IMPLEMENTING AND AUDIT OF THE CODES OF CONDUCT

AUTHORS

Dr. Balázs Rátai

Dr. Tamás Szádeczky

Dr. Gergely László Szőke

The Project is co-funded by the European Union's Fundamental Rights and Citizenship Programme

DECEMBER, 2012

CONTENT

1. SELF-REGULATION, AUDIT AND CERTIFICATION SCHEMES IN THE FIELD OF DATA PROTECTION

Author: Gergely László Szőke

1.1. Endeavours toward Self-Regulation

In the absence of a unified regulation at the federal level, industrial self-regulation (relating to data protection) plays an important role in the United States, which is founded on the business-based approach according to which the characters of business life are capable of developing a regulation that meets consumer requirements[1] thereby preventing state regulation.[2]

As opposed to this, in Europe, the adoption of the Data Protection Directive[3] has established a more or less uniform European regulation, which seems to render the different forms of self-regulation less necessary.[4] At the same time, the Directive does not exclude these forms, but rather positively supports them: Article 27 expressly lays down the possibility of adopting codes of conduct. This Article also enables the elaborators of codes to submit them to the opinion of the national data protection authority or to the Article 29 Working Party, which are to determine whether the codes are in accordance with the national provisions.[5] So far only the codes of two organizations have been granted recognition at the European level:[6] that of the International Air Transportation Association (IATA) and that of the Federation of European Direct and Interactive Marketing (FEDMA).

Another possible direction of self-regulation is standardisation, which differs from other forms of self-regulation basically in that it is elaborated within the frames of some organization in charge of standards.[7] Among the most important researches relating to standardisation one may mention the project entitled "Initiative on Privacy Standardization in Europe" (IPSE) launched in 2000 within the frames of the European Committee of Standardization Information Society Standardization System (CEN/ISSS), the final report of which[8] contains numerous important statements concerning the possibilities and limitations of standardisation, questions relating to Data Protection Audit and Privacy Enhancing

[1] Ruiter/Warnier 2011, p. 364.
[2] Jóri, 2005, p. 53.
[3] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[4] See: Bennett/Raab, 2006, pp. 155-159., Robinson/Graux/Botterman/Valeri, 2009, pp. 9-10., and Nouwt, 2010, pp. 284-285. Industrial self-regulation endeavours may fail because of data subjects' lack of „data protection demands" and, in connection with this, also because of the „business" logics of market characters. The former problem could be reduced by increasing data protection awareness. Ilten/Guagnin/Hempel, 2012, pp. 240-241., 246.
[5] Directive 95/46/EC, Article 27
[6] Data from 2009, see: Robinson/Graux/Botterman/Valeri, 2009, p. 9. According to another later source, there is only one recognized code of conduct: that of FEDMA, see: Nouwt, 2010, p. 284.
[7] Dumortier/Goemans, 2000, p. 29.
[8] Initiative on Privacy Standardization in Europe, Final Report CEN/ISSS Secretariat, Brussels, 2002.

Technologies.[9] The document comes to the final conclusion that establishing a global and comprehensive standard is not a timely issue,[10] but there is consensus that further steps should be taken, on the one hand, to analyse the topic and, on the other hand, to elaborate voluntary guidance. As a result of this, an informal standardization document package (referred to as CEN Workshop Agreement) consisting of five documents was born in 2005, followed by another package consisting of additional three documents in 2010.[11] Their contents will be reviewed in the following chapters.[12]

A further possible direction of self-regulation – not replacing but supplementing the ones above – is regulation (policy, rules, Code of Practice, etc.) adopted at the level of the data controller, the scope of which does not extend to whole sectors/branches of industry, but only to the given organization or group of organizations (e.g. group of companies). In this range particular mention should be made of the gaining ground of Binding Corporate Rules,[13] the increasing role of which in data protection regulation (relating primarily to transfers of data to a third country) is also confirmed by the documents of the Article 29 Working Party dealing with BCR.[14] It is also to be noted that several European Acts on data protection require certain organizations to adopt internal rules relating to data protection (and data security) and/or to appoint an internal data protection officer.[15] BENNETT and RAAB also regard Privacy Commitments as a type of self-regulation, behind which, however, there may not always be underlying detailed and thorough codes of practice.[16] Nevertheless, on the whole, the significance of these internal norms will obviously increase as a result of the new regulatory frames of European data protection.

Although throughout this chapter we have consistently used the term "self-regulation", it must be added that – in contradistinction to the United States, for example, – in Europe, codes of conduct, standards or internal forms of regulation cannot typically substitute state regulation, but may rather play the role of supplementary, specifying "rules of implementation", therefore, more precisely, they are to be regarded as co-regulation.

Finally, mention should also be made of the institution of data protection audit and certification (privacy seals)[17] – closely connected with the logics of the former regulatory systems –, which may also be perceived as a system of "supervision" relating to the norms

[9] Privacy Enhancing Technology (PET)
[10] For a summary of the report, see: Jóri, 2009, pp. 289-295.
[11] Winn, 2010, pp. 198-199.
[12] On the role of standardization, see also: Bennett/Raab, 2006, pp. 159-164.
[13] Binding Corporate Rules
[14] See, inter alia: Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data (WP133) Working Document setting up a framework for the structure of Binding Corporate Rules (WP 154), and Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules (WP195).
[15] See, for instance, in Hungary, § 24 of the new Data Protection Act, in accordance with which an internal data protection officer must be appointed and data protection and data security rules shall be adopted by authorities of nation-wide jurisdiction, data controllers and processors engaged in processing data files of employment and criminal records, financial institutions, and providers of electronic communications and public utility services; and in Germany, points 4f-4g of the Federal Data Protection Act (BDSG) on the internal data protection officer.
[16] Bennett/Raab, 2006, pp. 153-154.
[17] Robinson/Graux/Botterman/Valeri, 2009 p. 9.

created within the frames of the various types of self-regulation/co-regulation mentioned above.

Our present research focuses primarily on regulatory measures adopted at the level of the data controller and the possibility of elaborating an adequate privacy management system as well as its audit and certification.

1.2. Self-regulation in the framework of the new European data protection regime

European Union legislation has put on its agenda the replacement of the Data Protection Directive of 1995 with a new Data Protection Regulation, which may – due to the legal source being changed to Regulation – on the one hand, establish a more uniform European regulatory environment, and which is, on the other hand, intended to meet the data protection challenges raised by the latest technological developments – mainly the spread of the Internet and so-called "Web 2.0" services. On 25 January 2012, the Commission published the first draft of the Regulation,[18] which would provide a more detailed regulation in the area of data protection than the earlier one.

1.2.1. Obligations imposed on data controllers and data processors

In many parts the proposal is clearly directed at compelling data controllers and data processors to place significantly greater emphasis than earlier on questions relating to data processing and internal regulation: the draft Regulation devotes a separate chapter to the obligations imposed on the data controller and data processor. While agreeing with this change in the direction of regulation, we should mention that compared to the earlier regulation these sections impose considerable additional tasks (and administrative burden) on data controllers, especially on data controllers working for larger organizations or those carrying out data processing as their "main activity". Therefore, these points may, expectedly, give rise to further serious debates, and it is not at all unlikely that, as a result of the compromises reached during the legislative process, a smaller or greater part of these obligations will not be incorporated in the final text at all or will be incorporated only in a form imposing a smaller burden. Further on, we will provide a brief summary of the main points relating to the obligations of data controllers/processors.

1. The sections entitled "Responsibility of the Controller", as a matter of fact, give a summary of further responsibilities, and they render it the controller's task to adopt policies (codes of practice, rules) corresponding to these responsibilities as well as to demonstrate that he has taken the necessary measures. These further responsibilities include keeping adequate documentation, implementing data security requirements, performing a data protection impact assessment, complying with the requirements for prior authorisation and designating a data

[18] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final

protection officer.[19] Apart from this, the data controller is required to implement mechanisms to ensure the verification of the effectiveness of the said mneasures, and, if proportionate, this verification shall be carried out by independent internal or external auditors.[20]

2. The Proposal for the Regulation lays down an extensive obligation for data controllers/processors to maintain documentation, from which exemption is made for natural persons processing personal data without a commercial interest and enterprises or organisations employing fewer than 250 persons that are processing personal data only as an activity ancillary to their main activities. Documentation must extend to the purposes of data processing, the legitimate interests pursued by the controller, the person of the data controller/processor, a description of categories of persons concerned (data subjects, recipients of data), erasure of data, data transfer processes[21] – in short, all relevant circumstances of data processing. Thus, the data controller is obliged to disclose and catalogue each of his processing operations one by one (according to the individual data processing purposes) and document them duly. At the same time, the prescription of the documentation obligation replaces the obligation contained in the currently effective Directive relating to the reporting of individual data processing operations to the authorities.[22]

3. Article 30 relating to data security measures imposes on data controllers an obligation that basically corresponds to the provisions of the currently effective Directive, supplementing it with the condition that the data controller shall take these measures "following an evaluation of the risks". The Commission is empowered to adopt delegated acts concerning the data security rules.[23]

4. The text of the draft Regulation contains[24] two principles having constituted the subject of discussions in academic legal literature for years: the principles of data protection by design[25] and data protection by default.[26] Compliance with the principle of "privacy by design" presupposes that data controllers consciously think over and plan their individual data processing operations and already during planning – be it IT development, the elaboration of a new code of practice or the procuring of a filing or client-managing software – they have regard to the fulfilment of data protection and data security requirements.[27] On the other hand,

[19] Proposal for a Data Protection Regulation, Article 22 (1)-(2)
[20] Proposal for a Data Protection Regulation, Article 22 (3). The Commission shall be empowered to adopt delegated acts for appropriate measures for the verification and auditing mechanisms and as regards the criteria for proportionality. [Article 22 (4)]
[21] Proposal for a Data Protection Regulation, Article 28 (1)-(2), (4)
[22] Proposal for a Data Protection Regulation, Explanatory Memorandum, Point 3.4.4.1.
[23] Proposal for a Data Protection Regulation, Article 30.
[24] Proposal for a Data Protection Regulation, Article 23.
[25] In the English version of the norm one may read: "data protection by design", while in academic legal literature it is mainly known as the principle of "privacy by design".
[26] In the English version of the norm one may read: "data protection by default", while in academic legal literature it is mainly known as the principle of "privacy by default".
[27] On the notion of privacy by design, see, for instance: Cavoukian (2009), p. 3. and Le Métayer, 2010, pp. 323-324.

the essence of the principle of "privacy by default" lies in the fact that as a default setting, data controllers offer an option that serves the purpose of protecting privacy better.[28]

5. The Proposal for the Regulation lays down the obligation to carry out data protection impact assessment[29] concerning data processing where processing operations present specific risks to the rights of data subjects by virtue of their nature, scope or purposes.[30] The exemplary list contained in Article 33 (2) provides a few criteria to determine if a data processing operation presents a specific risk. Such a data processing operation is, for example, a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual. Such data processing operations could be software-supported operations for client evaluation, credit assessment, but also the collection of personal data in a company management system – these means are relatively often used by the bigger characters of business life.[31] The Proposal for the Regulation also evaluates as a specific risk the processing of certain sensitive data, video surveillance of publicly accessible areas, some data processing operations relating to children, etc. Based on the above, it may be concluded in general that the obligation to carry out data protection impact assesment concerns only a well-defined, but rather wide range of data controllers.

6. Compared to the present situation a significant additional obligation is imposed on data controllers by the general prescription of "data breach notification" – applicable under the effective European rules only to service providers in the telecommunications sector.[32] Its essence lies in the fact that in the case of personal data breach[33] the data controller is obliged to notify the authority or, in some cases, also those concerned.

7. In accordance with Article 35 of the Proposal for the Regulation, the controller and the processor shall designate a data protection officer in any case where

- the processing is carried out by a public authority or body, or
- the processing is carried out by an enterprise employing 250 persons or more, or

[28] This principle arises primarily concerning the privacy settings of various social networking websites, but it may also be interpreted in a wider context. On data protection issues relating to social networking websites, see: Polefkó, 2010

[29] The expression used by the English version of the Directive is: "data protection impact assessment". In academic legal literature the term "privacy impact assessment" (PIA) is also accepted.

[30] Proposal for a Data Protection Regulation, Article 33 (1)

[31] Thus, the Proposal for a Data Protection Regulation reacts to the most critical question of data protection: the phenomenon of (automated) profiling. For more detail on the problems relating to profiling, see: Hildebrandt/Gutwirth, 2010.

[32] Bíró/Szádeczky/Szőke, 2011, pp. 46-48. For a detailed analysis of the data breach notification, see: Barcelo/Traung, 2010

[33] "Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". Proposal for a Data Protection Regulation, Article 4 (9)

- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.

The draft Regulation also specifies the rules relating to the status and tasks of the data protection officer.[34]

Concerning the planned new Regulation, it must be repeatedly emphasized that these sections may become modified significantly before they are finally adopted and that numerous questions of detail will be filled with content by Commission rules of implementation, about which no material information is available at present.

Therefore, it is not possible to determine the extent of the actual obligations for the time being, but the direction of the rules can be clearly identified. On the whole, the obligations contained in the above sections will surely lead to the result (even if they are later implemented in a milder form) that some data controllers and especially a well-defined, but rather wide range of data controllers will assess their data processing activity a lot more consciously than before, and if required, build detailed internal data processing systems (codes of practice, mechanisms) and also document them properly. Data controlling organizations must – if only in order to determine the obligations imposed on them – clarify at least the following circumstances:

- if they carry out data processing only as an activity ancillary to their main activities, or this is their core activity;[35]
- if their activity can present specific risks to the rights of data subjects;
- if their core activities consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.

The objective of compliance with the obligations contained in the Proposal may be furthered by establishing the privacy management system outlined by us, which will be explained in detail in later chapters – however, with regard to the topic of the research, in the present essay, only concerning the code of conduct regulating the monitoring of employees.

1.2.2. Elaboration of codes of conduct and certification

Basically, the planned new Regulation provides for the creation of codes of conduct similarly to the provisions contained in the Directive in effect. The elaborators of codes would still have the possibility to submit them to the opinion of the national data protection authority or to the Commission,[36] which are to determine whether the codes are in accordance with the national provisions.[37]

[34] Proposal for a Data Protection Regulation, Article 33 (1)
[35] As typical examples for the latter, one may mention – among many others – enterprises or social networking websites dealing with direct marketing or data mining.
[36] At present, draft codes may be submitted to the opinion of the Article 29 Working Party, therefore, this task would be transferred to the Commission.
[37] Proposal for a Data Protection Regulation, Article 38 (1)-(3)

At the same time, it is a novelty that the draft Regulation incorporates an article on data protection certification and seals, according to which – in a rather soft law-type formulation – the Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors.[38] Besides this - and it may also indicate the seriousness of the "declaration of intent" – the Commission would be empowered to adopt delegated acts for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms.[39]

1.3. Data Protection Audit and Certification

Following a review of possible forms of self-regulation and an analysis of the expected impact of the new European data protection framework on this area, we will discuss the institutions of data protection audit and certification also in detail. First of all, it is worth reviewing basic notions relating to audit, types of audit/certification, and the advantages and disadvantages of data protection audit. For this review we will primarily use the relevant – mostly foreign – academic literature, ISO sources relating to the certification of standards and already existing data protection audit methodologies.

1.3.1. Definition of data protection audit and certification

Although the notion of data protection audit appears directly in legal academic literature and several distinct methodologies concerning data protection audit, it is worth, first of all, having a look at the – rather neutral – notion of audit used by the ISO standard group. According to this: "audit means a systematic, independent and documented process aimed at the obtaining and objective assessment of audit evidence in order to establish to what extent audit criteria are met."[40]

For the definition of data protection audit, we will rely on one of the CEN Workshop Agreement documents. According to this, data protection audit is a systematic and independent examination to determine whether activities involving the processing of personal data are carried out in accordance with an organization's data protection policies and procedures, and whether this processing meets the requirements of the EU Directive.[41]

With the help of these two definitions, we will attempt to create a definition containing the basic elements of both notions. Based on this, data protection audit is an independent, systematic and documented examination based on the collecting and objective assessment of

[38] Proposal for a Data Protection Regulation, Article 39 (1)
[39] Proposal for a Data Protection Regulation, Article 39 (2)
[40] The definition of the MSZ ISO 19011 standard is referred to by: Berényi/Szintay/Tóthné Kiss, 2011, Point 5.1
[41] CEN, 2005 p. 8. The Handbook issued by the Information Commissioner of the United Kingdom uses a basically identical notion, see: ICO, 2001, p. 1.4

audit evidence[42] to determine whether the data processing activity[43] of an organization is carried out in accordance with the rules governing this activity.[44]

Audit is usually (but not necessarily) followed by certification as well, which essentially means the issuing of a certificate for a definite period of time based on the favourable audit report. Therefore, certification must in any case be preceded by a process of audit.

1.3.2. Types of audit/certification

Based on legal academic literature, data protection audit may be classified from different aspects.

1.3.2.1. Instrument audit and system audit

Academic literature on quality management systems, similarly to literature dealing with data protection audit, distinguishes between the audit of various instruments and products (or in other words: product certification) and the auditing of the data protection system (system audit or system certification).

The certification of some instrument (product) constitutes a guarantee that the product complies with the applicable legal instruments, the prescribed standards and other documents (contractual requirements).[45] As a matter of fact, instrument audit for reasons of data protection is a one-off process aimed at the auditing and, in particular cases, the certification of the data protection and data security reliability of hardware and software products, which may significantly alleviate the selection of instruments that are reliable from the aspect of data protection.[46]

The purpose of system audit is to evaluate the data protection activity of an organization in accordance with the above definition. Data protection audit interpreted as system audit presumes the setting up of a data protection management system that integrates and concretizes the obligations imposed upon data controllers by the regulation.[47] In the present study data protection audit is to be interpreted clearly as system audit.

1.3.2.2. Internal, supplier and external audit

Based on the person/organization carrying out the audit, it is possible to distinguish between internal, supplier and external audit.

---

[42] Such audit evidence may include rules and regulations, codes of practice, instructions, guides, data protection clauses of contracts, complaints relating to personal data, records, information based on oral interviews etc.

[43] The term "activity" is interpreted in its widest sense so as to include the existence of data protection documents, the actual data protection operations, plans connected with system development etc.

[44] "Rules governing this activity" are also taken in a wide sense so as to include all documents laying down rules relating to data processing: Acts of Parliament and other legal instruments, policies, rules and regulations, contractual terms etc.

[45] Szigeti/Végső/Kiss, 2003, 6.2.

[46] Balogh/Jóri/Polyák, 2002, p. 390.

[47] For a detailed analysis of data protection audit as system audit and, in connection with this, for Roßnagel's conception of audit, see: Balogh/Jóri/Polyák, 2002, pp. 334-340.

In the case of internal audit the data processing organization in question itself carries out and documents the examination and evaluation.[48] If an organization has an internal data protection supervisor or an organizational unit in charge of data protection, it is this person or organizational unit that is usually responsible for internal audit. Internal audit is not typically accompanied by the issuance of a separate certificate, but internal audit carried out at specific intervals may be prescribed as a precondition for the continued use of some certificate for several years.

Supplier audit usually takes place where an organization outsources its data protection activity and it would like to ascertain the compliance of the partner's data protection system.[49]

Finally, in the case of external audit, audit is carried out by an organ that is separate and independent of the organ in question: this organ may be the data protection authority of the given state (one may find examples for this in some European countries) or some other market actor. Organizations interested in data protection audit may also sometimes link the use of the data protection certification service with some other certification, typically the certification of information security and quality management systems.[50]

1.3.2.3. Adequacy audit and compliance audit

Based on the ICO Data Protection Audit Manual and the Hungarian research analysing it, it is possible to distinguish between adequacy audit and compliance audit.

Adequacy audit is aimed at establishing whether the various documents found at the data processing organization: rules and regulations, policies, practical guidance etc. comply with the provisions of central data protection rules. This stage of the audit does not necessarily require on-the-spot inquiry, only the documents need to be reviewed.

Compliance audit is aimed at establishing whether the actual operation (data processing practice) of the data processing organization complies with its documented rules and regulations and the laws. This procedure requires the performance of on-the-spot examinations and usually also the collection of information from colleagues.[51]

It is obvious that compliance audit is significantly more thorough, since it is directed at the revelation and evaluation of the actual situation and not only the examination of the lawfulness of documentation.

It is to be noted that, based on similar criteria, compliance evaluation may also be classified into three types. BENNETT and RAAB specifies "compliance of policy", which essentially means the same as compliance existing as a result of adequacy audit. In the authors' opinion, "compliance of procedure" proves that the given organization has adopted adequate mechanisms to implement and perform its codes, while the third type, "compliance of

[48] ICO, 2001, p. 1.5. It is referred to as "First Party Audit" by the ICO document.
[49] ICO, 2001, p. 1.5. The ICO uses the terms "Second Party Audit" or "Supplier Audit".
[50] ICO, 2001, pp. 1.5-1.6. The ICO uses the expression "Third Party Audit". For a Hungarian summary of the individual types of audit based on the ICO document, see also: Balogh/Jóri/Polyák, 2002, pp. 382-383.
[51] ICO, 2001, pp. 2.2-2.3., Balogh/Jóri/Polyák, 2002, pp. 384-385.

practice" shows that the actual activity of the given organization complies with the applicable codes.[52] The latter case basically corresponds to the case of compliance audit.

1.3.3. Advantages and disadvantages of data protection audit – the motivation of the organizations concerned

Right at first glance it is obvious that preparation for the audit required for data protection certification presumes that the given organization conducts a thorough examination of its documents and practice relating to data protection, therefore, the institution of data protection audit greatly contributes to enhancing the data protection awareness and sensitivity of data controllers. Audit presupposes the systematic recording of data protection ideas and objectives as well as the preliminary outlining of the system of means for their implementation. One may bring the counter-argument that voluntary audit is not suitable for the general and wide-spread improvement of the level of data protection, because the data controllers participating in it are probably the ones who have ensured high-level protection previously as well; on the other hand, those placing less emphasis on data protection requirements are not involved in it.[53]

At the same time, it may constitute a significant motivation factor for data controllers that the adequate communication of the certificate connected with the successful audit can also increase clients' and citizens' confidence in the given organization.[54] Therefore, data protection efforts may also mean a potential competition advantage.[55]

As a further motivation one may regard the avoidance of disadvantages resulting from the unlawful processing of data, mainly fines imposed by the authorities. The review of data processing activities, which are becoming increasingly complex, means a growing challenge for data processing organizations as well, however, without thorough examination and evaluation the given organization cannot simply be assured that all its data processing activities really comply with the law. It is to be noted that the development of European data protection law clearly points in a direction that presupposes a more conscious attitude on the part of data controllers toward their own data protection systems.

Moreover, an advantage flowing from auditing may be that the internal procedures of organizations become easier to control,[56] in other words, "putting in order" data processing processes may also fit well into the improvement of the general management system of the given organization.

It is to be added as a final remark that the continuous development of the branch of industry dealing with information security may also lead to (legal) data protection issues coming to the foreground. This is explained by the fact that in several situations information security

[52] Bennett/Raab, 2006, p. 259.
[53] Alexander Roßnagel's conception and its criticism by Hans-Ludwig Drews and Hans Jürgen Kranz are cited by: Balogh/Jóri/Polyák 2002, p. 329.
[54] Consumer confidence has a great significance in special fields such as electronic commerce, for example, (comprising a diversity of online services).
[55] Balogh/Jóri/Polyák 2002, pp. 330-331.
[56] Thomas Königshofen's thoughts are cited by Balogh/Jóri/Polyák 2002, p. 331.

standards also prescribe compliance with legal requirements, therefore, the examination of data protection questions in more or less depth cannot be avoided even during the audit of information security management systems.

1.3.4. The Regulation of Data Protection Audit in Hungary

Hungarian data protection literature has dealt with the introduction of the institution of data protection audit for years.[57] The New Data Protection Act[58] provides for the legal institution; the date of entry into force of the sections relating to auditing is 1 January 2013. According to the approved text of the Act, data protection audit is a service provided by the data protection authority at the request of the data controller which is aimed at the implementation of a high level of data protection and data security through the evaluation of the ongoing or planned data processing activities based on professional criteria defined and published by the authority.[59] The Act renders it unambiguous that the authority carries out auditing not within its administrative competence, but as a service, so its result cannot be an administrative decision. Accordingly, the authority records the result of the audit in the evaluation report on the audit, in which it may make recommendations to the data controller. Therefore, the evaluation is not binding either on the data controller or the authority. Failure to perform the provisions contained in the evaluation does not itself carry any sanction; on the other hand, the implementation of recommendations does not guarantee lawful operation either. The Act expressly lays down that data protection audit shall not restrict the exercise of other competences by the authority. Therefore, it is not possible to exclude even the possibility that the evaluation of the audit is inconsistent with a subsequent administrative decision.

The Act makes not provision as to whether the data protection authority shall issue a certificate about the lawfulness of the data controller or the given data processing activity. Nonetheless, issuing such a certificate would significantly restrict the authority's scope of action during subsequent administrative proceedings. It is not clear either to what extent the evaluation criteria taken into account concerning the audit may go beyond the statutory requirements and what incentives may be offered by the authority in order to ensure that data protection terms and conditions could possibly exceed statutory requirements.

Consequently, the Hungarian regulation leaves it to the data protection authority to give a detailed definition of the aims, methods and procedure of auditing. Foreign examples reveal the fact that auditing carried out by the data protection authority is also at least partly directed at the assessment of compliance with data protection requirements that exceed the requirements laid down by statute and that are based on voluntary commitments made by the data controller. The success of the legal institution will basically depend on the rules of detail and the market evaluation of the result of auditing.

At present – without knowledge of the detailed methodology of the Authority relating to data protection audit – the risk concerning the legal institution seems to lie in the fact that it

[57] On the same topic, see: Polyák/Szőke, 2011.
[58] Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter New DPA)
[59] § 69 of the New DPA

merges authority competences and non-authority competences, and at the same time, it fails to clarify to what extent the aim of auditing differs from the authority inspection examining the lawfulness of data processing and how the data controller may benefit from it. In other areas of law,[60] auditing is not usually carried out by the authorities, but professional and economic organizations, and the authority of the given branch of industry is, at most, in charge of the supervision and registration of those organizations. The result of auditing is usually a certificate verifying compliance with some system of quality requirements. The certificate may be a precondition for carrying out some activity, but in some cases solely some presumed market advantage is attached to it. However, enshrining the institution of auditing in law does not exclude the possibility of auditing and certification functioning on a market basis, a significant advantage of which may be, for example, the assumption of liability by the certifying organ, which liability may extend – in the area defined by the certification – to damage caused incidentally by the certified organ or to indemnification in respect of data protection fines imposed upon the organization.

On the other hand, the performance of data protection auditing by a data protection authority is not unprecedented in Europe. In the UK it is the Information Commissioner who is in charge of auditing, but he may also exercise this competence through the involvement of an external expert. The Commissioner evaluates the level of implementation of a good data protection practice with the consent of the data controller. Pursuant to the English Data Protection Act, "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 complies with the requirements of the Data Protection Act.[61] Concerning the exercise of this right the Commissioner elaborated and published a data protection audit methodology manual in 2001,[62] replaced by a new guide[63] in 2012.[64] Auditing is aimed at the examination of compliance with statutory requirements and the organization's own data protection system, the revelation of deficiencies and weaknesses as well as supplying information for the review of the data protection system. An organization's own data protection system may define stricter requirements than those provided for by the statute. The end result of auditing comprises information received from the Commissioner and the issue of guidance for improving data protection practices; however, no sanctions are applicable.

Apart from this, in Germany, for example, the data protection authority of the state of Schleswig-Holstein carries out data protection auditing of public law data controllers who have voluntarily decided to participate in this. The procedure is aimed at examining whether the data protection objectives set voluntarily by the data controller can be implemented through the measures set for them. As a result of the procedure the authority issues a

[60] See, for example, Act CXXXIII of 2009 on the activities of organizations evaluating compliance; Act XXXV of 2001 on electronic signatures
[61] Data Protection Act 1998 of the UK, Art. 51
[62] ICO, 2001
[63] ICO, 2012
[64] Although the Data Protection Audit Manual published in 2001 has been withdrawn formally (see: Morgan/Boardman, 2012, p. 58.), but because it is significantly more detailed than the new guidance, it is considered an important legal academic source and it is referred to several times in the present study as well.

certificate, which serves as a guarantee for citizens that the given administrative organ carries out a conscious data protection activity. On the whole, this procedure is clearly separated from the supervision of the lawfulness of data processing by the authority, its fundamental aim being to increase the consciousness of data protection activity within the organization as well as to ensure that the level of data protection exceeds statutory guarantees.[65]

In spite of the existing European examples, we are of the opinion that it is best if data protection audit is carried out by market actors. In this case it is always possible to guarantee the confidential processing of the data of the audited undertaking, the full separation of the auditing and certification process from authority inspection, and questions relating to liability assumed as a result of the issue of the certificate may be disambiguated based on civil law rules. Data protection audit and certification may fit well into the practice developed relating to existing information security standards, since the majority of methods applied in that practice may also be used during data protection audit.

Instead of the regulation in force, it would have been more advantageous to regulate by statute the conditions of data protection certification carried out by market actors. Such conditions could include the registration obligation of organs carrying out the certification, laying down specific requirements for becoming an auditor, the regulation of questions relating to liability etc. In the absence of this, at present, data protection audit may be carried out within the framework of counselling activity based on the general rules of civil law.

On the other hand, the present Hungarian statutory regulation provides for audit to be carried out by authorities at the special request of data controllers, therefore, there is room for both the institutions of audit carried out by an authority and audit conducted on a market basis. Data controllers may decide, on weighing both the advantages and disadvantages of each procedure, which auditing organization is more desirable for them. The authority procedure may be attractive primarily for state and local government organs (some foreign models permit auditing to be carried out by authorities only in the case of state organs), which have no business secrets and may not afford market-based auditing due to the scarcity of their financial resources.

[65] See the website of Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, https://www.datenschutzzentrum.de/index.htm [2012.10.25]

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

Authors: Balázs Rátai, Tamás Szádeczky, Gergely László Szőke

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 had 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 at 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.

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

[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.

[68] See Chapter 1.3.3.

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

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 of 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.

[69] MSZ EN ISO 9000:2005, 3.2.2.
[70] MSZ EN ISO 9000:2005, 3.2.3.

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

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

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.

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.

---

[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

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].
- 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).

[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.

- 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. Chapter 3.4. deals with this issue in detail.

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

[76] MSZ EN ISO 19011:2003, 5.2.2.

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 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

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

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

3. THE ROLE OF THE TECHNOLOGY – AUDITING AND CERTIFICATION IN THE FIELD OF DATA SECURITY

Author: Tamás Szádeczky

3.1. Technologies of workplace surveillance

The need for the introduction of surveillance systems in the workplace is not a novelty. As DAVID LYON and ELIA ZUREIK suggest in their book.[82] the fear of being monitored by society first appeared in fiction in the 1960s, while actual intensive workplace surveillance began in the 1990s. As an actual example they refer to the "call management services" which were offered by several telecommunication companies in Kingston, Ontario in 1993; these services enabled employers to fully monitor all calls. Since then due to technological development the range of surveillance devices has substantially been widened, which is shown by this study.

3.1.1. Camera surveillance

Camera surveillance or CCTV surveillance touches upon a number of constitutional fundamental rights such as the right to dignity, the protection of personal data, the protection of private secrets, the inviolability of the home, the right to peaceful assembly, the freedom of expression, the free exercise of religion and the right to freedom of movement. However, some limitations may be accepted in the case of workplace application following the test of necessity and proportionality.

The primary device of camera surveillance is the traditional camera which converts light entering through the lens into electric signals by the help of a charge-coupled device (CCD). This signal can be transmitted and processed both in analogue and digital mode. A CCD sensor can sense a much broader electromagnetic spectrum than the human eye; consequently in addition to the visible light it shows sensitivity in the ultraviolet band to a small degree and in the infrared band to a substantial degree. That is why it is possible to record images of an appropriate quality outdoors at night by infrared lighting. Depending on the mode of transmitting video signals, there are analogue (traditional) and IP cameras. In the case of a traditional camera the video signal was transmitted by a network built up of coax cable especially for this purpose. Hence its name: closed circuit television (CCTV). It is difficult to physically interfere in the system, see or modify the signal. The typical recording component of the traditional system was the time lapse video recorder. This solution stored the recording in a broken manner, by storing still images every few seconds. They are now replaced by digital recorders; however access is usually still available only on the spot. The family of IP cameras breaks out from this circle; they provide wide-ranging (e.g. web-based) access to live camera images even with remote recording. In systems created improperly, unauthorized persons may easily gain access to the processed data. A further problem may be the extremely wide optic angle (PTZs and cameras with wide angle lenses) or the remarkably high definition

[82] Lyon/Zureik, 1996

(Gigapixel cameras) which enable the observer to have access to parts of the images not belonging to the monitored area or exceeding the need of the observation concerning details.

From a legal point of view personal data means any data relating to an identifiable natural person and any conclusion inferred from such data regardless of how difficult it is to restore the connection between the data and the given person. The quality of the definition of the pictures is important with regard to ability to identify and thus to establishing the connection with the natural person, however, it is not the sole criterion as identification is possible even in the case of poorer definition as well, for example on the basis of the front door of the home or habits. Under the European Union directive on data protection, processing personal information means any operation or set of operations performed upon personal data, thus even the inspection of personal data. It follows that not only recording images but mere surveillance also qualifies as processing personal data. According to the interpretation by the Constitutional Court, processing personal data qualifies as the limitation of the right to informational self-determination, thus the principles of necessity, proportionality, suitability and being statutorily regulated must be followed in all cases. The principles of data protection are purpose limitation, data minimum, the requirement of fair data processing, the requirement of data security, the requirement of transparency and ensuring the rights of those involved, all of which must be respected in the course of camera surveillance.

If camera surveillance is carried out on private property or on a part of private property open to the public – and it is not carried out by the owner – it is appropriately regulated by act CXXXIII of 2005 on the rules of personal and property protection and private investigation activity, under which a camera surveillance system can only be designed by a person satisfying the professional requirements stipulated by law and who has been entered in the designer register. Maintenance and operation are subject to permission by the police. The forms of electronic surveillance which enable the recording of images or sound and images with sound can be applied for the purpose of protecting human life, physical integrity and personal liberty, safekeeping of hazardous substances, protecting business, bank and securities secrets and in the interest of the protection of property. Even in such cases they can be applied only on condition the perception of infringements, catching the offenders in the act, the avoidance of such offences and providing evidence for such infringements are impossible with any other means, further the use of such technical devices does not exceed the necessary extent and it does not entail the disproportionate limitation on the right to informational self-determination.

3.1.2. Access control systems

Entrance to protected areas such as workplaces can be controlled electronically by an access control system, which automatically means processing personal data. Access control systems can be classified according to the technology of identification and devices applied. There are three factors of identification: knowledge, possession and features. Knowledge based identification includes passwords and PIN codes. One disadvantage of them is that they can be multiplied unrestrictedly so no one knows how many persons know the code. In addition,

those authorized to access often forget their codes. The issues of data protection concerning their application – in case they are bound to persons – are the same as those of cards.

The other factor of identification is possession, which means the use of a certain physical device to control access. This is typically done by a (data)card. The purpose of datacards is to store data for the purposes of identification, access and any other purposes. These devices can be sorted by their method of storage and type. Storage capacity, security and applicability depend on the type of these devices.

The oldest datacard is the punch card in which the presence and absence of holes on a paper medium embodied data. Reading the cards can be contact electric (whether two contacts facing each other contact or not) or optical (whether light shines through the hole or not). Cards can store only a small amount of data, 80-90 bytes and their use is also very slow and difficult. They were basically used for storing data at the dawn of computer technology; nowadays they do not have any practical importance. The principle however can be used for identification purposes, for example dining vouchers in a canteen are plastic cards on which certain patterns of holes represent serial numbers. The card is read optically, and after comparing the data with the database in the computer of the till, the cardholder's entitlement to having a meal in the given part of the day can be established. The genuineness of the card can be determined by having a close look at it; due to its simplicity it cannot be used for identification without supervision.

A traditional, widely known type of datacard is the magnetic card. Here the data medium is a magnetic metal stripe embedded into a plastic card. It is read by a magnetic reading head familiar from tape recorders, thus it requires the contact between the card and the reader. The technology is defined by several standards, for example ISO 7811, 7812 and 7813. The amount of data stored is also limited here, around 100 bytes. In the case of a bank card for example the same data are stored as are visible on the card supplemented with some controlling data.[83] These cards are still used due to their simplicity. They are suitable for identification without supervision. Their safety can largely be enhanced by the use of PIN codes. They can be forged without substantial preparedness by reading the magnetic stripe and magnetizing a blank card. It follows that identification by taking a close look is also important here.

Barcode cards which store data in one or two dimensional barcodes are also in general use. The amount of data that can be stored in this way is smaller than what can be stored on magnetic cards, in the case of one dimensional (linear) barcodes only a few bytes. Information is encoded according to international standards, EAN 8 and EAN 13 codes introduced in 1978 are commonly used. In the Hungarian Republic both the Tax ID number and the Social Security ID Number were displayed on tax cards and social security cards in one dimensional linear codes. The square patterned data matrix code introduced in the 1990s was launched as a further development of the linear code. The data storage capacity of the black-and-white data

[83] Padilla, 2002.

matrix can reach 2335 alphanumeric characters[84]. Its best known version is the code system of PDF417, which is used on police IDs. The whole data content of the IDs are also displayed in two dimensional barcodes. This code system is also used by the ABEV programme on tax returns filled in on a computer. The nowadays popular QR code, which can easily be read by mobile devices due to its shaping, is similar to it.

A drawback of these methods is that barcodes can be photocopied, read and forged. In order to avoid these, the barcode can be covered by a special coating which can only be made visible by infrared light. This method makes forging a lot more difficult.

Laser cards are far less widespread due to their costliness. On such hard plastic cards there is a data carrier stripe of 1.6-3.5 cm width fabricated with a technical solution similar to that of compact discs which can be read by a laser beam. They are not used in Hungary, but digital data are stored on various documents certifying citizenship in Canada, the United States of America, Costa Rica and Italy and vehicle registration in India. The amount of storable data is far bigger than in the case of former methods: 1.1MB, 1.8 MB or 2.8MB.[85]

A common feature of the cards described so far is that their data content can hardly be modified or if so, only with difficulty and they do not contain an active element which might make their use safer. In case the data stored need to be modified, some other method must be introduced. A simple solution can be the case of phone cards used in Italy in the 90s, where the telephone printed black rectangles (inevitably with a special ink for the sake of security) on the white stripe on the card in proportion to the units used. The phone card could be used as long as there was a white surface on it. It was checked optically. The data content of magnetic cards can also be modified if there is a data eraser placed in the reader. A more complicated but safer solution is the application of memory circuits, where a non-volatile memory circuit which is electronically reprogrammable (EEPROM) is built in a plastic card so that data can be stored and modified on it. Such a solution is used for instance in the case of Hungarian phone cards. Forgery, in case commerce memory circuits are used, is not too difficult; moreover a programme can be written for the emulation of the operation by leading out the contact points and connecting them to a computer thus deceiving the reading device.

The use of cards was revolutionized by the introduction of active cards on which data can be written and read plus the card is capable of processing data and performing mathematical operations. The central part of active cards is the microcontroller. A microcontroller is practically a quasi complete computer integrated on one small circuit plate (chip). It contains a processor, a non-volatile memory (ROM, FLASH), a random access memory (RAM), input and output ports (I/O) and other supplementary elements (for example a clock, a comparator etc.) in one package. This, as an active element, enables the implementation of fourth generation crypto systems[86] thus providing active protection for the data stored and access to them. It can hold 1-256 kilobyte data depending on its type. Both contact and non-contact (non-touch) datacards can be created by using microcontrollers. Smart cards (intelligent cards,

[84] Eiler, 2008, p. 44.
[85] Cf. LaserCard Corporation
[86] Symmetric and asymmetric key computer encryption-decryption algorithms, such as DES, AES, RSA, etc.

chip cards) are such contact cards. In Hungary they are used in student cards in higher education and recently in bank cards. This is the primary device for storing the private keys of electronic signatures. Several international standards deal with chip cards both from functional and security points of view.[87] Such a functional standard is for example ISO/IEC 7816. A direct contact is needed when reading the datacard which creates a direct electric contact with the pinouts of the microcontroller. Obviously, this is the fastest and most secure method of data transmission.

Proximity cards (RFID, radio cards) are contactless active datacards with microcontrollers. The active device used in them is basically the same as the one used in contact smart cards, the main difference lies in the fact that radio frequency is used to establish contact with the reader. It works on the principle that there is an antenna coil embedded in the datacard which is connected to the microcontroller. There is no power supply in its baseline version; it gets the energy needed for its operation from the electromagnetic field generated by the reader. Thus, when moving the card towards the reader, it is turned on automatically and starts to modulate the electromagnetic field in a certain way, for example it sends the ID number of the card. The reader checks whether that particular number is included in the database and authorizes for example entrance depending on it. The defect of this system is easy to recognize as only the space with the given electromagnetic frequency is needed for obtaining data. The card "divulges" its ID number to any reader, thus even to a reader operated by a malicious person. The card is copied by simply writing this number on a blank card. To avoid this, this system can be combined with identifying the reader as well. In this case when the card gets into the electromagnetic space, it only gives a signal about its presence and then the reader sends its ID code. The card will only give its own ID number if the reader's code is stored on the list of authorized readers in the memory of the card. Data transmission can be made more complicated by classifying transmission for example by requiring electronic signature. Due to radio frequency data transmission the speed of transmission and consequently the amount of data are far smaller than in the case of smart cards; usually data with 26-37 bit length are used. By the help of a battery embedded in the card the length can be stretched from the baseline from few times 10 cm to even 10 m (long range proximity). The technology is described by the ISO/IEC 14443 standard. These active cards can be made safe enough to be used in public documents for identification purposes on their own or in a supplementary manner. The next generation of active cards is the application of cards with biometric security elements.

The third factor of identification, namely identification based on a feature can be realized by biometric solutions. The most characteristic element of the exterior of the human body is the face, which, besides its socio-communicative functions, is the primary means of the identification of persons through visual perception due to the insufficient development of the other senses (e.g. smelling) of Homo Sapiens. Its application is instinctive and the human race has always deployed it. The first trace of using other biometric features – that is certain unique characteristics of the human body – is the use of fingerprints for the identification of

[87] For further details see Hassler, 2010

children in China in the 14th century, which was described by the explorer JOAO DE BARROS.[88] In Europe a Parisian police officer, Alphonse Bertillon introduced a system of identification based on the measurements of the human body for identifying criminals in 1890. His method was in use until the mass occurrence of false identifications. Based on Bertillon's work, identification based on fingerprints was introduced by Richard Edward Henry at the Scotland Yard. In the 20th century Karl Pearson, an applied mathematician of the University College of London made a huge progress in the field of biometrics. In the 1960s an essential progress was made in the field of the analysis of signature dynamics, which is still used by the military and national security sectors. In the wake of intensified terrorism the state application of biometric identification has increased in the United States and in Western Europe.

At present the following identification systems based on biometric features exist:

- fingerprint,
- hand geometry,
- palm print,
- vein recognition,
- dynamic handgrip recognition,
- skull heat map,
- 2D facial recognition,
- 3D facial recognition,
- iris[89] recognition,
- retina[90] recognition,
- voice recognition,
- signature dynamics,
- keystroke dynamics,
- DNA,
- gait recognition.

These are more or less deployed for identifying persons. The mathematical description and storage of biometric features allow for the more precise identification of persons based on unique features.

Biometric identification raises further issues in the field of data protection. As biometric data are tied to the person for ever, and the direct mapping of bodily features may contain medical data as well, their handling can be possible only in exceptional cases and after the careful consideration of necessity and proportionality.

The three factors described above can be used separately or in any combination for identification purposes, this latter enhances the security of access, while at the same time can change the ranking and appropriateness of the system from the aspect of data protection.

[88] Roberts, 2012
[89] Coloured part round the pupil of the eye
[90] The blood vessel pattern of the layer of the membrane at the back of the eyeball, the eye has to be illuminated by harsh light, which caused severe opposition on the side of the subjects. The new technology using infrared light has diminished opposition and has given an impetus for further development.

3.1.3. The application of ICT devices

The innovation of ICT services runs parallel with the development of computers and networks. The outsourcing of certain services started right from the beginning, in 1962: H. Ross Perot established the company called Electronic Data Systems (EDS), the ancestor of the outsourcing business. The company specialized in performing the informatics operational tasks their clients did not want to perform within their organisation. There were only a few experts available on the American market at that time, so outsourcing solved this problem, too. The standardisation of office workstations and central software management can be provided for in an outsourcing contract. The service supplier can take over the operation of the servers of the client and can even run the services of the client together with the services of other clients on its own hardware. In such a case the service supplier must guarantee the secure separation of the given services. The most important element of an outsourcing contract is to include a Service level Agreement (SLA), which stipulates all essential terms and conditions: availability index, time to repair and recovery, time to respond, penalties, rewards etc.

Outsourcing the secondary, ancillary tasks has been of great business importance ever since. In Hungary MATÁV also outsourced its IT operational activity to EDS in the '90s and it is still outsourced by them – now as Magyar Telekom [Hungarian Telecom] – within the T-group.

Management information systems which ensure information for decision-making in an adequate form came into being in 1990. Data stores for assisting decision-making were created in 1995 and data mining also started then. Integrated business management systems appeared at the end of the '90s. CRM (Customer Relationship Management) systems became widespread in 2000 and this year sees the flourishing of electronic retail trade (Amazon, e-Bay and web shops) which have the ordered goods delivered by courier services. Social networks appeared: wiw.hu (2002), facebook.com (2004) and twitter.com (2006).[91]

Outsourcing informatics services slowed down and came to a halt in the first decade of the new millennium due to the cheap information devices and the great number of well trained IT experts. However, the past decade pointed out once again the possible advantage of outsourcing: outsourcing changed into activity optimization and huge multinational informatics service providers started to offer their different services which can replace most of the services operated at the particular organisations. Such service was provided from a calculation cloud. The name comes from the icon used in informatics in which a cloud stands for networks whose inner structure is not important, only the input and output are of importance.

As regards the technical part, the corner stone of the service is virtualization, which has been on the market for a decade but has gained real significance and become really widespread only in recent years. In the framework of virtualization one or more virtual systems (guest) are run on one or more physical systems (host). The hardware running the virtual system is

[91] Racskó, 2011.

not real but obtains its resources from the host system. In a virtualized system the resources of the host system can be allocated among the guest systems in any manner. Virtual systems are supervised by the hypervisor programme. With virtualization, complete systems with virtualized network elements can be created. In this way, for example five servers separated by firewalls may be running on three physical machines and processor time and memory are granted depending on needs. It follows, that it is impossible to know on which physical host a given guest server is running, it can be determined only by the help of the hypervisor, but it may run on all the three.

Cloud computing differs from virtualization in that virtualized systems are realised on physically separate premises with operating personnel, high availability and high level optimization.

Cloud services can be classified according to the nature of the service provided each of which is called XaaS – something as a service. Thus, basically there is infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). In addition to these major categories there are other elements too, such as development as a service (DaaS) used by Salesforce.

In the framework of IaaS, the supplier provides a virtual hardware environment for the client. This includes the virtual system with storage space and network infrastructure operated by the supplier. The operating system and the applications are installed and maintained by the client. In the case of PaaS, the scope of the supervision of the supplier is broader: it provides the operating system, the database, certain applications and development tools in addition to the virtual system. The client installs and supervises the applications. In the case of SaaS, the supplier provides all elements of the environment, while the client has access to the functionality of software. The environment is usually accessed through a thin client by the help of a browser. The user merely uploads data and is responsible only for them. The client can use certain applications, like word processors, spreadsheets, other office applications and any special software or CRM systems. The service fee may be calculated on the basis of the number of accesses or time but in either case the client pays only for the actual use.

At present only a few cloud services with narrow scope are available. Google offers office applications. Amazon, Rackspace Hosting, Yahoo and Microsoft offer virtual machines, Salesforce provides CRM system and Zoho all these.

Google provides a SaaS service under the brand name Google Apps.[92] In the framework of the service a business email system can be created, for which 25GB disc space, spam filtering and 99.9% availability is provided. It allows for using a common company-wide calendar, scheduling events, sharing calendars and synchronizing the contents of such calendars with the calendars of mobile devices. It also includes document management, text files, spreadsheets and presentations can be uploaded and edited. Company email groups can be created, contents can be shared and archived and all contents and antecedents can easily be retrieved. Websites can be created with the company's own domain name, secure connections

[92] See Google Apps for companies. http://www.google.com/intl/hu/enterprise/apps/business

and separate sites can be created thus company intranet can be replaced with this service. Internal video sharing is also possible. The fee of the service is quite reasonable, $ 50 per user per year. It is far cheaper for Hungarian SMEs than maintaining such infrastructure and services from their own sources. Besides, assistance is available on the phone and via email 24 hours a day. Guaranteed availability includes eight hours of service interruption per year. Web based customer service is provided on a self-service basis through an encrypted SSL channel. The filtering of unwanted emails can be individually customized. Common password can be defined as a security requirement, emails can be forwarded and there is a possibility of the migration of former contents.

Another similar software as a service is Salesforce.[93] It offers various applications to businesses, such as software automating sales and managing customer relationship, tools performing customer service and support. The use of the software development tool (force.com) costs 90 cents per access and any application using the above services can be developed by this tool, such as data processing, process supporting and business intelligence applications. To highlight the difference, the company called this service development as a service. Its low access fee enables smaller organisations to use high level tools for developing their applications. It has more than fifty thousand applications available. These include for example debt management, human resource management, time management and food ingredient management. A great advantage of such pricing is that development costs can be directly assigned to the different organisational units. In this way it can be established how much the particular departments spent and how many time units can further be assigned to them. This price is currently a discount price which will later rise to $5. Unlimited use costs $50 per user. It includes the use of the development platform but the use of other systems, for example CRM system is extra. The third similar provider is Amazon, which, unlike the others, provides infrastructure under the brand name Amazon Elastic Compute Cloud (EC2)[94] and not service or platform. This practically means that a virtual machine can be used for a fee which includes a computing capacity, memory capacity and hard disc store space. This environment can be used through various operating systems and other system level applications, such as databases, application development tools and authentication management. Own virtualized environments can also be uploaded. Invoicing for the service is based on the resources used. Computing performance is measured in EC2 compute units. The service can be tried for free for one year with a basic LINUX package. The price of the services ranges from $0.095 to $1.16 per hour in the European region.

The fourth provider is Microsoft, which offers a .NET platform as a service under the brand name Windows Azure.[95] In this way it can run any Windows application on practically any platform. The guaranteed availability is 99.95%. Prices are basically calculated in a manner to be the same as the prices quoted by Amazon but they include a new factor as well, namely store transactions. This may substantially increase the overall cost.

[93] See Salesforce.com, http://www.salesforce.com
[94] See Amazon Elastic Compute Cloud. http://aws.amazon.com/ec2/
[95] See Windows Azure. http://www.windowsazure.com

On the homepage of Microsoft there is a calculator for determining the total cost of ownership (TCO) of the Azure services for a period of three years and it can be compared with the cost of the systems operated on the premises of the business. Not surprisingly, the Azure is the winner according to the calculations.

According to the rules of the cloud services such a public utility-like service is on the whole cheaper than the systems operated at the particular companies even if it entails higher costs as only actual use is invoiced for. Dynamic resource allocation is always more favourable than planning based on prediction because if the prediction is not accurate, the resource is simply not used. The total cost is the sum of the various partial costs unlike in the case of traditional systems where it can be higher. The resource needs are summed up and in this way the otherwise fluctuating tendency of use is levelled up. Due to the huge computing capacity included in the cloud, the cloud is better protected against different distributed attacks. Parallel processing can substantially accelerate business intelligence applications. As the different resources are allocated to different premises, the system is more reliable and less vulnerable for example in the case of natural disasters as opposed to the company's data centre, which can generally be found on the premises of the company; the data centres of the cloud are established at optimal places (energy, telecommunication).

Gartner, an advisory company acting on the market of IT products and services which is famous among others for its predictions, prepares the expected lifecycle curve of technologies. Cloud applications have commanded a great interest since 2009, they nearly reached the peak in 2010 and they are predicted to become fully ripe within two to five years. The next similar area will be the creation of public clouds.[96]

One of the advantages of cloud services is that in return for a low fee you get a well scalable system which can easily be configured with shared resources and network operation.

In respect of cloud services, being bound to a service provider represents the prime security challenge.[97] This means that the systems and applications currently deployed in the cloud are not standard and do not allow for permeability on the small market. While importing data when using the service is easy and backed by the provider, exporting data is extremely irksome and is deliberately made difficult by providers once the service is cancelled. A further special problem is that in the case of software as a service exporting data hardly makes any sense as relations stored in the CRM database by Salesforce are difficult to interpret outside the database. It is quite likely to happen, its impact is moderate and on the whole its risk level is high. This problem may occur when changing providers and also if the provider goes into liquidation. In such a case the whole database may be lost. However, its likelihood is low according to different surveys since providers are multinational companies of solid capital listed on the American stock exchange.

A further risk is the loss of control over the system operating in the cloud, which may occur due to the non-clarified allocation of roles, the undetermined system of responsibilities and

[96] Fenn, 2010
[97] Catteddu/Hogben, 2009

the inaccessibility of the source code. Its likelihood is regarded to be quite high, its impact quite high in the case of IaaS and low in the case of SaaS and the resultant risk high.

The third greatest risk derives from unsuitability. The suitability of the systems must be certified for the sake of compliance with different statutory instruments and standards, but the cloud does not allow for this. Its reason is that assuring the possibility of an audit would mean an excessive cost for the provider who is not compelled to better cooperate with the client on the seller's market. Its likelihood is regarded to be quite high, its impact quite high and its resultant risk high.

Services rendered in this way are really cost effective, big corporations install their computer fleet in the neighbourhood of power plants and transatlantic data cables so that their operating cost can be the fraction of their own server operated on the premises of the corporation. Considering the increased price sensitivity of business entities due to the economic downturn, the price of the service is the main factor to be taken into consideration when purchasing. In the case of an own server, the building, the maintenance of environmental conditions (temperature, humidity), electricity, expert personnel, etc. must be paid for. In the case of a remote service, it is enough to pay for an IT expert and the service which, in addition, is a well traceable cost element.

This was a $17 billion business in 2009 but will grow to be worth $45 billion in 2013 according to the prediction by IDC. The tendency will be similar in other parts of the world as well, for example in the European Union including Hungary, only its development will take longer. Although costs and environmental pollution can be minimized by this solution, it raises security and statutory compliance issues which at present seem impossible to be solved in Europe. Cloud service providers build their computing centres in different parts of the world and as resources are dynamically allocated, even they cannot tell in which part of the world the service we use or our clients' data are at the given moment.[98] Under the effective European data protection directives data can be transferred to places where data protection is the same as in Europe, consequently it will exclude most of the premises of the providers. Individual contracts cannot be concluded with the providers (taken the size of small and medium enterprises), neither do they undertake the requirements concerning availability and compliance which were standard in the case of outsourcing agreements. At present this is a seller's market thus service providers do not care for these needs and concerns, however, as market gets saturated, they will offer more sophisticated solutions. For instance European personal data may exclusively be managed in cloud servers located in Europe or a new European supplier may enter the market just for this reason. Entering the market requires an unbelievably huge amount of money, suppliers currently present on the market offer the resources of their systems built formerly for other purposes in the framework of cloud services.

In addition to cloud services, using spyware, monitoring traffic and telephone tapping are regarded as a danger to employees' data. A spyware is an application running in the

[98] Spivey, 2009

background on the computer which records the activity or parts of the activity performed on the computer and then sends this information to a third party. It can also be used by employers when the spyware installed on the computers of all employees sends a report to the employer for example about the time spent on working on the computer, websites visited or even characters typed and mouse activities.

Monitoring network traffic for surveillance purposes can be performed at all network junctions but it typically occurs at the external firewall of the company (protecting the internet connection). External network traffic can be monitored and recorded there or even the whole traffic can be recorded. The employer typically records the websites visited and can permit or prohibit access to websites in a whitelist- and blacklist-based manner. If there is no recording only filtering, there is no data protection dimension attached to its implementation, however, in all other cases there is.

Data recording devices which are specially produced for monitoring system administrators in an unchangeable and inaccessible manner are now available on the market. Such systems allow for recording the activities of privileged users in an undeletable way. It is an essential issue who can have access to, delete and modify such recorded data. System administrators are typically authorized to have access to and modify anything. This should be taken into account when determining rules. There is no pint in stipulating that recorded data may be seen by a panel consisting of the managing director, the human resource manager and the representatives of the employees if technically the system administrator can do the same at any time. Technical (not only legal) measures ensuring lawful access should be introduced.

There has been a long established need on the side of employers for defining and displaying on a map the exact physical position of employees, however, the possibility of it is quite new. Tachographs could only record the distance covered and the speed at the beginning of the ‘90s, but today real-time monitoring is possible which is mainly ensured by satellite navigation systems (GPS) and wireless telecommunication systems. The position of the employee can be defined for the purposes of the protection of life and property (e.g. protected persons, transport of valuables), assessing the amount of work performed (e.g. transport of goods) or simply recording working hours (where is the employee? in the office, with a client or at home?). The most precise method of monitoring is to place a GPS receiver in one of the devices (typically in the company car) of the employee and it sends the actual position to the data centre through the data connection of the built-in mobile phone module. A further possibility available at most of the mobile phone companies is to define the approximate position from the data of the mobile phone network and then send it to the client. This service is available to fleet subscribers.

3.2. Privacy enhancing technologies

The concept of privacy enhancing technologies **(**PET) can be defined as follows:

Privacy-Enhancing Technologies is a system of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or

unwanted processing of personal data, without the loss of the functionality of the information system.[99]

According to some interpretations the concept of PET includes for instance the following:[100]

- encrypted storage of biometric data from which the original image of the fingerprints cannot be restored
- the possibility that data subjects can check and update their personal data through an encrypted connection
- tagging data by which the data protection conditions of use attached to the data can be reached directly

Nevertheless, the most significant progress can be noticed in the area of privacy policy languages.[101]

Such languages make it possible to reconcile various data processing needs with authorizations. It happens more and more often that a web page asks for authorization to store data storing cookies or we cannot read the conditions of data processing until afterwards. On the contrary, in the case of privacy policy languages both the data required by the provider and the authorizations to be given by the user can be specified in advance. Before the actual commencement of data processing the machines of the provider and the user cross check the data protection settings through a data protection communication layer and then proceed accordingly. In the case of so called external languages it normally does not mean the enforcement of the settings, it has only a declarative purpose. However, in the case of internal languages which are typically used by enterprises, settings are enforced. An example of external languages is Platform for Privacy Preferences (P3P), accepted by W3C, which is an XML based structured language. It can be used by the help of accessories in browsers common nowadays. Its latest, 1.1 version appeared in 2006. Although it is quite popular, mainly in the United States, it has several defects. For instance, settings cannot be enforced, the settings of multiple users cannot be handled jointly and neither can detailed legal provisions be appropriately dealt with. APPEL (A P3P Preference Exchange Language) and XPref languages were created to complement and improve it. Enterprise Privacy Authorization Language (EPAL) and eXtensible Access Control Markup Language (XACML) are internal privacy policy languages. IBM Tivoli Privacy Manager enables the use of privacy policy languages and the enforcement of internal data processing rules in a corporate environment.

In addition to the languages, techniques ensuring data minimization and anonymization have an important role; these techniques terminate the personal character of the data unlike traditional technologies which ensure the less efficient confidentiality by encrypting personal data, storing and dispatching them in a secure manner. According to European data protection law personal data retain their personal character and enjoy legal protection as long as they can be linked to the natural data subject. This link is terminated by anonymization and the

[99] Blarkom/Borking/Olk, 2003
[100] ICO, 2007
[101] Wang/Kobsa, 2008

personal identity of the data subject is separated from the digital traces of the online activities performed by him.[102]

One such solution is the strip identifying headers and resend technology, which appeared in the form of anonymous email remailer and anonymizer proxy services, such as Connexion Anonymizer.

Another option is onion routing, where data subjects establish contact with the provider through several proxy servers randomly connected to each other. As proxy servers do not keep the log files about connections and they operate in different countries under different jurisdictions, the real location of the data subject is practically impossible to be determined. A huge drawback of this procedure is that unlike former means, in addition to providing a certain level of protection of personal data, it has become one of the basic means of cybercrime by covering the exact location of the attacker.

Another method is k-anonymity, which hides data in a mass like steganography. According to the underlying concept, if the data of the data subjects are processed jointly, groups can be created in which all data can be connected to k data subjects, thus these data cannot unambiguously be connected to a particular person.[103]

Another method for data minimization is pseudonymity. Pseudonyms can be classified as public pseudonyms where the link between the pseudonym and the data subject is initially public and initially unlinked pseudonyms where the link – at least in the beginning – is known only to the data subject.[104] In this latter case the pseudonym must unambiguously identify the given data subject enabling for example the administration of affairs at an authority. Consequently, the issue cannot be solved by randomly selecting a user name or an email account. The first group of public pseudonyms is the easiest to realize but it does not mean real data protection. The second group includes state identifiers (identity card number and social security number) and identity broker services. The third group can be realized by biometric identifiers not stored centrally, which represents the greatest technical challenge.

Authentication and identity management is rather an issue of information security than PET. Authentication can be implemented in well-known ways: on the basis of knowledge (e.g. password), possession (e.g. chip card) or characteristics (e.g. fingerprint). However, it is an issue of data protection whether the data subject has the possibility to differentiate profiles and use the different services with different profiles; the identity management system protects our private sphere in this way. The OpenID system is one such solution.[105]

The core of the applicability of PET systems is usability, satisfying the needs of ergonomics and convenience. These technologies are not as widespread in Europe as they were expected to be.[106]

[102] Gürses/Berendt, 2012, p. 305.
[103] Sweeney, 2002, pp. 557-570.
[104] Raguse/Langfeldt/Hansen, 2008
[105] see: www.openid.net
[106] Székely, 2008

3.3. The accountability of data protection requirements

Data protection is typically an area for lawyers, while data security is an area for IT experts; consequently their language is based on their professional language, respectively. Nevertheless, laws on data protection regulate the area of data security as well. Due to the statutory regulation of information security, at present there is a gap between legislation and the application of law (lawyers) and the implementers of the provisions (information specialists). Its reason is that it is hard to recognize the technical content behind the legal requirements. Requirements are superficial, the main reason for which is technology-independence, but this superficiality makes the application of law far more difficult.[107] For example what the following provision covers is uncertain: "controllers [...] shall make arrangements for and carry out data processing operations in a way so as to ensure full respect for the right to privacy of data subjects in due compliance with the provisions of this Act and other regulations on data protection"[108]. Virus detector, backing up to DVDs, offsite backup or complex external audit in compliance with ISO/IEC 27001 standard? The answer might be compliance with the relevant standards, but to what extent? Relying on his commonsense, the information specialist tries to assess what is worth introducing, but where is the borderline of negligence? How can compensation be sought if damage is caused?

Security is always implemented on the basis of risks and business needs endeavouring to achieve proportional protection. Now we are going to give an overview of security measures taken in the IT centre of a big corporation which can be tailored according to the needs of smaller organisations. Proposals concerning actual implementation are always put forward by an expert after due consideration and risk analysis and approved of by the management.

In respect of the regulatedness of information security, data protection can be regarded as an area regulated superficially,[109] as statutory provisions have been stipulated but have not been detailed by the legislator, consequently those applying the law and those obliged to observe the law can interpret them only with difficulty which makes voluntarily abiding by the law extremely difficult. The problem is aggravated by the fact that the legislator used the terminology of civil law when stipulating the statutory requirements, thus expressions like "best expectable" and "adequate" are frequently used. In most of the cases the obligor of the statutory provisions does not – and cannot – have the professional knowledge required to directly interpret these requirements. Moreover, these requirements have severe legal consequences including fines imposed by authorities, criminal responsibility and compensation enforceable in a civil proceeding.

Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information deals with the informational security aspect of data protection in one subsection superficially stipulating the rules to be observed by data controllers and data processors in the course of their activities.

[107] Reidenberg, 1998, p. 584.
[108] New DPA, § 7
[109] Szádeczky, 2011

In part of the Privacy Act entitled "Data security requirement" the following is provided: Controllers, and within their sphere of competence, data processors must implement adequate safeguards and appropriate technical and organizational measures to protect personal data, as well as adequate procedural rules to enforce the provisions of this Act and other regulations concerning confidentiality and security of data processing.[110] Relying on the detailed analysis by ANDRÁS JÓRI[111] it can be claimed that data security and thus a particular part of informational security falls under the scope of the statutory regulation pertaining to data protection. Subsection (1) reinforces the connection between data protection and data security and prescribes the prevalence of the requirements of data protection taken in narrow sense in information systems and thus the application of the requirements connected to data quality and purpose boundness. It provides for compliance with other provisions of law thus with acts and statutory instruments on sectoral data protection (e.g. Act XLVII of 1997 on the Processing and Protection of Health Care Data and Associated Personal Data and Act CXII of 1996 on Credit Institutions and Financial Enterprises) and on data protection (e.g. Act CLV of 2009 on the Protection of Classified Data and Government Decree No. 161/2010. (V. 6.) on the Detailed Rules of Electronic Security of Classified Data and the Authorization and Official Supervision of Encrypting Activities). These areas can be regulated to a depth other than the area of data protection.

Handling medical data might create a new dimension of abuse especially in information systems. This is why this area is paid much attention all over the world both by legislation (e.g. US Health Insurance Portability and Accountability Act, HIPAA) and standardization (e.g. ISO 27799, ISO 22857).[112] Its recognition incited the Hungarian legislator as well to adopt a special sectoral regulation on handling medical data, although the practical realization of the higher level protection is far from being perfect.[113] The Commissioner for Data Protection has a lot of cases in connection with handling medical data.[114]

The expected measures and rules of procedure have not been defined. The possible measures and procedures are not known, though the obligor can proceed basically correctly if he creates his technical data protection on the basis of informational security standards. However, the fact that the requirements laid down in the standards stipulate an excessively high protection which is not proportionate to the dangers personal data are exposed to. When establishing protection, proportionality should be a consideration, otherwise the cost of protection will be unnecessarily high. The Privacy Act emphasizes proportional protection: "In determining the measures to ensure security of processing, data controllers and processors shall proceed taking into account the latest technical development and the state of the art of their implementation. Where alternate data processing solutions are available, the one selected shall ensure the

[110] New DPA, § 7 (2)
[111] Jóri, 2005, p. 258.
[112] Kokolakis/Lambrinoudakis, 2005, p. 49.
[113] Alexin, 2010, p. 104.
[114] For further details see Trócsányi, 2007

highest level of protection of personal data, except if this would entail unreasonable hardship for the data controller."[115]

"Data must be protected by means of suitable measures against unauthorized access, alteration, transmission, public disclosure, deletion or destruction, as well as damage and accidental loss, and to ensure that stored data cannot be corrupted and rendered inaccessible due to any changes in or modification of the applied technique."[116] The legislator gives examples of risk elements which in general correspond to industrial groupings. It is advisable to make a risk analysis about risks endangering the system and process of handling and processing data and about their occurrence and though it is not required by the act on data protection, in areas regulated in detail – like the financial sector – it may be so and it may also be a professional expectation. The statutory provision expressly refers to the case of becoming inaccessible due to changes in the applied technique, which highlights the greatest danger of computer literacy, i.e. the problems of the long term storage of electronic data.[117]

In the course of its investigation the authority for data protection has powers to inspect all documents of the controller inspected, presumed to have any bearing on the case at hand, and may request copies of such documents, can have access to any data processing operation presumed to have any bearing on the case at hand, can enter any premises where data processing takes place and may request written or oral information.[118] Data protection inspections covered certain aspects of the fulfilment of requirements which fundamentally affect the informational security of data, though not in its entirety. Thus formally the commissioner for data protection examined the management of authentication, logging in IT systems,[119] and the existence of physical security measures within the framework of county inspections.[120]

The extent of the implementation of data protection measures can be examined, which may be performed by an internal audit, an external enterprise or the authority according to the German model (based on ROßNAGEL).[121] There is a demand for data protection audit even in the United States, where data protection is not regulated in detail.[122] At present audits can be implemented by external enterprises in Hungary. Voluntary external official audits are also possible.

Notwithstanding all this, the provisions referred to above do not determine the extent of the expected controls over informational security, the way of complying with them or their rules of procedure. There is no statutory instrument on the implementation of the act or other – for example official – recommendation concerning it. There is no judicial case law concerning substantial security measures either.

---

[115] New DPA, § 7 (6)
[116] New DPA, § 7 (3)
[117] Szádeczky, 2010. pp. 123-136.
[118] New DPA, § 54 (1)
[119] DPC, 755/H/1997 and DPC, 756/H/1997
[120] DPC, 194/H/1999, DPC, 196/H/1999 and DPC, 435/H/1999
[121] Balogh/Jóri/Polyák, 2002. p. 325.
[122] DeJarnette/Morin, 2010.

Data security is an important element when determining the aspects of data protection audit. The requirements laid down by the new act on data protection are far more detailed in this respect. First of all it stipulates as a general principle that data controllers must plan and perform all data processing activities so as to ensure the protection of the private sphere of those concerned in the course of applying the act on data protection and other provisions of law pertaining to data processing (principle of privacy by design). When determining and applying measures ensuring data security, data controllers and data processors must take account of developments in technology and from among the available options choose the solution which ensures the highest level of the protection of personal data unless it would entail unreasonable hardship for the controller.[123] These provisions extend the data protection approach which expressly connects the assertion of data protection guarantees to the relevant security and organisational procedures of the controller and which has already been established in electronic telecommunications and electronic commerce[124] over the whole area of data protection regulation. This approach brings about the appreciation of data protection requirements and is based on the perception that the statutory conditions of data protection cannot prevail without adequate data security. In addition to this, the act sets forth a number of concrete expectations from the prevention of unauthorized data input and the controllability of access to the data processing system to the assurance that installed systems may, in case of interruption, be restored;[125] these expectations must be observed by data controllers and processors and can be included in the aspects of auditing.

An undisputedly positive feature of the new regulation is that it at least refers to the principle of security proportional to risk; nevertheless, it is still a considerable compliance risk that the legislator hardly provides any specification as to the actual level of data security. In this respect information security and quality control standards can give guidance. The alignment of the requirements of law and information security is described in Chapter 4.

It follows from the above that data protection auditing and certification – whether performed by the authorities or market actors – must cover data security requirements to a certain extent. Considering that the certification of data security standards is a common service[126], taking into consideration the methods applied in such procedures of certification when elaborating the methodology of data protection audits seems to be more than reasonable.

3.4. Aligning the requirements of data security

The solution to the problem caused by the difference between the vague requirements set forth by law and the concrete technical security measures is to align certain elements of a well-known and widely applied standard with the statutory requirements concerning information security, which can serve as a basis and reference point for both parties (the legal and the informatics side).

[123] New DPA, § 7 (1), (6)
[124] See Section 13/A (3) of Act C of 2003 on Electronic Communications and on Electronic Commerce and Information Society Services
[125] New DPA, § 7 (5)
[126] Reference to standards etc.

Two information security standards can be suitable for serving as a unified framework system when applying a certain system of rules pertaining to information security and governance. By matching the requirements of standards with statutory provisions pertaining to information security and establishing mutual alignment, the requirements laid down in statutory instruments and in this way translated into the language of informatics can be implemented on the basis of the detailed specifications of information security standards. Data protection regulations stipulate an adequately small number of concrete information security requirements which can be given a positive form in this way. Alignment can be implemented by matching the smallest requirement unit of the chosen standard (the purpose of the control or regulation depending on the standard) with a section of the data protection provision. The extent of coverage (alignment) can be defined at four levels:

- Surpassed: as regards content, the statutory provision surpasses the given requirement unit in respect of information security;
- Total coverage: the statutory provision fully corresponds to the given requirement unit in respect of information security;
- Partial coverage with one or more overlapping aspects: the statutory provision partially corresponds to the given requirement unit in respect of information security, in other words the statutory instrument does not provide for the security aim defined in the whole requirement unit;
- No coverage: the statutory instrument does not provide for the implementation of the given requirement unit.

Coverage is expected to be partial or missing due to the vagueness of legal regulation. Statutory requirements mainly concern the information criteria of confidentiality, integrity and availability. It is not surprising as they are considered to be of utmost importance by the data protection directive and by national regulations.

The general requirements stipulated in statutory instruments pertaining to data protection can be aligned with a lot of controls, though in a less defined way. These alignments should be established through professional discussions and conciliations, which mean that they will contain subjective elements. However, such wide professional discussions and several rounds of conciliation facilitate the process of these subjective elements turning into general practice. Materials of this kind do not have a finite state. If we run out of proposals aiming at the improvement of the present state of affairs, the amendments of statutory instruments and standards will still require further changes.

3.4.1. Using best practice

If we are about to implement security measures, one choice is to use general best practice. This chapter shows what measures are expectable from a middle sized information-oriented company.

When designing buildings, close attention must be paid to architectural security so that the computer room should be located on the ground floor of an inner building. Possible points of physical entry, protection against natural and artificial waters, vibration caused by traffic

outside and shielding against electromagnetic radiation must also be taken into consideration. In certain cases protection against explosives and chemicals must also be provided.

The aim is to have concentric circles of protection around the building. This means the implementation of adequate shell and outdoor protection. In the case of the parts of buildings above ground level protection against electromagnetic radiation can be implemented by a Faraday cage. In the case of underground parts of buildings the structure of reinforced concrete in itself can be regarded sufficient.

One of the most important resources of the machine room is electrical power, the adequate supply of which and also its emergency supply must be ensured at several levels. Input power to the facility should be fed into from two separate substations with adequate protection. Continuous power supply should be ensured by applying uninterruptable power supplies which can overcome short power disruptions. For cases of longer interruptions diesel generators can be installed.

The importance of maintaining the adequate environment can hardly be overemphasized in this field. The temperature and humidity of the air can be maintained at the appropriate level by air conditioning appliances, at the installation of which redundancy and replaceability should be kept in mind. Air conditioning machines should be installed in pairs, moreover, it is most useful if a neighbouring appliance can perform the task of another appliance in the case of a shortfall. The close connection between long term data storage and the humidity of air can be shown when saving both online and offline (on a data carrier).

In addition to the fire-protection equipment usual in buildings, the protection of server rooms must meet stricter requirements in terms of faster fire-fighting and damage minimization. As regards sensing fire, the installation of aspirating smoke detectors which sense fire faster and with more certainty is general practice. It consists of a central fan unit, a network of sampling pipes to draw in air and an analysing appliance built in the server room. As this solution is rather costly, optical smoke detectors are still more widespread. As regards fire-fighting, the use of an automatic fire extinguishing system is a fundamental requirement. Fire is usually extinguished by some inert gas, but there are attempts to use water fog fire extinguishers.

Although server rooms are guarded similarly to other facilities, creating protected sectors and differentiating between authorized accesses based on roles are of a greater importance. One fundamental requirement is to manage central authentication by a two-factor authentication, for example by proximity card and PIN code identification. Rights are expediently allocated in a central unit with the joint consent of the direct superior of the given employee, the person in charge of the business process and the operational or security leader of the server. Authentications allocated in this manner should be reviewed at least annually together with the automatic or manual comparison of authentications and permits. The cause of any derogation must be examined. Logging entries into the facilities can be done only for a limited period of time; that is why any illegal entries and authentication transgressions must be detected and investigated within this period. Data that can be used as evidence can usually be stored longer, until a report is made to the police or a disciplinary proceeding is closed. When creating security sectors, areas used by maintenance and logistics staff should

physically be separated from IT sectors. Servers should also be placed in different rooms according to the different functional and security aspects. The camera surveillance of protected sectors, especially passageways and working areas is also necessary. Recordings made here should also be kept for three days. Server rooms should not have windows or doors opening to unprotected spaces. If they do, the protection of such server rooms require utmost attention by using security gratings, glass break detectors and passive infrared sensors installed on the protected side.

Passive infrared sensors should also be used in the protected area itself. There should be sluice doors for security purposes but for the protection of life they must open by a door handle from the side of the server room with the emergency key placed next to the door. Its purpose is to ensure immediate escape in the case of flooding with extinguishing gases. A press-button for blocking the release of the extinguishing gas must also be placed inside the protected room for the protection of life.

The network of the information system must be separated from the internet, which is usually implemented by hardware firewalls. All outside traffic must flow through firewalls and in the case of protected data by deploying encrypted protocols (e.g. HTTPS, SFTP, SSH). Traffic inside the server room may flow without encryption provided leaking from the network and unauthorized access can be excluded. Logging in the servers should be made possible by access allocated individually to persons and authorized at several levels just like in the case of entry to the server room. Both successful and unsuccessful logins to the servers and in the case of strictly protected systems each activity must be logged; these logs must also be protected. Logs should be gathered to a central place (log server), to which only the staff of the security department can have access. Logging activity is indispensable for the purposes of evidencing and detecting illegal acts. Log files should frequently be saved for example daily just like the system and these backup files should be stored at some other premises which will not be affected by a disaster striking the server room. If traffic between premises flows electronically, it must be implemented in an encrypted form and sent and received contents must be compared with each other; if transport is performed physically, the security procedures common in the case of transporting valuables must be followed.

Disaster situations in which the infrastructure of the organisation can significantly be damaged or destroyed deserve particularly careful attention and planning in the case of important systems. The technical documentation of the planning is called Disaster Recovery Plan (DRP), which contains the organisational and technical tasks required in the case of a disaster together with the detailed description of recovery. This includes the order of purchasing and configuring the systems to be used for recovery, the method of recovering the data and the provision of the appropriate operating staff. For the case of disaster situations a spare system identical with the live system may be kept running continually outside the premises or a system installed outside the premises but used only in an emergency. Another solution is to conclude a contract with the distributor of the hardware in which the distributor undertakes to provide the appropriate hardware within a short time. An often neglected task is to carry out disaster testing to check the operability and feasibility of the plan. During disaster testing it is useful though not indispensable to shut down the live systems since it can cause

shortfalls in the service if plans and measures are not appropriate. A more frequently used method is to have the staff practise the steps of the plan on the test system. Another plan in connection with disasters is the Business Continuity Plan (BCP), which approaches the problem from a business aspect, from the aspect of ensuring the continual operation of business processes.

The procedures and methods described above can be regarded as best practices of the industry, however, the requirements imposed on them depend very much on the given area. For instance in the case of financial institutions the authorities expect the fulfilment of the strict security requirements described above, while statutory provisions are not as strict in the case of an electric telecommunication provider. In other, less regulated areas, for example in electronic commerce and in handling personal data the legislator expects the application of the above methods to an even smaller extent. However, endeavouring to observe these requirements, as best practice of the industry, can be expected so that the organisations provide the protection that can be expected of them. Nevertheless, the relationship between endeavouring and implementing should be determined.

3.4.2. COBIT

In 1992 Information Systems Audit and Control Association (ISACA) as an internationally appreciated American IT auditor association and IT Governance Institute (ITGI) jointly developed the Control Objectives for Information and Related Technology (COBIT), a de facto information security standard, as the framework system of IT governance. It stipulates requirements for several information processes. COBIT is a generally accepted collection of practices, actually a method of information auditing and governance assistance, based on business requirements. It has never become a de jure standard, and compliance to it cannot be certified. COBIT 4.1 contains 34 high level processes including 210 control goals centred on four areas:

- Planning and Organization
- Acquisition and Implementation
- Delivery and Support
- Monitoring and Evaluation

COBIT processes are as follows:[127]

- Planning and Organization
  - PO1 Define a strategic IT plan
  - PO2 Define the information architecture
  - PO3 Determine technological direction
  - PO4 Define the IT processes, organisation and relationships
  - PO5 Manage the IT investment
  - PO6 Communicate management aims and direction
  - PO7 Manage IT human resources

[127] COBIT 4.1. ©1996-2007 ITGI.

    - PO8 Manage quality
    - PO9 Assess and manage IT risks
    - PO10 Manage projects
- Acquisition and Implementation
    - AI1 Identify automated solutions
    - AI2 Acquire and maintain application software
    - AI3 Acquire and maintain technology infrastructure
    - AI4 Enable operation and use
    - AI5 Procure IT resources
    - AI6 Manage changes
    - AI7 Install and accredit solutions and changes
- Delivery and Support
    - DS1 Define and manage service levels
    - DS2 Manage third-party services
    - DS3 Manage performance and capacity
    - DS4 Ensure continuous service
    - DS5 Ensure systems security
    - DS6 Identify and allocate costs
    - DS7 Educate and train users
    - DS8 Manage service desk and incidents
    - DS9 Manage the configuration
    - DS10 Manage problems
    - DS11 Manage data
    - DS12 Manage the physical environment
    - DS13 Manage operations
- Monitoring and Evaluation
    - ME1 Monitor and evaluate IT performance
    - ME2 Monitor and evaluate internal control
    - ME3 Ensure compliance with external requirements
    - ME4 Provide IT governance

According to COBIT the focus areas of IT governance are as follows:

- Strategic alignment focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.
- Value delivery is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of IT.
- Resource management is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure.

- Risk management requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organisation.
- Performance measurement tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

COBIT pays marked attention to the theoretical background of IT governance, thus it analyzes the essence and the areas of IT governance and the interference and interrelation between the various requirements from a number of aspects. Although cooperation with other standards is not included in the express objectives of COBIT, several alignments have been made for example with ITIL, ISO/IEC 27002 and PMBOK standards through ISACA.

Since certification is not possible according to COBIT, no authentic data are available concerning how wide-spread it is. However, two globally recognised information security examinations which are recognised also by the United States Department of Defense (DoD) [128] namely the Certified Information Systems Auditor (CISA) and the Certified Information Security Manager (CISM) exams are based on COBIT. COBIT is the primary standard in the financial sector.

A further argument for applying COBIT is that it has already been aligned with several other systems of rules including ISO/IEC 17799 (now ISO/IEC 27002) PMBOK, ITIL, PRINCE2, COSO ERM, NIST FISMA standards and the Sarbanes-Oxley acts.

3.4.3. ISO/IEC 27001

A family of standards was set off in the United Kingdom and now they are well-known and used all over the world. BS 7799, a standard developed by the Department of Trade and Industry (DTI) in 1995, collects information security requirements applicable at management level. This became an international standard under the name ISO/IEC 17799. BS 7799-2, as a standard for information security management system, was developed in 1999 and attached to the former BS 7799, which was renumbered as BS 7799-1, and became international under the name ISO/IEC 27001, after which ISO/IEC 17799 was also renumbered as ISO/IEC 27002 and this was the start of the development of a family of standards for management systems like ISO 9000 series. A unique feature of the original standard was that it specified security requirements starting out from business needs in a top-down manner. ISO/IEC 27001 was developed to serve as a model for the development, implementation, operation, monitoring, auditing, maintenance and improvement of information security management systems (IBIR, ISMS).[129] The standard is process-centred, applies the Plan-Do-Check-Act (PDCA) model and the implemented IBIR can be integrated into existing quality control (ISO

[128] Department of Defense, Directive 8570
[129] ISO/IEC 27001:2005, p. 19.

9001) and environmental management (ISO 14001) systems. In respect of requirements the standard ISO/IEC 27002 should be used.

The most important members of ISO/IEC 27000 standard series published or in preparation are as follows:

- ISO/IEC 27000:2009 Information security management systems – Overview and vocabulary: it describes the main principles of the standard series and defines the key terms.
- ISO/IEC 27001:2005 Information security management systems – Requirements: it describes the requirements of the management system; its latest version is in preparation.
- ISO/IEC 27002:2005 Code of practice for information security management: it describes the requirements of practice; its latest version is in preparation.
- ISO/IEC 27003:2010 Information security management system implementation guidance: it gives guidance for implementation.
- ISO/IEC 27004:2009 Information security management – Measurement: it deals with measuring the level of security.
- ISO/IEC 27005:2011 Information security risk management: it describes the methods of assessing risk; it was developed from ISO/IEC 13335-3 and ISO/IEC 13335-4.
- ISO/IEC 27006:2011 Requirements for bodies providing audit and certification of information security management systems: it specifies the requirements for bodies providing certification under ISO/IEC 27001.
- ISO/IEC 27007:2011 Guidelines for information security management systems auditing: it contains guidelines concerning the method of auditing.
- ISO/IEC TR 27008:2011 Guidance for auditors on ISMS controls: it provides guidance for auditors about controls under ISO/IEC 27002.
- ISO/IEC 27010:2012 Information security management for inter-sector and inter-organizational communications: it is about communication between organizations belonging to different sectors.
- ISO/IEC 27011:2008 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002: it contains special requirements for telecommunication providers.
- ISO/IEC DIS 27013 Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001: this standard will give guidance on the integrated implementation of IBIR under ITIL and ISO/IEC 27001 standards, in preparation.
- ISO/IEC DIS 27014 Information security governance framework: it will specify the framework of information security governance, in preparation.
- ISO/IEC PDTR 27015 ISM guidelines for financial and insurance service sector: it will provide guidance for the financial and insurance sectors, in preparation.
- ISO 27799:2008 Health informatics – Information security management in health using ISO/IEC 27002: it contains special requirements for health care providers.

The chapters of ISO/IEC 27001:2005 standard are as follows:

0. Introduction
1. Scope
2. Normative references
3. Terms and definitions
4. Information security management system
5. Management responsibility
6. Internal ISMS audits
7. Management review of the ISMS
8. ISMS improvements

Annex A (mandatory): Control objectives and controls

Annex B (informative): OECD principles and this International Standard

Annex C (informative): Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard

Considering that compliance with the standard can be certified, it may bring a business advantage to the company. As certification is performed by private companies and there is no mandatory register, it is nearly impossible to specify the exact number of certified companies in the world. However, there is an international register where those certified can voluntarily have their certificates registered. According to this register, the current number of ISO 27001 certificates is 7940. The certificates broken down to countries are as follows:[130]

Japan	4152	Netherlands	24	Belgium	3
UK	573	Saudi Arabia	24	Gibraltar	3
India	546	UAE	19	Lithuania	3
Taiwan	461	Bulgaria	18	Macau	3
China	393	Iran	18	Albania	3
Germany	228	Portugal	18	Bosnia Herzegovina	2
Czech Republic	112	Argentina	17	Cyprus	2
Korea	107	Philippines	16	Ecuador	2
USA	105	Indonesia	15	Jersey	2
Italy	82	Pakistan	15	Kazakhstan	2
Spain	72	Colombia	14	Luxembourg	2
Hungary	71	Russian Federation	14	Macedonia	2
Malaysia	66	Vietnam	14	Malta	2
Poland	61	Iceland	13	Mauritius	2
Thailand	59	Kuwait	11	Ukraine	2
Greece	50	Canada	10	Armenia	1
Ireland	48	Norway	10	Bangladesh	1
Austria	42	Sweden	10	Belarus	1
Turkey	35	Switzerland	9	Bolivia	1
Turkey	35	Bahrain	8	Denmark	1
France	34	Peru	7	Estonia	1
Hong Kong	32	Chile	5	Kyrgyzstan	1
Australia	30	Egypt	5	Lebanon	1

[130] International Register of ISMS Certificates. http://www.iso27001certificates.com/ Version 215 August 2012

Singapore	29	Oman	5	Moldova	1
Croatia	27	Qatar	5	New Zealand	1
Slovenia	26	Sri Lanka	5	Sudan	1
Mexico	25	South Africa	5	Uruguay	1
Slovakia	25	Dominican Republic	4	Yemen	1
Brazil	24	Morocco	4	**Total**	**7940**

These figures are obviously not fully reliable but can largely be regarded correct. The number of certificates issued does not correspond to the number of organizations certified. One organization may obtain several certificates because of the validity of scope, premises or time.

Due to the fact that this standard is used globally and is certifiable, it is particularly suitable for compliance purposes. In case an inspected organization has an ISO/IEC 27001 certificate covering the scope of the inspection, there is no need to examine again whether these requirements have been met.

LITERATURE AND REFERENCES

Alexin, Zoltán (2010): Adatvédelmi törvényünk – kisebb hibákkal, Infokommunikáció és Jog, Issue 3.

Barcelo, Rosa - Traung, Peter (2010): The Emerging European Union Security Breach Legal Framework: The 2002/58 e Privacy Directive and Beyond. In.: Gutwirth, Serge – Poullet, Yves – De Hert, Paul (eds.):Data Protection in a Profiled World, Springer, pp. 77-104.

Balogh, Zsolt György – Jóri, András – Polyák, Gábor (2002): Adatvédelmi „legjobb gyakorlat" kialakítása az elektronikus közigazgatásban, Kézirat, Pécsi Tudományegyetem, Állam és Jogtudományi Kar, Pécs

Bennett, Colin J. – Raab, Charles D. (2006): The Governance of Privacy. Policy Instruments in Global Perspective, The MIT Press

Berényi, László – Szintay, István – Tóthné Kiss, Anett (2011): Minőségügy alapjai, Miskolci Egyetem, Vezetéstudományi Intézet
http://www.szervez.uni-miskolc.hu/blaci/minmen/index.html [28.10.2012]

Bíró, János – Szádeczky, Tamás – Szőke, Gergely László (2011): A hírközlési szolgáltatók értesítési kötelezettsége a személyes adatok megsértése esetén (data breach notification), Infokommunikáció és Jog, Issue 2.

Blarkom, G.W. van – Borking, J.J. – Olk, J.G.E. (eds., 2003): Handbook of Privacy and Privacy-Enhancing Technologies. The Case of Intelligent Software Agents. TNO-FEL, The Hague

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

Cavoukian, Ann (2009): Privacy by Design. Take the Challenge http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf [18.10.2012]

CEN (2005): CEN Workshop Agreement (CWA), 15262-2005 on Inventory of Data Protection Auditing Practices, ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/DPP/CWA15262-00-2005-Apr.pdf [21.10.2012]

Dehghantanha, Ali (2011): Formal Methods for Analyzing Privacy Policies. Techniques for Formal Representing, Analyzing, and Processing Privacy Policies, LAP LAMBERT Academic Publishing

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

Dumortier, Jos – Goemans, Caroline (2000): Data Privacy and Standardization. Discusssion Paper prepared for the CEN/ISSS Open Seminar on Data Protection, K.U. Leuven, ICRI, https://www.law.kuleuven.be/icri/publications/90CEN-Paper.pdf [20.10.2012]

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

DPC, 755/H/1997, Az adatvédelmi biztos beszámolója 1997. Budapest, Adatvédelmi Biztos Irodája

DPC, 756/H/1997, Az adatvédelmi biztos beszámolója 1997. Budapest, Adatvédelmi Biztos Irodája

DPC, 194/H/1999, Az adatvédelmi biztos beszámolója 1999. Budapest, Adatvédelmi Biztos Irodája

DPC, 196/H/1999, Az adatvédelmi biztos beszámolója 1999. Budapest, Adatvédelmi Biztos Irodája

DPC, 435/H/1999, Az adatvédelmi biztos beszámolója 1999. Budapest, Adatvédelmi Biztos Irodája

Fenn, Jackie (2010): 2010 Emerging Technologies Hype Cycle is Here, http://blogs.gartner.com/hypecyclebook/2010/09/07/2010-emerging-technologies-hype-cycle-is-here [02.04.2011]

Guerin, Lisa (2011): Smart Policies for Workplace Technologies. Email, Blogs, Cell Phones & More, Nolo

Gürses, Seda – Berendt, Bettina (2012): PETs in the Surveillance Society: A Critical Review of the Potentials and Limitations of the Privacy as Confidentiality. In.: Gutwirth, Serge – Poullet, Yves – De Hert, Paul (eds.):Data Protection in a Profiled World, Springer, pp. 301-321.

Hassler, Vesna (2010): IT Security and Smart Card Standards. http://www.infosys.tuwien.ac.at/Staff/vh/papers/std.ps.gz [01.11.2010]

Herold, Rebecca (2011): Managing an Information Security and Privacy Awareness and Training Program, CRC Press, Taylor&Francis Group, Boca Raton

Hildebrandt, Mireille – Gutwirth, Serge (2010): Profiling the European Citizen. Cross-Disciplinary Perspectives, Springer

ICO (2001): Data Protection Audit Manual, UK Information Commissioner's Office, http://www.privacylaws.com/documents/external/data_protection_complete_audit_guide.pdf [11.10.2012]

ICO (2007): Data Protection Technical Guidance Note: Privacy enhancing technologies (PETs), UK Information Commissioner's Office http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_enhancing_technologies_v2.pdf [15.11.2012]

ICO (2012): Auditing data protection. A guide to ICO data protection audits. UK Information Commissioner's Office http://www.ico.gov.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Detailed_specialist_guides/guide_to_ico_data_protection_audits_v2.ashx [20.11.2012]

Initiative on Privacy Standardization in Europe (2002): Final Report, CEN/ISSS Secretariat, Brussels, http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Documents/ipsefinalreportwebversion.pdf [20.10.2012]

Ilten, Carla – Guagnin, Daniel – Hempel, Leon (2012): Privacy Self-regulation Throug Awareness? A Critical Investigation into the Market Structure of the Security Field. In: Gutwirth, Serge – Leenes, Ronald – De Hert, Paul – Poullet, Yves (eds.): European Data Protection: In Good Health? Springer, pp. 233-247.

ISO/IEC 27001:2005 Information security management systems – Requirements: it describes the requirements of the management system.

Jóri, András (2005): Adatvédelmi kézikönyv, Osiris, Budapest

Jóri, András (2009): Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése, PhD thesis, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar Doktori Iskola

Kokolakis, Spyros – Lambrinoudakis, Costas (2005): ICT Security Standards for Healthcare Applications, UPGRADE European Journal for the Informatics Professional, Issue. 4.

LaserCard Corporation: LaserCard® Optical Memory Card. http://www.lasercard.com/products.php?key=83 [01.11.2012]

Lyon, David – Zureik, Elia (1996): Computers, Surveillance & Privacy, University of Minnesota Press

Macdonald, Linda (2008): Data Protection: Legal Compliance and Good Practice for Employers, Tottel Publishing, Haywards Heaths

Le Métayer, Daniel (2010): Privacy by Design: A Matter of Choice. In: Gutwirth, Serge – Poullet, Yves – De Hert, Paul (eds.):Data Protection in a Profiled World, Springer, pp. 323-334.

Morgan, Richard – Boardman, Ruth (2012): Data Protection Strategy. Implementing Data Protection Compliance, Sweet & Maxwell, London

MSZ EN ISO 9000:2005. Minőségirányítási rendszerek. Alapok és szótár

MSZ EN ISO 19011:2003. Útmutató minőségirányítási és/vagy környezetközpontú irányítási rendszerek auditjához

Nouwt, Sjaak (2010): Towards a Common European Approach to Data Protection: A Critical Analysis of Data Protection Perspectives of the Council of Europe and the European Union. In: Gutwirth, Serge – Poullet, Yves – De Hert, Paul – De Terwangne, Cécile – Nouwt, Sjaak (eds.): Reinventing Data Protection? Springer, pp. 275-292.

Padilla, Visdómine Luis (2002): Track format of magnetic stripe cards. http://www.gae.ucm.es/~padilla/extrawork/tracks.html [01.11.2012]

Polefkó, Patrik (2010): Barátok és bizonytalanságok közt, avagy a közösségi oldalakról adatvédelmi szemszögből (1. rész), Infokommunikáció és Jog, Issue 3.

Polyák, Gábor – Szőke, Gergely László (2011): Elszalasztott lehetőség? Az új adatvédelmi törvény főbb rendelkezései. In.: Drinóczi, Tímea (ed.): *Magyarország új alkotmányossága*, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, Pécs, pp. 155-177.

Racskó, Péter (2011): Cloud computing – informatika és kommunikáció a felhőben. Lecture on the OBH-NKI course, Budapest, 21.03.2011.

Raguse, M. – Langfeldt, O. – Hansen, M. (2008): Preparatory Action on the enhancement of the European industrial potential in the field of Security research (PASR) Deliverable 3.3 Proposal Report. PRISE, Kiel http://www.prise.oeaw.ac.at/docs/PRISE_D_6.2_Criteria_for_privacy_enhancing_security_technologies.pdf [30.10.2012]

Reidenberg, Joel R. (1998): Lex Informatica: The Formulation of Information Policy Rules Through Technology, Texas Law Review, Issue. 3

Roberts, Will (2012): Biometrics history: a story starting 2500 years ago. http://www.video-surveillance-guide.com/biometrics-history.htm [01.11.2012]

Robinson, Neil – Graux, Hans – Botterman, Maarten – Valeri, Lorenzo (2009): Review of the European Data Protection Directive, Rand Corporation, http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf [18.10.2012]

Ruiter, Joep – Warnier, Martijn (2011): Privacy Regulations for Cloud Computing: Compliance and Implementation in Theory and Practice. In: Gutwirth, Serge – Poullet, Yves – De Hert, Paul – Leenes, Ronald (eds.): Computers, Privacy and Data Protection: an Element of Choice, Springer, pp. 361-376.

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

Sweeney. L. (2002): K-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, Issue 5, pp. 557-570.

Szádeczky, Tamás (2010): Problems of Digital Sustainability, Acta Polytechnica Hungarica, Journal of Applied Sciences, Issue 3, pp. 123-136.

Szádeczky, Tamás (2011): Szabályozott biztonság. Az informatikai biztonság szabályozásának elmélete, gyakorlata és az alkalmazás megkönnyítésére felállított módszertan. PhD thesis. University of Pécs, Pécs

Székely, Iván (2008): A privátszférát erősítő technológiák, http://pet-portal.eu/old/files/articles/2008/12/Szekely_Ivan_A_privatszferat_erosito_technologiak_NHIT.pdf [10.11.2012]

Szigeti, Ferenc – Végső, Károly – Kiss, István (2003): Minőségirányítási ismeretek, Nyíregyházi Főiskola, http://mmfk.nyf.hu/min/index.htm [28.10.2012]

Trócsányi, Sára (2007): Egészségügyi adatok kezelése a gyakorlatban. Válogatás az adatvédelmi biztos eseteiből, Infokommunikáció és Jog, Issue 3.

Wang, Yang – Kobsa, Alfred (2008): Privacy-Enhancing Technologies. In: Gupta, M. – Sharman, R. (eds.): Handbook of Research on Social and Organizational Liabilities in Information Security. Hershey, IGI Global

Winn, J. K. (2010): Technical Standard sas Data Protection Regulation. In.: Gutwirth, Serge – Poullet, Yves – De Hert, Paul – De Terwangne, Cécile – Nouwt, Sjaak (eds.): Reinventing Data Protection? Springer, pp. 191-206.