DOI: 10.31915/NWS.2019.4

GDPR és a köznevelési intézmények – a GDPR bevezetésének 13+1 lépése a köznevelési intézményekben

Albert Ágota
adatvédelmi tisztviselő
dralbertagota @gdprszakszeruen.hu

GDPR in the institutions of public education
The topic of this presentation is the steps of the formation of an adequate data protection of the GDPR instructions in the institutions of public education and the discussion of the most important problems, which are particularly related to these institutions: how can we start becoming GDPR-compatible? What are the greatest obstacles (besides the issue of how to take pictures) and „how we can put out the fire"? How does an institution of public education differ from a „simple" member of any market?

Since the 25th of May, 2018, these institutions – independent from their maintainer – are being regulated by the GDPR, which means a great challange to them. Apart from the vast amount of data that has to be processed daily, they face situations like

- the processing of data is regulated by a number of sector laws (law on educational register, law on public education, Public Servants' Act, Labour Code, law on taxes, etc.)
- the special composition of the data subjects (children, parents, employees, other data subjects)
- as data controllers they have complex social network (maintainer, local authority, community of parents, student organizations, churches, supervising organs, different authorities, business partners, foreign partner intitutions etc.), through which significant transfers of personal data happen
- they can process data not only as data controllers but also as data processors, (e.g.: secondary school entrance exams, organizing high level „érettségi" etc.) and
- the supervision of employees and students requires a different approach from schools than from a traditional member of the market (using the followings (e.g.): register of working hours, video monitoring system, smart devices and internet in the possession of institutions).

Keywords: GDPR, public education, data protection

Hogyan válhat egy intézmény GDPR-kompatibilissé?

1. lépés

Tudatosítsuk, a GDPR igen is vonatkozik az intézményünkre. Ha homokba dugjuk a fejünket és azt mondjuk hogy nem, attól még igen. Sőt, mindenért az adatkezelő, azaz az intézményvezető a felelős egyszemélyben. Azonban nem elég, ha csak az igazgató érzi úgy, a nyakába szakadt még egy teljesítendő feladat, hanem az

iskola minden alkalmazottjának tudnia kell, ha adatot kezel, azt a GDPR előírásainak megfelelően kell tennie. Vonatkozik ez az osztályfőnökökre, a rendszergazdára, az iskolapszichológusra és a portásra is, mindenkire, aki valamilyen módon személyes adattal kapcsolatba kerül. Természetesen más adatokhoz fér hozzá egy gazdasági és másokhoz a könyvtáros, éppen ezért fontos, hogy mindenki tisztában legyen a jogosultságával és felelősségi körével.

2. lépés

Vegyünk igénybe szakembert. A rendelet alkotói úgy gondolták, az iskolák mint közérdek alapján közfeladatot végrehajtó intézmények az adatvédelem szempontjából „veszélyes üzemek", ezért kötelező adatvédelmi tisztviselőt (a szakzsargonban DPO-t) kinevezniük. Ez a fenntartó kötelessége, a kinevezés elmaradása GDPR-ellenes. Az adatvédelem speciális ismereteket követel, amelyek nem lesznek meg attól, hogy például egy pedagógusra rátestáljuk ezt a feladatot. Sőt, előtanulmányok nélkül egy-két napos intenzív GDPR kurzus is maximum annyira elég, hogy az áldozatban tudatosuljon, mennyi mindent nem tud. Olyan személy sem lehet DPO, aki munkaköréből adódóan felelős az adatvédelmi szabályozás betartásáért (pl. az intézmény vezetője).

Az adatvédelmi tisztviselő csak tanácsokat adhat, a döntés az adatkezelőé, ahogy a felelősség is.

3. lépés

Térképezzük fel, milyen személyes adatokat kezel az iskolánk. Ahogy az egészségügy, úgy a köznevelés is elképzelhetetlen adathegyek nélkül.
Az adatok feltérképezéséhez elkerülhetetlen az olyan alapfogalmak megismerése, pl. mi a személyes adat és mit jelentenek a személyes adat különleges kategóriái, hiszen ezek pontos behatárolása nélkül elsikkadhatnak igen fontos adatkezelések. Személyes adat egy osztályzat? Igen. És különleges személyes adat az, hogy Bence vagy Hanna mogyoróallergiás? Igen. És az személyes adat, hogy az ötödikesek közül a magas vörös kölyök intőt kapott? Igen, amennyiben az ötödikesek között annyi magas vörös kölyök van, hogy már ennyi információval is beazonosítható az adott diák.

A harmadik lépés tehát fellelni az intézményben a személyes adatokat, beazonosítani az adatkezeléseket és olyan adattérképeket gyártani, amelyek alapján tisztázható egy-egy adat életútja, azaz

- melyik adat honnan és hogyan érkezett be (szülőtől, tanulótól, fenntartótól stb.),
- ki kezeli azt házon belül (titkárság, osztályfőnök, gazdasági kolléga stb.),
- hol és hogyan tároljuk (papíron, elektronikusan vagy mindkettőn),
- hogyan, hova és mi alapján továbbítjuk (lásd a köznevelési törvény felsorolását) és
- mikor kell leselejtezni (megsemmisíteni) azt.

4. lépés
Tisztítsuk meg az adatvagyont. A felesleges munka elkerülése érdekében el kell döntenünk, hogy mely adatot kezelhetjük tovább és melyet nem. Főbb szempontok:

- **az adott adat kezelése megfelel az alapelveknek?** Jogszerűen, tisztességesen és átláthatóan kezeljük?
- **van jogalapunk az adott személyes adat kezelésére?** Ha nincs, akkor vagy teljesíteni kell a hivatkozott jogalaphoz szükséges feltételt (pl. be kell szerezni a hozzájárulást), vagy kíméletlenül ki kell selejtezni (meg kell semmisíteni) azt. A „mindig így szoktuk" jogalapot a GDPR nem ismeri, a hozzájárulás pedig – a közhiedelemmel ellentétben – nem univerzálisan használható jogalap, mivel az bármikor visszavonható, illetve egyes helyzetekben (pl. alá- és fölérendeltségi viszonyban, megkérdőjelezhető önkéntesség esetén) nem alkalmazható.
- **időben szavatos még az adott adat?** A vonatkozó jogszabályok (pl. 20/2012. (VIII. 31.) EMMI rendelet 1. sz. melléklete), illetve az intézményünk irattári terve tájékoztatást nyújt, hogy melyik adat meddig őrizhető. Ha lejárt a megőrzési idő, a kezelés nem jogszerű.
- **szükség van az adott adatkezelésre? Van konkrét cél** vagy csak raktározzuk az adatot, majd csak jó lesz valamire? Ha nincs cél, az adat kezelése nem jogszerű.
- **az adatkezelés céljának eléréséhez feltétlen szükség van az adott adatra?** A GDPR elkötelezett híve az adattakarékosságnak, azaz nem támogatja olyan adat kezelését, amely nem szükséges az adott cél eléréséhez. A felesleges adatoktól szintén meg kell szabadulnunk.
- **helyes, pontos az adat?** Ha nem az, akkor kijavítható, helyesbíthető? Ha nem, döntenünk kell a sorsáról. A pontatlan, hibás személyes adat is személyes adat.
- **megfelelő biztonságot biztosítunk az adatnak?**

Minél nagyobb és minél régebbi az intézményünk, annál nagyobb a feltérképezés és kiválogatás munkaigénye, ráadásul nem ez az a feladat, amit gyakornokokra felelősen rá lehetne bízni.

Ha lekarcsúsítottuk az adatvagyonunkat, jöhet az **adattérképek újrarajzolása**. Ezek már alkalmas kiinduló pontjai az iskola adatkezelési nyilvántartásának, amely a GDPR alapján kötelező, és amelyet egy adatvédelmi hatósági ellenőrzés során – az elszámoltathatóság elvének megfelelően – be kell tudni mutatnunk. Ahogy az iskola leltározza a számítógépeit, labdáit meg csontvázait, úgy az adatkezeléseit is leltároznia kell.

5. lépés
Határozzuk meg az egyes adatkezelések követelményeit. Az adatkezelések döntő többségében jogszabályok határozzák meg, hogy milyen adatot kezelhet, hova továbbíthat az iskola. Az iskolák közérdekű feladataik végrehajtásához szükséges adatkezeléseknél a jogalap a GDPR 6. cikk (1) bekezdés e) pontjában meghatározott közérdek lesz és ez a jogalap – a felügyeleti hatóság álláspontja szerint – elnyeli a

további adatkezelési jogalapokat, valamint be kell tartani a GDPR alapelveit is.

Vannak olyan adatkezelések, amelyek bonyolultabbak, mint egy átlag munkáltató adatkezelései. Egy iskolában pl. sokkal nehezebb a munkahelyi és magánhasználatot elkülöníteni – decemberben a pedagógus használatában lévő számítógépről keresett beigli recept a karácsonyi vacsorához kell vagy a hagyományokkal foglalkozó osztályfőnöki órára? A cicalány007@ e-mail cím a titkos barátnő címe vagy egy diák anyukájáé, netalán magáé a diáké? Talán nincs még egy olyan munkáltató, ahol a magánszférát olyan nehéz elválasztani a munkahelyi kötelezettségek teljesítésétől, mint egy átlagos iskola.

Lehet még „problémás" adatkezeléseket sorolni, pl. a „normál" körülmények között általában jogos érdekre hivatkozó adatkezelésekhez milyen jogalap használható az iskolákban? Például:

- az intézményben felszerelt kamerák felvételeivel,
- a diákok internethasználatának ellenőrzésével,
- az iskolai rendezvényen készült tömegfelvételekkel kapcsolatos adatkezelés, amelyeken nemcsak a ballagó diák van, hanem közeli és távoli rokonsága nullától száz éves korig, és amely képek a modern technikának köszönhetően bármikor portréfotó minőségre nagyíthatók.

Az adattovábbítások vizsgálata is szükséges, hiszen az iskola nemcsak jogszabály alapján továbbít adatokat harmadik személyeknek, hanem pl. testvériskolai kapcsolattartás vagy versenyekre jelentkezés keretében is. Sőt, iskolai kórustalálkozót szervezhetnek pl. Kínában, amely harmadik országnak számít, szállást pedig oda is foglalni kell sok-sok személyes adat megadásával. Ráadásul az adattovábbítást nyilván kell tartanunk, különben hogyan fogjuk tudni megmondani az érintettnek, hogy mikor, hova, kinek, mi alapján és milyen garanciákkal továbbítottuk a személyes adatait?

Kétségeink eldöntésében segítséget nyújthatnak a NAIH anyagai.[1]

6. lépés

Igazítsuk a belső szabályzatainkat és utasításainkat a GDPR előírásaihoz. Az iskoláknak kötelező adatvédelmi szabályzatot készíteniük, a GDPR azonban a konkrét tartalmat az adatkezelőre bízza.

Mi legyen benne? Amit fontosnak tartunk, pl.:

- adatkezelések részletes leírása, különösen a speciális eseteké (pl. tanulmányi és tantestületi kirándulással, iskolaújsággal, intézményi honlappal kapcsolatos adatkezelések, dokumentum másolatok kezelése stb.)
- adatfeldolgozókkal kapcsolatos rendelkezések, illetve az olyan adatkezelések leírása, amelyek esetében az iskolánk adatfeldolgozó (pl. központi felmérések, tanulmányi versenyek stb.)

1 https://www.naih.hu/adatvedelmi-allasfoglalasok,-jelentesek.html

- érintetti jogok leírása és a jogok érvényesítésének módja (az érintetti tájékoztatás formái és kötelező tartalma, érintetti kérelmekre válaszadásnak, a hozzájárulás visszavonásának, az adatkezelés ellen tiltakozásnak, törlési kérelemnek adminisztrációja stb.)
- kötelező, illetve elszámoltathatósági szempontból fontos nyilvántartások tartalma (pl. az adatkezelések, adattovábbítások és adatvédelmi incidensek nyilvántartása stb.)
- adatvédelmi incidens esetén követendő protokoll előre elkészített nyomtatványokkal, nehogy a nagy kapkodásban kimaradjon valami,
- olyan speciális adatkezelések, mint osztálycsoport létrehozása közösségi oldalon, oktatással kapcsolatos appok használata (pl. Kahoot!), tanárok-diákok saját IoT-eszközeinek használata stb.
- beépített adatvédelem érvényesítéséhez szükséges eljárások (pl. adatok biztonságos tárolásának, továbbításának módja, jogosultságok kiosztásának elvei stb.)
- az adatvédelmi tisztviselő feladatai és hatásköre.
- Az adatvédelmi és adatbiztonsági szabályzaton kívül szükségünk van még egyéb dokumentumokra is, pl.
- speciális szabályzatok megalkotása (kameraműködtetési, beléptetési, informatikai, információ biztonsági, image policy stb.)
- érdekmérlegelési tesztek végzésének eljárásrendje, kockázatfelmérés és kezelés módszerei stb.

7. lépés
Készítsük el az adatkezelési tájékoztatókat. A GDPR sarkalatos pontja az érintettek tájékoztatása, ennek elmaradása komoly szankciókat vonhat maga után annyi kedvezménnyel, hogy költségvetési intézmény esetén a maximális közigazgatási bírság 20 millió forint.

Milyen tájékoztatókra van szükség? Célszerű minimum három adatkezelési tájékoztatót készíteni, egyet a diákoknak, egyet a szülőknek, egyet pedig az alkalmazottaknak. A fenntartónak gondolnia kell még olyan egyéb érintettekre is, mint pl. a szerződéses partnerek, nekik is kell készíteni tájékoztatót.

Az általános adatkezelési tájékoztató általában az iskola honlapján kap helyet, de mindenképpen kell nyomtatott verzió is, amely az intézmény titkárságán bármikor elérhető. A speciális, egy-egy adatkezelésre vonatkozó tájékoztatók helyet kaphatnak pl. a beiratkozási és hozzájárulást kérő nyomtatványokon is, így később nincs vita a tekintetben, hogy megtörtént-e az érintettek szükséges tájékoztatása.

8. lépés
Ültessük át a gyakorlatba a gyerekekkel kapcsolatos eltéréseket. Pl. mi legyen a 14-18 év közötti gyerekkel illetve akkor, ha nagykorú lesz a diák? Ki férhet hozzá a tanuló adataihoz, ki gyakorolja a szülői felügyeleti jogot? A szülőnek mindenről joga van tudni, vagy adott esetben a szülővel szemben is védeni kell a gyermek jogait? Elmondhatja-e az iskola, hogy informatika órán milyen témákra keresett

rá a tinédzser a neten, vagy jobb ezekről hallgatni? Milyen plusz garanciákat kell beépíteni az adatkezelésekbe akkor, ha az érintett 18 éven aluli?

A GDPR alapján a diákoknak szóló adatkezelési tájékoztatót úgy kell megfogalmazni, hogy korosztályuknak megfelelő mértékben ők is megérthessék az abban foglaltakat és legyenek tisztában pl. azzal, hogy nem kell nekik olyan fotót eltűrniük az iskola honlapján, amelyen nagyon nem tetszenek maguknak. A tájékoztató készülhet sok oldalas írásos verzióban, de érdemes megfontolni a videofilm vagy képregény formátumot is.

9. lépés
Tegyünk azért, hogy az érintettek gyakorolhassák jogaikat, betartva a jogszabályban foglalt határidőt. Nem szabad elfelejtenünk, hogy a szülők speciális érintettek egyrészt saját jogon, másrészt gyermekeik miatt, frusztrációjuk pedig az egeket verheti pl. azért, mert a fiuk vagy lányuk egyfolytában a fülüket rágja, milyen előnytelen kép van róluk az iskola honlapján és legyenek szívesek, intézkedjenek a kép eltávolíttatása érdekében. Éppen ezért célszerű az érintetti kérelmek megfelelő rendezése érdekében a belső adatkezelési szabályzatban részletesen rögzíteni az eljárásrendet és minden esetben bevonni az adatvédelmi tisztviselőt is.

10. lépés
Alakítsuk ki az adatvédelmi incidens protokollunkat – és nemcsak a leírása fontos, hanem a begyakorlása is, akár próbaincidens keretében. A 72 órás hatósági bejelentési határidő nagyon rövid és minden egyes bejelentés egyben önfeljelentés is, amely vizsgálatot von maga után. Az incidenskezelés pedig nem annyi, hogy széttárjuk a kezünket, ez most így sikerült, máskor majd biztos gondosabbak leszünk és kicsit nehezebben lopják majd el a tanáriból a nyitott ablakon keresztül azt a laptopot, amely titkosítás nélkül tartalmazott adatot több száz gyerekről és szüleikről.

11. lépés
Ne felejtkezzünk el a beépített adatvédelemről. A GDPR összetolja az adatkezelést és az adatvédelmet, az adatkezelőnek pedig mindent meg kell tennie annak érdekében, hogy az érintettek a lehető legnagyobb biztonságban tudják a személyes adataikat. Az adatbiztonság fontos része pl. a számítógépes rendszer védelme, de ide tartoznak olyan triviális dolgok is, mint a jogosultságok kiosztása, a jelszavakkal kapcsolatos előírások betartatása, a rendszeres biztonsági mentés, a tiszta asztal politika, a szekrények és fiókok zárása, a leselejtezett papírok megsemmisítése stb. Ajánlatos megismerkednünk olyan technikákkal is, mint az álnevesítés, az anonimizálás és a titkosítás és figyelembe kell venni mindezeket már az adatkezelések megtervezése folyamán is.

12. lépés
Oktatás és bevezetés. A polcra feltett 500 oldalnyi szabályzat még nem jelenti azt, hogy az iskolánk megfelel a GDPR követelményeinek. Az adatvédelmi kultúrának be kell épülnie a mindennapokba, és nemcsak beépülnie kell, hanem bizonyítanunk

is tudni kell, hogy a rendeletnek megfelelően jártunk el. Ehhez szükséges az alkalmazottak képzése, hiszen nem egy személyben az igazgató kezeli az adatokat, hanem minden egyes tanár, pedagógiai asszisztens és még a portás is. Ez nem azt jelenti, hogy mindenkinek tudnia kell mindent, hanem azt, hogy a saját területén mindenki sajátítsa el a szükséges ismereteket, és ne csak bemagolja, hanem alkalmazza is az előírásokat. Az elvileg és általában képzéseknek semmi értelme, csakis annak, ha az alkalmazottak munkaköri szintjükhöz kapcsolódva szereznek értelmezhető tudást.

13. lépés

Nemzetközi kapcsolatok. Az iskoláknak szerteágazó nemzetközi kapcsolatai lehetnek, és nemcsak a nemzetiségi iskoláknak, hanem a két tanítási nyelvűeknek, nyelvtagozatosoknak és a „sima" intézményeknek is. A nemzetközi kapcsolatok elengedhetetlen része az adattovábbítás külföldi illetőségű adatkezelő vagy nemzetközi szervezet számára, akár személyes adatok, akár különleges adatok formájában. A GDPR alapján az Európai Gazdasági Térség országai belföldnek számítanak és vannak olyan országok is, amelyek a Bizottság véleménye szerint garantálják az uniós védelemnek megfelelő védelmi szintet, ilyen pl. Svájc, Japán és Uruguay, míg olyan országok, mint az Egyesült Államok, Ukrajna vagy Szerbia harmadik országnak számítanak. Ezekbe az országokba irányuló adattovábbítás esetén speciális feltételeknek kell teljesülnie, amelyek fennállását az iskolának kell bizonyítania akkor is, ha csak Kárpátaljára ruccan ki egy pár napra a 10/a. osztály.

13 + 1. lépés

Kövessünk nyomon az eseményeket és reagáljunk, ha szükséges. Kétszer ugyanabba a folyóba nem lehet belelépni és ez igaz az adatvédelemre is. Még ha az uniós rendelet maga nem is változik gyakran, a hazai ágazati jogszabályok bármikor módosulhatnak, ahogy várhatóan a jogértelmezés is idővel egyre kifinomultabb lesz. Nemcsak arra van szükség, hogy az iskola ellenőrizze a saját adatvédelmi gyakorlatát és folyamatosan az újabb és újabb igényekhez igazítsa azt, hanem arra is, hogy a jogértelmezésnek megfelelő irányvonalat kövesse. Ez az a terület, ahol szintén elengedhetetlenül szükséges az adatvédelmi tisztviselő közreműködése.