2. METHODOLOGY TO IMPLEMENT AND AUDIT OF A PRIVACY MANAGEMENT SYSTEM CONCERNING MONITORING IN EMPLOYMENT RELATIONSHIPS

Balázs Rátai, Tamás Szádeczky,
Gergely László Szőke

1 December 2012

2.1. The concept of the Code of Conduct

2.1.1. The general or the specific nature of the Code

When developing the Code, first of all it has to be clarified how detailed the provisions pertaining to employee monitoring should be.

Having studied the German and Hungarian regulation on data protection in employment relationships, in particular monitoring employees with technical equipment, the conclusion could be drawn that general rules were quite rare in a regulatory environment based on fragmentary case law. The lawfulness of the use of a device for monitoring/surveillance in a workplace depends on the actual features of the given case: the nature of employment, the provisions of all the rules and regulations concerning to the given employment relation (including both the general and sectoral data protection rules and the special rules pertaining to employment relations), the technical features of the monitoring device, the purpose of monitoring etc.

2.1.2. The wide scope of applicability of the Code

When developing the universal Code of Conduct, we strove to make it applicable in a wide area regardless of the nature of employment and domestic regulation. This ensures that the achievements of the research program can be applied in a wider scope than the participating countries (Germany and Hungary), i.e. in other EU Member States as well.

Taking into consideration what has been said so far, it seems impossible to develop a Code of Conduct with a very special detailed rules applicable without any changes to diverse employment relations and actual cases all over Europe.

However, a Code with a too general wording cannot mean too much real help for employers. To this end, jurisdiction specific Codes focusing on either domestic law or on a special area of law can be developed to supplement the universal Code of Conduct. We developed two national Codes with somewhat different approaches within the framework of the project.

The Code focusing on Hungarian jurisdiction – due to the lack of sectoral regulation and fragmentary legal practice – is in fact a kind of aid for the interpretation and implementation of the universal Code of Conduct. It specifies no further normative rules or at least only a few, it rather collects what other sources of law pertaining to a given issue must be taken into consideration.

It is a bit more feasible to create a detailed normative regulation in Germany mainly due to the greater volume of case law and in particular to the extensive legal literature dealing with it.

Thus, when developing the universal and the national Codes, we followed a fairly open concept which makes it possible that the results of the research can be utilized in all EU Member States and not only in two of them. The general nature of the provisions of the universal Code of Conduct and its approach based on "management system" enable the development of further jurisdiction specific Codes for either a particular EU Member State or a certain sector (e.g. healthcare) within a Member State.

2.1.3. Approach based on "management system"

It follows that the role of the Code is not to function as a model-law[66] and make it possible for the employer to adopt it without any further measures as the internal regulation of monitoring in employment relationships. Instead, the Code tries to regulate data protection issues at local level by establishing a data protection management system modelling on ISO standards, in particular ISO 9001 and ISO 27001 and provides guidelines for it.[67]

The Code of Conduct only partially describes what an employer can or cannot do while monitoring employees, it rather places the emphasis on how the employer can develop a system which in the end guarantees the lawfulness of control at the workplace.

[66] It should be noted that some special model-regulations for the internal regulation of particular technologies are offered in special literature. For the details of jurisdiction specific regulations concerning the USA see Guerin, 2011, while for the analysis and proposals on the implementation of the code created by the Information Commissioner of the United Kingdom see Macdonald, 2008, pp. 160-190.

[67] Establishing a data protection management system also appeared in the data protection audit concept of Alexander Roßnagel. Roßnagel's theory is cited in Balogh/Jóri/Polyák, 2002, pp. 340-343.

2.1.4. Applicability and certifiability

The advantages of and motivations for data protection auditing and certification have already been described,[68] nevertheless it should be emphasised that only methods raising the actual level of data protection which do not impose unreasonable obligations on the organisations concerned are worth elaborating. Thus, when developing the Code, it was an important aspect that the Code can be introduced gradually at the certain data controller and – mainly the first steps – should not impose an unreasonable burden on the implementing organisations in terms of money and workload.

In addition, further important aspects were the applicability and certifiability of the Code, in other words it should contain requirements the fulfilment of which can objectively be checked, consequently it can clearly be decided whether the measures of the given employer comply with the provisions of the Code or not.

2.2. The implementation of the Code: establishing a data protection management system

The implementation of the Code can basically be carried out by establishing a data protection management system for monitoring employees with technical devices. In this research data protection management system does not mean a requirement concerning a certain technical system; this notion can be defined like the notions of quality control and information security management systems. A management system is a system to establish policy and objectives and to achieve those objectives.[69] A quality management system is a management system to govern and control an organization with regard to quality.[70] Consequently, the definition of a data protection management system can be given by replacing one word: a management system to govern and control an organization with regard to the protection of personal data. From a conceptual point of view, there is not too much difference between the data protection management system and the other management systems except that legal and not technical requirements pertain to it.

The major steps of establishing a data protection management system on the basis of the Code are:

1) Collecting the binding rules applying to the given organisation.
2) Preparing the appropriate internal documentation.
3) Adjusting the actual operation of the organisation to the documentation.

[68] See Chapter 1.3.3.
[69] MSZ EN ISO 9000:2005, 3.2.2.
[70] MSZ EN ISO 9000:2005, 3.2.3.

2.2.1. Collecting the binding rules

It is expressly highlighted in the Code that it shall not replace any binding rules and regulations of the given state, moreover one of the first steps the organisation has to take in the process of the implementation of the Code is to collect all relevant rules applying to monitoring in employment relationships. These include first of all the general and sectoral data protection statutory instruments, statutory instruments pertaining to employment relations, further special rules and regulations of the given industrial sector (collective agreements, codes of conduct of the industrial sector, instructions issued by the superior organ, etc.) and finally the universal Code of Conduct itself. In addition to the binding rules, conclusions drawn from the case law of the courts and the data protection authority are advised to be treated as compulsory requirements. Jurisdiction specific codes of conduct are great help when collecting these binding rules.

2.2.2. Preparing the appropriate internal documentation

Once the rules are collected, the internal documentation complying with them has to be prepared. At least four documents are required for the implementation of the Code of Conduct:

1) Applicability Statement;
2) Privacy Policy;
3) Information documents;
4) Account of security measures.

2.2.2.1. Applicability Statement

Annex I of the Code of Conduct contains the Applicability Statement. The Statement is like a questionnaire and when the data controlling organisation fills it in, it makes a statement how each provision of the Code is realised at the given organisation.

While filling in the Applicability Statement, the data controller thoroughly examines its own data processing procedures and makes a catalogue of them. In respect of the controlling/monitoring technologies related to data processing, it stipulates their

- purpose;
- the causal relationship between the aim to be reached and the application of technology;
- the legal basis of data processing; and
- the retention period of data.

In addition, it also makes a statement on

- how those concerned are informed;
- whether secret monitoring is performed and if yes, under what terms and conditions;
- what data protection measures have been introduced;

- what form the co-operation with employees takes;
- how those participating in data processing are trained;
- what form the data protection documentation takes; and finally
- how it concretises the provisions of the Code (e.g. in a privacy policy)

in the course of data processing.

2.2.2.2. Privacy Policy

The implementation of the Code technically means the creation of an internal regulation (privacy policy) or the amendment of an existing one. The policy must expressly deal with all the issues mentioned in the Applicability Statement and must do so in compliance with it, moreover express reference must be made to specify which particular provision of the Code each provision of the policy serves (section 12.1 of the Code expressly requires it).

2.2.2.3. Information documents

One of the key requirements concerning the protection of personal data is the appropriate and detailed information of those concerned.[71] Section 6 of the Code expressly provides that employees must be informed. A possible method of informing employees is to refer to the relevant privacy policy in respect of matters of detail when informing employees about the fact of data controlling.

2.2.2.4. Account of security measures

Taking appropriate data security measures is a further statutory requirement. As it is expressed in Chapter 3.4, it is hard to say what actual measures are required to achieve statutory compliance. Information security standards may provide guidance for such issues but most of the organisations do not apply or get such standards certified. Thus the implementation of the Code basically expect the data controlling organisation to sum up what measures it takes for the sake of information security in a document.

2.2.3. Adjusting the actual operation of the organisation to the documentation

Once the above steps have been taken, there is only one thing that can ensure the enforcement of the Code, namely if those laid down in the documents described above are actually realised (at the level of "real actions"): the employer really provides the new employees with the relevant information, access to certain personal data is really restricted etc. It should be noted that the realisation of such activity is also advisable to be recorded in one way or another, which later may be used as audit evidence in the course of auditing and certification.

[71] Articles 10-11 of Directive 95/46/EC, Section 20 of the new Act on Data Protection

A key element in the implementation of the privacy policy can be the appropriate training of the employees taking part in data processing, which is also provided for in the Code. However, carrying out the information security and data processing training programmes is not a trivial task at all, but participants can be made committed by a complex motivation system.[72]

2.3. Audit and certification of data protection management systems

The audit and certification of a data protection management system presupposes the establishment of a system described in the previous section. The audit is to assess the compliance of this system.

Now we would like to describe the methodology of the audit and certification of data protection management systems. When developing this methodology, auditing does not have to be "re-invented", financial auditing and management systems auditing have a substantial literature and practice, and there are some widely used special methodologies for auditing data protection management systems as well. As it has already been mentioned, the methodology described in this chapter relies on the norm system of the ISO family of standards relating to management systems and their certification,[73] the relevant Workshop Agreements of the CEN and the auditing methodology developed by the Information Commissioner of the United Kingdom.

The workshop agreements elaborated by the European Committee for Standardization provide general technical descriptions (which generally can be given in the form of an algorithm)[74] and a requirement-system in the area of data protection on the basis of the data protection directive. Thus for example a checklist covering the full scope of data protection documentation can be created on the basis of the workshop agreement and national requirements:

- Copies of the notifications submitted to the authorities[75].

[72] Herold, 2011. p. 7. pp. 36-41.

[73] There are several standards for the audit and certification of management systems, such as:

- ISO 9001:2008 Quality management systems – Requirements
- ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 17021:2011 Conformity assessment – Requirements for bodies providing audit and certification of management systems
- ISO 19011:2011 Guidelines for auditing management systems
- ISO/IEC 27006:2011 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007:2011 Information technology – Security techniques – Guidelines for information security management systems auditing

[74] Turning the text of statutory instruments and regulations into the form of an algorithm and creating from it a formally accountable system of requirements is not an easy task but is essential when it comes to performing an audit. How to turn a privacy policy into an algorithm has its own fascinating special literature but this direction of research exceeds the limits of this study (on this issue see Dehghantanha, 2011.)

[75] It means the data protection authority or any supervisory organization to which reports on data protection and data security must be submitted or which exercise such supervision.

- Acknowledgements of receipt by the authority.
- Internal procedures, instructions or guidelines regarding the obligation to notify the authorities.
- Announcements, letters and leaflets on data protection.
- Internal procedures, instructions or guidelines regarding the obligation to notify those concerned.
- The internal document defining the legal ground for and the purpose of data processing.
- Internal procedures, instructions or guidelines for collecting and processing personal data.
- Internal regulations, procedures, instructions or other guidelines concerning data retention periods, archiving and the destruction of personal data.
- Internal procedures, instructions or guidelines concerning the quality (accuracy, completeness and up-to-date status) of personal data.
- Information on the rights of the data subject and the regulation and information on the possibility of legal remedy.
- Information security policy.
- Information security plan (system plan, disaster plans).
- Requirements for protection when performing administrative work.
- Procedures, instructions or guidelines regarding safeguarding and transporting data carriers.
- Procedures regarding back-up copies.
- Plans and instructions regarding spare copies, reconstruction and contingency.
- Plans and instructions regarding archiving and destroying data.
- Rules concerning sending personal data by post or by e-mail and e-mail code of conduct.
- Authentication procedure.
- Instructions regarding secrecy and handling security incidents and system faults.
- Contracts with data processors, including detailed rules on data processing.
- Documentation concerning the periodical checks of compliance with legal provisions (internal and external audits, inspections by the authorities).
- Permission from competent authority to transfer data across international borders, binding corporate rules (BCR), evidence regarding the appropriateness of storing data in a third country, internal procedures, instructions or guidelines.
- Data protection policy (descriptions of personal data protection objectives and strategy).
- Guidelines regarding the collection of personal data.
- Guidelines regarding the handling of personal data.
- Guidelines regarding the disclosure and transfer of personal data.
- Guidelines regarding the deletion of personal data.
- Procedure regarding the handling and reporting of abuses of personal data or complaints about personal data protection.
- A description of the internal data protection organization (organogram and persons responsible).
- The job description of the head of the internal data protection organization.

- Data protection filing guidelines.
- Data protection plan and data protection communication plan.
- Detailed descriptions of data processing operations.
- Materials on data protection used to train, inform and raise the awareness of management and employees.
- Self-assessment reports and internal and external audit reports.
- Guidelines regarding what to do in case of new, changed or stopped data processing operations.
- Instructions regarding measures concerning privacy enhancing technologies (PET).
- Information on the characteristics of the infrastructure in which personal data is processed (hardware, data carriers, software, networks, databases, plans for architecture).

2.3.1. The provisions of the Code of Conduct on auditing

As it has already been mentioned, when developing the Code of Conduct, the aim was to create a system of norms which can be certified. Section 13 of the Code provides for the assessment of compliance and the explanation attached to it lists the requirements on the basis of which compliance or non-compliance can be established. The Code specifies that the condition of the issuance of a certificate is a positive audit report. The certificate is valid for three years, the condition of which may be an annual internal audit required on the basis of the audit report.

Auditing and certification carried out in line with the Code of Conduct is basically a system audit performed by an independent external organ and qualifies as a compliance audit with regard to the subject-matter of the inspection as it extends to the actual operation (the practice of data controlling) of the data controlling organisation in addition to the documentation.

2.3.2. The point(s) of reference for compliance

It seems reasonable to briefly state exactly which norm is the basis of the examination of compliance. Firstly and formally the answer is clear: the fulfilment of the requirements of the universal Code of Conduct must be examined during the audit.

However, the Code itself prescribes that the data controller shall comply with all relevant domestic and international binding rules; consequently their collection is indispensable during implementation. It follows that in the course of compliance assessment, compliance with these rules is part of the subject-matter of the inspection, to which national (jurisdiction specific) Codes give great help.

Finally, issues related to information security should be mentioned as a special area. The Code refers to this requirement in general but it is hard to determine in general what actual measures comply with these provisions in each case.

2.3.3. The audit process

2.3.3.1. Principles

Certain general provisions under ISO/IEC 17021 concerning to audit of management systems such as the requirements of impartiality, independence and incompatibility between the audited organization and the auditors (which are also expressly laid down in the Code) can easily be applied in the case of data protection audits. A constant problem of this area is that the standard prohibits certification bodies from performing consultancy work. Its justification is disputed by the profession. We are of the opinion that in the area of data protection audit the exclusion of the conflict of interests in persons is sufficient: in other words the person having participated in the development of the data protection management system as a consultant cannot be the auditor of that particular system.

2.3.3.2. Defining the scope

The first and most important issue in the course of auditing/certification is the definition of the scope, in other words to determine which areas (organisational units) and which instances of data processing it covers.[76] The scope of the auditing performed on the basis of the Code basically overlaps with the scope of the Code: it extends to all instances of data processing related to monitoring by technical means in employment relationships at all organisational units of the given data controller.

The scope of the audit carried out on the basis of the Code of Conduct cannot be determined more widely, but in order to facilitate the gradual introduction of the Code, it is possible to introduce it in a narrower circle and audit only certain instances of data processing at the given organisation. In this case, when issuing the certificate, it must be made clear that the scope of the audit was narrower than that of the Code.

2.3.3.3. Making and implementing an audit plan

Auditing should be carried out in line with a schedule prepared in advance and which is specified in the audit plan. The audit plan includes – among others – the purpose of the audit, the list of the audit criteria and other documents, the scope of the audit, the members of the audit team, their responsibilities, the time, venue and expected duration of the on the spot audit activities etc.[77]

Both on the spot audit activities and the inspection of documents may be necessary in the course of an audit in the interest of collecting audit evidence. Any document concerning data processing[78] and any document obtained during a personal interview can qualify as audit evidence.

The applicability audit and the compliancy audit, which are referred to as the two types of audit, can be regarded as phases of the audit.[79] These two phases are well

[76] MSZ EN ISO 19011:2003, 5.2.2.
[77] MSZ EN ISO 19011:2003, 6.4.1.
[78] Chapter 2.3. contains the exhaustive list of potential documents.
[79] ICO 2001, pp. 3.9, 3.17

worth being separated in the course of auditing under the Code: in the first round the completeness of the collection of rules relevant to the organisation and the compliance of the internal regulations with these rules should be examined, while in the second round the compliance of the actual practice of the data controlling organisation with these internal regulations should be examined.

2.3.3.4. Findings of the audit

As a result of the audit, the compliance or non-compliance of the whole or parts of the system can be established; in addition the audit report may include proposals for improvement. Non-compliance can be established if there is a prescribed requirement which is not fulfilled, it is caused by one or more omissions and there is objective evidence proving non-compliance.

It should be noted that under the provisions of the Code a certificate can be issued only on the basis of a positive audit report, i.e. a report not including non-compliance.

2.3.3.5. Preparing an audit report

The last step of the process of auditing is the preparation of an audit report. The report contains the most important parameters of the audit (such as its purpose, scope and the name of the client), the time and the venue of the on the spot audit activities, the audit criteria and the findings of the audit.[80]

2.3.4. Certification

Some of the advantages of an audit[81] can be exploited only if the efforts taken to this end and the positive results verifying them can appropriately be communicated to the general public. Thus it is advisable to attach the issuance of a certificate to the audit.

Induced by this realization, the Code of Conduct itself provides for the possibility of certification. The Code-related certificate of a Privacy Friendly Workplace can be requested from the organisation authorized to issue this certificate, that is the Research Center for Information and Communications Technology Law of the University of Pécs, Faculty of Law. The certificate can be issued upon the submission of a positive audit report not older than three months. The certificate authorises the given data controller to use the Privacy Seal of a Privacy Friendly Workplace.

Privacy Seal of a Privacy Friendly Workplace

[80] MSZ EN ISO 19011:2003, 6.6.1.
[81] See Chapter 1.3.3.