UNIVERSAL CODE ON THE PROTECTION OF PERSONAL DATA ACQUIRED THROUGH MONITORING IN EMPLOYMENT RELATIONSHIPS

AUTHORS

Dr. Zsolt György Balogh

Dipl.-Jur. Falk Hagedorn

Dr. Balázs Rátai

Dr. Gergely László Szőke

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

DECEMBER, 2012

Content

Part I

1. Purpose and scope

1.1.

The purpose of this code (hereinafter referred to as: Code) is to

a) provide requirements for the processing of personal data of employees acquired through monitoring of the activity of employees by technical means;

b) define the framework of the privacy management system that enables employers to process personal data compliant with the rules applicable to the employment relationship;

c) define the framework of compliance assessment and certification of the privacy management system of the employer against the requirements of this Code.

1.2.

The requirements of the Code have been developed in line with 'ILO Code of practice on the protection of worker's personal data'[1] and on the basis of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

2. Definitions and interpretation

2.1.

a) *monitoring:* is the collection and recording of personal data with the help of technical means (e.g. using computers, cameras, video equipment, sound devices, telephones and other communication equipment, equipments that are capable of establishing identity or location), which process personal data independently of the actions of the employee;

b) *secret monitoring:* monitoring that is carried out without informing the employees about the realization of the monitoring;

c) *rules applicable to the employment relationship:* laws, relevant obligatory regulations, and the authoritative guidance of supervisory institutions and courts, which are

[1] An ILO code of practice – Protection of workers' personal data, International Labour Office, Geneva, 1997

applicable either because of the nature of the employment relationship or as a result of the circumstances of the monitoring;

2.2.

Terms used by the Code relating to the processing of personal data shall be interpreted on the basis of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and on the basis of the rules applicable to the employment relationship.

2.3.

Terms used by the Code relating to the employment relationship (e.g. employer, employee) shall be interpreted on the basis of the rules applicable to the employment relationship.

3. Principles

3.1.

Principles of personal data protection (e.g.: finality, proportionality, transparency, accuracy, security, confidentiality, partnership, co-operation and no waiver for privacy rights) shall be adhered during monitoring of employees and during the processing of the personal data that is acquired through monitoring.

3.2.

During monitoring of employees and during the processing of the personal data that is acquired through monitoring the principles of labour law also have to be taken into account.

Part II

4. Legal basis of monitoring

4.1.

Monitoring shall only be carried out if laws applicable to the employment relationship provide this possibility or in case the employee had given its consent in advance.

4.2.

The monitoring of employees on the basis of their consent shall only be done in exceptional circumstances.

4.3.

Monitoring of employees shall not be carried out in relation to activities of employees that are not related to the fulfilment of rights and obligations of the employment relationship.

5. Purpose of monitoring and retention of data acquired through monitoring

5.1.

Monitoring of employees shall have a legitimate purpose that directly relates to the control of fulfilment of rights and obligations connected to the employment relationship.

5.2.

Continuous monitoring shall only be carried out by the employer if it is required for the protection of health, safety or property of the employer or others.

5.3.

The use of equipments provided by the employer to the employee shall not in itself justify the monitoring of the employees.

5.4.

Employers shall clearly articulate the purpose of monitoring with reference to the rights and obligations connected to the employment relationship. Employers shall also clearly articulate the causal relationship between the monitoring and its purpose.

5.5.

Monitoring of employees shall take into account the rights of third parties to the protection their personal data in relation to the monitoring of employees.

5.6.

Employers shall regularly evaluate whether the applied methods of monitoring are suitable for achieving the purpose of monitoring. The evaluation shall also take into account ethical, economic and psychological aspects of monitoring.

5.7.

Employers shall define the retention period of personal data that is acquired during monitoring. Personal data of former employees shall be processed only for a predefined period after the cessation of the employment relationship.

6. Informing workers in advance

6.1.

Employees shall be informed in advance of the monitoring. Information provided to the employees about monitoring shall include clear and comprehensive explanation about

a) the purpose of/reasons for monitoring,
b) the duration and extent of monitoring,
c) the methods and techniques used for monitoring,
d) the data to be collected via monitoring,
e) the use and time of storage of the data by the employer, and
f) rights of the employees and the employers.

7. Additional requirements for secret monitoring

7.1.

Secret monitoring of employees shall only be carried out by the employer if there is suspicion on reasonable grounds of

a) criminal activity or
b) other serious wrongdoing listed in the privacy policy of the employer

7.2.

Secret monitoring shall only be carried out for a pre-defined period. Personal data acquired during secret monitoring shall be evaluated. Impartiality of the evaluation shall be ensured. The evaluation report shall be submitted to review to a person who did not take part in the decision making about the secret monitoring and the acquisition of data.

7.3.

Data acquired during secret monitoring shall be deleted immediately if it does not provide evidence for the suspected criminal activity or serious wrongdoing.

7.4.

Employees shall also be informed in advance about the possibility of secret monitoring.

8. Security aspects

8.1.

Employers shall ensure the security of the processing of data relating to the monitoring of employees.

8.2.

If the employer has a certified information security management system, it shall be presumed that the employer ensures the security of the processing of personal data relating to the monitoring of employees if the information security management system covers all aspects of data processing that relates to the monitoring of employees.

9. Co-operation between employers and employees

9.1.

Employers shall regularly seek the opinion of employees about the monitoring.

9.2.

Employers shall establish procedures that ensure that employees can access information about the processing of their personal data in relation to monitoring the activity of the employer.

9.3.

Employers shall establish procedures for the rectification, erasure or blocking of data the

processing of which does not comply with the rules applicable to the employment relationship.

10. Training of staff

10.1.

Persons that participate in monitoring of employees shall be adequately trained about the personal data protection aspects of monitoring.

11. Documentation of data processing

11.1.

Employers shall keep a comprehensive documentation of the data processing in relation to the monitoring of employees.

Part III

12. Specification of requirements

12.1.

Requirements of the Code shall be reflected in the privacy policy of the employer with reference to the Code and shall be specified according to the rules applicable to the employment relationship. Specification of the requirements shall also include the requirements that are only applicable to the specific monitoring methods used by the employer.

13. Compliance assessment and certification

13.1.

In order to assess compliance level of the data processing with the requirements of the Code employers shall provide a detailed account on how conformity with the requirements is

achieved.

13.2.

Auditing of the compliance with the requirements of the Code shall be carried out by an independent privacy expert, who is registered by the certification body. The auditor or the audit team must be competent in auditing information security aspects of personal data processing. Audit report shall provide a detailed account of the state of compliance with the requirements of the Code.

13.3.

An application for certification is possible at the certification body, upon submission of an audit report not older than 3 months. An applicability statement shall also be submitted together with the certification request. The certification body will review the audit report and decide whether the certification can be obtained within 2 months. The obtained certification is valid for 3 years, with yearly surveillance if the audit report indicates the necessity of yearly surveillance.

13.4.

Certification body is the Research Centre for ICT Law (IKJK), University of Pécs Faculty of Law. The certification body also carries out the registration of independent privacy experts.

Annex I.

Applicability statement

Part I

Monitoring of employees by the employer (description of types of monitoring that is applied by the employer)

type of monitoring	**description of monitoring**

Personal data collected and recorded by the different types of monitoring

type of monitoring	**collected/recorded data**

Part II

4-5. Legal basis and purpose of monitoring

Summary about the basis and purpose of processing personal data during monitoring

[table: column1: purpose of monitoring (with reference to rights and obligations connected to the employment relationship); column2: list of used monitoring methods; column3: causal relationship; column4: legal basis]

purpose	applied monitoring methods	causal relationship	legal basis

Retention period of the personal data acquired during monitoring

Evaluation of the applied monitoring methods

6. Informing workers in advance

Informing employees in advance of the monitoring

Provision of clear and comprehensive explanation about the monitoring

7. Secret monitoring

Secret monitoring

Informing employees about the possibility of secret monitoring in advance

Provision of clear and comprehensive explanation about the secret monitoring to the employees

Wrongdoings which may result in secret monitoring

Period of secret monitoring

Impartial evaluation of the personal data that is acquired through secret monitoring

8. Security aspects

Ensuring the security of the processing of personal data relating to the monitoring of employees

Information security management system at the employer

9. Co-operation between employers and employees

Consultation with employees

Procedures that ensure access to information about data processing

Procedures for the rectification, erasure or blocking of data processing

10. Training of personal
Personal participating in the monitoring of employees Training provided to the persons about the personal data protection aspects of monitoring participating in the monitoring of employees
11. Documentation of data processing
Internal documentation of the data processing in relation to the monitoring of the employees
Part III
12. Specification of requirements
Privacy policy of the employer Specification of and references to the requirements of the Code in the privacy policy

place, date

[signature of the representative of the data controller]

Annex II.

Accredited jurisdiction or sector specific codes of conduct

Accreditation of the jurisdiction or sector specific codes of conduct can be requested from the Research Centre for ICT Law (IKJK), University of Pécs. For further information about the accreditation process please contact IKJK.

Annex III.

Commentary on the Universal code on the protection of personal data acquired through monitoring in employment relationships

Introduction

Employers have always been monitoring the work of employees in one way or another. As monitoring technologies become more and more available, because of rapid technological development and parallel decrease in the cost of investment and maintenance of monitoring solutions, it is becoming ever more tempting for employers to control the activities of their employees by monitoring them.

Thus we can see that the use of monitoring technologies is becoming ubiquitous in working environments, therefore personal data protection problems relating to the use of such technologies are also becoming more and more common in employment relationships.

Additionally the use of monitoring technologies can in itself create distrust between employers and employees, and in some extreme cases they can even drastically reduce the effectiveness of work of employees, but may also lead to situations in which the rights of employees to personal data protection is violated. Neither outcome is desirable for an employer, therefore employers started to look for solutions that can remedy the detrimental effects created by the use of monitoring technologies.

Part I.

1. Purpose and scope

Purpose of the Code

The ‘Universal code on the protection of personal data acquired through monitoring by technical means in employment relationships’ (hereinafter referred to as: Code) sets standards for the management of personal data protection problems arising from the use of monitoring solutions. The Code is in line with international and European Union personal data protection requirements, standards and best practices.

The structure and content of the Code is designed in a way that supports the internal and independent external personal data protection compliance audit of the monitoring activity carried out by employers.

The Code specifically defines the compliancy audit requirements and emphasises the concept that properly balanced, personal data protection friendly monitoring of employees can only be achieved and maintained if monitoring related personal data processing is properly regulated, documented and if the effectiveness of the monitoring methods is internally and externally

evaluated at regular intervals.

Scope of the Code

The requirements of the Code do not intend to pre-empt any national or international binding rules that apply to the monitoring related personal data processing. None of the rules and requirements of the Code can be interpreted in a way that it is providing exemptions from these binding rules. On the contrary the Code requires employers to collect all relevant binding rules and concretize the requirements of the Code according to these binding rules that are applicable because of their specific situation (e.g.: product or service they make or provide, industry they are active in, country that they operate).

This means in practice that compliance with the Code is evaluated in two steps. The first step is the evaluation of the completeness and adequacy of the binding rules that are applicable to the specific situation of the employer. The second step is the evaluation of the compliancy with the binding rules that are applicable to the specific situation of the employers. This second evaluation however, must be based on the statement of applicability, which is defined by the Code itself and which can be found in the annex of the Code.

Structure of the Code

The Code consists of three main parts. The first part defines the scope and purpose of the Code. It also contains definitions and sets rules for the interpretation of the Code. The second part contains the requirements. The third part contains the rules of compliance evaluation.

The Code has 3 annexes. Annex I contains the applicability statement. Annex II contains list of accepted jurisdiction specific ("national") or sector specific codes of conduct that are created in order to facilitate the collection of the binding rules that are applicable in certain jurisdictions or in certain sectors within specific jurisdiction. Annex III contains the explanations of the Code.

2. Definitions and interpretation

Definitions given by the Code

The Code for its purpose introduces the definition of three terms: a) monitoring; b) secret monitoring; and c) rules applicable to the employment relationship.

Monitoring

The term monitoring broadly refers to the use of technical means that collect and record personal data automatically about employees irrespective of their actions. Personal data collection activities about employees that are carried out by individuals fall outside the scope

of the Code, even if data recording is assisted by technical means (e.g.: receptionist recording the name of employees that are entering the building in a word document).

Secret Monitoring

Secret monitoring refers to activities carried out by the employer for its own purposes. Monitoring carried out for the purpose of law enforcement and for reasons stemming out of national security are not covered by the definition. The dividing line between open and secret monitoring is drawn by the fact whether employees are informed about the actual usage ('realization') of the monitoring solution or not.

Rules applicable to the employment relationship

The term 'rules applicable to the employment relationship' is a wide reference to the binding rules and regulations that are applicable to the relationship between the employer and employee.

References to jurisdiction specific regulations

Regarding the meaning of terms used by the Code in relation to personal data protection the Code refers to the definitions of the EU data protection directive and to the data protection regulation of the jurisdiction which is relevant in case of the employment relationship.

Similarly regarding the meaning of the terms used by the Code in relation to employment, the Code refers to the labour law of the jurisdiction which is relevant in case of the employment relationship.

3. Principles

Principles of personal data protection also provide guidelines for data controllers to achieve compliance with personal data protection regulations. The Code references the principles of personal data protection in general and requires employers to comply with these principles.

The most common principles are directly referenced by the Code as examples. These are

a) finality,
b) proportionality,
c) transparency,
d) accuracy, security and confidentiality,
e) partnership, co-operation,
f) no waiver for privacy rights.

These principles are also directly reflected in the rules of the Code.

Finality

According to the general principles of privacy protection legitimate processing of personal data shall only aim at an explicit and legitimate purpose. Personal data of employees shall be collected and processed only for reasons directly relevant to the employment. Processing of personal data for any purpose different from the original purpose of data collection shall infringe the privacy rights of the employee.

Legitimate purposes in relevance of employment

Personal data acquired from electronic monitoring can be legally used for evaluating employee performance, however should not be the only factor in this respect.

Illegitimate purposes

Processing of personal data acquired from electronic monitoring for the purpose of property protection may not infringe the privacy of the employee and should not be used to control the behaviour of employee.

Anti discrimination principle

The processing of personal data shall not have the effect of unlawfully discriminating in employment or occupation.

Legality

Processing of the employee personal data shall always be in accordance with the relevant Council of Europe (CoE) and European Union (EU) community regulation as well as the applicable domestic law.

Most relevant CoE documents

a) European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Art. 8
b) Council of Europe's Convention (108) for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Most relevant EU documents

a) Charter of Fundamental Rights of the European Union
b) Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data

Proportionality

The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or processed. Proportionality shall be interpreted both in relation to the kind of data and the time of processing operations.

Transparency

Transparency is the strong guarantee of both the fair and legitimate data processing and the equilibrium of competing interests of employer and employee. Employees must be informed all the relevant circumstances of data processing.

Necessary elements of transparent data processing

Purpose, content and time of data processing as well as the name and address of data controller and data processor are elementary criteria of lawful and just information.

Rights of the data subject

The data subject shall be granted the right to access his/her personal data record and the right of rectification.

Employees and representatives shall be kept informed of any data collection processes, the rules that govern that process, and their rights.

Data subject may also comment the processed data and the data processing actions performed by the employer.

In case of data misuse data subjects are also free to notify supervisory authorities and seek remedies in civil litigation in compliance with national law.

Accuracy, security and confidentiality

Accuracy of data records

Only reliable data records can support the mutual interests of employer and employees. Employers shall keep data records accurate and up to date. Inaccurate or incomplete data records shall be erased or rectified.

Data security

Employer have to take reasonable and proportionate technical and organisational measures to protect the personal data files 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.

Confidentiality

Personal data records constitute confidential content. Staff members having access to personal data files shall adhere to the rule of confidentiality in accordance with the jurisdiction specific data protection laws and regulations.

Training

All of the persons who participate in processing of personal data shall be regularly trained on principles of just and fair data processing, the data security measures and their personal role in

procedure.

Partnership and co-operation

Employers, workers' representatives, employment agencies and employees are expected to act according to the spirit of co-operation.

Developing of privacy policy

All the afore-mentioned partners shall cooperate in protecting personal data and in developing policies on workers' privacy.

Regular supervision of privacy policy

Employer shall take regular assessment of the data processing system and perform amendments for the sake of reduced amount of personal data processed and improve the methods of privacy protection. Enhanced techniques of data protection – like privacy by design and privacy impact assessment – may be the principle guidelines of further developments.

Employees shall be informed in advance about the details of forthcoming alterations of data processing and the surveillance system.

No waiver for privacy rights

Privacy is deemed as one of the inalienable, but derogable human rights. Consequently also in employment relationship employee may not waive his/her privacy rights.

Part II.

4. Legal basis of monitoring

The Code states that monitoring of employees on the basis of their consent can be done only in exceptional circumstances. This means in practice that employers have to justify whenever monitoring is not carried out on the basis of laws applicable to the employment relationship. The Code prefers the option of non-consent based data processing, because employees are usually in weak bargaining positions, which makes the voluntary nature of their consent usually questionable. The requirement to justify consent based monitoring helps to prevent problems that may arise from the unbalanced bargaining position of employees and employers.

The Code also states that monitoring has to relate to the fulfilment of rights and obligations of the employment relationship. In this respect the burden of proof also stays with the employers.

5. Purpose of monitoring and retention of data acquired through monitoring

The Code introduces some restrictions relating to the purpose of monitoring.

a) It requires that monitoring shall relate to the rights and obligations defined by the employment relationship.
b) It allows continuous monitoring only for the purpose of protection of health, safety or property.
c) It excludes the possibility of monitoring on the sole ground of using equipment that is owned by the employer.

The Code requires the employers to justify clearly the purpose of monitoring and explain the causal relationship between the applied monitoring method and the purpose of the monitoring.

The Code also obliges employers to take into account the rights of third parties (e.g.: others who send e-mails to the employers) in order to minimize the risk of infringing the rights of those whose activities are likely to be monitored as part of the monitoring of employees, but who are not employees.

The Code obliges employers to regularly evaluate the effectiveness and necessity of monitoring. The evaluation shall not be limited to the compliance of the monitoring with data protection regulation, but shall also include the evaluation of ethical, psychological and economic aspects of monitoring.

The Code requires employers to define in advance the retention period of personal data that is acquired through monitoring. The Code also requires employers to define in advance the retention period of former employee data after the cessation of the employment relationship.

6. Informing workers in advance

The Code highlights the necessity of informing employees about monitoring in advance in clear and comprehensive manner. Informing data subjects about data processing is a general requirement of every data protection regulation, but in employment relationship it is of utmost importance to ensure that the information provided is comprehensive and understandable by the employees and covers all aspects of data processing relating to the monitoring of their activities. During compliance assessment in line with the Code these two aspects (comprehensiveness and comprehensibility) will be the core of the evaluation in relation to the information requirements.

7. Additional requirements for secret monitoring

The rules of the Code relating to secret monitoring cover only the situations when secret monitoring is carried out by the employer. Thus secret monitoring used by public authorities within the workplace does not fall under the scope of the rules of the Code.

It is important to highlight that in some cases there is a fine dividing line between secret and non-secret monitoring. Monitoring of e-mail correspondence of employees is a good example. In case of e-mail monitoring it is usually unknown to the employees when actually employers look into their e-mail correspondence, thus monitoring is happening practically secretly. However, rules relating to secret monitoring only apply to situations when employees are not informed about the realization of the monitoring solution, thus the instalment of monitoring equipment or the initiation of monitoring method or process is unknown to the employees. To put it simply the scope of secret monitoring covers only situations where the initiation of data acquisition or the type of data acquisition method used is unknown to the employees.

Since secret monitoring is a serious intrusion into the personal sphere and can have serious consequences both for the employees and employers, the Code restricts the possibility of secret monitoring to preliminarily defined situations where criminal activity or other preliminary listed serious wrongdoing can be reasonably suspected on the side of employees.

Compliance with the Code can only be achieved in relation to secret monitoring if employers are informed about the possibility of secret monitoring in advance and the employer ensures the impartial evaluation of the results of secret monitoring.

It is also important to mention that in most of the jurisdictions secret monitoring by employers is expressly or indirectly prohibited by law, so the rules of the Code relating to secret monitoring can only be applied if no such prohibition is applicable.

8. Security aspects

Ensuring the security of data processing is a general requirement of data protection regulations. The Code reiterates in this respect this generally accepted requirement.

Additionally the Code takes the position that an information security management system that is implemented by the data controller can only be considered a proper solution if the scope of the information security management system covers all aspects of data processing relating to the monitoring of employees.

Compliance with the Code can only be achieved if the security of data processing is ensured. This aspect of data processing shall be evaluated during compliance assessment and certification. The audit report foreseen by point 13 of the Code shall contain an evaluation of the adequacy of the security measures implemented by the employer in relation to the

processing of data acquired through monitoring.

9. Co-operation between employers and employees

Co-operation between employers and employees is a general principle of labour law. In larger organizations co-operation usually takes the form of formal consultation between employers and employee representatives. In case of existence of such formal consultation procedures, the fulfilment of this requirement can be achieved by introducing the topic of monitoring into the consultation procedures. However, in smaller organizations, where such formal consultation does not exist specific forms of opinion seeking shall be developed in order to achieve compliance with the Code.

Employers shall ensure that procedures exist that help to channel employee complaints about data processing in relation to monitoring into a meaningful discussion between the employer and employees. These procedures can be simple and preference shall be given to solutions that foster mutual trust.

10. Training of staff

Knowledge about data processing related requirements is a prerequisite of lawful data processing. Therefore it has an utmost importance to ensure that people that are involved into monitoring of employees possess the necessary knowledge about data protection requirements.

So as to achieve compliance with the Code as a starting point employers shall document what knowledge of the people have about data protection who participate in the monitoring of employees.

11. Documentation of data processing

Compliance with data protection regulations cannot be achieved without a full and through understanding of data processing activities. Therefore the Code requires employers to document all elements of data processing relating to monitoring of employees. It is useful to start the documentation with the creation of the applicability statement that can be found in Annex I of the Code in order to achieve compliance with the Code in relation to the documentation requirement.

Part III.

12. Specification of requirements

The requirements of the Code do not intend to pre-empt any national or international binding rule that applies to the monitoring related personal data processing. The Code requires employers to collect all relevant binding rules and concretize the requirements of the Code according to these binding rules that are applicable because of their specific situation (e.g.: product or service they make or provide, industry they are active in, country in which they operate).

This means in practice that compliance with the Code is evaluated in two steps. The first step is the evaluation of the completeness and adequacy of the binding rules that are applicable to the specific situation of the employer. The second step is the evaluation of the compliance with the binding rules that are applicable to the specific situation of the employers.

In order to achieve compliance with the Code employers shall list in the applicability statement the elements of their internal regulations that implement the requirements of the Code.

13. Compliance assessment and certification

Fulfilment of the administrative requirements of the Code, constitute the basis of a privacy management system that helps to show that monitoring related personal data processing is carried out in line with the requirements of the Code.

The administrative requirements of the Code are the following:

a) description of how conformity with the requirements of the Code is achieved by the employer (point 13.1 of the Code),
b) reflection of the requirements of the Code in the privacy policy of the employer with reference to the Code (point 12.1 of the Code),
c) comprehensive documentation of the data processing in relation to the monitoring of employees (point 11.1 of the Code),
d) period of secret monitoring shall be preliminary defined (point 7.2. of the Code),
e) evaluation report about the personal data that is acquired during secret monitoring (point 7.2. of the Code),
f) clear articulation of the purpose of monitoring with reference to the rights and obligations connected to the employment relationship (point 5.4 of the Code),

g) clear articulation of the causal relationship between the monitoring and the purpose of monitoring (point 5.4 of the Code),
h) yearly evaluation report about suitability of the applied monitoring methods (point 5.6 of the Code),
i) determination of the retention period of personal data that is acquired during monitoring (point 5.7 of the Code).

An additional implicit administrative requirement is the creation of privacy policy.

Compliance with the Code can be audited and certified. For certification the Code requires the submission of a positive audit report and a signed copy of the applicability statement. The audit report shall be prepared and signed by an independent registered privacy expert.

Certification request can be submitted within 6 months after the issuance of a positive audit report to the certification body. The certification body is the Research Centre for ICT Law (IKJK, www.ikjk.hu), University of Pécs Faculty of Law.

The certification body also carries out tasks relating to the registration of independent privacy experts.