek, a tárolási követelmények és az informatikai erőforrások életciklusai. Meg kell hozni olyan rendelkezéseket, mint például a feladatok rangsorolása, a hibatűrő mechanizmusok és az erőforrás szétosztási eljárások. A vezetésnek gondoskodnia kell arról, hogy a rendkívüli helyzetekre vonatkozó tervek megfelelően foglalkozzanak az egyes informatikai erőforrások rendelkezésére állásával, kapacitásával és teljesítményével.	BAI04.05	R	**37. §** (1) A [közzétételre kötelezett szervek] tevékenységükhöz kapcsolódóan az 1. melléklet szerinti általános közzétételi listában meghatározott adatokat az 1. mellékletben foglaltak szerint közzéteszik.
DS3.5	Figyelemmel kísérés és jelentéskészítés Az informatikai erőforrások teljesítményét és kapacitását folyamatosan figyelemmel kell kísérni. A begyűjtött adatoknak két célt kell szolgálnia: ▪ Az informatikán belül az aktuális teljesítményt fenn kell tartani és finomítani kell, és az olyan kérdéseket rendezni kell, mint például az alkalmazkodó képesség, a rendkívüli helyzetek, a jelenlegi és az előre jelzett munkaterhek, az adattárolási tervek és az erőforrás beszerzés ▪ A nyújtott szolgáltatások rendelkezésre állásáról jelentést kell készíteni az üzleti területek számára a szolgáltatási szint megállapodások által előírtaknak megfelelően. ▪ Az összes rendkívüli eseményre vonatkozó	BAI04.04	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	jelentésnek tartalmaznia kell a helyesbítő intézkedésekre vonatkozó ajánlásokat.			
DS4	**A szolgáltatás folyamatosságának biztosítása**			
DS4.1	Informatikai működésfolyamatossági keretrendszer Informatikai működésfolyamatossági keretrendszert kell kidolgozni annak érdekében, hogy egy következetes folyamat alkalmazásával támogathassa a vállalati működésfolyamatosság menedzsmentet. A keretrendszer célja az kell, hogy legyen, hogy segítséget nyújtson az infrastruktúra szükséges alkalmazkodóképességének meghatározásához, és vezérelje a katasztrófa helyreállítási és az informatikai működésfolyamatossági tervek kidolgozását. A keretrendszernek foglalkoznia kell a működésfolyamatosság menedzsment szervezeti felépítésével, tartalmaznia kell a belső és a külső szolgáltatók szerepköreit, feladatait és felelősségeit, a vezetésüket, ügyfeleiket és azokat a tervezési folyamatokat, amelyek létrehozzák a katasztrófa helyreállítási és az informatikai működésfolyamatossági tervek dokumentálásának, tesztelésének és végrehajtásának szabályait és szerkezetét. A tervnek foglalkoznia kell az olyan elemekkel, mint például a kritikus fontosságú erőforrások beazonosítása, a kulcsfontosságú függőségek kimutatása, a kritikus erőforrások, az alternatív feldolgozás rendelkezésre állásának figyelemmel kísérése és jelentése, valamint a mentések és a visszaállítások alapelvei.	DSS04.01-02	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
DS4.2	Informatikai működésfolyamatossági tervek Informatikai működésfolyamatossági terveket kell kidolgozni a keretrendszer alapján, melyeket úgy kell megtervezni, hogy csökkentsék a jelentős üzemszünetek kulcsfontosságú üzleti funkciókra és folyamatokra gyakorolt hatását. A tervnek a potenciális üzleti hatások kockázatának megértésére kell épülnie, és foglalkoznia kell az összes kritikus fontosságú informatikai szolgáltatással kapcsolatos alkalmazkodóképességi, alternatív adatfeldolgozási és helyreállítási képességi követelményekkel. Tartalmazniuk kell használati útmutatókat, szerepköröket é s felelősségeket, eljárásokat, kommunikációs folyamatokat és tesztelési módszert.	DSS04.03	R	**7. §** (3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen. **7. §** (5) A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				további intézkedésekkel biztosítja e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát
DS4.3	Létfontosságú informatikai erőforrások Az informatikai működésfolyamatossági tervben leginkább kritikus fontosságúként azonosított elemekre kell koncentrálni, az alkalmazkodóképesség megteremtése, és a helyreállítási helyzetekben a fontossági sorrend kialakítása érdekében. El kell kerülni, hogy a kevésbé kritikus fontosságú elemek helyreállítása elvonja a figyelmet, és gondoskodni kell a megfelelő reagálásról és helyreállításról a rangsorolt üzleti igényekkel összhangban, biztosítva, hogy a költségek elfogadható szinten belül legyenek, és betartva a szabályozási és szerződéses követelményeket. A különböző szintekre vonatkozóan figyelembe kell venni az alkalmazkodási képességre, a rugalmas reagálásra, a válaszadásra és helyreállításra vonatkozó követelményeket, például egy és négy óra közötti, négy és 24 óra közötti, 24 órát meghaladó és a kritikus fontosságú üzleti működés időszakaira vonatkozóan.	DSS04.04	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
DS4.4	Informatikai működésfolyamatossági terv naprakészen tartása Ösztönözni kell az informatikai vezetést a változtatás engedélyezési eljárások előírására, és végrehajtására annak biztosítása érdekében, hogy az informatikai működésfolyamatossági terv folyamatosan naprakész legyen, és folyamatosan tükrözze a tényleges üzleti követelményeket. Az eljárások és felelősségek változtatásait világosan és időben kell ismertetni.	DSS04.02-05	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
DS4.5	Informatikai működésfolyamatossági terv tesztelése Az informatikai működésfolyamatossági terv rendszeresen kell tesztelni annak biztosítása érdekében, hogy az informatikai rendszerek eredményesen helyreállíthatók legyenek, a hiányosságokkal foglalkozzanak, és a terv megfeleljen a céloknak. Ehhez gondos	DSS04.04	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról,

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	előkészítésére, dokumentálására és a teszteredményeknek a jelentésére van szükség, és a teszteredményeknek megfelelően egy intézkedési tervet kell megvalósítani. Egy-egy alkalmazási rendszer helyreállítási teszt terjedelmét vizsgálni kell, az integrált teszt forgatókönyvek, a teljes körű tesztelés és az integrált szoftver szállítói tesztelés szempontjából.			köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
DS4.6	Informatikai működésfolyamatossági terv oktatása Az összes érintett fél számára rendszeres képzéseket kell tartani, a rendkívüli helyzetekben, illetve a katasztrófa esetén követendő eljárásokat, szerepeiket és felelősségeiket illetően. A képzés helyességének ellenőrzését, és továbbfejlesztését a rendkívüli helyzet kezelési tesztek eredményeinek megfelelően hajtják végre.	DSS04.06	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
DS4.7	Informatikai működésfolyamatossági terv terjesztése Annak megállapítása, hogy létezik egy meghatározott és kézben tartott terjesztési stratégia annak biztosítása érdekében, hogy a tervek kiosztása helyesen és biztonságosan történjék, és azok rendelkezésre álljanak a megfelelően felhatalmazott érdekelt felek részére akkor és ahol, amikor azokra szükség van. Figyelmet kell szentelni annak, hogy a tervek hozzáférhetőek legyenek minden katasztrófa helyzetben.	DSS04.03	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
DS4.8	Informatikai szolgáltatások helyreállítása és folytatása Az informatika helyreállítása és a szolgáltatások	DSS04.03	R	**7. §** (3) Az adatokat megfelelő intézkedésekkel

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	újraindításának időszaka alatt megteendő intézkedések megtervezése. Ez kiterjedhet a tartalék helyszínek igénybe vételére, az alternatív feldolgozás beindítására, az ügyfelekkel és az érdekelt felekkel történő kommunikációra és az újraindítási eljárásokra. Biztosítani kell azt, hogy az üzleti területek tisztában legyenek az informatikai helyreállítási időkkel, és az üzleti helyreállítási és újraindítási igények kielégítéséhez szükséges technológiai beruházások mértékével.			védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.
DS4.9	Mentések és tartalékeszközök telephelyen kívüli tárolása Az informatikai helyreállítási és az üzleti működésfolyamatossági tervekhez szükséges összes kritikus fontosságú mentési adat-hordozót (média), dokumentációt és egyéb informatikai erőforrásokat a telephelyen kívüli kell tárolni. A tartalék adattároló tartalmát meg kell határozni az üzleti folyamat felelősök és az informatikai munkatársak közreműködésével. A telephelyen kívüli adattároló létesítményt az adatosztályozási szabályzatnak és a vállalat médiatárolási gyakorlatainak megfelelően kell kezelni. Az informatikai vezetésnek gondoskodnia kell arról, hogy a külső telephelyre vonatkozó megállapodások időszakonként, de minimum évente értékelésre kerüljenek a tartalom, a környezetvédelem és a biztonság szempontjából. Gondoskodni kell a hardverek és szoftverek kompatibilitásáról az archivált adatok helyreállítása érdekében, és időszakonként tesztelni és frissíteni kell az archivált adatokat.	DSS04.07	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
DS4.10	Helyreállítás utáni felülvizsgálat Meg kell határozni, hogy az informatikai vezetés bevezetett-e eljárásokat a terv megfelelőségének felmérésére, az informatikai funkciónak a katasztrófa után történő sikeres újraindítását illetően és a terv ennek megfelelően történő aktualizálása érdekében.	DSS04.08	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				juttatásához szükségesek.***
DS5	**A rendszerek biztonságának megvalósítása**			
DS5.1	Informatikai biztonság menedzsment Az informatikai biztonság irányítása a megfelelő legmagasabb szervezeti szinten kell legyen, annak érdekében, hogy a biztonsági intézkedések menedzselése összhangban legyen az üzleti követelményekkel.	APO13.01 APO13.03	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
DS5.2	Informatikai biztonsági terv Az üzleti, kockázati és megfelelőségi követelményeket le kell fordítani egy átfogó informatikai biztonsági tervre, figyelembe véve az informatikai infrastruktúrát és a biztonsági kultúrát. Gondoskodni kell arról, hogy a terv megvalósításra kerüljön a biztonsági irányelvek és eljárások formájában, továbbá pénzügyi befektetések révén a szolgáltatásokba, személyzetbe, szoftverekbe és hardverekbe. A biztonsági irányelveket és eljárásokat ismertetni kell az érdekelt felek és a felhasználók felé.	APO13.02	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
DS5.3	Személyazonosítás kezelése Gondoskodni kell arról, hogy az összes (belső, külső és ideiglenes) felhasználó és az informatikai rendszereken (üzleti alkalmazások, informatikai környezet, rendszerműveletek, fejlesztés és karbantartás) végzett tevékenységük egyedileg beazonosítható legyenek. A felhasználók azonosítását lehetővé kell tenni hitelesítési mechanizmusokon keresztül. Meg kell győződni arról, hogy a rendszerekre és az adatokra vonatkozó felhasználói hozzáférési jogok összhangban vannak a meghatározott és dokumentált üzleti igényekkel, és hogy a	DSS05.04	T	**7. §** (3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	felhasználói azonosítókhoz csatolták-e a munkaköri leírásokat. Gondoskodni kell arról, hogy a felhasználói hozzáférési jogokat a felhasználó illetékes vezetői kérelmezzék, és azokat a rendszerek felelősei hagyják jóvá, és a biztonságért felelős személy állítsa be. A felhasználói azonosítókat és a hozzáférési jogok egy központi adattárban kell naprakészen tartani. Gazdaságos műszaki és eljárási rendek bevezetése és naprakészen tartása a felhasználói azonosítás bevezetése, a hitelesítés megvalósítása és a hozzáférési jogok betartatása érdekében.			megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.
DS5.4	Felhasználói fiókok kezelése Foglalkozni kell a felhasználói fiókok és a kapcsolódó felhasználói jogosultságok igénylésével, kialakításával, kiadásával, felfüggesztésével, módosításával és lezárásával a felhasználói fiókkezelő eljárások csoportjának segítségével. Ki kell egészíteni egy jóváhagyási eljárással, amely főbb pontjaiban ismerteti azokat az adatgazdákat és rendszer felelősöket, akik a hozzáférési jogosultságokat megadják. Ezeket az eljárásokat az összes felhasználó esetében alkalmazni kell, beleértve az adminisztrátorokat (kiemelt jogosultságokkal rendelkező felhasználók), valamint a belső és külső felhasználókat mind a normál, mind a rendkívüli eseményekre vonatkozóan. A vállalat rendszereihez és információihoz történő hozzáféréssel kapcsolatos jogokat és kötelezettségeket szerződésben kell rögzíteni az összes felhasználó típusra. Az összes fiók és kapcsolódó jogosultságok rendszeres vezetői felülvizsgálatát el kell végezni.	DSS05.04	T	**7. §** (3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.
DS5.5	Biztonság tesztelése, felügyelete és figyelemmel kísérése Az informatikai biztonság megvalósítását aktívan és kezdeményezően kell tesztelni és nyomon követni. Az informatikai biztonságot idejekorán, ismételten kell bevizsgálni annak biztosítása érdekében, hogy a vállalat jóváhagyott alap informatikai biztonsági szintjét fenntartsák. Egy naplózási és egy figyelemmel kísérési funkciónak kell lehetővé tennie az olyan szokatlan, és/vagy abnormális tevékenységek korai megelőzését, és / vagy észlelését és azt követően időben történő jelentését, amelyekkel lehet, hogy foglalkozni kell.	DSS05.07	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
DS5.6	Biztonsági rendkívüli esemény meghatározása A lehetséges biztonsági rendkívüli események jellemzőit világosan meg kell határozni, és	DSS02.01	R	**7. §** (2) Az adatkezelő, illetve tevékenységi

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	ismertetni kell annak érdekében, hogy azokat a rendkívüli esemény és problémakezelő folyamat helyesen osztályozni és kezelni tudja.			körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
DS5.7	Biztonsági technológiák védelme A biztonsággal kapcsolatos technológiát úgy kell megvalósítani, hogy az ellent tudjon állni az engedély nélküli módosításnak, és a biztonsági dokumentációt nem szabad szükségtelenül nyilvánosságra hozni.	DSS05.05	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
DS5.8	Kriptográfiai kulcsok kezelése Gondoskodni kell arról, hogy a kriptográfiai kulcsok létrehozásának, megváltoztatásának, visszavonásának, megsemmisítésének, kiosztásának, tanúsításának, tárolásának, bevitelének, használatának és archiválásának szervezését szolgáló irányelvek és eljárások működjenek annak érdekében, hogy a kulcsok módosítás és engedély nélküli feltárás elleni védelme biztosított legyen.	DSS05.03	R	**7. §** (3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				válás ellen.
DS5.9	Kártevő szoftverek megelőzése, felismerése és hatásuk korrigálása Megelőző, észlelő és helyesbítő intézkedéseket kell bevezetni (különösen naprakész biztonsági frissítések és vírusvédelem) a szervezet minden területén az információrendszerek és az informatika kártékony szoftverektől való védelme érdekében (például vírusok, férgek, kémszoftverek és kéretlen üzenetek).	DSS05.01	R	**7. §** (3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.
DS5.10	Hálózatbiztonság A hálózatoktól és a hálózatokhoz történő hozzáférés engedélyezése és a hálózatokból történő és a hálózatokba irányuló információáramlás ellenőrzéséhez biztonsági módszereket és azokhoz kapcsolódó irányítási eljárásokat kell alkalmazni (például tűzfalakat, biztonsági készülékeket, hálózati szegmentációt, behatolás észlelés).	DSS05.02	T	**7. §** (3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.
DS5.11	Bizalmas adatok cseréje A bizalmas tranzakciós adatok cseréje csak megbízható útvonalon keresztül, illetve olyan adathordozó segítségével történhet, amelyek kontrolljai biztosítják a tartalom hitelességét, az átadás bizonyíthatóságát, az átvétel bizonyíthatóságát és az eredet letagadhatatlanságát.	DSS05.02	R	**7. §** (3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				fakadó hozzáférhetetlenné válás ellen.
DS6	**A költségek azonosítása és felosztása**			
DS6.1	Informatikai szolgáltatások költségeinek meghatározása Az összes informatikai költséget be kell azonosítani és leképezi informatikai szolgáltatásokra egy átlátható költségmodell támogatása érdekében. Az informatikai szolgáltatásoknak úgy kell az üzleti folyamatokhoz kapcsolódnia, hogy az üzleti területek képesek legyenek beazonosítani a kapcsolódó szolgáltatás számlázási érték nagyságrendeket.	APO06.04	N	
DS6.2	Informatikai költségek nyilvántartása A tényleges költségek rögzíteni kell és fel kell osztani a vállalati költségmodell szerint. Az előrejelzések és a tényleges költségek közötti eltéréseket elemezni és jelenteni kell a vállalat pénzügyi mutatórendszereinek megfelelően.	APO06.01	N	
DS6.3	Költségmodellezés és költségfelszámítás Olyan szolgáltatás meghatározásokra épülő, informatikai költségmodellt kell bevezetni és használni, amely támogatja a szolgáltatásonkénti költségkiszámlázási arányok számítását. Az informatikai költségmodellnek biztosítania kell azt, hogy a szolgáltatások felszámítása beazonosítható, mérhető és előre megjósolható legyen a felhasználók által az erőforrások szabályos felhasználásának ösztönzése céljából.	APO06.04	N	
DS6.4	Költségmodell naprakészen tartása A költség/kiszámlázási modell helyénvalóságát rendszeresen felül kell vizsgálni és össze kell hasonlítani a folyamatosan fejlődő üzleti és informatikai tevékenységekre való alkalmazhatóság és a helyénvalóság fenntartása érdekében.	APO06.04	N	
DS7	**A felhasználók oktatása és képzése**			
DS7.1	Oktatási és képzési igények beazonosítása Minden alkalmazotti célcsoport számára egyéni tanrend et kell kidolgozni és rendszeresen aktualizálni az alábbiak figyelembe vételével: • Jelenlegi és jövőbeli üzleti igények és stratégia • Az információ vagyoni értéke • Vállalati értékek (erkölcsi értékek, kontroll és biztonsági kultúra, stb.) • Új informatikai infrastruktúra és szoftver (úgymint szoftvercsomagok, alkalmazások) bevezetése • Jelenlegi és jövőbeli szakértelem, kompetencia profilok, és tanúsítvány és/vagy bizonyítvány szükségessége, illetve az előírt ismételt tanúsítás • Megvalósítás módszerei (például osztálytermi, web-alapú), célcsoport	APO07.03	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	mérete, hozzáférhetőség és időzítés			
DS7.2	Képzés és oktatás megtartása Az azonosított oktatási és képzési igények alapján a célcsoportokat és tagjaikat, a hatékony képzésbiztosítási mechanizmusokat, tanárokat, oktatókat és mentorokat be kell azonosítani. Az oktatókat ki kell nevezni és a képzési eseményeket időben kell megszervezni. A regisztráció (beleértve az előfeltételeket), a részvétel és a képzéseken nyújtott teljesítmény értékeléseit nyilván kell tartani.	APO07.03	N	
DS7.3	Megtartott képzések értékelése Az oktatási és képzési tartalomszolgáltatást értékelni kell a teljesítést követően az alkalmazhatóság, a minőség, az eredményesség, a tudás elsajátítása, a költség és az érték szempontjából. Ennek az értékelésnek az eredményeit vissza kell csatolni az új tantervek meghatározásához és a képzések megtartásához.	APO07.03	N	
DS8	**A rendkívüli események kezelése és a felhasználói támogatás működtetése**			
DS8.1	Felhasználói támogatás Egy felhasználói támogatás funkciót kell létrehozni, melyen keresztül a felhasználók kapcsolatba léphetnek az informatikával az összes hívás, bejelentett rendkívüli esemény, szolgáltatás igény és információ kérés nyilvántartása, közlése, megoldásra átadása és elemzése céljából. Olyan figyelemmel kísérési és eszkalációs (felterjesztési) eljárásokat kell alkalmazni a megfelelő szolgáltatási szint megállapodások jóváhagyott szolgáltatási szintjei alapján, melyek lehetővé teszik bármely olyan bejelentett ügy osztályozását és rangsorolását, mint például a rendkívüli esemény, szolgáltatás igény, illetve információkérés. A végfelhasználók felhasználói támogatással és az informatikai szolgáltatások minőségével való elégedettségét mérni kell.	-	R	**11. §** (2) Az automatizált adatfeldolgozással hozott döntés esetén az érintettet - kérelmére - tájékoztatni kell az alkalmazott módszerről és annak lényegéről, valamint az érintettnek álláspontja kifejtésére lehetőséget kell biztosítani. **14. §** Az érintett kérelmezheti az adatkezelőnél a) tájékoztatását személyes adatai kezeléséről, b) személyes adatainak helyesbítését, valamint c) személyes adatainak - a kötelező adatkezelés kivételével - törlését vagy zárolását. **15. §** (1) Az érintett kérelmére az adatkezelő tájékoztatást ad az érintett általa kezelt,

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				illetve az általa megbízott adatfeldolgozó által feldolgozott adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, továbbá - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről.
DS8.2	A felhasználói kérdések nyilvántartása A hívások, rendkívüli események, szolgáltatás igények és információ kérések naplózását és nyomon követését, lehetővé tevő funkciót és rendszert kell létrehozni. Ennek szorosan együtt kell működnie az olyan folyamatokkal, mint például a rendkívüli események kezelése, a problémakezelés, a változáskezelés, a kapacitáskezelés és a rendelkezésre állás kezelése. A rendkívüli eseményeket az üzleti és szolgáltatási prioritás szerint kell besorolni, és ha szükséges, akkor a megfelelő problémakezelő munkacsoporthoz kell irányítani. Az ügyfeleket tájékoztatni kell kéréseik állapotáról.	DSS02.01-03	R	**7. §** (5) A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják; d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe; f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön. **15. §** (4) Az adatkezelő köteles a kérelem benyújtásától számított

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				legrövidebb idő alatt, legfeljebb azonban 30 napon belül írásban, közérthető formában megadni a tájékoztatást.
DS8.3	Rendkívüli események eszkalációja Olyan felhasználói támogatási eljárásokat kell kialakítani, hogy az azonnal meg nem oldható rendkívüli eseményeket megfelelően eszkalálni (felterjeszteni) lehessen a szolgáltatói szint megállapodásban meghatározott határértékek szerint, és amennyiben az helyénvaló, akkor áthidaló megoldásokat kell biztosítani. Gondoskodni kell arról, hogy a rendkívüli esemény tulajdonosi szerep és az esemény életciklusának figyelemmel kísérése a felhasználói támogatásnál maradjon a felhasználói rendkívüli események esetében, függetlenül attól, hogy melyik informatikai munkacsoport dolgozik a megoldáson.	DSS02.04	N	
DS8.4	Rendkívüli események lezárása Eljárásokat kell bevezetni az ügyfélkérések rendezésének időben történő figyelemmel kísérése érdekében. Amikor a rendkívüli eseményt megoldották, gondoskodni kell arról, hogy a felhasználói támogatás rögzítse a megoldás lépéseit és meg kell győződni arról, hogy a megtett intézkedéseket az ügyfél jóváhagyta. Továbbá a meg nem oldott rendkívüli eseményeket nyilván kell tartani, és jelenteni kell (ismert hibák és áthidaló megoldások) a helyes problémakezeléshez szükséges információ biztosítása érdekében.	DSS02.05-06	R	**16. §** (2) A tájékoztatás megtagadása esetén az adatkezelő írásban közli az érintettel, hogy a felvilágosítás megtagadására e törvény mely rendelkezése alapján került sor. A felvilágosítás megtagadása esetén az adatkezelő tájékoztatja az érintettet a bírósági jogorvoslat, továbbá a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (a továbbiakban: Hatóság) fordulás lehetőségéről. **18. §** (1) A helyesbítésről, a zárolásról, a megjelölésről és a törlésről az érintettet, továbbá mindazokat értesíteni kell, akiknek korábban az adatot adatkezelés céljára továbbították.

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				Az értesítés mellőzhető, ha ez az adatkezelés céljára való tekintettel az érintett jogos érdekét nem sérti.
DS8.5	Jelentéskészítés és trendelemzés Jelentéseket kell készíteni a felhasználói támogatás tevékenységéről annak érdekében, hogy a vezetés mérni tudja a szolgáltatások teljesítményét és a szolgáltatások válaszideit, és hogy be lehessen azonosítani a trendeket, illetve az ismétlődő problémákat annak érdekében, hogy a szolgáltatást folyamatosan javítani lehessen.	DSS02.07	R	**16. §** (3) Az elutasított kérelmekről az adatkezelő a Hatóságot évente a tárgyévet követő év január 31-éig értesíti.
DS9	**Konfigurációkezelés**			
DS9.1	Konfigurációs nyilvántartás és alapértelmezett értékek Támogató eszközt kell bevezetni és központi adattárat kell létrehozni, mely tartalmazza a konfigurációs elemekre vonatkozó összes lényeges információt. Az összes eszköz és az eszközök változásait figyelemmel kell kísérni és rögzíteni kell. Minden rendszerre és szolgáltatásra vonatkozóan konfigurációelemek alapértékeit nyilván kell tartani azért, hogy ellenőrző pontként szolgáljon, amihez vissza lehet térni a változtatások után.	BAI10.01-02 BAI10.04 DSS02.01	N	
DS9.2	Konfigurációs elemek beazonosítása és karbantartása Konfigurációs eljárások működtetése a konfigurációs adattár összes változása kezelésének és naplózásának támogatása érdekében. Ezen eljárások integrálása a változáskezelési, rendkívüli esemény-kezelési és a problémakezelési eljárásokkal.	BAI10.03	N	
DS9.3	A konfiguráció sértetlenségének felülvizsgálata A konfigurációs adatokat a jelenlegi és a múltbeli konfiguráció sértetlenségének ellenőrzése és helyességének megerősítése érdekében való időszakos felülvizsgálata. A telepített szoftverek időszakos felülvizsgálata a szoftverhasználatra vonatkozó irányelv alapján a magán, illetve licenc nélküli szoftverek, illetve bármely olyan szoftver példány beazonosítása érdekében, amely az érvényes licenc megállapodások felett került telepítésre. A hibákat és az eltéréseket jelenteni kell, intézkedéseket kell hozni, és azokat helyesbíteni kell.	BAI10.04-05 DSS02.05	N	
DS10	**Problémakezelés**			
DS10.1	Problémák azonosítása és osztályozása Olyan folyamatokat kell bevezetni, amelyek a rendkívüli események kezelésének részeként azonosított problémákat jelentik és osztályozzák. A problémák osztályozásának lépései hasonlóak a rendkívüli események osztályozásának lépéseihez; céljuk az, hogy meghatározzák a kategóriát, a hatást, a sürgősséget és a prioritást. A problémákat értelemszerűen be kell sorolni a	DSS03.01	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	vonatkozó csoportokba, illetve területekbe (például hardver, szoftver, támogató szoftver). Ezen csoportok megfelelhetnek a felhasználói és az ügyfélbázis szervezeti felelősségeinek, és e csoportok alapján kell a problémákat kiosztani a támogatást végző munkatársaknak.			
DS10.2	Problémák nyomon követése és megoldása Gondoskodni kell arról, hogy a problémakezelő rendszer megfelelő auditálhatósági napló szolgáltatásokat biztosítson az összes bejelentett probléma nyomon követésének, elemzésének és alapvető okának az alábbiak figyelembe vételével történő meghatározása érdekében: • Az összes érintett konfiguráció-elem • Kiemelkedő problémák és rendkívüli események • Ismert és gyanított hibák • A probléma trendek nyomon követése A probléma gyökerét azonosítani kell és tartósan fenntartható megoldásokat kell kialakítani, változtatás kérelmek bevezetett változtatáskezelési folyamaton keresztüli kezdeményezhetők. A megoldási folyamat teljes menete során a problémakezelésnek rendszeresen jelentést kell kapnia a változáskezeléstől a problémák és a hibák megoldására irányuló előrehaladásról. A problémakezelésnek figyelemmel kell kísérnie a problémáknak és az ismert hibáknak a felhasználói szolgáltatásokra gyakorolt folyamatos hatását. Abban az esetben, ha ez a hatás súlyossá válik, a problémakezelésnek eszkalálnia kell a problémát, elképzelhető, hogy egy megfelelő bizottság elé történő terjesztés révén, szükség szerint egy változtatási kérelem prioritásának növelése, vagy egy sürgős változtatás bevezetése érdekében. A probléma megoldás szolgáltatási szint megállapodásban rögzítettekhez képest való előrehaladásának figyelemmel kísérése.	DSS03.02	R	**10. §** (1) Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit e törvény, valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. Az általa adott utasítások jogszerűségéért az adatkezelő felel.
DS10.3	Probléma lezárása Eljárás bevezetése a problémajegyek lezárása érdekében vagy az ismert hiba sikeres kiküszöbölésének visszaigazolása után vagy azt követően, hogy megállapodás született az üzleti területekkel a probléma alternatív megoldásáról.	DSS03.03-04	N	
DS10.4	Konfiguráció-, rendkívüli esemény- és problémakezelés integrációja A konfiguráció-, rendkívüli esemény- és problémakezelés vonatkozó folyamatainak integrálása a problémák eredményes kezelésének biztosítása és a javítások lehetővé tétele érdekében.	DSS03.05	N	
DS11	**Az adatok kezelése**			
DS11.1	Adatkezelés üzleti követelményei Ellenőrizni kell azt, hogy a feldolgozásra várt összes adat megérkezett-e és teljes mértékben, pontosan és időben kell, hogy feldolgozásra kerüljön, és hogy az összes kimenet biztosítva lett	DSS01.01	T	**4. §** (4) Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és - ha az

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	az üzleti követelményeknek megfelelően. Az újraindítási és újrafeldolgozási igények támogatása.			adatkezelés céljára tekintettel szükséges - naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.
DS11.2	Adattárolási és megőrzési intézkedések A hatékony és eredményes adattárolás, megőrzés és archiválás eljárásainak meghatározása és megvalósítása az üzleti célkitűzéseknek, a szervezet biztonsági irányelvének és szabályozási követelményeinek a kielégítése érdekében.	DSS04.08 DSS06.04	T	**7. §** (3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen. **17. §** (1) Ha a személyes adat a valóságnak nem felel meg, és a valóságnak megfelelő személyes adat az adatkezelő rendelkezésére áll, a személyes adatot az adatkezelő helyesbíti. **17. §** (2) A személyes adatot törölni kell, ha a) kezelése jogellenes; b) az érintett - a 14. § c) pontjában foglaltak szerint - kéri; c) az hiányos vagy téves - és ez az állapot jogszerűen nem orvosolható -, feltéve, hogy a törlést törvény nem zárja ki; d) az adatkezelés célja megszűnt, vagy

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				az adatok tárolásának törvényben meghatározott határideje lejárt; e) azt a bíróság vagy a Hatóság elrendelte. **33. §** (1) Az e törvény alapján kötelezően közzéteendő közérdekű adatokat internetes honlapon, digitális formában, bárki számára, személyazonosítás nélkül, korlátozástól mentesen, kinyomtatható és részleteiben is adatvesztés és -torzulás nélkül kimásolható módon, a betekintés, a letöltés, a nyomtatás, a kimásolás és a hálózati adatátvitel szempontjából is díjmentesen kell hozzáférhetővé tenni (a továbbiakban: elektronikus közzététel). A közzétett adatok megismerése személyes adatok közléséhez nem köthető.[348]
DS11.3	Adathordozó-könyvtár kezelési rendszer A tárolt és archivált adathordozók leltárának karbantartását szolgáló eljárások meghatározása és megvalósítása, azok használhatóságának és sértetlenségének biztosítása érdekében.	DSS04.08	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb

[348] csak a közérdekű adatok vonatkozásában

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
DS11.4	Selejtezés utáni adat megsemmisítés Eljárások meghatározása és megvalósítása annak biztosítása érdekében, hogy a bizalmas adatok és szoftverek védelmére vonatkozó üzleti követelmények kielégítésre kerüljenek, amikor az adatokat és a hardvereket selejtezés után elhelyezik, illetve áthelyezik.	DSS05.06 DSS06.05-06	T	**7. §** (3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.
DS11.5	Mentés és helyreállítás A rendszerek, alkalmazások, adatok és dokumentációk mentésére és helyreállítására vonatkozó eljárások meghatározása és megvalósítása, az üzleti követelményekkel és a működésfolyamatossági tervvel összhangban.	DSS04.08	R	**7. §** (3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.
DS11.6	Adatkezelés biztonsági követelményei Az adatok fogadására, feldolgozására, tárolására és kiadására vonatkozó biztonsági követelmények azonosításával és alkalmazásával kapcsolatos irányelvek és eljárások meghatározása és megvalósítása az üzleti célkitűzések elérése, valamint a szervezet biztonsági irányelvének és a szabályozási követelményeknek a kielégítése érdekében.	DSS01.01 DSS05.02-05 DSS06.03 DSS06.06	T	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
DS12	**A fizikai környezet biztosítása**			
DS12.1	Gépterem kiválasztása és felépítése Az üzleti stratégiához kapcsolt technológiai stratégia támogatása érdekében meg kell határozni, és ki kell választani az informatikai berendezések fizikai helyszíneit. A helyszín kiválasztásakor és a telephely építészeti megtervezésekor számításba kell venni a természetes és az emberek által okozott katasztrófákkal kapcsolatos kockázatot, továbbá figyelembe kell vennie a vonatkozó törvényeket és szabályozásokat, például a munkavállalással kapcsolatos munkahelyi egészségügyi és biztonsági rendeleteket.	DSS01.04-05 DSS05.05	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.***
DS12.2	Fizikai biztonsági intézkedések A fizikai biztonsági intézkedések meghatározása és megvalósítása az üzleti követelményekkel összhangban a helyszín és a fizikai eszközök biztonságának megteremtése érdekében. A fizikai biztonsági intézkedéseknek képeseknek kell lenniük a lopással, hőmérséklettel, tűzzel, füsttel, vízzel, rezgéssel, terrorral, vandalizmussal, áramkimaradásokkal, vegyszerekkel, illetve robbanószerekkel kapcsolatos kockázatok eredményes megelőzésére, észlelésére és enyhítésére.	DSS05.05	R	**7. §** (3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.
DS12.3	Fizikai hozzáférés A telephelyekre, épületekbe és területekre való belépés jogának megadására, korlátozására és visszavonására vonatkozó eljárásokat meg kell határozni és üzleti igényeknek megfelelően meg kell valósítani, beleértve a vészhelyzetekre vonatkozó eljárásokat is. A telephelyekhez, épületekhez és területekhez történő belépésnek indokoltnak, engedélyezettnek, naplózottnak és	DSS05.05	R	**7. §** (3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás,

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	figyelemmel kísértnek kell lennie. Ennek vonatkoznia kell az összes olyan személyre, aki belép a telephelyekre, beleértve a személyzetet, az ideiglenes személyzetet, az ügyfeleket, az szállítókat, a látogatókat, illetve bármely más külső felet.			nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen..
DS12.4	A környezeti tényezőkkel szembeni védelem A környezeti tényezők elleni védelmet szolgáló intézkedések megtervezése és megvalósítása. Speciális berendezések és eszközök telepítése a környezet figyelemmel kísérése és kontrollálása érdekében.	DSS01.04	R	**7. §** (3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.
DS12.5	Fizikai létesítmények kezelése A létesítmények kezelése, beleértve az áram és kommunikációs berendezéseket, a törvényekkel és a szabályozásokkal, a műszaki és üzleti követelményekkel, a szállítói specifikációkkal, és a munkahelyi egészségügyi és biztonsági útmutatásokkal összhangban.	DSS01.05	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
DS13	**Az üzemeltetés irányítása**			
DS13.1	Üzemeltetési eljárások és utasítások Az informatikai üzemeltetés eljárásainak meghatározása, megvalósítása és karbantartása annak biztosítása érdekében, hogy az üzemeltetéssel foglalkozó munkatársak ismerjék a	DSS01.01	R	**10. §** (1) Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	rájuk vonatkozó összes üzemeltetési feladatot. Az üzemeltetési eljárásoknak ki kell terjednie a műszak átadására (a tevékenység formális átadására, az állapot aktualizálásokra, az üzemeltetési problémákra, az eszkalációs eljárásokra és a pillanatnyi felelősségekre vonatkozó jelentésekre) az elfogadott szolgáltatási szintek támogatása és a folyamatos működés biztosítása érdekében.			kötelezettségeit e törvény, valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. Az általa adott utasítások jogszerűségéért az adatkezelő felel.
DS13.2	Műveletek ütemezése A műveletek, folyamatok és feladatok ütemezésének a leghatékonyabb szekvenciába szervezése, maximalizálva az áteresztőképességet és a kihasználást az üzleti követelmények teljesítése érdekében.	DSS01.01	N	
DS13.3	Informatikai infrastruktúra figyelemmel kísérése Az informatikai infrastruktúra és a kapcsolódó események figyelemmel kísérésére vonatkozó eljárások meghatározása és megvalósítása. Gondoskodni kell arról, hogy elegendő történeti idősoros információ kerüljön eltárolásra az üzemeltetési naplókban, a műveletek és a műveleteket körülvevő, illetve azokat támogató egyéb tevékenységek időbeli sorrendjének rekonstruálásának, felülvizsgálatának és kivizsgálásának lehetővé tétele érdekében.	DSS01.03	N	
DS13.4	Bizalmas dokumentumok és kimeneti adatokat előállító eszközök Megfelelő fizikai óvintézkedések, szigorú számadású bizonylatok nyilvántartására vonatkozó eljárások és leltárkezelés bevezetése az olyan bizalmas informatikai vagyonelemekre vonatkozóan, mint például a speciális formanyomtatványok, átruházható értékpapírok (forgatmányok), speciális célú nyomtatók, illetve biztonsági hardver eszközök.	DSS05.06	N	
DS13.5	Hardver megelőző karbantartása Az infrastruktúra időben történő karbantartását biztosító eljárások meghatározása és megvalósítása, a hibák, illetve teljesítmény visszaesések gyakoriságának és hatásának csökkentése érdekében.	BAI09.02	N	
ME1	**Az informatika teljesítményének figyelemmel kísérése és értékelése**			
ME1.1	Figyelemmel kísérésre használt módszer Általános figyelemmel kísérési és nyomon követési keretrendszert és módszert kell bevezetni azért, hogy az informatikai megoldás és szolgáltatás nyújtás teljesítmény mérése céljából meg kell határozni a teljesítmény mérés kiterjedését, módszertanát és eljárását, valamint az informatika üzleti tevékenységhez történő hozzájárulásának nyomon követését. A keretrendszert integrálni kell a vállalat teljesítmény menedzsment rendszerével.	MEA01.01	N	
ME1.2	Figyelemmel kísérési adatok meghatározása és	MEA01.02-	R	**10. §** (1) Az

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	gyűjtése Együtt kell működni az üzleti területekkel a teljesítmény célok egy kiegyensúlyozott csoportjának meghatározásában, és azokat az üzleti és az egyéb érintett érdekelt felekkel jóvá kell hagyatni. Ipari normákból a mérési alapokat kell meg határozni a célokkal való összehasonlításhoz, és a célok mérése érdekében begyűjtendő rendelkezésre álló adatokat azonosítni kell. Az adatok időben és pontosan történő begyűjtését szolgáló folyamatok kell bevezetni a célokhoz képesti előrehaladás jelentése érdekében.	03		adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit e törvény, valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. Az általa adott utasítások jogszerűségéért az adatkezelő felel.
ME1.3	Figyelemmel kísérés módszere Olyan teljesítmény figyelemmel kísérési módszert kell bevezetni (például kiegyensúlyozott stratégiai mutatószám rendszer), amely nyilvántartja a célokat; rögzíti a méréseket; az informatika teljesítmény tömör, mindenre kiterjedő áttekintését biztosítja; és amely illeszkedik a vállalati figyelemmel kísérési rendszerhez.	MEA01.03	N	
ME1.4	Teljesítményértékelés A teljesítményt a célokhoz viszonyítva rendszeresen felül kell vizsgálni, az esetleges eltérések okának elemzése és helyesbítési intézkedések kezdeményezése a mögöttes okok rendezése céljából. Megfelelő időpontokban probléma gyökerét feltáró elemzéseket kell végezni az eltérésekkel kapcsolatban.	MEA01.04	N	
ME1.5	Igazgatótanácsi és felsővezetői jelentések Az informatikának felsővezetői jelentéseket kell készíteni az üzleti tevékenységhez történő hozzájárulásáról, konkrétan a vállalat beruházási program portfoliójának értelmében, nevezetesen az informatika révén megvalósítható, valamint az egyedi beruházási programok informatikai megoldásai és szolgáltatásai teljesítményéről. Az állapot jelentésekben ki kell térni, hogy milyen mértékben teljesültek a tervezett célkitűzések, kerültek felhasználásra a költségvetésben tervezett erőforrások, érték el a kitűzött teljesítménycélokat és enyhítették a beazonosított kockázatokat. Fel kell készülni a felső vezetés részéről kezdeményezett felülvizsgálatra, amely a jelentős eltérésekre vonatkozó helyreállítási intézkedésekre történő javaslattételhez vezethet. A jelentést át kell adni a felső vezetésnek és a vezetői felülvizsgálatról meg kell kérni a visszajelzéseket.	MEA01.04	N	
ME1.6	Helyreállító tevékenységek Helyesbítési intézkedések kell beazonosítani és kezdeményezni a teljesítmény figyelemmel kísérése, felmérése és jelentése alapján. Ennek ki kell terjednie az összes figyelemmel kísérési, jelentési és felmérési tevékenység alábbiakon keresztül történő utókövetésére:	MEA01.05	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	▪ Vezetői válaszok felülvizsgálata, egyeztetése és megállapítása ▪ A helyesbítéssel kapcsolatos felelősség delegálása ▪ A végrehajtott intézkedések eredményeinek nyomon követése			
ME2	**A belső irányítási és ellenőrzési rendszer figyelemmel kísérése és értékelése**			
ME2.1	A belső irányítási és ellenőrzési keretrendszer figyelemmel kísérése Az informatikai kontroll környezetet és kontroll keretrendszert folyamatosan figyelemmel kell kísérni, összehasonlító értékeléseket kell végezni és fejleszteni kell a szervezet célkitűzéseinek elérése érdekében.	MEA02.01-02	N	
ME2.2	Ellenőrző felülvizsgálat A belső informatikai vezetői felülvizsgálati kontrollok hatékonyságát és eredményességét figyelemmel kell kísérni és értékelni kell.	MEA02.01	N	
ME2.3	Kontrollok sérülése A kontrollok sérülését be kell azonosítani, továbbá a hátterükben rejlő alapvető okokat elemezni kell és be kell azonosítani. A kontrollok sérülését eszkalálni kell és az érdekelt feleknek megfelelően jelenteni. A szükséges helyesbítési intézkedéseket meg kell tenni.	MEA02.04	N	
ME2.4	Kontroll önértékelés A vezetésnek az informatikai folyamatok, irányelvek és szerződések feletti kontroll teljességét és eredményességét értékelni kell, egy folyamatos önértékelési programon keresztül.	MEA02.03	N	
ME2.5	A belső irányítási és ellenőrzési rendszer értékelése Szükség esetén be kell szerezni a belső kontrollok teljességére és eredményességére vonatkozó további garanciát a külső felek által készített felülvizsgálatokon keresztül.	MEA02.06-08	N	
ME2.6	Belső irányítási és ellenőrzési rendszer a külső feleknél A külső szolgáltatók belső irányítási és ellenőrzési rendszerét fel kell mérni. Meg kell győződni arról, hogy a külső szolgáltatók megfelelnek a jogi és szabályozási követelményeknek, és a szerződéses kötelezettségeknek.	MEA02.01	N	
ME2.7	Helyreállító tevékenységek A kontroll értékelésekből és jelentésekből eredő helyreállító intézkedéseket beazonosítani, kezdeményezni, nyomon követni kell és meg kell azokat valósítani.	MEA02.04	N	
ME3	**Külső követelményeknek való megfelelőség biztosítása**			
ME3.1	A külső jogi, szabályozói és szerződéses megfelelőségi követelmények azonosítása Az olyan helyi és nemzetközi törvényeket, rendeleteket és egyéb külső követelményeket folyamatosan be kell azonosítása, amelyeknek meg kell felelni, és amelyeknek be kell épülnie a	MEA03.01	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	szervezet informatikai irányelveibe, szabványaiba, eljárásaiba és módszertanaiba.			az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek. **11. §** (1) Kizárólag automatizált adatfeldolgozással az érintett személyes jellemzőinek értékelésén alapuló döntés meghozatalára csak akkor kerülhet sor, ha a döntést a) valamely szerződés megkötése vagy teljesítése során hozták, feltéve hogy azt az érintett kezdeményezte, vagy b) olyan törvény teszi lehetővé, amely az érintett jogos érdekeit biztosító intézkedéseket is megállapítja.
ME3.2	Külső követelményekre adott válaszok optimalizálása Az informatikai irányelveket, szabványokat, eljárásokat és módszertanokat felül kell vizsgálni és ki kell igazítani annak biztosítása érdekében, hogy a jogi, szabályozási és szerződési követelményeknek megfeleljenek, és erről tájékoztatást adjanak.	MEA03.02	R	**7. §** (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
				juttatásához szükségesek.
ME3.3	A külső követelményeknek való megfelelőség értékelése Meg kell győződni arról, hogy az informatikai irányelvek, szabványok, eljárások és módszertanok megfelelnek a jogi és szabályozási követelményeknek.	MEA03.03	N	
ME3.4	Bizonyosság nyújtása a megfelelőségről A megfelelőséget, és a belső utasításokból, illetve külső jogi, szabályozási, illetve szerződéses követelményekből származtatott összes belső irányelv betartását igazoló bizonyosságot kell beszerezni és azt jelenteni kell; meg kell győződni arról, hogy az esetleges megfelelőségi hiányosságokat rendezték, a helyesbítő intézkedéseket az azokért felelős folyamatfelelős időben megtette.	MEA03.04	N	
ME3.5	Integrált jelentéskészítés A jogi, szabályozási és szerződéses követelményekre vonatkozó informatikai jelentést integrálni kell az egyéb üzleti funkciók hasonló jelentéseivel.	MEA03.04	N	
ME4	**Az informatikai irányítás megteremtése**			
ME4.1	Informatikai irányítási keretrendszer kialakítása Az informatikai irányítási keretrendszert meg kell határozni, működtetni kell, és összhangba kell hozni az általános vállalatirányítási és kontroll környezettel. A keretrendszert egy megfelelő informatikai folyamat és kontroll modellre kell építeni, és gondoskodni kell az egyértelmű elszámoltathatóságról és a továbbá olyan eljárásokra kell építeni, amelyek a belső irányítási és ellenőrzési rendszer, valamint vezetői felügyelet összeomlását megakadályozzák. Meg kell győződni arról, hogy az informatikai irányítási keretrendszer gondoskodik a törvényekkel és a szabályozásokkal kapcsolatos megfelelőségről, és összhangban van a vállalat stratégiáival és célkitűzéseivel, és egyben visszaigazolja azok teljesítését. Az informatikai irányítás állapotáról és az aktuális ügyekről jelentéseket kell készíteni.	EDM01	N	
ME4.2	A stratégia illesztése Lehetővé kell tenni, hogy az igazgatótanács és a felső vezetés megértse az olyan stratégiai informatikai kérdéseket, mint például az informatika, a technológiai kérdések és a képességek szerepe. Gondoskodni kell arról, hogy az üzleti területek és az informatika ugyanúgy értelmezze az informatikának az üzleti stratégiához való lehetséges hozzájárulását. Együtt kell működni az igazgatótanáccsal és a létrehozott irányító testületekkel, például az informatikai stratégiai bizottsággal azért, hogy a vezetés részére az informatikával kapcsolatosan egy stratégiai iránymutatás nyújtsanak, gondoskodni kell arról, hogy a stratégia és a	-	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	célkitűzések lépcsőzetesen beépüljenek az szervezeti egységekbe és az informatikai funkciókba, és hogy kialakuljon a bizalom az üzleti területek és az informatika között. Lehetővé kell tenni az informatika összhangba hozását az üzleti tevékenységgel a stratégia és a működtetés terén, ösztönözve az üzleti területek és az informatika közös felelősségvállalását a stratégiai döntések meghozatala és az informatikával támogatott beruházások előnyeinek elérése tekintetében.			
ME4.3	Értékelő állítás Az informatikával támogatott beruházási programokat, és egyéb informatikai vagyonelemeket és szolgáltatásokat menedzselni kell annak biztosítása érdekében, hogy a lehető legnagyobb értéket teremtsék meg a vállalat stratégiájának és célkitűzéseinek támogatása közben. Gondoskodni kell arról, hogy az informatikával támogatott beruházások várható üzleti eredményeit és az ezen eredmények eléréséhez szükséges erőfeszítések teljes terjedelmét megértsék; hogy átfogó és következetes üzleti terveket készítsenek és hagyjanak jóvá az érdekelt felek; hogy a vagyonelemekkel és a beruházásokkal teljes gazdasági életciklusuk során gazdálkodnak, és hogy az olyan hasznok realizálását aktívan menedzseljék, mint például az új szolgáltatásokhoz történő hozzájárulás, a hatékonyság fokozás és az ügyfél igényekre való javított reagálóképesség. A portfolió, program és projekt menedzsment fegyelmezett módszerének betartatása, ragaszkodva ahhoz, hogy az üzleti területek felvállalják az összes informatikával támogatott beruházás tulajdonosi szerepét, továbbá hogy az informatika biztosítsa az informatikai képességek és szolgáltatások nyújtásával járó költségek optimalizálását.	EDM02	N	
ME4.4	Erőforrás gazdálkodás A beruházások, az informatikai erőforrások felhasználását és elkülönítését felügyelni kell az informatikai kezdeményezések és működés rendszeres értékelésén keresztül, a megfelelő erőforrások biztosításának, és a jelenlegi és a jövőbeli stratégiai célkitűzésekkel és az üzleti alapkövetelményekkel történő összhang biztosítása érdekében.	EDM04	N	
ME4.5	Kockázatkezelés Együtt kell működni az igazgatótanáccsal a vállalat informatikai kockázatvállalási hajlandóságának meghatározásában, és az arra vonatkozó bizonyosság beszerzésében, hogy az informatikai kockázatkezelési eljárások megfelelően biztosítják azt, hogy a tényleges informatikai kockázat mértéke ne haladja meg az igazgatótanács által felvállaltat. A kockázatkezelésért való felelősséget be kell	EDM03	N	

COBIT 4.1 kontroll célkitűzés[347]		COBIT	Információs törvény	
		5	lefed.	követelmény
	építeni a szervezetbe, biztosítva azt, hogy az üzlet és az informatika rendszeresen értékelje és jelentse az informatikával kapcsolatos kockázatokat és hatásaikat, és hogy a vállalat informatikai kockázati pozíciója az összes érdekelt fél által látható legyen.			
ME4.6	Teljesítménymérés Meg kell győződni arról, hogy a jóváhagyott informatikai célkitűzések kielégítették vagy túlteljesítették, illetve hogy az informatikai célok előrehaladása megfelel az elvárásoknak. Azokban az esetekben, amikor a jóváhagyott célkitűzések teljesítése nem sikerült, illetve az előrehaladás nem felel meg az elvárásoknak, akkor felül kell vizsgálni a vezetés helyreigazító intézkedéseit. Az érintett portfoliók, programok és az informatika teljesítményét jelenteni kell az igazgatótanácsnak, alátámasztva olyan jelentésekkel, melyek lehetővé teszik, hogy a felső vezetés felül tudja vizsgálni a vállalat előrehaladását a kijelölt célok tekintetében.	EDM01.03 EDM02.03 EDM03.03 EDM04.03	N	
ME4.7	Független bizonyosság nyújtás Független bizonyosság nyújtást (belső, illetve külső) kell beszerezni az informatika vonatkozó törvényeknek és szabályozásoknak való megfelelőségéről; a szervezet irányelveiről, szabványairól és eljárásairól; az általánosan elfogadott gyakorlatokról; és az informatika eredményességéről és hatékonyságáról.	MEA02.05-07 MEA02-08	N	

IT rendszerekkel szemben támasztott általános követelmények

COBIT 4.1 kontroll célkitűzés		COBIT	információs törvény	
		5	lefed.	követelmény
AC	**Alkalmazás kontroll célkitűzések**			
AC1	Forrásadatok előkészítése és engedélyezése Gondoskodni kell arról, hogy a forrás dokumentumokat felhatalmazott és szakképzett személyzet készítse bevezetett eljárásokat követve, mely során figyelembe kell venni a felelősségek megfelelő elhatárolását a dokumentumok létrehozásakor és jóváhagyásakor. A hibák és a mulasztások minimalizálhatók a jó bemeneti formanyomtatvány tervezés segítségével. A hibákat és a szabálytalanságokat azonosítani kell annak érdekében, hogy lejelenthetőek és helyesbíthetőek legyenek.	DSS06.02 DSS06.03 BAI03.02 BAI03.03 BAI03.05 BAI03.07	R	**4. §** (4) Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és - ha az adatkezelés céljára tekintettel szükséges - naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani. **7. §** (5) A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja a) a jogosulatlan adatbevitel megakadályozását; b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását; c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják; d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe; e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

COBIT 4.1 kontroll célkitűzés		COBIT 5	információs törvény lefed.	információs törvény követelmény
AC2	Forrásadatok összegyűjtése és bevitele Gondoskodni kell arról, hogy az adatbevitelt felhatalmazott és minősített személyzet megfelelő időzítés szerint végezze. A tévesen bevitt adatok helyesbítését, és ismételt bevitelét oly módon kell végrehajtani, hogy az adatbeviteli tranzakciók ne sértsék meg az eredeti jogosultsági szinteket. Ahol felhasználható a helyreállításhoz, ott az eredeti forrás dokumentumokat meg kell őrizni a szükséges időtartamig.	DSS06.02	R	**4. §** (4) Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és - ha az adatkezelés céljára tekintettel szükséges - naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani. **7. §** (5) A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja a) a jogosulatlan adatbevitel megakadályozását; b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását; c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják; d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe; e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

COBIT 4.1 kontroll célkitűzés		COBIT	információs törvény	
		5	lefed.	követelmény
AC3	Pontossági, teljességi és hitelességi ellenőrzések Gondoskodni kell arról, hogy a tranzakciók pontosak, teljesek és érvényesek legyenek. A bemeneti, szerkesztett, illetve helyesbítésre visszaküldött adatok érvényesítése a keletkezésükhöz lehető legközelebb eső ponton kell történjen.	DSS06.02	R	**4. §** (4) Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és - ha az adatkezelés céljára tekintettel szükséges - naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani. **7. §** (5) A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja a) a jogosulatlan adatbevitel megakadályozását; b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását; c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják; d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe; e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

COBIT 4.1 kontroll célkitűzés		COBIT	információs törvény	
		5	lefed.	követelmény
AC4	Feldolgozás sértetlensége és érvényessége Az adatok sértetlenségét és érvényességét fenn kell tartani a teljes feldolgozási ciklus alatt. A hibás tranzakciók felismerése nem szakíthatja meg az érvényes tranzakciók feldolgozását.	DSS06.02	R	**4. §** (4) Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és - ha az adatkezelés céljára tekintettel szükséges - naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani. **7. §** (5) A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja a) a jogosulatlan adatbevitel megakadályozását; b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását; c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják; d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe; e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

COBIT 4.1 kontroll célkitűzés		COBIT	információs törvény	
		5	lefed.	követelmény
AC5	Kimenet felülvizsgálat, egyeztetés és hibakezelés Eljárásokat és a kapcsolódó felelősségeket úgy kell kialakítani, hogy biztosítsa a kimeneteket engedélyezett módon való kezelését, a kimenetek a megfelelő címzetthez való eljuttatását, és a továbbítás alatti védelmüket; és hogy a kimenet pontosságának ellenőrzése, felismerése és korrigálása megtörténjék, és hogy a kimenetként adott információkat felhasználják.	DSS06.02	R	**4. §** (4) Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és - ha az adatkezelés céljára tekintettel szükséges - naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani. **7. §** (5) A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja a) a jogosulatlan adatbevitel megakadályozását; b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását; c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják; d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe; e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

	COBIT 4.1 kontroll célkitűzés	COBIT 5	információs törvény lefed.	információs törvény követelmény
AC6	Tranzakció hitelesítése és sértetlensége A belső alkalmazások és az üzleti/üzemeltetési funkciók között a tranzakciós adatok (a vállalaton belüli, illetve kívüli) továbbítása előtt, ellenőrizni kell a szabályos címzést, az eredet hiteleségét és a tartalom sértetlenségét. A hitelességet és sértetlenséget meg kell őrizni az adattovábbítás, illetve a szállítás alatt is.	DSS06.02	R	**7. §** (3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen. **7. §** (5) A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja a) a jogosulatlan adatbevitel megakadályozását; b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását; c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják; d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe; e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

Folyamatokkal szemben támasztott általános követelmények

COBIT 4.1 kontroll célkitűzés*		információs törvény	
		lefed.	követelmény
PC	**Folyamat kontroll célkitűzések**		
PC1	Folyamat céljai és célkitűzései Konkrét, mérhető, végrehajtható, reális, eredmény orientált és időszerű (SMARRT: specific, measurable, actionable, realistic, results-oriented and timely) folyamat célok és célkitűzések meghatározása és közvetítése az egyes informatikai folyamatok eredményes végrehajtása érdekében. Gondoskodni arról, hogy azok a célok kapcsolódnak az üzleti célokhoz és azokat megfelelő metrikák támogatják.	T	**4. §** (1) Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie.
PC2	Folyamat felelősség Egy folyamat felelőst ki kell jelölni minden egyes informatikai folyamathoz, egyértelműen meg kell határozni a folyamatfelelős szerepkörét és felelősségeit. Ilyenek például a folyamattervezés felelőssége, a többi folyamattal történő együttműködés, a végső eredmények elszámoltathatósága, a folyamat teljesítmény mérése és a javítási lehetőségek beazonosítása.	T	**10. §** (1) Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit e törvény, valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. Az általa adott utasítások jogszerűségéért az adatkezelő felel.
PC3	Folyamat megismételhetőség Minden egyes kulcsfontosságú folyamatot úgy kell megtervezni és kialakítani, hogy az ismételhető legyen, és következetesen az elvárt eredményeket állítsa elő. A tevékenységeknek egy olyan logikus, de rugalmas és skálázható sorrendjét kell biztosítani, ami elvezet a kívánt eredményekhez, és kellőképpen rugalmas ahhoz, hogy lekezelje a kivételeket és a rendkívüli helyzeteket. Ahol csak lehetséges konzisztens folyamatokat kell használni, és testre szabást csak akkor szabad alkalmazni, amikor az elkerülhetetlen.	N	
PC4	Szerepkörök és felelősségek Meg kell határozni a folyamat kulcsfontosságú tevékenységeit és végtermékeit. Egyértelmű szerepköröket és felelősségeket kell kijelölni és ismertetni azokat a kulcsfontosságú tevékenységek és dokumentálásuk eredményes és hatékony végrehajtása, valamint a folyamat végtermékeiért való elszámoltathatóság biztosítása érdekében.	R	**10. §** (1) Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit e törvény, valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. Az általa adott utasítások jogszerűségéért az adatkezelő felel.

COBIT 4.1 kontroll célkitűzés*		információs törvény	
		lefed.	követelmény
PC5	Irányelv, tervek és eljárások Meg kell határozni, és ismertetni, hogy az összes olyan irányelv, terv, eljárás, amely egy informatikai folyamatot vezérel, hogyan kerül dokumentálásra, felülvizsgálatra, aktualizálásra, jóváhagyásra, eltárolásra, ismertetésre, és képzés céljából történő felhasználásra. Ezen tevékenységek mindegyikére vonatkozóan felelősöket kell kijelölni, és a helyes végrehajtásukat megfelelő időnként felül kell vizsgálni. Gondoskodni kell arról, hogy az irányelvek, tervek és eljárások elérhetők, helyesek, naprakészek legyenek és megértették őket.	R	**10. §** (1) Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit e törvény, valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. Az általa adott utasítások jogszerűségéért az adatkezelő felel.
PC6	Folyamat teljesítményének javítása Metrikák egy olyan csoportját kell meghatározni, amelyek rálátást biztosítanak a folyamat eredményeire és teljesítményére. Olyan tervcélokat kell kijelölni, amelyek tükrözik a folyamat céljait és olyan teljesítmény mutatókat kell bevezetni, amelyek lehetővé teszik a folyamat céljainak az elérését. Meg kell határozni, hogy az adatokat hogyan gyűjtik be. A tényleges mérési eredményeket össze kell hasonlítani a célokkal és eltérések esetén, amennyibe arra szükség van, a megfelelő intézkedések kell tenni. A metrikákat, a célokat és a módszereket össze kell hangolni az informatika általános teljesítmény figyelemmel kísérési módszerével.	N	

* A COBIT 4.1 folyamat kontroll célkitűzési nincsenek megfeleltetve a COBIT 5 célkitűzéseihez.

7. Értékelés

A részletes megfeleltetés során látszott, hogy az „F”, mint felülmúlt lefedettségi kategória nem fordult elő, az Infotv. minden esetben legfeljebb olyan követelményt állított, mint a COBIT, de a teljes lefedettség is ritka. Látható, hogy a törvényi követelmények alapvetően a bizalmasság, sértetlenség és rendelkezésre állás információ-kritériumok köré csoportosulnak. Az Infotv. 7. §-ában deklarált általános követelmények igen sok kontrollnak megfeleltethetőek, kevésbé meghatározott módon. Ezért amelyik informatikai folyamatban a bizalmasság, sértetlenség vagy rendelkezésre állás COBIT Információ-kritériumok közül bármelyiket elsődlegesnek tekintjük, ott az Infotv. 10. § (1) bekezdését megfeleltetettnek tekintjük. Ezen eseteket ***-gal jelöltük. Minden egyéb megfeleltetés szakmai mérlegelés és egyeztetés útján alakult ki.

8. Hivatkozások

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

IT Governance Institute, COBIT 4.1, USA, 2007

IT Governance Institute: COBIT 4.1 Magyar változat, ISACA-Információrendszer Ellenőrök Egyesülete, Budapest, 2007

Jimmy Heschl: COBIT® Mapping, Mapping of ISO/IEC 17799:2005 With COBIT® 4.0

2. sz. függelék: Infotv.-COBIT visszakereső kulcs

A visszakereső kulcs az 1. sz. függelékben található COBIT-Infotv. megfeleltetéshez az ellenkező irányból, tehát az információs törvény teljes törvényszövegében a COBIT vonatkozó pontjaira történő hivatkozással segíti az alkalmazást. A hivatkozások lábjegyzetben kerültek feltüntetésre. Ahol a hivatkozás kifejezetten egy szóra vagy kifejezésre utal, ott a szó vagy kifejezés végén került feltüntetésre a lábjegyzet sorszáma, amíg a teljes bekezdésre vonatkozó hivatkozó hivatkozás esetén a bekezdés végén található a lábjegyzet jelölése.

2011. évi CXII. törvény

az információs önrendelkezési jogról és az információszabadságról[349]

Az Országgyűlés az információs önrendelkezési jog és az információszabadság biztosítása érdekében, a személyes adatok védelmét, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez való jog érvényesülését szolgáló alapvető szabályokról, valamint az ezen szabályok ellenőrzésére hivatott hatóságról az Alaptörvény végrehajtására, az Alaptörvény VI. cikke alapján a következő törvényt alkotja:

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. A törvény célja

1. § E törvény célja az adatok kezelésére vonatkozó alapvető szabályok meghatározása annak érdekében, hogy a természetes személyek magánszféráját az adatkezelők tiszteletben tartsák, valamint a közügyek átláthatósága a közérdekű és a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő jog érvényesítésével megvalósuljon.

2. A törvény hatálya

2. § (1) E törvény hatálya a Magyarország területén folytatott minden olyan adatkezelésre és adatfeldolgozásra kiterjed, amely természetes személy adataira, valamint közérdekű adatra vagy közérdekből nyilvános adatra vonatkozik.

(2) E törvényt a teljesen vagy részben automatizált eszközzel, valamint a manuális módon végzett adatkezelésre és adatfeldolgozásra egyaránt alkalmazni kell.

(3) E törvényben foglaltakat kell alkalmazni, ha az Európai Unió területén kívül személyes adatok kezelését folytató adatkezelő az adatfeldolgozással Magyarország területén székhellyel, telephellyel, fiókteleppel vagy lakóhellyel, tartózkodási hellyel rendelkező adatfeldolgozót bíz meg, vagy itt lévő eszközt használ fel, kivéve, ha ez az eszköz csak az Európai Unió területén átmenő adatforgalom célját szolgálja. Az ilyen adatkezelőnek Magyarország területén képviselőt kell kineveznie.

(4) Nem kell alkalmazni e törvény rendelkezéseit a természetes személynek a kizárólag saját személyes céljait szolgáló adatkezeléseire.

[349] hatályos 2018. 01. 01-től

(5) A közszféra információinak további felhasználására vonatkozóan törvény az adatszolgáltatás módjára és feltételeire, az azért fizetendő ellenértékre, valamint a jogorvoslatra vonatkozóan e törvénytől eltérő szabályokat állapíthat meg.

3. Értelmező rendelkezések

3. § E törvény alkalmazása során:[350]

1. *érintett:* bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy;

2. *személyes adat:* az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés;

3. *különleges adat:*

a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,

b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

4. *bűnügyi személyes adat:* a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;

5. *közérdekű adat:* az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

6. *közérdekből nyilvános adat:* a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;

7. *hozzájárulás:* az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adat – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez;

8. *tiltakozás:* az érintett nyilatkozata, amellyel személyes adatának kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri;

9. *adatkezelő:* az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

10. *adatkezelés:* az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása

[350] PO2.3

vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;

11. *adattovábbítás:* az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

12. *nyilvánosságra hozatal:* az adat bárki számára történő hozzáférhetővé tétele;

13. *adattörlés:* az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;

14. *adatmegjelölés:* az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;

15. *adatzárolás:* az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;

16. *adatmegsemmisítés:* az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;

17. *adatfeldolgozás:* az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adaton végzik;

18. *adatfeldolgozó:* az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi;

19. *adatfelelős:* az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;

20. *adatközlő:* az a közfeladatot ellátó szerv, amely – ha az adatfelelős nem maga teszi közzé az adatot – az adatfelelős által hozzá eljuttatott adatot honlapon közzéteszi;

21. *adatállomány:* az egy nyilvántartásban kezelt adatok összessége;

22. *harmadik személy:* olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval;

23. *EGT-állam:* az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez;

24. *harmadik ország:* minden olyan állam, amely nem EGT-állam.

25. *kötelező szervezeti szabályozás:* több országban, de köztük legalább egy EGT-államban is tevékenységet folytató adatkezelő vagy adatkezelők csoportja által elfogadott és a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) által jóváhagyott, az adatkezelőre vagy adatkezelők csoportjára nézve kötelező belső adatvédelmi szabályzat, amely a harmadik országba történő adattovábbítás esetén a személyes adatok védelmét az adatkezelő vagy adatkezelők csoportjának egyoldalú kötelezettségvállalása útján biztosítja;

26. *adatvédelmi incidens:* személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés.

II. FEJEZET

A SZEMÉLYES ADATOK VÉDELME

4. Az adatkezelés elvei

4. § (1)[351] Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie.

(2) Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

(3) A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.

(4)[352] Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és – ha az adatkezelés céljára tekintettel szükséges – naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.

(5) A személyes adatok kezelését tisztességesnek és törvényesnek kell tekinteni, ha az érintett véleménynyilvánítási szabadságának biztosítása érdekében az érintett véleményét megismerni kívánó személy az érintett lakóhelyén vagy tartózkodási helyén felkeresi, feltéve, hogy az érintett személyes adatait e törvény rendelkezéseinek megfelelően kezelik és a személyes megkeresés nem üzleti célra irányul. A személyes megkeresésre a munka törvénykönyve szerinti munkaszüneti napon nem kerülhet sor.

5. Az adatkezelés jogalapja

5. § (1) Személyes adat akkor kezelhető, ha

a) ahhoz az érintett hozzájárul, vagy

b) azt törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzat rendelete közérdeken alapuló célból elrendeli (a továbbiakban: kötelező adatkezelés).

(2) Különleges adat a 6. §-ban meghatározott esetekben, valamint akkor kezelhető, ha

a) az adatkezeléshez az érintett írásban hozzájárul,

b) a 3. § 3. pont *a)* alpontjában foglalt adatok esetében az törvényben kihirdetett nemzetközi szerződés végrehajtásához szükséges, vagy azt az Alaptörvényben biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűncselekmények megelőzése vagy üldözése érdekében vagy honvédelmi érdekből törvény elrendeli, vagy

c) a 3. § 3. pont *b)* alpontjában foglalt adatok esetében törvény közérdeken alapuló célból elrendeli.

(3) Kötelező adatkezelés esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg.

(4) Kizárólag állami vagy önkormányzati szerv kezelheti az állam bűncselekmények megelőzésére és üldözésére irányuló, valamint közigazgatási és igazságszolgáltatási feladatainak

[351] PC1
[352] DS11.1, AC1, AC2, AC3, AC4, AC5

ellátása céljából kezelt bűnügyi személyes adatokat, valamint a szabálysértési, a polgári peres és nemperes ügyekre vonatkozó adatokat tartalmazó nyilvántartásokat.

6. § (1) Személyes adat kezelhető akkor is, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése

a) az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy

b) az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.

(2) Ha az érintett cselekvőképtelensége folytán vagy más elháríthatatlan okból nem képes hozzájárulását megadni, akkor a saját vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges mértékben a hozzájárulás akadályainak fennállása alatt az érintett személyes adatai kezelhetőek.

(3) A 16. életévét betöltött kiskorú érintett hozzájárulását tartalmazó jognyilatkozatának érvényességéhez törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása nem szükséges.

(4) Ha a hozzájáruláson alapuló adatkezelés célja az adatkezelővel írásban kötött szerződés végrehajtása, a szerződésnek tartalmaznia kell minden olyan információt, amelyet a személyes adatok kezelése szempontjából – e törvény alapján – az érintettnek ismernie kell, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, a felhasználás célját, az adatok továbbításának tényét, címzettjeit, adatfeldolgozó igénybevételének tényét. A szerződésnek félreérthetetlen módon tartalmaznia kell, hogy az érintett aláírásával hozzájárul adatainak a szerződésben meghatározottak szerinti kezeléséhez.

(5) Ha a személyes adat felvételére az érintett hozzájárulásával került sor, az adatkezelő a felvett adatokat törvény eltérő rendelkezésének hiányában

a) a rá vonatkozó jogi kötelezettség teljesítése céljából, vagy

b) az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából, ha ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll

további külön hozzájárulás nélkül, valamint az érintett hozzájárulásának visszavonását követően is kezelheti.

(6) Az érintett kérelmére, kezdeményezésére indult bírósági vagy hatósági eljárásban az eljárás lefolytatásához szükséges személyes adatok tekintetében, az érintett kérelmére indult más ügyben az általa megadott személyes adatok tekintetében az érintett hozzájárulását vélelmezni kell.

(7) Az érintett hozzájárulását megadottnak kell tekinteni az érintett közszereplése során általa közölt vagy nyilvánosságra hozatalra általa átadott személyes adatok tekintetében.

(8) Kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg.

6. Az adatbiztonság követelménye

7. § (1)[353] Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az e törvény és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét.

(2)[354] Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és

[353] PO1.5

kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

(3)[355] Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

(4)[356] A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok – kivéve ha azt törvény lehetővé teszi – közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.

(5)[357] A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja

a) a jogosulatlan adatbevitel megakadályozását;

b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;

c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;

d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;

e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és

f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

(6)[358] Az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek.

7. Adattovábbítás külföldre

8. § (1) Személyes adatot e törvény hatálya alá tartozó adatkezelő vagy adatfeldolgozó harmadik országban adatkezelést folytató adatkezelő részére akkor továbbíthat, vagy harmadik országban adatfeldolgozást végző adatfeldolgozó részére akkor adhat át, ha

a) ahhoz az érintett kifejezetten hozzájárult, vagy

b) az adatkezelésnek az 5. §-ban, illetve a 6. §-ban előírt feltételei teljesülnek, és – a 6. § (2) bekezdésében foglalt esetet kivéve – a harmadik országban az átadott adatok kezelése, valamint feldolgozása során biztosított a személyes adatok megfelelő szintű védelme.

(2) A személyes adatok megfelelő szintű védelme akkor biztosított, ha

a) az Európai Unió kötelező jogi aktusa azt megállapítja,

---

[354] PO2.1, PO2.2, PO2.3, PO2.4, PO3.1, PO3.2, PO3.4, PO3.5, PO4.8, PO9.1, PO9.2, PO9.3, PO9.4, PO9.5, PO9.6, AI2.4, AI6.1, AI6.2, AI6.3, AI6.4, AI6.5, DS4.1, DS4.2, DS4.3, DS4.4, DS4.5, DS4.6, DS4.7, DS4.9, DS4.10, DS5.1, DS5.2, DS5.5, DS5.6, DS5.7, DS11.3, DS11.6, DS12.1, DS12.5, ME3.1, ME3.2
[355] AI7.5, DS4.8, DS5.3, DS5.4, DS5.8, DS5.9, DS5.10, DS5.11, DS11.2, DS11.4, DS11.5, DS12.2, DS12.3, DS12.4, AC6
[356] PO2.2
[357] DS4.2, DS8.2, AC1, AC2, AC3, AC4, AC5, AC6
[358] PO9.1

b) a harmadik ország és Magyarország között az érintetteknek a 14. §-ban foglalt jogai érvényesítésére, a jogorvoslati jog biztosítására, valamint az adatkezelés, illetve az adatfeldolgozás független ellenőrzésére vonatkozó garanciális szabályokat tartalmazó nemzetközi szerződés van hatályban, vagy

c) az adatkezelés, illetve az adatfeldolgozás kötelező szervezeti szabályozásnak megfelelően történik.

(3) Személyes adatok a nemzetközi jogsegélyről, az adóügyi információcseréről, valamint a kettős adóztatás elkerüléséről szóló nemzetközi szerződés végrehajtása érdekében, a nemzetközi szerződésben meghatározott célból, feltételekkel és adatkörben – a (2) bekezdésben meghatározott feltételek hiányában is – továbbíthatók harmadik országba.

(4) Az EGT-államba irányuló adattovábbítást úgy kell tekinteni, mintha Magyarország területén belüli adattovábbításra kerülne sor.

8. Az adatkezelés korlátai

9. § (1) Ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusának rendelkezése alapján az adatkezelő személyes adatot akként vesz át, hogy az adattovábbító adatkezelő az adattovábbítással egyidejűleg jelzi a személyes adat

a) kezelésének lehetséges célját,

b) kezelésének lehetséges időtartamát,

c) továbbításának lehetséges címzettjeit,

d) érintettje e törvényben biztosított jogainak korlátozását, vagy

e) kezelésének egyéb korlátozását

(a továbbiakban együtt: adatkezelési korlátozás), a személyes adatokat átvevő adatkezelő (a továbbiakban: adatátvevő) a személyes adatot az adatkezelési korlátozásnak megfelelő terjedelemben és módon kezeli, az érintett jogait az adatkezelési korlátozásnak megfelelően biztosítja.

(2) Az adatátvevő az adatkezelési korlátozásra tekintet nélkül is kezelheti a személyes adatot és biztosíthatja az érintett jogait, ha ahhoz az adattovábbító adatkezelő előzetes hozzájárulását adta.

(3) Törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusának rendelkezése alapján az adatkezelő a személyes adat továbbításával egyidejűleg a címzettet tájékoztatja az alkalmazandó adatkezelési korlátozásról.

(4) A (2) bekezdésben meghatározott hozzájárulást az adatkezelő akkor adhatja meg, ha az nem ütközik a Magyarország joghatósága alatt álló jogalanyok tekintetében alkalmazandó jogi rendelkezésbe.

(5) Az adattovábbító adatkezelőt – kérelmére – az adatátvevő tájékoztatja az átvett személyes adatok felhasználásáról.

9. Adatfeldolgozás

10. § (1)[359] Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit e törvény, valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. Az általa adott utasítások jogszerűségéért az adatkezelő felel.

(2) Az adatfeldolgozó az adatkezelő rendelkezése szerint vehet igénybe további adatfeldolgozót.

[359] PO4.9, DS10.2, DS13.1, ME1.2, PC2, PC4, PC5

(3)[360] Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni.

(4)[361] Az adatfeldolgozásra vonatkozó szerződést írásba kell foglalni. Az adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt.

10. Automatizált adatfeldolgozással hozott döntés

11. § (1)[362] Kizárólag automatizált adatfeldolgozással az érintett személyes jellemzőinek értékelésén alapuló döntés meghozatalára csak akkor kerülhet sor, ha a döntést

a) valamely szerződés megkötése vagy teljesítése során hozták, feltéve hogy azt az érintett kezdeményezte, vagy

b) olyan törvény teszi lehetővé, amely az érintett jogos érdekeit biztosító intézkedéseket is megállapítja.

(2) Az automatizált adatfeldolgozással hozott döntés esetén az érintettet – kérelmére – tájékoztatni kell az alkalmazott módszerről és annak lényegéről, valamint az érintettnek álláspontja kifejtésére lehetőséget kell biztosítani.

11. Személyes adatok kezelése tudományos kutatás során

12. § (1) Tudományos kutatás céljára felvett személyes adat csak tudományos kutatás céljára használható fel.

(2)[363] A személyes adat érintettel való kapcsolatának megállapítását – mihelyt a kutatási cél megengedi – véglegesen lehetetlenné kell tenni. Ennek megtörténtéig is külön kell tárolni azokat az adatokat, amelyek meghatározott vagy meghatározható természetes személy azonosítására alkalmasak. Ezek az adatok egyéb adatokkal csak akkor kapcsolhatók össze, ha az a kutatás céljára szükséges.

(3) A tudományos kutatást végző szerv vagy személy személyes adatot csak akkor hozhat nyilvánosságra, ha

a) az érintett ahhoz hozzájárult, vagy

b) az a történelmi eseményekről folytatott kutatások eredményeinek bemutatásához szükséges.

12. Személyes adatok felhasználása statisztikai célra

13. § (1) A kötelező adatkezelés keretében kezelt személyes adatokat – ha törvény eltérően nem rendelkezik – a Központi Statisztikai Hivatal statisztikai célból egyedi azonosításra alkalmas módon átveheti és törvényben meghatározottak szerint kezelheti.

(2) A statisztikai célra felvett, átvett vagy feldolgozott személyes adatok – ha törvény eltérően nem rendelkezik – csak statisztikai célra kezelhetők. A személyes adatok statisztikai célra történő kezelésének részletes szabályait külön törvény határozza meg.

[360] PO4.11
[361] PO4.14, DS1.3
[362] AI1.1, ME3.1
[363] DS8.1

13. Az érintettek jogai és érvényesítésük

14. §[364] Az érintett kérelmezheti az adatkezelőnél

a) tájékoztatását személyes adatai kezeléséről,

b) személyes adatainak helyesbítését, valamint

c) személyes adatainak – a kötelező adatkezelés kivételével – törlését vagy zárolását.

15. § (1)[365] Az érintett kérelmére az adatkezelő tájékoztatást ad az érintett általa kezelt, illetve az általa vagy rendelkezése szerint megbízott adatfeldolgozó által feldolgozott adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá – az érintett személyes adatainak továbbítása esetén – az adattovábbítás jogalapjáról és címzettjéről.

(1a) Az adatkezelő – ha belső adatvédelmi felelőssel rendelkezik, a belső adatvédelmi felelős útján – az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

(1b) Az elektronikus hírközlésről szóló törvény hatálya alá tartozó adatkezelő az (1a) bekezdésben meghatározott kötelezettségét az elektronikus hírközlésről szóló törvényben meghatározott, a személyes adatok megsértésének eseteit tartalmazó nyilvántartás vezetésével is teljesítheti.

(2) Az adatkezelő az adattovábbítás jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából adattovábbítási nyilvántartást vezet, amely tartalmazza az általa kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

(3) Az (1a) és a (2) bekezdés szerinti adatok nyilvántartásban való megőrzésére irányuló – és ennek alapján a tájékoztatási – kötelezettség időtartamát az adatkezelést előíró jogszabály korlátozhatja. E korlátozás körében személyes adatok esetében öt évnél, különleges adatok esetében pedig húsz évnél rövidebb időtartam nem állapítható meg.

(4) [366] Az adatkezelő köteles a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 25 napon belül, közérthető formában, az érintett erre irányuló kérelmére írásban megadni a tájékoztatást.

(5) A (4) bekezdésben foglalt tájékoztatás ingyenes, ha a tájékoztatást kérő a folyó évben azonos adatkörre vonatkozóan tájékoztatási kérelmet az adatkezelőhöz még nem nyújtott be. Egyéb esetekben költségtérítés állapítható meg. A költségtérítés mértékét a felek között létrejött szerződés is rögzítheti. A már megfizetett költségtérítést vissza kell téríteni, ha az adatokat jogellenesen kezelték, vagy a tájékoztatás kérése helyesbítéshez vezetett.

16. § (1)[367] Az érintett tájékoztatását az adatkezelő csak a 9. § (1) bekezdésében, valamint a 19. §-ban meghatározott esetekben tagadhatja meg.

(2) A tájékoztatás megtagadása esetén az adatkezelő írásban közli az érintettel, hogy a felvilágosítás megtagadására e törvény mely rendelkezése alapján került sor. A felvilágosítás

[364] DS8.1
[365] DS8.1
[366] DS8.2
[367] DS8.4

megtagadása esetén az adatkezelő tájékoztatja az érintettet a bírósági jogorvoslat, továbbá a Hatósághoz fordulás lehetőségéről.

(3) [368] Az elutasított kérelmekről az adatkezelő a Hatóságot évente a tárgyévet követő év január 31-éig értesíti.

17. § (1) [369] Ha a személyes adat a valóságnak nem felel meg, és a valóságnak megfelelő személyes adat az adatkezelő rendelkezésére áll, a személyes adatot az adatkezelő helyesbíti.

(2) [370] A személyes adatot törölni kell, ha

a) kezelése jogellenes;

b) az érintett – a 14. § *c)* pontjában foglaltak szerint – kéri;

c) az hiányos vagy téves – és ez az állapot jogszerűen nem orvosolható –, feltéve, hogy a törlést törvény nem zárja ki;

d) az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben meghatározott határideje lejárt;

e) azt a bíróság vagy a Hatóság elrendelte.

(3) A (2) bekezdés *d)* pontjában meghatározott esetben a törlési kötelezettség nem vonatkozik azon személyes adatra, amelynek adathordozóját a levéltári anyag védelmére vonatkozó jogszabály értelmében levéltári őrizetbe kell adni.

(4) Törlés helyett az adatkezelő zárolja a személyes adatot, ha az érintett ezt kéri, vagy ha a rendelkezésére álló információk alapján feltételezhető, hogy a törlés sértené az érintett jogos érdekeit. Az így zárolt személyes adat kizárólag addig kezelhető, ameddig fennáll az az adatkezelési cél, amely a személyes adat törlését kizárta.

(5) Az adatkezelő megjelöli az általa kezelt személyes adatot, ha az érintett vitatja annak helyességét vagy pontosságát, de a vitatott személyes adat helytelensége vagy pontatlansága nem állapítható meg egyértelműen.

18. § (1) [371] A helyesbítésről, a zárolásról, a megjelölésről és a törlésről az érintettet, továbbá mindazokat értesíteni kell, akiknek korábban az adatot adatkezelés céljára továbbították. Az értesítés mellőzhető, ha ez az adatkezelés céljára való tekintettel az érintett jogos érdekét nem sérti.

(2) Ha az adatkezelő az érintett helyesbítés, zárolás vagy törlés iránti kérelmét nem teljesíti, a kérelem kézhezvételét követő 25 napon belül írásban vagy az érintett hozzájárulásával elektronikus úton közli a helyesbítés, zárolás vagy törlés iránti kérelem elutasításának ténybeli és jogi indokait. A helyesbítés, törlés vagy zárolás iránti kérelem elutasítása esetén az adatkezelő tájékoztatja az érintettet a bírósági jogorvoslat, továbbá a Hatósághoz fordulás lehetőségéről.

19. § Az érintettnek a 14–18. §-ban meghatározott jogait törvény korlátozhatja az állam külső és belső biztonsága, így a honvédelem, a nemzetbiztonság, a bűncselekmények megelőzése vagy üldözése, a büntetés-végrehajtás biztonsága érdekében, továbbá állami vagy önkormányzati gazdasági vagy pénzügyi érdekből, az Európai Unió jelentős gazdasági vagy pénzügyi érdekéből, valamint a foglalkozások gyakorlásával összefüggő fegyelmi és etikai vétségek, a munkajogi és munkavédelmi kötelezettségszegések megelőzése és feltárása céljából – beleértve minden esetben az ellenőrzést és a felügyeletet is –, továbbá az érintett vagy mások jogainak védelme érdekében.

14. Az érintett előzetes tájékoztatásának követelménye

[368] DS8.5
[369] DS11.2
[370] DS11.2
[371] DS8.4

20. § (1) Az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés hozzájáruláson alapul vagy kötelező.

(2) Az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az érintett személyes adatait az adatkezelő a 6. § (5) bekezdése alapján kezeli, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

(3) Kötelező adatkezelés esetén a tájékoztatás megtörténhet a (2) bekezdés szerinti információkat tartalmazó jogszabályi rendelkezésekre való utalás nyilvánosságra hozatalával is.

(4) Ha az érintettek személyes tájékoztatása lehetetlen vagy aránytalan költséggel járna, a tájékoztatás megtörténhet az alábbi információk nyilvánosságra hozatalával is:

a) az adatgyűjtés ténye,

b) az érintettek köre,

c) az adatgyűjtés célja,

d) az adatkezelés időtartama,

e) az adatok megismerésére jogosult lehetséges adatkezelők személye,

f) az érintettek adatkezeléssel kapcsolatos jogainak és jogorvoslati lehetőségeinek ismertetése, valamint

g) ha az adatkezelés adatvédelmi nyilvántartásba vételének van helye, az adatkezelés nyilvántartási száma, kivéve a 68. § (2) bekezdésében foglalt esetet.

15. Tiltakozás személyes adat kezelése ellen

21. § (1) Az érintett tiltakozhat személyes adatának kezelése ellen,

a) ha a személyes adatok kezelése vagy továbbítása kizárólag az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez vagy az adatkezelő, adatátvevő vagy harmadik személy jogos érdekének érvényesítéséhez szükséges, kivéve kötelező adatkezelés esetén;

b) ha a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik; valamint

c) törvényben meghatározott egyéb esetben.

(2) Az adatkezelő a tiltakozást a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb 15 napon belül megvizsgálja, annak megalapozottsága kérdésében döntést hoz, és döntéséről a kérelmezőt írásban tájékoztatja.

(3) Ha az adatkezelő az érintett tiltakozásának megalapozottságát megállapítja, az adatkezelést – beleértve a további adatfelvételt és adattovábbítást is – megszünteti, és az adatokat zárolja, valamint a tiltakozásról, továbbá az annak alapján tett intézkedésekről értesíti mindazokat, akik részére a tiltakozással érintett személyes adatot korábban továbbította, és akik kötelesek intézkedni a tiltakozási jog érvényesítése érdekében.

(4) Ha az érintett az adatkezelőnek a (2) bekezdés alapján meghozott döntésével nem ért egyet, illetve ha az adatkezelő a (2) bekezdés szerinti határidőt elmulasztja, az érintett – a döntés közlésétől, illetve a határidő utolsó napjától számított 30 napon belül – a 22. §-ban meghatározott módon bírósághoz fordulhat.

(5) Ha az adatátvevő jogának érvényesítéséhez szükséges adatokat az érintett tiltakozása miatt nem kapja meg, a (3) bekezdés alapján történő értesítés közlésétől számított 15 napon belül, az adatokhoz való hozzájutás érdekében – a 22. §-ban meghatározott módon – bírósághoz fordulhat az adatkezelő ellen. Az adatkezelő az érintettet is perbe hívhatja.

(6) Ha az adatkezelő a (3) bekezdés szerinti értesítést elmulasztja, az adatátvevő felvilágosítást kérhet az adatátadás meghiúsulásával kapcsolatos körülményekről az adatkezelőtől, amely felvilágosítást az adatkezelő az adatátvevő erre irányuló kérelmének kézbesítését követő 8 napon belül köteles megadni. Felvilágosítás kérése esetén az adatátvevő a felvilágosítás megadásától, de legkésőbb az arra nyitva álló határidőtől számított 15 napon belül fordulhat bírósághoz az adatkezelő ellen. Az adatkezelő az érintettet is perbe hívhatja.

(7) Az adatkezelő az érintett adatát nem törölheti, ha az adatkezelést törvény rendelte el. Az adat azonban nem továbbítható az adatátvevő részére, ha az adatkezelő egyetértett a tiltakozással, vagy a bíróság a tiltakozás jogosságát megállapította.

16. Bírósági jogérvényesítés

22. § (1) Az érintett a jogainak megsértése esetén, valamint a 21. §-ban meghatározott esetekben az adatátvevő az adatkezelő ellen bírósághoz fordulhat. A bíróság az ügyben soron kívül jár el.

(2) Azt, hogy az adatkezelés a jogszabályban foglaltaknak megfelel, az adatkezelő köteles bizonyítani. A 21. § (5) és (6) bekezdése szerinti esetben a részére történő adattovábbítás jogszerűségét az adatátvevő köteles bizonyítani.

(3) A pert az érintett – választása szerint – a lakóhelye vagy tartózkodási helye szerint illetékes törvényszék előtt is megindíthatja.

(4) A perben fél lehet az is, akinek egyébként nincs perbeli jogképessége. A perbe a Hatóság az érintett pernyertessége érdekében beavatkozhat.

(5) Ha a bíróság a kérelemnek helyt ad, az adatkezelőt a tájékoztatás megadására, az adat helyesbítésére, zárolására, törlésére, az automatizált adatfeldolgozással hozott döntés megsemmisítésére, az érintett tiltakozási jogának figyelembevételére, illetve a 21. §-ban meghatározott adatátvevő által kért adat kiadására kötelezi.

(6) Ha a bíróság a 21. §-ban meghatározott esetekben az adatátvevő kérelmét elutasítja, az adatkezelő köteles az érintett személyes adatát az ítélet közlésétől számított 3 napon belül törölni. Az adatkezelő köteles az adatokat akkor is törölni, ha az adatátvevő a 21. § (5), illetve (6) bekezdésében meghatározott határidőn belül nem fordul bírósághoz.

(7) A bíróság elrendelheti ítéletének – az adatkezelő azonosító adatainak közzétételével történő – nyilvánosságra hozatalát, ha azt az adatvédelem érdekei és nagyobb számú érintett e törvényben védett jogai megkövetelik.

17. Kártérítés és sérelemdíj

23. § (1) Ha az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak kárt okoz, köteles azt megtéríteni.

(2) Ha az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével az érintett személyiségi jogát megsérti, az érintett az adatkezelőtől sérelemdíjat követelhet.

(3) Az érintettel szemben az adatkezelő felel az adatfeldolgozó által okozott kárért és az adatkezelő köteles megfizetni az érintettnek az adatfeldolgozó által okozott személyiségi jogsértés esetén járó sérelemdíjat is. Az adatkezelő mentesül az okozott kárért való felelősség és a sérelemdíj

megfizetésének kötelezettsége alól, ha bizonyítja, hogy a kárt vagy az érintett személyiségi jogának sérelmét az adatkezelés körén kívül eső elháríthatatlan ok idézte elő.

(4) Nem kell megtéríteni a kárt és nem követelhető a sérelemdíj annyiban, amennyiben a kár a károsult vagy a személyiségi jog megsértésével okozott jogsérelem az érintett szándékos vagy súlyosan gondatlan magatartásából származott.

18. Belső adatvédelmi felelős és adatvédelmi szabályzat

24. § (1)[372] Az adatkezelő, illetve az adatfeldolgozó szervezetén belül, közvetlenül a szerv vezetőjének felügyelete alá tartozó – jogi, közigazgatási, informatikai vagy ezeknek megfelelő, felsőfokú végzettséggel rendelkező – belső adatvédelmi felelőst kell kinevezni vagy megbízni

a) az országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelő, illetve feldolgozó adatkezelőnél és adatfeldolgozónál;

b) a pénzügyi szervezetnél;

c) az elektronikus hírközlési és közüzemi szolgáltatónál.

(2) [373] A belső adatvédelmi felelős

a) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;

b) ellenőrzi e törvény és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását;

c) kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;

d) elkészíti a belső adatvédelmi és adatbiztonsági szabályzatot;

e) vezeti a belső adatvédelmi nyilvántartást;

f) gondoskodik az adatvédelmi ismeretek oktatásáról.

(3) Az (1) bekezdésben meghatározott adatkezelőknek, valamint – az adatvédelmi nyilvántartásba bejelentési kötelezettség alá nem eső adatkezelők kivételével – egyéb állami és önkormányzati adatkezelőknek e törvény végrehajtása érdekében adatvédelmi és adatbiztonsági szabályzatot kell készíteniük.

19. A belső adatvédelmi felelősök konferenciája

25. § (1) A belső adatvédelmi felelősök konferenciája (a továbbiakban: konferencia) a Hatóság és a belső adatvédelmi felelősök rendszeres szakmai kapcsolattartását szolgálja, célja a személyes adatok védelmére és a közérdekű adatok megismerésére vonatkozó jogszabályok alkalmazása során az egységes joggyakorlat kialakítása.

(2) A konferenciát a Hatóság elnöke szükség szerint, de évente legalább egyszer hívja össze, és meghatározza napirendjét.

(3) A konferencia tagja minden olyan adatkezelő vagy adatfeldolgozó belső adatvédelmi felelőse, amelynél a felelős kinevezése törvény alapján kötelező.

[372] PO4.6, PO4.9
[373] PO4.8, PO4.10, PO6.4, PO7.4

(4) A konferencia tagjai lehetnek azon adatkezelők és adatfeldolgozók belső adatvédelmi felelősei, amelyek esetében a kinevezés nem kötelező. E célból a Hatóság által vezetett belső adatvédelmi felelősi nyilvántartásba bejelentkezhetnek.

(5) A Hatóság a kapcsolattartás céljából belső adatvédelmi felelősi nyilvántartást vezet a konferencia tagjairól. A nyilvántartás tartalmazza a belső adatvédelmi felelős nevét, postai és elektronikus levélcímét, továbbá a képviselt adatkezelő vagy adatfeldolgozó megnevezését.

(6) A nyilvántartásban a Hatóság az (5) bekezdés szerinti adatokat a belső adatvédelmi felelős e megbízatásának megszűnéséről való tudomásszerzéséig tartja nyilván.

III. FEJEZET

A KÖZÉRDEKŰ ADATOK MEGISMERÉSE

20. A közérdekű adatok megismerésének általános szabályai

26. § (1) Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szervnek vagy személynek (a továbbiakban együtt: közfeladatot ellátó szerv) lehetővé kell tennie, hogy a kezelésében lévő közérdekű adatot és közérdekből nyilvános adatot – az e törvényben meghatározott kivételekkel – erre irányuló igény alapján bárki megismerhesse.

(2) Közérdekből nyilvános adat a közfeladatot ellátó szerv feladat- és hatáskörében eljáró személy neve, feladatköre, munkaköre, vezetői megbízása, a közfeladat ellátásával összefüggő egyéb személyes adata, valamint azok a személyes adatai, amelyek megismerhetőségét törvény előírja. A közérdekből nyilvános személyes adatok a célhoz kötött adatkezelés elvének tiszteletben tartásával terjeszthetőek. A közérdekből nyilvános személyes adatok honlapon történő közzétételére az 1. melléklet és a közfeladatot ellátó személy jogállására vonatkozó külön törvény rendelkezései irányadóak.

(3) Ha törvény másként nem rendelkezik, közérdekből nyilvános adat a jogszabály vagy állami, illetőleg helyi önkormányzati szervvel kötött szerződés alapján kötelezően igénybe veendő vagy más módon ki nem elégíthető szolgáltatást nyújtó szervek vagy személyek kezelésében lévő, e tevékenységükre vonatkozó, személyes adatnak nem minősülő adat.

(4) A (3) bekezdésben meghatározott szerv vagy személy a (3) bekezdésben meghatározott adatok megismerésére irányuló igény teljesítése során a 28–31. § szerint jár el.

27. § (1) A közérdekű vagy közérdekből nyilvános adat nem ismerhető meg, ha az a minősített adat védelméről szóló törvény szerinti minősített adat.

(2) A közérdekű és közérdekből nyilvános adatok megismeréséhez való jogot – az adatfajták meghatározásával – törvény

a) honvédelmi érdekből;

b) nemzetbiztonsági érdekből;

c) bűncselekmények üldözése vagy megelőzése érdekében;

d) környezet- vagy természetvédelmi érdekből;

e) központi pénzügyi vagy devizapolitikai érdekből;

f) külügyi kapcsolatokra, nemzetközi szervezetekkel való kapcsolatokra tekintettel;

g) bírósági vagy közigazgatási hatósági eljárásra tekintettel;

h) a szellemi tulajdonhoz fűződő jogra tekintettel

korlátozhatja.

(3) Közérdekből nyilvános adatként nem minősül üzleti titoknak a központi és a helyi önkormányzati költségvetés, illetve az európai uniós támogatás felhasználásával, költségvetést érintő juttatással, kedvezménnyel, az állami és önkormányzati vagyon kezelésével, birtoklásával, használatával, hasznosításával, az azzal való rendelkezéssel, annak megterhelésével, az ilyen vagyont érintő bármilyen jog megszerzésével kapcsolatos adat, valamint az az adat, amelynek megismerését vagy nyilvánosságra hozatalát külön törvény közérdekből elrendeli. A nyilvánosságra hozatal azonban nem eredményezheti az olyan adatokhoz – így különösen a védett ismerethez – való hozzáférést, amelyek megismerése az üzleti tevékenység végzése szempontjából aránytalan sérelmet okozna, feltéve hogy ez nem akadályozza meg a közérdekből nyilvános adat megismerésének lehetőségét.

(3a) Az a természetes személy, jogi személy vagy jogi személyiséggel nem rendelkező szervezet, aki vagy amely az államháztartás alrendszerébe tartozó valamely személlyel pénzügyi vagy üzleti kapcsolatot létesít, köteles e jogviszonnyal összefüggő és a (3) bekezdés alapján közérdekből nyilvános adatra vonatkozóan – erre irányuló igény esetén – bárki számára tájékoztatást adni. A tájékoztatási kötelezettség a közérdekből nyilvános adatok nyilvánosságra hozatalával vagy a korábban már elektronikus formában nyilvánosságra hozott adatot tartalmazó nyilvános forrás megjelölésével is teljesíthető.

(3b) Ha a (3a) bekezdés alapján tájékoztatásra kötelezett a tájékoztatást megtagadja, a tájékoztatást igénylő a tájékoztatásra kötelezett felett törvényességi felügyelet gyakorlására jogosult szerv eljárását kezdeményezheti.

(4) A közérdekű adatok megismerése korlátozható uniós jogi aktus alapján az Európai Unió jelentős pénzügy- vagy gazdaságpolitikai érdekére tekintettel, beleértve a monetáris, a költségvetési és az adópolitikai érdeket is.

(5) A közfeladatot ellátó szerv feladat- és hatáskörébe tartozó döntés meghozatalára irányuló eljárás során készített vagy rögzített, a döntés megalapozását szolgáló adat a keletkezésétől számított tíz évig nem nyilvános. Ezen adatok megismerését – az adat megismeréséhez és a megismerhetőség kizárásához fűződő közérdek súlyának mérlegelésével – az azt kezelő szerv vezetője engedélyezheti.

(6) A döntés megalapozását szolgáló adat megismerésére irányuló igény – az (5) bekezdésben meghatározott időtartamon belül – a döntés meghozatalát követően akkor utasítható el, ha az adat további jövőbeli döntés megalapozását is szolgálja, vagy az adat megismerése a közfeladatot ellátó szerv törvényes működési rendjét vagy feladat- és hatáskörének illetéktelen külső befolyástól mentes ellátását, így különösen az adatot keletkeztető álláspontjának a döntések előkészítése során történő szabad kifejtését veszélyeztetné.

(7) Jogszabály a döntés megalapozását szolgáló egyes adatok megismerhetőségének korlátozására az (5) bekezdésben meghatározottnál rövidebb időtartamot állapíthat meg.

(8) E fejezet rendelkezései nem alkalmazhatók a közhitelű nyilvántartásból történő – külön törvényben szabályozott – adatszolgáltatásra.

21. A közérdekű adat megismerése iránti igény

28. § (1) A közérdekű adat megismerése iránt szóban, írásban vagy elektronikus úton bárki igényt nyújthat be. A közérdekből nyilvános adatok megismerésére a közérdekű adatok megismerésére vonatkozó rendelkezéseket kell alkalmazni.

(2) Ha törvény másként nem rendelkezik, az adatigénylő személyes adatai csak annyiban kezelhetők, amennyiben az az igény teljesítéséhez, az igénynek a 29. § (1a) bekezdésében meghatározott szempont alapján való vizsgálatához, illetve az igény teljesítéséért megállapított költségtérítés megfizetéséhez szükséges. A 29. § (1a) bekezdésében meghatározott idő elteltét, illetve a költségek megfizetését követően az igénylő személyes adatait haladéktalanul törölni kell.

(3) Ha az adatigénylés nem egyértelmű, az adatkezelő felhívja az igénylőt az igény pontosítására.

29. § (1) A közérdekű adat megismerésére irányuló igénynek az adatot kezelő közfeladatot ellátó szerv az igény beérkezését követő legrövidebb idő alatt, legfeljebb azonban 15 napon belül tesz eleget.

(1a) Az adatigénylésnek az adatot kezelő közfeladatot ellátó szerv nem köteles eleget tenni abban a részben, amelyben az azonos igénylő által egy éven belül benyújtott, azonos adatkörre irányuló adatigényléssel megegyezik, feltéve, hogy az azonos adatkörbe tartozó adatokban változás nem állt be.

(1b) Az adatigénylésnek az adatot kezelő közfeladatot ellátó szerv nem köteles eleget tenni, ha az igénylő nem adja meg nevét, nem természetes személy igénylő esetén megnevezését, valamint azt az elérhetőséget, amelyen számára az adatigényléssel kapcsolatos bármely tájékoztatás és értesítés megadható.

(2) Ha az adatigénylés jelentős terjedelmű, illetve nagyszámú adatra vonatkozik, vagy az adatigénylés teljesítése a közfeladatot ellátó szerv alaptevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével jár, az (1) bekezdésben meghatározott határidő egy alkalommal 15 nappal meghosszabbítható. Erről az igénylőt az igény beérkezését követő 15 napon belül tájékoztatni kell.

(2a) Ha az igénylés olyan adatra vonatkozik, amelyet az Európai Unió valamely intézménye vagy tagállama állított elő, az adatkezelő haladéktalanul megkeresi az Európai Unió érintett intézményét vagy tagállamát és erről az igénylőt tájékoztatja. A tájékoztatás megtételétől az Európai Unió érintett intézménye vagy tagállama válaszának az adatkezelőhöz való beérkezéséig terjedő időtartam az adatigénylés teljesítésére rendelkezésre álló határidőbe nem számít bele.

(3) Az adatokat tartalmazó dokumentumról vagy dokumentumrészről, annak tárolási módjától függetlenül az igénylő másolatot kaphat. Az adatot kezelő közfeladatot ellátó szerv az adatigénylés teljesítéséért – az azzal kapcsolatban felmerült költség mértékéig terjedően – költségtérítést állapíthat meg, amelynek összegéről az igénylőt az igény teljesítését megelőzően tájékoztatni kell.

(3a) Az igénylő a (3) bekezdés alapján kapott tájékoztatás kézhezvételét követő 30 napon belül nyilatkozik arról, hogy az igénylését fenntartja-e. A tájékoztatás megtételétől az igénylő nyilatkozatának az adatkezelőhöz való beérkezéséig terjedő időtartam az adatigénylés teljesítésére rendelkezésre álló határidőbe nem számít bele. Ha az igénylő az igényét fenntartja, a költségtérítést az adatkezelő által megállapított, legalább 15 napos határidőben köteles az adatkezelő részére megfizetni.

(4) Ha az adatigénylés teljesítése a közfeladatot ellátó szerv alaptevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével jár, vagy az a dokumentum vagy dokumentumrész, amelyről az igénylő másolatot igényelt, jelentős terjedelmű, illetve a költségtérítés mértéke meghaladja a kormányrendeletben meghatározott összeget, az adatigénylést a költségtérítésnek az igénylő általi megfizetését követő 15 napon belül kell teljesíteni. Arról, hogy az adatigénylés teljesítése a közfeladatot ellátó szerv alaptevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével jár, illetve a másolatként igényelt dokumentum vagy dokumentumrész jelentős terjedelmű, továbbá a költségtérítés mértékéről, valamint az adatigénylés teljesítésének a másolatkészítést nem igénylő lehetőségeiről az igénylőt az igény beérkezését követő 15 napon belül tájékoztatni kell.

(5) A költségtérítés mértékének meghatározása során az alábbi költségelemek vehetők figyelembe:

a) az igényelt adatokat tartalmazó adathordozó költsége,

b) az igényelt adatokat tartalmazó adathordozó az igénylő részére történő kézbesítésének költsége, valamint

c) ha az adatigénylés teljesítése a közfeladatot ellátó szerv alaptevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével jár, az adatigénylés teljesítésével összefüggő munkaerő-ráfordítás költsége.

(6) Az (5) bekezdésben meghatározott költségelemek megállapítható mértékét jogszabály határozza meg.

30. § (1) Ha a közérdekű adatot tartalmazó dokumentum az igénylő által meg nem ismerhető adatot is tartalmaz, a másolaton a meg nem ismerhető adatot felismerhetetlenné kell tenni.

(2) Az adatigénylésnek közérthető formában és – amennyiben ezt az adatot kezelő közfeladatot ellátó szerv aránytalan nehézség nélkül teljesíteni képes – az igénylő által kívánt formában, illetve módon kell eleget tenni. Ha a kért adatot korábban már elektronikus formában nyilvánosságra hozták, az igény teljesíthető az adatot tartalmazó nyilvános forrás megjelölésével is. Az adatigénylést nem lehet elutasítani arra való hivatkozással, hogy annak közérthető formában nem lehet eleget tenni.

(3) Az igény teljesítésének megtagadásáról, annak indokaival, valamint az igénylőt e törvény alapján megillető jogorvoslati lehetőségekről való tájékoztatással együtt, az igény beérkezését követő 15 napon belül írásban vagy – ha az igényben elektronikus levelezési címét közölte – elektronikus levélben értesíteni kell az igénylőt. Az elutasított kérelmekről, valamint az elutasítások indokairól az adatkezelő nyilvántartást vezet, és az abban foglaltakról minden évben január 31-éig tájékoztatja a Hatóságot.

(4) A közérdekű adat megismerése iránti igény teljesítése nem tagadható meg azért, mert a nem magyar anyanyelvű igénylő az igényét anyanyelvén vagy az általa értett más nyelven fogalmazza meg.

(5) Ha a közérdekű adat megismerése iránti igény teljesítésének megtagadása tekintetében törvény az adatkezelő mérlegelését teszi lehetővé, a megtagadás alapját szűken kell értelmezni, és a közérdekű adat megismerésére irányuló igény teljesítése kizárólag abban az esetben tagadható meg, ha a megtagadás alapjául szolgáló közérdek nagyobb súlyú a közérdekű adat megismerésére irányuló igény teljesítéséhez fűződő közérdeknél.

(6) A közfeladatot ellátó szervnek a közérdekű adatok megismerésére irányuló igények teljesítésének rendjét rögzítő szabályzatot kell készítenie.

(7) A közfeladatot ellátó szerv gazdálkodásának átfogó, számlaszintű, illetve tételes ellenőrzésére irányuló adatmegismerésekre külön törvények rendelkezései irányadók. Erre való hivatkozással az adatkezelő az adatigénylést az igénylés tárgyát képező irat másolata helyett a jogviszony alanyainak, a jogviszony típusának, a jogviszony tárgyának, a szolgáltatás és ellenszolgáltatás mértékének és teljesítése időpontjának megjelölésével is teljesítheti.

31. § (1) Az igénylő a közérdekű adat megismerésére vonatkozó igény elutasítása vagy a teljesítésre nyitva álló, vagy az adatkezelő által a 29. § (2) bekezdése szerint meghosszabbított határidő eredménytelen eltelte esetén, valamint az adatigénylés teljesítéséért megállapított költségtérítés összegének felülvizsgálata érdekében bírósághoz fordulhat.

(2) A megtagadás jogszerűségét és a megtagadás indokait, illetve az adatigénylés teljesítéséért megállapított költségtérítés összegének megalapozottságát az adatkezelőnek kell bizonyítania.

(3) A pert az igény elutasításának közlésétől, a határidő eredménytelen elteltétől, illetve a költségtérítés megfizetésére vonatkozó határidő lejártától számított harminc napon belül kell megindítani az igényt elutasító közfeladatot ellátó szerv ellen. Ha az igény elutasítása, nem teljesítése vagy az adatigénylés teljesítéséért megállapított költségtérítés összege miatt az igénylő a Hatóság vizsgálatának kezdeményezése érdekében a Hatóságnál bejelentést tesz, a pert a bejelentés érdemi vizsgálatának elutasításáról, a vizsgálat megszüntetéséről, az 55. § (1) bekezdés *b)* pontja szerinti lezárásáról szóló vagy az 58. § (3) bekezdése szerinti értesítés kézhezvételét követő harminc napon belül lehet megindítani. A perindításra rendelkezésre álló határidő elmulasztása esetén igazolásnak van helye.

(4) A perben fél lehet az is, akinek egyébként nincs perbeli jogképessége. A perbe a Hatóság az igénylő pernyertessége érdekében beavatkozhat.

(5) Az országos illetékességű közfeladatot ellátó szerv ellen indult per kivételével a per a járásbíróság hatáskörébe tartozik, és arra a törvényszék székhelyén lévő járásbíróság, Budapesten a Pesti Központi Kerületi Bíróság illetékes. A bíróság illetékességét az alperes közfeladatot ellátó szerv székhelye alapítja meg.

(6) A bíróság soron kívül jár el.

(6a) Ha a közérdekű adat megismerése iránti igény teljesítését az adatkezelő a 27. § (1) bekezdése alapján tagadja meg, és az adatot igénylő a közérdekű adat megismerésére vonatkozó igény elutasítása felülvizsgálatának érdekében az (1) bekezdésben meghatározottak alapján bírósághoz fordul, a bíróság a Hatóság titokfelügyeleti hatósági eljárását kezdeményezi, egyidejűleg a peres eljárást felfüggeszti. A titokfelügyeleti hatósági eljárást kezdeményező és az eljárást felfüggesztő végzés ellen nincs helye külön fellebbezésnek.

(7) Ha a bíróság a közérdekű adat igénylésére irányuló kérelemnek helyt ad, határozatában az adatkezelőt – az adatigénylés teljesítésére rendelkezésre álló határidő meghatározásával – a kért közérdekű adat közlésére kötelezi. A bíróság az adatigénylés teljesítéséért megállapított költségtérítés összegét megváltoztathatja, vagy a közfeladatot ellátó szervet a költségtérítés összegének megállapítása tekintetében új eljárásra kötelezheti.

IV. FEJEZET

A KÖZÉRDEKŰ ADATOK KÖZZÉTÉTELE

22. A közérdekű adatokra vonatkozó tájékoztatási kötelezettség

32. § A közfeladatot ellátó szerv a feladatkörébe tartozó ügyekben – így különösen az állami és önkormányzati költségvetésre és annak végrehajtására, az állami és önkormányzati vagyon kezelésére, a közpénzek felhasználására és az erre kötött szerződésekre, a piaci szereplők, a magánszervezetek és -személyek részére különleges vagy kizárólagos jogok biztosítására vonatkozóan – köteles elősegíteni és biztosítani a közvélemény pontos és gyors tájékoztatását.

23. Az elektronikus közzététel kötelezettsége

33. § (1)[374] Az e törvény alapján kötelezően közzéteendő közérdekű adatokat internetes honlapon, digitális formában, bárki számára, személyazonosítás nélkül, korlátozástól mentesen, kinyomtatható és részleteiben is adatvesztés és -torzulás nélkül kimásolható módon, a betekintés, a letöltés, a nyomtatás, a kimásolás és a hálózati adatátvitel szempontjából is díjmentesen kell hozzáférhetővé tenni (a továbbiakban: elektronikus közzététel). A közzétett adatok megismerése személyes adatok közléséhez nem köthető.

(2) A 37. § szerinti közzétételi listákon meghatározott adatait saját honlapján – ha törvény másként nem rendelkezik – közzéteszi

a) a Köztársasági Elnök Hivatala, az Országgyűlés Hivatala, az Alkotmánybíróság Hivatala, az Alapvető Jogok Biztosának Hivatala, az Állami Számvevőszék, a Magyar Tudományos Akadémia, a Magyar Művészeti Akadémia, az Országos Bírósági Hivatal, a Legfőbb Ügyészség,

b)

c) a központi államigazgatási szerv a kormánybizottság kivételével, továbbá az országos kamara, valamint

[374] DS11.2

d) a fővárosi és megyei kormányhivatal.

(3) A (2) bekezdésben nem szereplő közfeladatot ellátó szervek a 37. § szerinti elektronikus közzétételi kötelezettségüknek választásuk szerint saját vagy társulásaik által közösen működtetett, illetve a felügyeletüket, szakmai irányításukat vagy működésükkel kapcsolatos koordinációt ellátó szervek által fenntartott, valamint az erre a célra létrehozott központi honlapon való közzététellel is eleget tehetnek.

(4) Ha a közoktatási intézmény nem lát el országos vagy térségi feladatot, e törvény szerinti elektronikus közzétételi kötelezettségének az ágazati jogszabályokban meghatározott információs rendszerhez történő adatszolgáltatás teljesítésével eleget tesz.

34. § (1) Az adatokat nem a saját honlapon közzétevő adatfelelős – a 35. § alkalmazásával – a közzéteendő adatokat az adatközlőnek továbbítja, amely gondoskodik az adatok honlapon való közzétételéről, és arról, hogy egyértelmű legyen az, hogy az egyes közzétett közérdekű adatok melyik szervtől származnak, illetve melyikre vonatkoznak.

(2) Az adatközlő a közzétételre szolgáló honlapot úgy alakítja ki, hogy az adatok közzétételére alkalmas legyen, gondoskodik a folyamatos üzemeltetésről, az esetleges üzemzavar elhárításáról és az adatok frissítéséről.

(3) A közzétételre szolgáló honlapon közérthető formában tájékoztatást kell adni a közérdekű adatok egyedi igénylésének szabályairól. A tájékoztatásnak tartalmaznia kell az igénybe vehető jogorvoslati lehetőségek ismertetését is.

(4) A közzétételre szolgáló honlapon a közzétételi listákon meghatározott közérdekű adatokon kívül elektronikusan közzétehetőek más közérdekű és közérdekből nyilvános adatok is.

35. § (1) Az elektronikus közzétételre kötelezett adatfelelős szerv vezetője gondoskodik a 37. §-ban meghatározott közzétételi listákon szereplő adatok pontos, naprakész és folyamatos közzétételéről, az adatközlőnek való megküldéséről.

(2) A megküldött adatok elektronikus közzétételéért, folyamatos hozzáférhetőségéért, hitelességéért és az adatok frissítéséért az adatközlő felel.

(3) Az adatfelelős az (1) bekezdés szerinti, az adatközlő a (2) bekezdés szerinti kötelezettség teljesítésének részletes szabályait belső szabályzatban állapítja meg.

(4) Az elektronikusan közzétett adatok – ha e törvény vagy más jogszabály eltérően nem rendelkezik – a honlapról nem távolíthatóak el. A szerv megszűnése esetén a közzététel kötelezettsége a szerv jogutódját terheli.

36. § A 37. §-ban meghatározott közzétételi listákban szereplő adatok közzététele nem érinti az adott szervnek a közérdekű vagy közérdekből nyilvános adatok közzétételével kapcsolatos, más jogszabályban meghatározott kötelezettségeit.

24. A közzétételi listák

37. § (1)[375] A 33. § (2)–(4) bekezdésében meghatározott szervek (a továbbiakban együtt: közzétételre kötelezett szerv) – a (4) bekezdésben meghatározott kivétellel – tevékenységükhöz kapcsolódóan az 1. melléklet szerinti általános közzétételi listában meghatározott adatokat az 1. mellékletben foglaltak szerint közzéteszik.

(2) Jogszabály egyes ágazatokra, a közfeladatot ellátó szervtípusra vonatkozóan meghatározhat egyéb közzéteendő adatokat (a továbbiakban: különös közzétételi lista).

(3) A közzétételre kötelezett szerv vezetője – a Hatóság véleményének kikérésével –, valamint jogszabály a közfeladatot ellátó szervre, azok irányítása, felügyelete alá tartozó szervekre vagy

[375] DS3.4

azok egy részére kiterjedő hatállyal további kötelezően közzéteendő adatkört határozhat meg (a továbbiakban: egyedi közzétételi lista).

(4) A nemzetbiztonsági szolgálatok által közzéteendő adatok körét a Kormány – a Hatóság véleményének kikérésével – rendeletben állapítja meg.

(5) Testületi szervként működő közzétételre kötelezett szerv esetén az egyedi közzétételi lista megállapítása és módosítása – a Hatóság véleményének kikérésével – a testület hatáskörébe tartozik.

(6) A közzétételre kötelezett szerv vezetője a közzétételi listában nem szereplő közérdekű adatokra vonatkozó adatigénylések adatai alapján legalább évente felülvizsgálja az általa a (3) bekezdés szerint kiadott közzétételi listát, és a jelentős arányban vagy mennyiségben felmerült adatigénylések alapján azt kiegészíti.

(7) A közzétételi listában – a közzéteendő adat jellegétől függően – a közzététel gyakorisága is megállapítható.

(8) A különös és egyedi közzétételi listák elkészítésére, illetve kiegészítésére a Hatóság is javaslatot tehet.

24/A. A közérdekű adatok központi elektronikus jegyzéke és az egységes közadatkereső rendszer

37/A. § (1) Az elektronikusan közzétett adatok egyszerű és gyors elérhetősége érdekében az e törvény alapján közérdekű adat elektronikus közzétételére kötelezett szervek közérdekű adatot tartalmazó honlapjára, valamint az általuk fenntartott adatbázisra és nyilvántartásra vonatkozó leíró adatokat a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításáért felelős miniszter által működtetett, az erre a célra létrehozott honlapon közzétett központi elektronikus jegyzék összesítve tartalmazza.

(2) Az (1) bekezdésben meghatározott szerv közérdekű adataihoz való egységes szempontok szerinti elektronikus hozzáférést és a közérdekű adatok közötti keresés lehetőségét a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításáért felelős miniszter által működtetett egységes közadatkereső rendszer biztosítja.

37/B. § (1) Az adatfelelős gondoskodik a kezelésében lévő, közérdekű adatot tartalmazó honlapok, adatbázisok, illetve nyilvántartások leíró adatainak a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításáért felelős miniszternek történő továbbításáról és a továbbított közérdekű adatok rendszeres frissítéséről, valamint felel az egységes közadatkereső rendszerbe továbbított közérdekű adatok tartalmáért és a továbbított közérdekű adatok rendszeres frissítéséért is.

(2) A közérdekű adatokat tartalmazó adatbázisok, illetve nyilvántartások jegyzékének fenntartása, valamint az egységes közadatkereső rendszerhez való csatlakozás nem mentesíti az adatfelelőst az elektronikus közzététel kötelezettsége alól.

V. FEJEZET

A NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG

25. A Hatóság jogállása

38. § (1) A Hatóság autonóm államigazgatási szerv.

(2) A Hatóság feladata a személyes adatok védelméhez, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog érvényesülésének ellenőrzése és elősegítése.

(3) A Hatóság a (2) bekezdés szerinti feladatkörében az e törvényben meghatározottak szerint

a) bejelentés alapján vizsgálatot folytat;

b) hivatalból adatvédelmi hatósági eljárást folytathat;

c) hivatalból titokfelügyeleti hatósági eljárást folytathat;

d) a közérdekű adatokkal és a közérdekből nyilvános adatokkal kapcsolatos jogsértéssel összefüggésben bírósághoz fordulhat;

e) a más által indított perbe beavatkozhat;

f) adatvédelmi nyilvántartást vezet.

(4) A Hatóság a (2) bekezdés szerinti feladatkörében

a) javaslatot tehet a személyes adatok kezelését, valamint a közérdekű adatok és a közérdekből nyilvános adatok megismerését érintő jogszabályok megalkotására, illetve módosítására, véleményezi a feladatkörét érintő jogszabályok tervezetét;

b) tevékenységéről minden évben március 31-éig beszámolót hoz nyilvánosságra és a beszámolót benyújtja az Országgyűlésnek;

c) általános jelleggel vagy meghatározott adatkezelő részére ajánlást bocsát ki;

d) véleményezi a közfeladatot ellátó szerv tevékenységével kapcsolatosan az e törvény szerint közzéteendő adatokra vonatkozó különös, illetve egyedi közzétételi listákat;

e) törvényben meghatározott szervekkel vagy személyekkel együttműködve képviseli Magyarországot az Európai Unió közös adatvédelmi felügyelő testületeiben;

f) megszervezi a belső adatvédelmi felelősök konferenciáját;

g) meghatározza az adatvédelmi auditálás szakmai szempontjait;

h) az adatkezelő kérelmére adatvédelmi auditot folytathat le.

(5) A Hatóság független, csak a törvénynek van alárendelve, feladatkörében nem utasítható, a feladatát más szervektől elkülönülten, befolyásolástól mentesen látja el. A Hatóság számára feladatot csak törvény állapíthat meg.

26. A Hatóság költségvetése és gazdálkodása

39. § (1) A Hatóság fejezeti jogosítványokkal felruházott központi költségvetési szerv, amelynek költségvetése az Országgyűlés költségvetési fejezetén belül önálló címet képez.

(2) A Hatóság tárgyévi költségvetésének kiadási és bevételi főösszegei – az államháztartásról szóló törvényben meghatározott, az élet- és vagyonbiztonságot veszélyeztető elemi csapás, illetve annak következményei elhárítása érdekében meghozott átmeneti intézkedés, valamint a Hatóság saját vagy irányító szervi hatáskörében meghozott intézkedése kivételével – kizárólag az Országgyűlés által csökkenthetők.

(3) A Hatóság által kiszabott bírság a központi költségvetés bevétele.

(4) Az előző évi bevételeiből származó maradványt a Hatóság a következő években a feladatai teljesítésére felhasználhatja.

27. A Hatóság elnöke

40. § (1) A Hatóságot elnök vezeti. A Hatóság elnökét a miniszterelnök javaslatára a köztársasági elnök nevezi ki, azok közül a jogász végzettségű, az országgyűlési képviselők

választásán választható, magyar állampolgárok közül, akik az adatvédelmet vagy az információszabadságot érintő eljárások ellenőrzésében legalább tíz év szakmai tapasztalattal rendelkeznek, vagy e területek valamelyikén tudományos fokozatot szereztek.

(2) A Hatóság elnökének nem nevezhető ki az, aki a kinevezésre irányuló javaslat megtételének időpontját megelőző négy évben országgyűlési képviselő, nemzetiségi szószóló, európai parlamenti képviselő, köztársasági elnök, a Kormány tagja, államtitkár, helyi önkormányzati képviselő, polgármester, alpolgármester, főpolgármester, főpolgármester-helyettes, megyei közgyűlés elnöke vagy alelnöke, nemzetiségi önkormányzat tagja, illetve párt tisztségviselője vagy alkalmazottja volt.

(3) A köztársasági elnök a Hatóság elnökét kilenc évre nevezi ki.

(4) A Hatóság elnöke a kinevezését követően a köztársasági elnök előtt az egyes közjogi tisztségviselők esküjéről és fogadalmáról szóló törvény szerinti tartalommal esküt tesz.

41. § (1) A Hatóság elnöke nem lehet tagja pártnak, nem folytathat politikai tevékenységet, megbízatása összeegyeztethetetlen minden más állami vagy önkormányzati tisztséggel és megbízatással.

(2) A Hatóság elnöke más keresőfoglalkozást nem folytathat, és egyéb tevékenységéért – a tudományos, oktatói, művészeti, szerzői jogi védelem alá eső, lektori, szerkesztői és a nevelőszülői foglalkoztatási jogviszony keretében végzett tevékenységet kivéve – díjazást nem fogadhat el.

(3) A Hatóság elnöke nem lehet gazdasági társaság vezető tisztségviselője, felügyelőbizottságának tagja, továbbá gazdasági társaság személyes közreműködésre kötelezett tagja.

42. § (1) A Hatóság elnöke a kinevezését követő harminc napon belül, majd ezt követően minden évben január 31-ig, valamint a megbízatásának megszűnését követő harminc napon belül az országgyűlési képviselők vagyonnyilatkozatával azonos tartalmú vagyonnyilatkozatot tesz.

(2) A vagyonnyilatkozat-tétel elmulasztása esetén – a vagyonnyilatkozat benyújtásáig – a Hatóság elnöke tisztségét nem gyakorolhatja, javadalmazásban nem részesül.

(3) A vagyonnyilatkozat nyilvános, oldalhű másolatát a Hatóság honlapján haladéktalanul közzé kell tenni. A vagyonnyilatkozat a honlapról a Hatóság elnöke megbízatásának megszűnését követő egy év elteltéig nem távolítható el.

(4) A Hatóság elnökének vagyonnyilatkozatával kapcsolatos eljárást a miniszterelnöknél bárki kezdeményezheti a vagyonnyilatkozat konkrét tartalmára vonatkozó olyan tényállítással, amely konkrétan megjelöli a vagyonnyilatkozat kifogásolt részét és tartalmát. Ha a kezdeményezés nem felel meg az e bekezdésben foglalt követelményeknek, nyilvánvalóan alaptalan, vagy az ismételten benyújtott kezdeményezés új tényállítást vagy adatot nem tartalmaz, a miniszterelnök az eljárás lefolytatása nélkül elutasítja a kezdeményezést. A vagyonnyilatkozatban foglaltak valóságtartalmát a miniszterelnök ellenőrzi.

(5) A vagyonnyilatkozattal kapcsolatos eljárás során a miniszterelnök felhívására a Hatóság elnöke köteles a vagyonnyilatkozatában feltüntetett vagyoni, jövedelmi és érdekeltségi viszonyokat igazoló adatokat haladéktalanul, írásban bejelenteni a miniszterelnök részére. Az ellenőrzés eredményéről az adatok megküldésével a miniszterelnök tájékoztatja a köztársasági elnököt. Az adatokba csak a miniszterelnök és a köztársasági elnök tekinthet be.

(6) A Hatóság elnöke által benyújtott igazoló adatokat a vagyonnyilatkozattal kapcsolatos eljárás lezárulását követő harmincadik napon törölni kell.

43. § (1) A Hatóság elnöke miniszteri illetményre és juttatásokra jogosult, azzal, hogy a vezetői illetménypótlék mértéke a miniszteri vezetői illetménypótlék másfélszerese.

(2) A Hatóság elnökét naptári évenként negyven munkanap szabadság illeti meg.

44. § (1) A Hatóság elnöke a társadalombiztosítás ellátásaira való jogosultság szempontjából közszolgálati jogviszonyban foglalkoztatott biztosítottnak minősül.

(2) Az elnök megbízatásának időtartama közigazgatási szervnél közszolgálati jogviszonyban töltött időnek számít.

45. § (1) A Hatóság elnökének megbízatása megszűnik

a) a megbízatási idejének lejártával;

b) lemondásával;

c) halálával;

d) a kinevezéséhez szükséges feltételek hiányának vagy a vagyonnyilatkozat-tételi előírások megsértésének megállapításával;

e) összeférhetetlensége megállapításával;

f)

g)

(2) A Hatóság elnöke a miniszterelnök útján a köztársasági elnökhöz intézett írásbeli nyilatkozatával bármikor lemondhat megbízatásáról. A Hatóság elnökének megbízatása a lemondás közlését követő, a lemondásban megjelölt napon, ennek hiányában a lemondás közlésének napján szűnik meg. A lemondás érvényességéhez elfogadó nyilatkozat nem szükséges.

(3) Ha a Hatóság elnöke a 41. § szerinti összeférhetetlenségét a kinevezésétől számított harminc napon belül nem szünteti meg, vagy a tisztsége gyakorlása során vele szemben összeférhetetlenségi ok merül fel, a köztársasági elnök a miniszterelnök indítványára dönt az összeférhetetlenség megállapításának kérdésében.

(4)

(5)

(6) A Hatóság elnökének kinevezéséhez szükséges feltételek hiányát a miniszterelnök indítványára a köztársasági elnök állapítja meg. A köztársasági elnök – a miniszterelnök indítványára – megállapítja a vagyonnyilatkozat-tételi szabályok megsértését, ha a Hatóság elnöke vagyonnyilatkozatában szándékosan lényeges adatot, tényt valótlanul közöl.

(6a) A miniszterelnök a (3) és (6) bekezdés alapján megtett indítványát a köztársasági elnök és a Hatóság elnöke részére egyidejűleg megküldi.

(6b) A Hatóság elnöke az indítvány megalapozatlanságának megállapítása iránt az indítvány kézhezvételét követő harminc napon belül bírósághoz fordulhat, mely határidő elmulasztása esetén igazolásnak nincs helye. A pert a miniszterelnök ellen kell megindítani. A bíróság eljárására a polgári perrendtartásról szóló törvénynek a munkaviszonyból és a munkaviszony jellegű jogviszonyból származó perekre vonatkozó rendelkezéseit azzal az eltéréssel kell alkalmazni, hogy az ügyben a Fővárosi Közigazgatási és Munkaügyi Bíróság kizárólagos illetékességgel, soron kívül jár el, és a keresetet, valamint az ügy érdemében hozott jogerős döntését a bíróság a köztársasági elnökkel is közli.

(6c) Ha a Hatóság elnökének a (6b) bekezdés alapján benyújtott keresete alapján a bíróság jogerős ítéletében azt állapítja meg, hogy a miniszterelnök a (3) és (6) bekezdés alapján megtett indítványa megalapozatlan, a köztársasági elnök a Hatóság elnöke megbízatásának megszűnését nem állapítja meg.

(6d) A köztársasági elnök a miniszterelnök a (3) és (6) bekezdés alapján megtett indítványáról

a) ha a Hatóság elnöke a (6b) bekezdés szerinti határidőben nem fordul bírósághoz, a határidő lejártát követő tizenöt napon belül,

b) ha a Hatóság elnöke a (6b) bekezdés szerinti határidőben bírósághoz fordul, az ügy érdemében hozott jogerős döntés kézhezvételét követő tizenöt napon belül

dönt.

(7) A megbízatás az (1) bekezdés *a)* és *b)* pontja szerinti megszűnése esetén a Hatóság elnökét a megszűnéskori havi illetménye háromszorosának megfelelő összegű külön illetmény illeti meg.

(8) A köztársasági elnöknek a (3) és a (6) bekezdéssel és a 40. §-sal a hatáskörébe utalt döntéséhez ellenjegyzés nem szükséges.

45/A. § A Hatóság elnöke részt vehet és felszólalhat az Országgyűlés bizottságainak ülésén.

28. A Hatóság elnökének helyettese

46. § (1) A Hatóság elnökének munkáját az általa határozatlan időre kinevezett helyettes segíti. A Hatóság elnökhelyettese felett az elnök gyakorolja a munkáltatói jogokat.

(2) Az elnökhelyettesnek meg kell felelnie a Hatóság elnökének kinevezéséhez szükséges, a 40. § (1) és (2) bekezdésében előírt feltételeknek, azzal, hogy az adatvédelmet vagy az információszabadságot érintő eljárások ellenőrzésében öt év szakmai tapasztalattal kell rendelkeznie.

(3) Az elnökhelyettes összeférhetetlenségére a 41. §-ban foglaltakat megfelelően alkalmazni kell.

(4) Az elnökhelyettes az elnök akadályoztatása esetén, illetve ha az elnöki tisztség nincs betöltve, gyakorolja az elnök hatásköreit és ellátja feladatait.

47. § Az elnökhelyettes vagyonnyilatkozat-tételi kötelezettségére és a vagyonnyilatkozatával kapcsolatos eljárásra a 42. § rendelkezései megfelelően irányadóak, azzal, hogy a vagyonnyilatkozatával kapcsolatos eljárás során a miniszterelnök helyett a Hatóság elnöke jár el, és az ellenőrzés eredményéről nem kell tájékoztatni a köztársasági elnököt.

48. § (1) Az elnökhelyettes államtitkári illetményre és juttatásokra jogosult.

(2) Az elnökhelyettest naptári évenként negyven munkanap szabadság illeti meg.

(3) Az elnökhelyettes a társadalombiztosítás ellátásaira való jogosultság szempontjából közszolgálati jogviszonyban foglalkoztatott biztosítottnak minősül.

(4) Az elnökhelyettes megbízatásának időtartama közigazgatási szervnél közszolgálati jogviszonyban töltött időnek számít.

49. § (1) A Hatóság elnökhelyettesének megbízatása megszűnik

a) lemondásával;

b) halálával;

c) a kinevezéséhez szükséges feltételek hiányának megállapításával;

d) összeférhetetlensége megállapításával;

e) felmentésével;

f) a tisztségétől való megfosztással.

(2) A Hatóság elnökhelyettese a Hatóság elnökéhez intézett írásbeli nyilatkozatával bármikor lemondhat megbízatásáról. A Hatóság elnökhelyettesének megbízatása a lemondás közlését követő, a lemondásban megjelölt napon, ennek hiányában a lemondás közlésének napján szűnik meg. A lemondás érvényességéhez elfogadó nyilatkozat nem szükséges.

(3) Ha a Hatóság elnökhelyettese a 41. § szerinti összeférhetetlenségét a kinevezésétől számított harminc napon belül nem szünteti meg, vagy a tisztsége gyakorlása során vele szemben összeférhetetlenségi ok merül fel, a Hatóság elnöke dönt az összeférhetetlenség megállapításának kérdésében.

(4) A Hatóság elnöke felmenti a Hatóság elnökhelyettesét, ha a Hatóság elnökhelyettese neki fel nem róható okból kilencven napon túlmenően nem képes eleget tenni megbízatásából eredő feladatainak.

(5) A Hatóság elnöke a Hatóság elnökhelyettesét felmentheti, ezzel egyidejűleg a Hatóság elnökhelyettesének a Hatóságnál köztisztviselői munkakört és – az 51. § (1) bekezdésében meghatározott feltételek fennállásának hiányában is – vizsgálói megbízatást kell felajánlani.

(6) A Hatóság elnöke megfosztja tisztségétől a Hatóság elnökhelyettesét, ha a Hatóság elnökhelyettese neki felróható okból kilencven napon túlmenően nem tesz eleget megbízatásából eredő feladatainak, vagy vagyonnyilatkozatában szándékosan lényeges adatot, tényt valótlanul közöl.

(7) A Hatóság elnökhelyettesének kinevezéséhez szükséges feltételek hiányát a Hatóság elnöke állapítja meg.

(8) A megbízatás az (1) bekezdés *a)* és *e)* pontja szerinti megszűnése esetén a Hatóság elnökhelyettesét a megszűnéskori havi illetménye háromszorosának megfelelő összegű külön illetmény illeti meg.

29. A Hatóság személyi állománya

50. § A Hatóság köztisztviselői és munkavállalói felett a munkáltatói jogokat a Hatóság elnöke gyakorolja.

51. § (1) A Hatóság elnöke a Hatóság köztisztviselői létszámának legfeljebb húsz százalékáig vizsgálót nevezhet ki, a Hatóság azon köztisztviselői közül, akik felsőfokú informatikai vagy jogász végzettségűek és legalább három évet adatvédelmi szakértő vagy adatvédelmi felelős munkakörben töltöttek, valamint közigazgatási vagy jogi szakvizsgával, vagy közigazgatási tanulmányok szakirányú szakképzettséggel vagy kormányzati tanulmányok szakirányú szakképzettséggel rendelkeznek.

(2) A vizsgálói megbízatás határozatlan időre szól, amely a Hatóság elnöke által bármikor – indokolás nélkül – visszavonható. Ha a Hatóság elnöke a vizsgálói megbízatást visszavonja, a köztisztviselőt a vizsgálói megbízatását megelőzően betöltött utolsó munkakörébe kell visszahelyezni.

(3) A vizsgáló vezetői pótlék nélkül számított osztályvezetői illetményre jogosult.

VI. FEJEZET

A HATÓSÁG ELJÁRÁSAI

30. A Hatóság vizsgálata

52. § (1) A Hatóságnál bejelentéssel bárki vizsgálatot kezdeményezhet arra hivatkozással, hogy személyes adatok kezelésével, illetve a közérdekű adatok vagy a közérdekből nyilvános adatok megismeréséhez fűződő jogok gyakorlásával kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye fennáll.

(1a) A Hatóság vizsgálata a 31. § (1) bekezdésében meghatározott indokok valamelyikén alapuló bejelentés esetén az igény elutasításának közlésétől, a határidő eredménytelen elteltétől, illetve a

költségtérítés megfizetésére vonatkozó határidő lejártától számított egy éven belül kezdeményezhető.

(2) A Hatóság vizsgálata nem minősül közigazgatási hatósági eljárásnak.

(3) A Hatósághoz tett bejelentése miatt senkit sem érhet hátrány. A bejelentő kilétét a Hatóság csak akkor fedheti fel, ha ennek hiányában a vizsgálat nem lenne lefolytatható. Ha a bejelentő kéri, kilétét a Hatóság akkor sem fedheti fel, ha ennek hiányában a vizsgálat nem folytatható le. Erről a következményről a Hatóság a bejelentőt köteles tájékoztatni.

(4) A Hatóság vizsgálata ingyenes, a vizsgálat költségeit a Hatóság előlegezi és viseli.

53. § (1) A Hatóság – a (2) és (3) bekezdésben foglalt kivételekkel – a bejelentést köteles érdemben megvizsgálni.

(2) A Hatóság a bejelentést érdemi vizsgálat nélkül elutasíthatja, ha

a) a bejelentésben megjelölt jogsérelem csekély jelentőségű, vagy

b) a bejelentés névtelen.

(3) A Hatóság a bejelentést érdemi vizsgálat nélkül elutasítja, ha

a) az adott ügyben bírósági eljárás van folyamatban, vagy az ügyben korábban jogerős bírósági határozat született,

b) az 52. § (3) bekezdése szerinti tájékoztatás ellenére a bejelentő továbbra is kéri, hogy a kilétét ne fedjék fel,

c) a bejelentés nyilvánvalóan alaptalan,

d) az ismételten előterjesztett bejelentés érdemben új tényt, adatot nem tartalmaz,

e) a bejelentést az 52. § (1a) bekezdésében meghatározott határidőn túl nyújtották be.

(4) Ha a bejelentést az alapvető jogok biztosa tette, a Hatóság a bejelentést érdemi vizsgálat nélkül csak abban az esetben utasíthatja el, ha az adott ügyben bírósági eljárás van folyamatban, vagy az ügyben korábban jogerős bírósági határozat született.

(5) A Hatóság a vizsgálatot megszünteti, ha

a) a (3)–(4) bekezdés alapján a kérelem érdemi vizsgálat nélküli elutasításának lett volna helye, az elutasítási ok azonban a vizsgálat megindítását követően jutott a hatóság tudomására,

b) a vizsgálat folytatására okot adó körülmény már nem áll fenn.

(6) A Hatóság a bejelentés érdemi vizsgálatának elutasításáról, a vizsgálat megszüntetéséről és az elutasítás, illetve a megszüntetés indokairól értesíti a bejelentőt.

(7) A Hatóság a hatáskörébe nem tartozó ügyre vonatkozó bejelentést – a bejelentő egyidejű értesítése mellett – a bejelentésben foglaltak tekintetében eljárásra hatáskörrel rendelkező szervhez átteszi, ha a rendelkezésre álló adatok alapján a hatáskörrel rendelkező szerv kiléte megállapítható. Ha a Hatóság hatáskörébe nem tartozó ügyre vonatkozó bejelentés alapján a Hatóság azt állapítja meg, hogy az ügyben bírósági eljárás kezdeményezésének van helye, erről a bejelentőt értesíti.

54. § (1) A Hatóság a vizsgálat során

a) a vizsgált adatkezelő kezelésében levő, a vizsgált üggyel összefüggésbe hozható összes iratba betekinthet, illetve azokról másolatot kérhet,

b) a vizsgált üggyel összefüggésbe hozható adatkezelést megismerheti, az adatkezelés helyszínéül szolgáló helyiségbe beléphet,

c) a vizsgált adatkezelőtől, illetve az adatkezelő bármely munkatársától írásbeli és szóbeli felvilágosítást kérhet,

d) a vizsgált üggyel összefüggésbe hozható bármely szervezettől vagy személytől írásbeli felvilágosítást, illetve a vizsgált üggyel összefüggésbe hozható iratról másolatot kérhet, és

e) az adatkezelő hatóság felügyeleti szervének vezetőjét vizsgálat lefolytatására kérheti fel.

(2) A Hatóság (1) bekezdés szerinti kérésének a vizsgált adatkezelő, illetve az eljárási cselekménnyel érintett más szervezet vagy személy a Hatóság által megállapított határidőn belül köteles eleget tenni. A Hatóság által megállapított határidő az (1) bekezdés d) és e) pontja szerinti esetben tizenöt napnál rövidebb nem lehet.

(3) Az (1) bekezdés c) és d) pontja szerinti felvilágosítást az arra felhívott személy megtagadhatja, ha

a) az a személy, akit a Hatóság vizsgálatának alapját képező bejelentés érint, a Polgári Törvénykönyv szerinti hozzátartozója vagy volt házastársa;

b) a felvilágosítás során magát vagy a Polgári Törvénykönyv szerinti hozzátartozóját, illetve volt házastársát bűncselekmény elkövetésével vádolná, az azzal kapcsolatos kérdésben.

55. § (1) A Hatóság a bejelentés érkezésétől számított két hónapon belül,

a) ha a bejelentésben foglaltakat megalapozottnak tartja,

aa) az 56. §-ban, illetve az 57. §-ban meghatározott intézkedést tesz,

ab) a vizsgálatot lezárja, és a 60. § szerinti adatvédelmi hatósági eljárást indít, vagy

ac) a vizsgálatot lezárja, és a 62. § szerinti titokfelügyeleti hatósági eljárást indít;

b) ha a bejelentésben foglaltakat nem tartja megalapozottnak, a vizsgálatot lezárja.

(1a) Az (1) bekezdésben meghatározott határidőbe nem számít bele:

a) a tényállás tisztázásához szükséges adatok közlésére irányuló felhívástól az annak teljesítéséig terjedő idő,

b) a vizsgálattal összefüggő irat fordításához szükséges idő, valamint

c) a Hatóság működését legalább egy teljes napra akadályozó körülmény, ellehetetlenítő üzemzavar vagy más elháríthatatlan esemény időtartama.

(2) A vizsgálat eredményéről, a vizsgálat lezárásának indokáról, esetleges intézkedéséről, illetve hatósági eljárás megindításáról a Hatóság a bejelentőt értesíti.

56. § (1) Ha a Hatóság a személyes adatok kezelésével, illetve a közérdekű adatok vagy a közérdekből nyilvános adatok megismeréséhez fűződő jogok gyakorlásával kapcsolatos jogsérelem vagy annak közvetlen veszélye fennállását megalapozottnak tartja, az adatkezelőt a jogsérelem orvoslására, illetve annak közvetlen veszélye megszüntetésére szólítja fel.

(2) Az adatkezelő – egyetértése esetén – haladéktalanul megteszi az (1) bekezdés szerinti felszólításban megjelölt szükséges intézkedéseket, és a megtett intézkedéseiről, illetve – egyet nem értése esetén – álláspontjáról a felszólítás kézhezvételétől számított harminc napon belül írásban tájékoztatja a Hatóságot.

(3) A felügyeleti szervvel rendelkező adatkezelő hatóság esetében a Hatóság – ha az (1) bekezdés szerinti felszólítás nem vezetett eredményre – az adatkezelő szerv egyidejű tájékoztatása mellett ajánlást tehet az adatkezelő felügyeleti szervének. A Hatóság az adatkezelő felügyeleti szervének az (1) bekezdés szerinti felszólítás hiányában is közvetlenül ajánlást tehet, ha a jogsérelem orvoslása, illetve a jogsérelem közvetlen veszélyének megszüntetése álláspontja szerint ilyen módon hatékonyabban megtörténhet.

(4) A felügyeleti szerv az ajánlás tekintetében kialakított érdemi álláspontjáról, illetve a megtett intézkedésről az ajánlás kézhezvételétől számított harminc napon belül írásban tájékoztatja a Hatóságot.

57. § Ha a Hatóság a vizsgálata alapján azt állapítja meg, hogy a jogsérelem, illetve annak közvetlen veszélye valamely jogszabály vagy közjogi szervezetszabályozó eszköz fölösleges, nem egyértelmű vagy nem megfelelő rendelkezésére, illetve az adatkezeléssel összefüggő kérdések jogi szabályozásának hiányára vagy hiányosságára vezethető vissza, a jogsérelem, illetve annak közvetlen veszélye jövőbeni elkerülésének érdekében ajánlást tehet a jogszabályalkotásra, illetve a közjogi szervezetszabályozó eszköz kiadására jogosult szervnek, illetve a jogszabály előkészítőjének. Az ajánlásban a Hatóság javasolhatja a jogszabály, illetve a közjogi szervezetszabályozó eszköz módosítását, hatályon kívül helyezését vagy megalkotását. A megkeresett szerv az álláspontjáról, illetve az ajánlásban foglaltak szerint megtett intézkedéséről hatvan napon belül értesíti a Hatóságot.

58. § (1) Ha az 56. § szerinti felszólítás vagy ajánlás alapján a jogsérelem orvoslására, illetve a jogsérelem közvetlen veszélyének megszüntetésére nem került sor, a Hatóság az 56. § (2) bekezdése szerinti, illetve – ha ajánlás tételére került sor – az 56. § (4) bekezdése szerinti tájékoztatási határidő lejártát követő harminc napon belül dönt a szükséges további intézkedések megtételéről.

(2) Az (1) bekezdés szerinti esetben szükséges további intézkedésként a Hatóság

a) a 60. §-ban foglaltak szerint adatvédelmi hatósági eljárást indíthat,

b) a 62. §-ban foglaltak szerint titokfelügyeleti hatósági eljárást indíthat,

c) a 64. §-ban foglaltak szerint bírósági eljárást indíthat, vagy

d) az 59. §-ban foglaltak szerint jelentést készíthet.

(3) Az 56. § és az 57. § szerinti intézkedések eredményéről, illetve a (2) bekezdés szerinti további intézkedések megtételéről a Hatóság a bejelentőt értesíti.

31. A Hatóság jelentése

59. § (1) A Hatóság a bejelentés alapján lefolytatott vizsgálatról jelentést készíthet, ha az ügyben a Hatóság által hatósági eljárás vagy bírósági eljárás megindítására nem került sor.

(2) A jelentés tartalmazza a vizsgálat során feltárt tényeket, az ezeken alapuló megállapításokat és következtetéseket.

(3) A Hatóság jelentése nyilvános. A minősített adatot tartalmazó jelentést a Hatóság elnöke minősíti, vagy a minősítési jelölést megismétli. A minősített adatot vagy törvény által védett titkot tartalmazó jelentést úgy kell nyilvánosságra hozni, hogy a minősített adat vagy a törvény által védett egyéb titok ne legyen megismerhető.

(4) A Hatóságnak a titkosszolgálati eszközök és módszerek alkalmazására jogosult szervek e tevékenységével kapcsolatos vizsgálatáról készült jelentése nem tartalmazhat olyan adatot, amelyből a szerv adott ügyben folytatott titkos információgyűjtő tevékenységére lehetne következtetni.

(5) A Hatóság jelentése bíróság vagy más hatóság előtt nem támadható meg.

32. Adatvédelmi hatósági eljárás

60. § (1) A személyes adatok védelméhez való jog érvényesülése érdekében a Hatóság adatvédelmi hatósági eljárást indíthat, a (4) bekezdésben meghatározott esetben adatvédelmi hatósági eljárást indít.

(2)

(3) Az adatvédelmi hatósági eljárás kizárólag hivatalból indítható, az akkor sem minősül kérelemre indult eljárásnak, ha az adatvédelmi hatósági eljárást a Hatóság bejelentésen alapuló vizsgálata előzte meg. Ha azonban az adatvédelmi hatósági eljárást a Hatóság bejelentésen alapuló vizsgálata előzte meg, a bejelentőt az adatvédelmi hatósági eljárás megindításáról, illetve befejezéséről értesíteni kell.

(4) A Hatóság adatvédelmi hatósági eljárást indít, ha a bejelentésen alapuló vizsgálat alapján vagy egyébként valószínűsíthető a személyes adatok jogellenes kezelése, és a jogellenes adatkezelés

a) személyek széles körét érinti, vagy

b)

c) nagy érdeksérelmet vagy kárveszélyt idézhet elő.

(5) Az adatvédelmi hatósági eljárásban az ügyintézési határidő kilencven nap.

61. § (1) Az adatvédelmi hatósági eljárásban hozott határozatában a Hatóság

a) megállapíthatja a személyes adatok jogellenes kezelésének vagy feldolgozásának tényét,

b) elrendelheti a valóságnak nem megfelelő személyes adat helyesbítését,

c) elrendelheti a jogellenesen kezelt vagy feldolgozott személyes adatok zárolását, törlését vagy megsemmisítését,

d) megtilthatja a személyes adatok jogellenes kezelését vagy feldolgozását,

e) megtilthatja a személyes adatok külföldre történő továbbítását vagy átadását,

f) elrendelheti az érintett tájékoztatását, ha azt az adatkezelő jogellenesen tagadta meg, valamint

g) bírságot szabhat ki.

(2) A Hatóság elrendelheti határozatának – az adatkezelő azonosító adatainak közzétételével történő – nyilvánosságra hozatalát, ha a határozat személyek széles körét érinti, ha azt közfeladatot ellátó szerv tevékenységével összefüggésben hozta, vagy ha a bekövetkezett jogsérelem súlya a nyilvánosságra hozatalt indokolja.

(3) Az (1) bekezdés *g)* pontja szerint kiszabott bírság mértéke százezertől húszmillió forintig terjedhet.

(4) A Hatóság annak eldöntésében, hogy indokolt-e a bírság kiszabása, illetve a bírság mértékének megállapításában az eset összes körülményeit – így különösen a jogsértéssel érintettek körének nagyságát, a jogsértés súlyát és a jogsértés ismétlődő jellegét – veszi figyelembe.

(5) A határozat megtámadására nyitva álló keresetindítási határidő lejártáig, illetve közigazgatási per indítása esetén a bíróság jogerős határozatáig a vitatott adatkezeléssel érintett adatok nem törölhetők, illetve nem semmisíthetők meg.

33. Titokfelügyeleti hatósági eljárás

62. § (1) Ha a Hatóság vizsgálata alapján vagy egyébként valószínűsíthető, hogy a nemzeti minősített adat minősítése jogellenes, a Hatóság titokfelügyeleti hatósági eljárást indíthat.

(1a) Ha a bíróság a 31. § (6a) bekezdésében meghatározottak szerint a Hatóság titokfelügyeleti hatósági eljárását kezdeményezi, a Hatóság titokfelügyeleti hatósági eljárást indít.

(1b) A Hatóság titokfelügyeleti hatósági eljárása a Nemzeti Biztonsági Felügyeletnek a minősített adat védelméről szóló törvényben meghatározott feladatait nem érinti.

(2)

(2a) A titokfelügyeleti hatósági eljárásban és az ezen eljárásban hozott döntés megtámadására indított perben a minősített adatok kezelését a minősített adatok védelméről szóló törvényben és e törvényben meghatározott biztonsági követelményeknek megfelelően kell végezni.

(3) A titokfelügyeleti hatósági eljárás kizárólag hivatalból indítható, az akkor sem minősül kérelemre indult eljárásnak, ha a titokfelügyeleti hatósági eljárást a Hatóság bejelentésen alapuló vizsgálata előzte meg, vagy a titokfelügyeleti hatósági eljárást a bíróság a 31. § (6a) bekezdésében meghatározottak alapján kezdeményezte. Ha azonban a titokfelügyeleti hatósági eljárást a Hatóság bejelentésen alapuló vizsgálata előzte meg, a bejelentőt a titokfelügyeleti hatósági eljárás megindításáról és befejezéséről értesíteni kell.

(4) A titokfelügyeleti hatósági eljárásban ügyfél a minősítő.

(5) A titokfelügyeleti hatósági eljárásban a tényállás tisztázása során a tanú, a szakértő és a szemletárgy birtokosa meghallgatható akkor is, ha nem kapott felmentést a vizsgált nemzeti minősített adatra vonatkozó titoktartási kötelezettség alól.

(6) A titokfelügyeleti hatósági eljárásban az ügyintézési határidő kilencven nap.

63. § (1) A titokfelügyeleti hatósági eljárásban hozott határozatában a Hatóság

a) a nemzeti minősített adat minősítésére vonatkozó jogszabályok megsértésének megállapítása esetén a minősítőt a nemzeti minősített adat minősítési szintjének, illetve érvényességi idejének a jogszabályoknak megfelelő megváltoztatására vagy a minősítés megszüntetésére hívja fel, vagy

b) megállapítja, hogy a minősítő a nemzeti minősített adat minősítésére vonatkozó jogszabályoknak megfelelően járt el.

(2) A minősítő a Hatóság (1) bekezdés a) pontja szerinti határozatát a közlésétől számított hatvan napon belül támadhatja meg. A keresetlevél benyújtásának a határozat hatályosulására halasztó hatálya van. Ha a minősítő a határozat közlésétől számított hatvan napon belül nem fordul bírósághoz, a nemzeti minősített adat minősítése a határozat közlésétől számított hatvanegyedik napon a határozatban foglaltak szerint megszűnik, illetve minősítési szintje vagy érvényességi ideje a határozatban foglaltak szerint megváltozik.

(2a)

(3) A (2) bekezdésben meghatározott perben a bíróság zárt tárgyalást tart.

(4)

(5) A bíróság, illetve a Hatóság határozata nem érinti a minősítőnek a nemzeti minősített adat felülvizsgálatára vonatkozó, a minősített adat védelméről szóló törvény szerinti kötelezettségét.

(6) A perben csak olyan bíró járhat el, akinek a nemzetbiztonsági szolgálatokról szóló törvény szerinti nemzetbiztonsági ellenőrzését elvégezték.

(7) A (2) bekezdésben meghatározott per során a bírón, a felperesen és az alperesen kívüli személyek a minősített adatot csak akkor ismerhetik meg, ha az adat minősítési szintjének megfelelő személyi biztonsági tanúsítvánnyal rendelkeznek

34. A Hatóság által indítható per

64. § (1) Ha az adatkezelő az 56. § (1) bekezdésében foglalt felszólításnak nem tesz eleget, a közérdekű adatok és a közérdekből nyilvános adatokkal kapcsolatos jogsértés miatt a Hatóság az 56. § (2) bekezdése szerinti tájékoztatásra vonatkozó határidő lejártát követő harminc napon belül

keresettel kérheti a bíróságtól az adatkezelőnek a Hatóság felszólítása szerinti magatartásra való kötelezését.

(2) A bíróság hatáskörének és illetékességének megállapítására a 31. § (5) bekezdését kell alkalmazni.

(3) Azt, hogy az adatkezelés a jogszabályban foglaltaknak megfelel, az adatkezelő köteles bizonyítani.

(4) A perben fél lehet az is, akinek egyébként nincs perbeli jogképessége.

(5) A bíróság kérelemre elrendelheti ítéletének – az adatkezelő azonosító adatainak közzétételével történő – nyilvánosságra hozatalát, ha azt az adatvédelem, illetve az információszabadság érdekeinek és nagyobb számú érintett e törvényben védett jogainak védelme megköveteli.

34/A. A kötelező szervezeti szabályozás jóváhagyására irányuló eljárás

64/A. § (1) A kötelező szervezeti szabályozás jóváhagyását az adatkezelő kérelmezheti a Hatóságnál, azzal, hogy a kérelem kormányablaknál nem terjeszthető elő. Kötelező szervezeti szabályozás jóváhagyásának kérelmezésére nem jogosult az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény hatálya alá tartozó adatkezelő.

(2) A kötelező szervezeti szabályozás jóváhagyása iránti kérelemnek tartalmaznia kell

a) az adatkezelő vagy adatkezelők csoportja által végzett adatkezelésre vonatkozóan a 65. § (1) bekezdés *a)–j)* pontjában meghatározott adatokat vagy az adatkezelés nyilvántartási számát,

b) a kötelező szervezeti szabályozás tervezetét,

c) a kötelező szervezeti szabályozás kötelező jellegének igazolására szolgáló adatokat,

d) ha a kötelező szervezeti szabályozást más EGT-állam adatvédelmi hatósága jóváhagyta, az ennek igazolására szolgáló adatokat.

64/B. § A kötelező szervezeti szabályozás jóváhagyása iránti eljárásért miniszteri rendeletben meghatározott mértékű igazgatási szolgáltatási díjat kell fizetni.

64/C. § (1) A Hatóság a kötelező szervezeti szabályozás jóváhagyása iránti kérelmet kilencven napon belül bírálja el. A Hatóság a kötelező szervezeti szabályozás jóváhagyása iránti kérelem elbírálásakor a kötelező szervezeti szabályozást jóváhagyja, módosítását javasolja vagy a kérelmet elutasítja.

(2) A Hatóság az érintettek tájékoztatásának elősegítése érdekében honlapján közzéteszi a kötelező szervezeti szabályozást alkalmazó adatkezelő megnevezését.

35. Adatvédelmi nyilvántartás

65. § (1) Az adatkezelő személyes adatokra vonatkozó adatkezeléseiről, az érintettek tájékozódásának elősegítése érdekében a Hatóság hatósági nyilvántartást (a továbbiakban: adatvédelmi nyilvántartás) vezet, amely – a (2) bekezdésben meghatározott kivételekkel – tartalmazza

a) az adatkezelés célját,

b) az adatkezelés jogalapját,

c) az érintettek körét,

d) az érintettekre vonatkozó adatok leírását,

e) az adatok forrását,

f) az adatok kezelésének időtartamát,

g) a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló adattovábbításokat is,

h) az adatkezelő, valamint az adatfeldolgozó nevét és címét, a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét,

i) az alkalmazott adatfeldolgozási technológia jellegét,

j) a belső adatvédelmi felelős alkalmazása esetén annak nevét és elérhetőségi adatait.

(2) Az adatvédelmi nyilvántartás a nemzetbiztonsági szervek adatkezelései tekintetében a nemzetbiztonsági szerv nevét és címét, az adatkezelés célját és jogalapját tartalmazza.

(3) Nem vezet adatvédelmi nyilvántartást a Hatóság arról az adatkezelésről, amely

a) az adatkezelővel munkaviszonyban, tagsági viszonyban, óvodai nevelésben való részvételre irányuló, tanulói vagy tanulószerződéses jogviszonyban, kollégiumi tagsági viszonyban vagy – a pénzügyi szervezetek, közüzemi szolgáltatók, elektronikus hírközlési szolgáltatók ügyfelei kivételével – ügyfélkapcsolatban álló személyek adataira vonatkozik;

b) a bevett egyház belső szabálya szerint történik;

c) az egészségügyi ellátásban kezelt személy betegségével, egészségi állapotával kapcsolatos személyes adatokra vonatkozik gyógykezelés vagy az egészség megőrzése, társadalombiztosítási igény érvényesítése céljából;

d) az érintett anyagi és egyéb szociális támogatása céljából nyilvántartott személyes adatokra vonatkozik;

e) a hatósági, az ügyészségi és a bírósági eljárás által érintett személyeknek az eljárás lefolytatásával kapcsolatos személyes adataira, vagy a büntetés-végrehajtás során a büntetés-végrehajtással összefüggésben kezelt személyes adatokra vonatkozik;

f) a hivatalos statisztika célját szolgáló személyes adatokat tartalmaz, feltéve hogy – törvényben meghatározottak szerint – az adatok érintettel való kapcsolatának megállapítását véglegesen lehetetlenné teszik;

g) a médiaszolgáltatásokról és a tömegkommunikációról szóló törvény szerinti médiatartalom-szolgáltató olyan adatait tartalmazza, amelyek kizárólag saját tájékoztatási tevékenységét szolgálják;

h) a tudományos kutatás céljait szolgálja, ha az adatokat nem hozzák nyilvánosságra,

i) a levéltári őrizetbe vett iratokkal összefüggésben valósul meg.

(4) Az adatvédelmi nyilvántartás nyilvános, abba bárki betekinthet, az abban foglaltakról feljegyzést készíthet.

66. § (1) A személyes adatok kezelésének nyilvántartásba vételét az adatkezelő – a kötelező adatkezelés kivételével az adatkezelés megkezdése előtt – kérelmezi a Hatóságnál. A kötelező adatkezelés, valamint a 68. § (2) bekezdésben foglalt eset kivételével az adatkezelés a nyilvántartásba vételt megelőzően nem kezdhető meg.

(2) A kötelező adatkezelés nyilvántartásba vételét az adatkezelő az adatkezelést elrendelő jogszabály hatálybalépését követő húsz napon belül kérelmezi a Hatóságnál.

(3) A nyilvántartásba vétel szempontjából az eltérő célú adatkezelések önálló adatkezelésnek minősülnek, abban az esetben is, ha a kezelt adatok köre azonos.

(4) A nyilvántartásba vétel iránti kérelemnek tartalmaznia kell a 65. § (1), illetve (2) bekezdése szerinti adatokat.

67. § Az adatvédelmi nyilvántartásba vételért a kötelező adatkezelés nyilvántartásba vétele kivételével a miniszteri rendeletben meghatározott igazgatási szolgáltatási díjat kell fizetni.

68. § (1) A (3) bekezdésben foglalt kivétellel a Hatóság az adatkezelést a kérelem megérkezésétől számított nyolc napon belül nyilvántartásba veszi, ha a kérelem tartalmazza a 65. § (1), illetve (2) bekezdése szerinti adatokat.

(2) A (3) bekezdésben foglalt kivétellel ha a Hatóság a nyilvántartásba vétel iránti kérelmet határidőben nem bírálja el, az adatkezelő az adatkezelést a kérelemben foglaltak szerint megkezdheti.

(3) A (4) és (5) bekezdés szerinti adatkezelést a Hatóság a kérelem megérkezésétől számított negyven napon belül nyilvántartásba veszi, ha a kérelem tartalmazza a 65. § (1), illetve (2) bekezdése szerinti adatokat és az adatkezelőnél a jogszerű adatkezelés feltételei biztosíthatók.

(4) Ha a kérelem olyan – az (5) bekezdésben meghatározott – adatkezelés nyilvántartásba vételére irányul, amely az adatkezelő korábban nyilvántartásba vett adatkezelésével nem érintett adatállományra vonatkozik, illetve amely az adatkezelő korábban nyilvántartásba vett adatkezelésénél nem alkalmazott, új adatfeldolgozási technológia alkalmazását teszi szükségessé, a nyilvántartásba vétel feltétele, hogy az adatkezelőnél a jogszerű adatkezelés feltételei biztosíthatók legyenek.

(5) A (4) bekezdésben foglalt nyilvántartásba vételi feltétel, az abban meghatározottak szerint

a) az országos hatósági, munkaügyi és bűnügyi adatállományok kezelésére;

b) a pénzügyi szervezetek és közüzemi szolgáltatók ügyfelekre vonatkozó adatkezelésére;

c) az elektronikus hírközlési szolgáltatóknak a szolgáltatást igénybe vevőkre vonatkozó adatkezelésére

vonatkozik.

(6) A Hatóság az adatvédelmi nyilvántartásba vételi kérelemnek helyt adó határozatának tartalmaznia kell az adatkezelés nyilvántartási számát, amelyet az adatkezelőnek az adatok minden továbbításánál, nyilvánosságra hozásánál és az érintettnek való kiadásakor fel kell tüntetni. A nyilvántartási szám az adatkezelés azonosítására szolgál, és nem tanúsítja a nyilvántartásba vett adatkezelés jogszerűségét.

(7) A 65. § (1) bekezdés *b)–j)* pontja szerinti adatok megváltozása esetén az adatkezelő a változás bekövetkezésétől számított nyolc napon belül változásbejegyzési kérelmet nyújt be a Hatóságnak. A változásbejegyzési eljárásra az (1), (3) és (5) bekezdésben foglalt szabályokat megfelelően alkalmazni kell, azzal, hogy a kérelemnek csak a megváltozott adatokat kell tartalmaznia.

36. Adatvédelmi audit

69. § (1) Az adatvédelmi audit a Hatóság olyan szolgáltatása, amelynek célja a végzett vagy tervezett adatkezelési műveletek a Hatóság által meghatározott és közzétett szakmai szempontok szerinti értékelésén keresztül a magas szintű adatvédelem és adatbiztonság megvalósítása. Tervezett adatkezelési műveletek akkor vonhatók audit alá, ha az adatkezelésre vonatkozó koncepció kidolgozottsága ezt lehetővé teszi.

(2) Adatvédelmi auditot a Hatóság az adatkezelő kérelmére folytathat le. Az adatvédelmi audit lefolytatása iránti kérelem benyújtását követő tizenöt napon belül az adatvédelmi audit lefolytatásáért fizetendő ellenérték mértékét és az adatvédelmi audit elvégzésének várható időpontját a Hatóság közli az adatkezelővel. A Hatóság az adatvédelmi auditot abban az esetben

folytatja le, ha a Hatóság közlését követő tizenöt napon belül az adatkezelő nyilatkozik arról, hogy a Hatóság közlésében megállapított feltételek ismeretében az adatvédelmi audit lefolytatása iránti kérelmét fenntartja.

(3) Az adatvédelmi audit lefolytatásáért fizetendő ellenérték mértékét – az elvégzendő tevékenység mértékével arányosan – a Hatóság állapítja meg, az azonban nem haladhatja meg az ötmillió forintot. Az adatvédelmi audit lefolytatásáért fizetendő ellenérték a Hatóság bevétele.

(4) Az adatvédelmi audit eredményét a Hatóság az auditról készített értékelésben rögzíti. Az értékelés javaslatokat fogalmazhat meg az adatkezelő számára. Az értékelés tartalma az üzleti titokra alkalmazandó szabályok szerint ismerhető meg, az adatkezelő erre irányuló kérelmére azonban a Hatóság honlapján – a kérelemnek megfelelően – az értékelést vagy az értékelés összegző megállapításait közzéteszi.

(5) Az adatvédelmi audit a Hatóság e törvényben rögzített egyéb hatásköreinek gyakorlását nem korlátozza.

37. Büntető-, szabálysértési és fegyelmi eljárás kezdeményezése

70. § (1) Ha a Hatóság az eljárása során bűncselekmény elkövetésének alapos gyanúját észleli, büntetőeljárást kezdeményez az annak megindítására jogosult szervnél. Ha a Hatóság az eljárása során szabálysértés vagy fegyelmi vétség elkövetésének alapos gyanúját észleli, szabálysértési, illetve fegyelmi eljárást kezdeményez a szabálysértési, illetve a fegyelmi eljárás lefolytatására jogosult szervnél.

(2) Az (1) bekezdésben meghatározott szerv az eljárás megindításával kapcsolatos álláspontjáról – törvény eltérő rendelkezése hiányában – harminc napon belül, az eljárás eredményéről pedig az annak befejezését követő harminc napon belül tájékoztatja a Hatóságot.

38. Adatkezelés és titoktartás

71. § (1) A Hatóság eljárása során – az annak lefolytatásához szükséges mértékben és ideig – kezelheti mindazon személyes adatokat, valamint törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatokat, amelyek az eljárással összefüggnek, illetve amelyek kezelése az eljárás eredményes lefolytatása érdekében szükséges.

(2) A Hatóság a vizsgálata során beszerzett adatokat hatósági eljárásában felhasználhatja.

(2a) Védekezés céljából készült irat esetén az (1) és (2) bekezdésben foglaltakat az ügyvédi tevékenységről szóló törvényben meghatározott eltérésekkel kell alkalmazni.

(3) A Hatóság az e törvényben meghatározott eljárásai során az alapvető jogok biztosáról szóló 2011. évi CXI. törvény (a továbbiakban: Ajbtv.) 23. § (1) bekezdés *a)–f)* és *i)* pontjában, (2) bekezdésében, (3) bekezdés *c)–f)* pontjában, (4) bekezdés *c)–g)* pontjában, valamint (5) bekezdés*d*bekezdés *d)* pontjában meghatározott adatokat az Ajbtv. 23. § (7) bekezdésében meghatározottak szerint ismerheti meg.

(3a) A Hatóság a (3) bekezdésre tekintet nélkül megismerheti az Ajbtv. 23. § (3) bekezdés *e)* pontjában, (4) bekezdés *f)* pontjában és (5) bekezdés *d)* pontjában meghatározott adatot, ha az az együttműködő személy személyes adatainak védelmével kapcsolatban indult

a) vizsgálati eljárásban,

b) adatvédelmi hatósági eljárásban vagy

c) titokfelügyeleti hatósági eljárásban

szükséges.

(3b) A Hatóság a (3) bekezdésre tekintet nélkül megismerheti az Ajbtv. 23. § (3) bekezdés *f)* pontjában és (4) bekezdés *g)* pontjában meghatározott, a titkos információgyűjtésre használt eszközöket és módszereket alkalmazó személyek azonosítását lehetővé tevő adatot, ha az e személyek személyes adatainak védelmével kapcsolatban indult

a) vizsgálati eljárásban,

b) adatvédelmi hatósági eljárásban vagy

c) titokfelügyeleti hatósági eljárásban

szükséges.

(3c) Ha a Hatóság által vizsgálni kívánt irat olyan adatot is tartalmaz, amelyet a Hatóság csak a (3) bekezdés szerint ismerhet meg, az irat megismerését a meg nem ismerhető adat felismerhetetlenné tételével kell a Hatóság részére lehetővé tenni.

(4) A minősített adatot érintő adatkezeléssel kapcsolatos eljárása során a Hatóság elnökhelyettese, vezetői munkakört betöltő köztisztviselője és vizsgálója – ha megfelelő szintű személyi biztonsági tanúsítvánnyal rendelkezik – a minősített adatot a minősített adat védelméről szóló törvényben meghatározott felhasználói engedély nélkül is megismerheti.

(5) A Hatóság elnöke, elnökhelyettese és a Hatósággal közszolgálati jogviszonyban, valamint munkavégzésre irányuló egyéb jogviszonyban álló, illetve állt személyek – a más szervezet számára jogszabályban előírt adatszolgáltatást kivéve – e jogviszony fennállása alatt, és annak megszűnését követően is kötelesek megőrizni a Hatóság tevékenységével, annak ellátásával kapcsolatban tudomásukra jutott személyes adatot, minősített adatot, illetve törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatot, valamint minden olyan adatot, tényt vagy körülményt, amelyet a Hatóság nem köteles törvény előírásai szerint a nyilvánosság számára hozzáférhetővé tenni.

(6) Az (5) bekezdésben felsorolt személyek megőrzési kötelezettsége arra terjed ki, hogy a feladataik ellátásával kapcsolatban tudomásukra jutott adatokat, tényt vagy körülményt jogosulatlanul nem tehetik közzé, nem hasznosíthatják, és nem hozhatják harmadik személy tudomására.

VII. FEJEZET

ZÁRÓ RENDELKEZÉSEK

72. § (1) Felhatalmazást kap a Kormány, hogy rendeletben

a) állapítsa meg a közérdekű adatok elektronikus közzétételének részletszabályait,

b) állapítsa meg a közérdekű adat iránti igény teljesítéséért fizetendő költségtérítés megállapítható mértékét és a 29. § (4) bekezdése szerinti összeghatárt,

c) különös közzétételi listát állapíthasson meg,

d) állapítsa meg az egységes közadatkereső rendszer és a központi jegyzék adattartalmát, valamint az adatintegrációra vonatkozó szabályokat,

e) – a Hatóság véleményének kikérésével – állapítsa meg a nemzetbiztonsági szolgálatok által közzéteendő adatok körét.

(2) Felhatalmazást kap

a) a feladatkörrel rendelkező miniszter, hogy rendeletben az irányítása vagy felügyelete alá tartozó szervekre nézve különös közzétételi listát állapíthasson meg,

b) az e-közigazgatásért felelős miniszter, hogy rendeletben állapítsa meg a közzétételi listákon szereplő adatok közzétételéhez szükséges közzétételi mintákat,

c)

(3) Felhatalmazást kap az igazságügyért felelős miniszter, hogy a Hatóság véleményének kikérésével, az adópolitikáért felelős miniszterrel egyetértésben a kötelező szervezeti szabályozás jóváhagyásáért, az adatvédelmi nyilvántartásba vételért fizetendő igazgatási szolgáltatási díj mértékét, valamint a díj beszedésével, kezelésével, nyilvántartásával és visszatérítésével kapcsolatos részletes szabályokat rendeletben állapítsa meg.

73. § (1) E törvény – a (2) és (3) bekezdésben meghatározott kivételekkel – a kihirdetését követő napon lép hatályba.

(2) Az 1–37. §, a 38. § (1)–(3) bekezdése, a 38. § (4) bekezdés *a)–f)* pontja, a 38. § (5) bekezdése, a 39. §, a 41–68. §, a 70–72. §, a 75–77. § és a 79–88. §, valamint az 1. melléklet 2012. január 1-jén lép hatályba.

(3) A 38. § (4) bekezdés *g)* és *h)* pontja, valamint a 69. § 2013. január 1-jén lép hatályba.

73/A. § E törvénynek az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény módosításáról szóló 2013. évi XCI. törvénnyel megállapított 26. § (2) bekezdését és 30. § (7) bekezdését az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény módosításáról szóló 2013. évi XCI. törvény hatálybalépésekor folyamatban lévő eljárásokra is alkalmazni kell.

74. § A Hatóság első elnökére a miniszterelnök 2011. november 15-éig tesz javaslatot a köztársasági elnöknek. A Hatóság első elnökét a köztársasági elnök 2012. január 1-jei hatállyal nevezi ki.

75. § (1) Az adatvédelmi biztoshoz 2012. január 1-je előtt érkezett beadvány alapján folyamatban lévő ügyben az e törvényben foglaltak szerint a Hatóság jár el.

(2) Az adatvédelmi biztos feladatkörében 2012. január 1-jét megelőzően kezelt adatokat 2012. január 1-jétől a Hatóság kezeli.

(3) A 2012. január 1-jét megelőzően megkezdett, de az adatvédelmi nyilvántartásba 2012. január 1-jét megelőzően be nem jelentett, az e törvény szerinti adatvédelmi nyilvántartás hatálya alá eső adatkezelés nyilvántartásba vételét e törvény szabályai szerint 2012. június 30-ig kérelmezni kell a Hatóságnál, ennek hiányában az adatkezelés 2012. június 30-át követően nem folytatható. Nem folytatható az e bekezdés szerinti adatkezelés akkor sem, ha a nyilvántartásba vételére irányuló, 2011. december 31-ét követően benyújtott kérelem alapján a Hatóság a nyilvántartásba vételt elutasította.

76. § E törvény V. Fejezete az Alaptörvény VI. cikk (3) bekezdése alapján sarkalatosnak minősül.

77. § Ez a törvény

a) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelvnek,

b) a környezeti információkhoz való nyilvános hozzáférésről és a 90/313/EGK irányelv hatályon kívül helyezéséről szóló, 2003. január 28-i 2003/4/EK európai parlamenti és tanácsi irányelvnek,

c) a közszféra információinak további felhasználásáról szóló, 2003. november 17-i 2003/98/EK európai parlamenti és tanácsi irányelvnek,

d) a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről szóló, 2008. november 27-i 2008/977/IB tanácsi kerethatározatnak

e) a közszféra információinak további felhasználásáról szóló 2003/98/EK irányelv módosításáról szóló, 2013. június 26-i 2013/37/EU európai parlamenti és tanácsi irányelvnek

való megfelelést szolgálja.

78. § (1)–(2)

78. § (3)–(9)

79–89. §

1. melléklet a 2011. évi CXII. törvényhez
ÁLTALÁNOS KÖZZÉTÉTELI LISTA

I. Szervezeti, személyzeti adatok

	Adat	Frissítés	Megőrzés
1.	A közfeladatot ellátó szerv hivatalos neve, székhelye, postai címe, telefon- és telefaxszáma, elektronikus levélcíme, honlapja, ügyfélszolgálatának elérhetőségei	A változásokat követően azonnal	Az előző állapot törlendő
2.	A közfeladatot ellátó szerv szervezeti felépítése szervezeti egységek megjelölésével, az egyes szervezeti egységek feladatai	A változásokat követően azonnal	Az előző állapot törlendő
3.	A közfeladatot ellátó szerv vezetőinek és az egyes szervezeti egységek vezetőinek neve, beosztása, elérhetősége (telefon- és telefaxszáma, elektronikus levélcíme)	A változásokat követően azonnal	Az előző állapot törlendő
4.	A szervezeten belül illetékes ügyfélkapcsolati vezető neve, elérhetősége (telefon- és telefaxszáma, elektronikus levélcíme) és az ügyfélfogadási rend	A változásokat követően azonnal	Az előző állapot törlendő
5.	Testületi szerv esetén a testület létszáma, összetétele, tagjainak neve, beosztása, elérhetősége	A változásokat követően azonnal	Az előző állapot törlendő
6.	A közfeladatot ellátó szerv irányítása, felügyelete vagy ellenőrzése alatt álló, vagy alárendeltségében működő más közfeladatot ellátó szervek megnevezése, és 1. pontban meghatározott adatai	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával
7.	A közfeladatot ellátó szerv többségi tulajdonában álló, illetve részvételével működő gazdálkodó szervezet neve, székhelye, elérhetősége (postai címe, telefon- és telefaxszáma, elektronikus levélcíme),	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával

	tevékenységi köre, képviselőjének neve, a közfeladatot ellátó szerv részesedésének mértéke		
8.	A közfeladatot ellátó szerv által alapított közalapítványok neve, székhelye, elérhetősége (postai címe, telefon- és telefaxszáma, elektronikus levélcíme), alapító okirata, kezelő szervének tagjai	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával
9.	A közfeladatot ellátó szerv által alapított költségvetési szerv neve, székhelye, a költségvetési szervet alapító jogszabály megjelölése, illetve az azt alapító határozat, a költségvetési szerv alapító okirata, vezetője, honlapjának elérhetősége, működési engedélye	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával
10.	A közfeladatot ellátó szerv által alapított lapok neve, a szerkesztőség és kiadó neve és címe, valamint a főszerkesztő neve	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával
11.	A közfeladatot ellátó szerv felettes, illetve felügyeleti szervének, hatósági döntései tekintetében a fellebbezés elbírálására jogosult szervnek, ennek hiányában a közfeladatot ellátó szerv felett törvényességi ellenőrzést gyakorló szervnek az 1. pontban meghatározott adatai	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával

II. Tevékenységre, működésre vonatkozó adatok

	Adat	Frissítés	Megőrzés
1.	A közfeladatot ellátó szerv feladatát, hatáskörét és alaptevékenységét meghatározó, a szervre vonatkozó alapvető jogszabályok, közjogi szervezetszabályozó eszközök, valamint a szervezeti és működési szabályzat vagy ügyrend, az adatvédelmi és adatbiztonsági szabályzat hatályos és teljes szövege	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával
2.	Az országos illetékességű szervek, valamint a fővárosi és megyei kormányhivatal esetében a közfeladatot ellátó szerv feladatáról, tevékenységéről szóló tájékoztató magyar és angol nyelven	A változásokat követően azonnal	Az előző állapot törlendő
3.	A helyi önkormányzat önként vállalt feladatai	Negyedévente	Az előző állapot 1 évig archívumban tartásával

4.	Államigazgatási, önkormányzati, és egyéb hatósági ügyekben ügyfajtánként és eljárástípusonként a hatáskörrel rendelkező szerv megnevezése, hatáskör gyakorlásának átruházása esetén a ténylegesen eljáró szerv megnevezése, illetékességi területe, az ügyintézéshez szükséges dokumentumok, okmányok, eljárási illetékek (igazgatási szolgáltatási díjak) meghatározása, alapvető eljárási szabályok, az eljárást megindító irat benyújtásának módja (helye, ideje), ügyfélfogadás ideje, az ügyintézés határideje (elintézési, fellebbezési határidő), az ügyek intézését segítő útmutatók, az ügymenetre vonatkozó tájékoztatás és az ügyintézéshez használt letölthető formanyomtatványok, az igénybe vehető elektronikus programok elérése, időpontfoglalás, az ügytípusokhoz kapcsolódó jogszabályok jegyzéke, tájékoztatás az ügyfelet megillető jogokról és az ügyfelet terhelő kötelezettségekről	A változásokat követően azonnal	Az előző állapot törlendő
5.	A közfeladatot ellátó szerv által nyújtott vagy költségvetéséből finanszírozott közszolgáltatások megnevezése, tartalma, a közszolgáltatások igénybevételének rendje, a közszolgáltatásért fizetendő díj mértéke, az abból adott kedvezmények	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával
6.	A közfeladatot ellátó szerv által fenntartott adatbázisok, illetve nyilvántartások leíró adatai (név, formátum, az adatkezelés célja, jogalapja, időtartama, az érintettek köre, az adatok forrása, kérdőíves adatfelvétel esetén a kitöltendő kérdőív), az adatvédelmi nyilvántartásba bejelentendő nyilvántartásoknak az e törvény szerinti azonosító adatai; a közfeladatot ellátó szerv által – alaptevékenysége keretében – gyűjtött és feldolgozott adatok fajtái, a hozzáférés módja, a másolatkészítés költségei	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával
7.	A közfeladatot ellátó szerv nyilvános kiadványainak címe, témája, a hozzáférés módja, a kiadvány ingyenessége, illetve a költségtérítés mértéke	Negyedévente	Az előző állapot 1 évig archívumban tartásával
8.	A testületi szerv döntései előkészítésének rendje, az állampolgári közreműködés (véleményezés) módja, eljárási szabályai, a testületi szerv üléseinek helye, ideje, továbbá	A változásokat követően azonnal	Az előző állapot 1 évig archívumban

	nyilvánossága, döntései, ülésének jegyzőkönyvei, illetve összefoglalói; a testületi szerv szavazásának adatai, ha ezt jogszabály nem korlátozza		tartásával
9.	A törvény alapján közzéteendő jogszabálytervezetek és kapcsolódó dokumentumok; a helyi önkormányzat képviselő-testületének nyilvános ülésére benyújtott előterjesztések a benyújtás időpontjától	Törvény eltérő rendelkezése hiányában a benyújtás időpontját követően azonnal	Az előző állapot 1 évig archívumban tartásával
10.	A közfeladatot ellátó szerv által közzétett hirdetmények, közlemények	Folyamatosan	Legalább 1 évig archívumban tartásával
11.	A közfeladatot ellátó szerv által kiírt pályázatok szakmai leírása, azok eredményei és indokolásuk	Folyamatosan	Az előző állapot 1 évig archívumban tartásával
12.	A közfeladatot ellátó szervnél végzett alaptevékenységgel kapcsolatos vizsgálatok, ellenőrzések nyilvános megállapításai	A vizsgálatról szóló jelentés megismerését követően haladéktalanul	Az előző állapot 1 évig archívumban tartásával
13.	A közérdekű adatok megismerésére irányuló igények intézésének rendje, az illetékes szervezeti egység neve, elérhetősége, s ahol kijelölésre kerül, az adatvédelmi felelős, vagy az információs jogokkal foglalkozó személy neve	Negyedévente	Az előző állapot törlendő
14.	A közfeladatot ellátó szerv tevékenységére vonatkozó, jogszabályon alapuló statisztikai adatgyűjtés eredményei, időbeli változásuk	Negyedévente	Az előző állapot 1 évig archívumban tartásával
15.	A közérdekű adatokkal kapcsolatos kötelező statisztikai adatszolgáltatás adott szervre vonatkozó adatai	Negyedévente	Az előző állapot 1 évig archívumban tartásával
16.	Azon közérdekű adatok hasznosítására irányuló szerződések listája, amelyekben a közfeladatot ellátó szerv az egyik szerződő fél	Negyedévente	Az előző állapot 1 évig archívumban tartásával

17.	A közfeladatot ellátó szerv kezelésében lévő közérdekű adatok felhasználására, hasznosítására vonatkozó általános szerződési feltételek	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával
18.	A közfeladatot ellátó szervre vonatkozó különös és egyedi közzétételi lista	A változásokat követően azonnal	Az előző állapot törlendő
19.	A közfeladatot ellátó szerv kezelésében levő, a közadatok újrahasznosításáról szóló törvény szerint újrahasznosítás céljára elérhető kulturális közadatok listája a rendelkezésre álló formátumok megjelölésével, valamint a közfeladatot ellátó szerv kezelésében levő, a közadatok újrahasznosításáról szóló törvény szerint újrahasznosítható közadat típusokról való tájékoztatás, a rendelkezésre álló formátumok megjelölésével	A változásokat követő 15 napon belül	Az előző állapot 1 évig archívumban tartásával
20.	A 19. sor szerinti közadatok és kulturális közadatok újrahasznosítására vonatkozó általános szerződési feltételek elektronikusan szerkeszthető változata	A változásokat követő 15 napon belül	Az előző állapot törlendő
21.	A 19. sor szerinti közadatok és kulturális közadatok újrahasznosítás céljából történő rendelkezésre bocsátásáért fizetendő díjak általános jegyzéke, a díjszámítás alapját képező tényezőkkel együttesen	A változásokat követő 15 napon belül	Az előző állapot törlendő
22.	A közadatok újrahasznosításáról szóló törvény szerinti jogorvoslati tájékoztatás	A változásokat követő 15 napon belül	Az előző állapot törlendő
23.	A közfeladatot ellátó szerv által megkötött, a közadatok újrahasznosításáról szóló törvény szerint kötött kizárólagos jogot biztosító megállapodások szerződő feleinek megjelölése, a kizárólagosság időtartamának, tárgyának, valamint a megállapodás egyéb lényeges elemeinek megjelölése	A változásokat követő 15 napon belül	Az előző állapot törlendő
24.	A közfeladatot ellátó szerv által kötött, a közadatok újrahasznosításáról szóló törvény szerint a kulturális közadatok digitalizálására kizárólagos jogot biztosító megállapodások szövege	A változásokat követő 15 napon belül	Az előző állapot törlendő
25.	A közadatok újrahasznosításáról szóló törvény szerinti azon jogszabály, közjogi	A változásokat	Az előző állapot

	szervezetszabályozó eszköz, közszolgáltatási szerződés vagy más kötelező erővel bíró dokumentum (vagy az annak elérhetőségére mutató hivatkozás), amely az újrahasznosítás céljából rendelkezésre bocsátható közadat gyűjtésével, előállításával, feldolgozásával és terjesztésével összefüggő költségek jelentős részének saját bevételből való fedezését írja elő a közfeladatot ellátó szerv részére	követő 15 napon belül	törlendő

III. Gazdálkodási adatok

	Adat	Frissítés	Megőrzés
1.	A közfeladatot ellátó szerv éves költségvetése, számviteli törvény szerinti beszámolója vagy éves költségvetési beszámolója	A változásokat követően azonnal	A közzétételt követő 10 évig
2.	A közfeladatot ellátó szervnél foglalkoztatottak létszámára és személyi juttatásaira vonatkozó összesített adatok, illetve összesítve a vezetők és vezető tisztségviselők illetménye, munkabére, és rendszeres juttatásai, valamint költségtérítése, az egyéb alkalmazottaknak nyújtott juttatások fajtája és mértéke összesítve	Negyedévente	A külön jogszabályban meghatározott ideig, de legalább 1 évig archívumban tartásával
3.	A közfeladatot ellátó szerv által nyújtott, az államháztartásról szóló törvény szerinti költségvetési támogatások kedvezményezettjeinek nevére, a támogatás céljára, összegére, továbbá a támogatási program megvalósítási helyére vonatkozó adatok, kivéve, ha a közzététel előtt a költségvetési támogatást visszavonják vagy arról a kedvezményezett lemond	A döntés meghozatalát követő hatvanadik napig	A közzétételt követő 5 évig
4.	Az államháztartás pénzeszközei felhasználásával, az államháztartáshoz tartozó vagyonnal történő gazdálkodással összefüggő, ötmillió forintot elérő vagy azt meghaladó értékű árubeszerzésre, építési beruházásra, szolgáltatás megrendelésre, vagyonértékesítésre, vagyonhasznosításra, vagyon vagy vagyoni értékű jog átadására, valamint koncesszióba adásra vonatkozó szerződések megnevezése (típusa), tárgya, a szerződést kötő felek neve, a szerződés értéke, határozott időre kötött szerződés esetében annak időtartama, valamint az említett adatok változásai, a védelmi és biztonsági célú beszerzések adatai és a minősített adatok, továbbá a közbeszerzésekről szóló 2015. évi	A döntés meghozatalát követő hatvanadik napig	A közzétételt követő 5 évig

	CXLIII. törvény 9. § (1) bekezdés b) pontja szerinti beszerzések és az azok eredményeként kötött szerződések adatai kivételével A szerződés értéke alatt a szerződés tárgyáért kikötött – általános forgalmi adó nélkül számított – ellenszolgáltatást kell érteni, ingyenes ügylet esetén a vagyon piaci vagy könyv szerinti értéke közül a magasabb összeget kell figyelembe venni. Az időszakonként visszatérő – egy évnél hosszabb időtartamra kötött – szerződéseknél az érték kiszámításakor az ellenszolgáltatás egy évre számított összegét kell alapul venni. Az egy költségvetési évben ugyanazon szerződő féllel kötött azonos tárgyú szerződések értékét egybe kell számítani		
5.	A koncesszióról szóló törvényben meghatározott nyilvános adatok (pályázati kiírások, pályázók adatai, az elbírálásról készített emlékeztetők, pályázat eredménye)	Negyedévente	A külön jogszabályban meghatározott ideig, de legalább 1 évig archívumban tartásával
6.	A közfeladatot ellátó szerv által nem alapfeladatai ellátására (így különösen egyesület támogatására, foglalkoztatottai szakmai és munkavállalói érdek-képviseleti szervei számára, foglalkoztatottjai, ellátottjai oktatási, kulturális, szociális és sporttevékenységet segítő szervezet támogatására, alapítványok által ellátott feladatokkal összefüggő kifizetésre) fordított, ötmillió forintot meghaladó kifizetések	Negyedévente	A külön jogszabályban meghatározott ideig, de legalább 1 évig archívumban tartásával
7.	Az Európai Unió támogatásával megvalósuló fejlesztések leírása, az azokra vonatkozó szerződések	Negyedévente	Legalább 1 évig archívumban tartásával
8.	Közbeszerzési információk (éves terv, összegzés az ajánlatok elbírálásáról, a megkötött szerződésekről)	Negyedévente	Legalább 1 évig archívumban tartásával