# HUNGARIAN JURISDICTION SPECIFIC IMPLEMENTATION OF THE UNIVERSAL CODE ON THE PROTECTION OF PERSONAL DATA ACQUIRED THROUGH MONITORING IN EMPLOYMENT RELATIONSHIPS

## AUTHOR

### Dr. Balázs Rátai

## 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' 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.

*This is a Hungarian jurisdiction specific implementation of the 'Universal code on the protection of personal data acquired through monitoring in employment relationships' v. 1.0. 2012-12-31 (hereinafter referred to as: Code).*

*This implementation provides help for employers in developing and using monitoring solutions in line with the requirements of the Code.*

*The scope of the implementation is restricted to the Hungarian generic data protection and labour law regulations. Thus additional domain regulations also have to be observed by employers in order to ensure compliancy with all of the rules that are applicable to the employment relationship because of their respective situation.*

## 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;
   *No rules within the scope of the implementation provide a definition of*

3

*monitoring.*

*Relevant decisions of the data protection authority:*

a) DPC, 866/A/2006

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

*No rules within the scope of the implementation provide a definition of secret monitoring.*

c) rules applicable to the employment relationship: laws, relevant obligatory regulations, and the authoritative guidance of supervisory institutions and courts, which are applicable either because of the nature of the employment relationship or as a result of the circumstances of the monitoring;

*The following laws and regulations were taken into account during the implementation:*

a) *Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter referred to as: data protection act or DPA)*
b) *Act I of 2012 on the Labour Code (hereinafter referred to as: labour code or LC)*

## 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.

*Definition of terms used by this implementation of the Code relating to the processing of personal data can be found in section 3 of the DPA.*

## 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.

*Definition of terms used by this implementation of the Code relating to the employment relationship can be found in section 294 of the LC.*

## 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.

> *Principles of personal data protection that are referenced by the Code are all reflected by the DPA.*

### 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.

> *Principles of labour law can be found in sections 5-12 of the LC. Most relevant principles are:*
>
> a) *exercising of rights in good faith and fairly*
> b) *protection of legitimate interests*
> c) *protection of personal rights of employees*
> d) *equal treatment*

## 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.

> *Section 11 subsection (1) of the LC states that "Employers are allowed to monitor the behaviour of workers only to the extent pertaining to the employment relationship. The employers' actions of control, and the means and methods used, may not be at the expense of human dignity. The private life of workers may not be violated."*
>
> *Relevant decisions of the data protection authority:*
>
> a) *DPC, 40/K/2006*
> b) *DPC, 120/A/2004*
> c) *DPC, 1543/A/2004*

d) *DPC, 1722/A/2004*
e) *DPC, 1393/K/2006*
f) DPC, 866/A/2006
g) *DPC, 2511/K/2007*
h) *DPC, 1767/K/2006*
i) *DPC, 1672/K/2006*
j) *DPC, 3362/P/2009*
k) *DPC, 857/K/2009*
l) *DPC, 1092/P/2009*

## 4.2.

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

> *Section 9 subsection (3)of the LC states that "On general principle, worker may not waive their personal rights in advance. Any legal statement concerned with the personal rights of a worker shall be formally valid if made in writing." This practically means that consent of employees to processing of their personal data shall be made in writing, if the monitoring solution cannot be operated on the basis of Section 11 section (1) of the LC and therefore consent of the employee is needed to ensure legitimacy of processing personal data that is acquired through monitoring.*

## 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.

> *No rules within the scope of the implementation address this aspect of personal data processing.*

> *Relevant decisions of the data protection authority:*

> a) *DPC, 120/A/2004*
> b) *DPC, 1664/A/2006*
> c) *DPC, 920/K/2006*
> d) *DPC, 857/K/2009*
> e) *DPC, 636/K/2009*
> f) *DPC, 663/P/2009*

# 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.

*Section 10 subsection (1) of the LC states that "A worker may be requested to make a statement or to disclose certain information only if it does not violate his personal rights, and if deemed necessary for the conclusion, fulfilment or termination of the employment relationship."*

*Relevant decisions of the data protection authority:*

*a) DPC, 866/A/2006*
*b) DPC, 531/A/2004*
*c) DPC, 857/K/2009*
*d) DPC, 663/P/2009*

**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.

*No rules within the scope of the implementation address this aspect of personal data processing.*

**5.3.**

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

*No rules within the scope of the implementation address this aspect of personal data processing.*

**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.

*No rules within the scope of the implementation address this aspect of personal data processing.*

*Relevant decisions of the data protection authority:*

*a) DPC, 1454/K/2010*
*b) DPC, 926/H/2010*
*c) DPC, 857/K/2009*

**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.

*No rules within the scope of the implementation address this aspect of personal data processing.*

*Relevant decisions of the data protection authority:*

   a) *DPC, 40/K/2006*
   b) *DPC, 772/A/2000*
   c) *DPC, 841/K/2002*
   d) *DPC, 1767/K/2006*

## 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.

*No rules within the scope of the implementation address this aspect of personal data processing.*

## 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.

*No rules within the scope of the implementation address this aspect of personal data processing.*

# 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.

*Section 20 subsection (2) of the DPA states that "Before processing operations are*

*carried out the data subject shall be clearly and elaborately informed of all aspects concerning the processing of his personal data, such as the purpose for which his data is required and the legal basis, the person entitled to control the data and to carry out the processing, the duration of the proposed processing operation, if the data subject's personal data is processed in accordance with Subsection (5) of Section 6, and the persons to whom his data may be disclosed. Information shall also be provided on the data subject's rights and remedies"*

*Additionally section 11 subsection (2) of the LC states that "Employers shall inform their workers in advance concerning the technical means used for the surveillance of workers."*

*Relevant decisions of the data protection authority:*

a) *DPC, 531/A/2004*
b) *DPC, 800/K/2008*
c) *DPC, 461/A/1998*
d) *DPC, 475/H/2000*
e) DPC, 920/K/2006
f) *DPC, 857/K/2009*
g) *DPC, 1092/P/2009*

# 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.

> *Section 5 subsection (1) of the DPA states that "". Since other laws do not provide the possibility for employers to carry out secret monitoring of employees, therefore secret monitoring is of employees is not allowed in Hungary.*

> *Relevant decisions of the data protection authority:*

> a) *DPC, 1012/K/2005*
> b) *DPC, 570/A/2001*

## 8. Security aspects

## 8.1.

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

> *Section 7 of the DPA contains the data security requirements regarding personal data processing. Subsections (2) and (3) of this section states that "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. 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"*

> *Subsection (5) of section 7 of the DPA contains further detailed requirements regarding automated data processing. Monitoring solutions are usually automated data processing systems.*

> *In the selection of security solutions data controllers have to follow the rule of subsection (6) of section 7 of the DPA. This section states that "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 highest level of protection of personal data, except if this would entail unreasonable hardship for the data controller."*

*It is also worth to mention that data controllers are also liable for any damage caused to a data subject by any breach of data security requirements according to section 23 of the DPA.*

*Relevant decisions of the data protection authority:*

> a) *DPC, 922/2/2010*

## 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.

*No rules within the scope of the implementation address this aspect of personal data processing.*

## 9. Co-operation between employers and employees

## 9.1.

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

*The LC emphasises the general duty of employers and employees to co-operate. Section 6 subsection (2) states that "In exercising rights and discharging obligations, the parties involved shall act in the manner consistent with the principle of good faith and fairness, they shall be required to cooperate with one another, and they shall not engage in any conduct to breach the rights or legitimate interests of the other party."*

*Beside this general duty of co-operation there are no rules within the scope of the implementation that address this aspect of personal data processing.*

## 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.

*Section 15 subsection (1) of the DPA states that "Upon the data subject's request the data controller shall provide information concerning the data relating to him,*

*including those processed by a data processor on its behalf, the sources from where they were obtained, the purpose, grounds and duration of processing, the name and address of the data processor and on its activities relating to data processing, and - if the personal data of the data subject is made available to others - the legal basis and the recipients."*

*Beside these general rules of the DPA, there are no rules within the scope of the implementation that address this aspect of personal data processing.*

## 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.

*Section 21 of the DPA provides the data subject the possibility to object to the processing of data relating to him. Subsection (2) and (3) of section 21 of the DPA state that "In the event of objection, the controller shall investigate the cause of objection within the shortest possible time inside a fifteen-day time period, adopt a decision as to merits and shall notify the data subject in writing of its decision. If, according to the findings of the controller, the data subject's objection is justified, the controller shall terminate all processing operations (including data collection and transmission), block the data involved and notify all recipients to whom any of these data had previously been transferred concerning the objection and the ensuing measures, upon which these recipients shall also take measures regarding the enforcement of the objection.".*

*Beside these general rules of the DPA, there are no rules within the scope of the implementation that address this aspect of personal data processing.*

*Relevant decisions of the data protection authority:*

    *a) DPC, 922/2/2010*

## 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.

*No rules within the scope of the implementation address this aspect of personal data processing.*

## 11. Documentation of data processing

### 11.1.

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

> *Section 15 subsection (2) of the DPA states "With a view to exercising communication control and for the information of the data subject, the data controller shall maintain a transmission log, showing the date of time of transmission, the legal basis of transmission and the recipient, description of the personal data transmitted, and other information prescribed by the relevant legislation on data processing."*

> *Beside these specific rules of the DPA, there are no rules within the scope of the implementation that address this aspect of personal data processing..*

# 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.

> *No rules within the scope of the implementation address this aspect of personal data processing.*

## 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. The 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.

*No rules within the scope of the implementation address this aspect of personal data processing.*

# 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

# References

## Laws and regulations

1. Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information
2. Act I of 2012 on the Labour Code

## Decisions of the Data Protection Commissioner

1. DPC, 461/A/1998 [http://abi.atlatszo.hu/index.php?menu=beszamolok/1998/III/1/2/3, 15.12.2012]
2. DPC, 475/H/2000 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2000-2005.ZIP, 15.12.2012]
3. DPC, 772/A/2000 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2000-2005.ZIP, 15.12.2012]
4. DPC, 570/A/2001 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2000-2005.ZIP, 15.12.2012]
5. DPC, 841/K/2002 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2000-2005.ZIP, 15.12.2012]
6. DPC, 120/A/2004 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2000-2005.ZIP, 15.12.2012]
7. DPC, 531/A/2004 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2000-2005.ZIP, 15.12.2012]
8. DPC, 1543/A/2004 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2000-2005.ZIP, 15.12.2012]
9. DPC 1722/A/2004 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2000-2005.ZIP, 15.12.2012]
10. DPC, 1012/K/2005 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2000-2005.ZIP, 15.12.2012]
11. DPC, 40/K/2006 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2006.ZIP, 15.12.2012]
12. DPC, 866/A/2006 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2006.ZIP, 15.12.2012]
13. DPC, 920/K/2006 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2006.ZIP, 15.12.2012]
14. DPC, 1393/K/2006 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2006.ZIP, 15.12.2012]
15. DPC, 1664/A/2006 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2006.ZIP, 15.12.2012]

16. DPC, 1672/K/2006 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2006.ZIP, 15.12.2012]
17. DPC, 1767/K/2006 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2006.ZIP, 15.12.2012]
18. DPC, 2511/K/2007 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2007.ZIP, 15.12.2012]
19. DPC, 800/K/2008 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2008.ZIP, 15.12.2012]
20. DPC, 636/K/2009 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2009.ZIP, 15.12.2012]
21. DPC, 663/P/2009 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2009.ZIP, 15.12.2012]
22. DPC, 857/K/2009 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2009.ZIP, 15.12.2012]
23. DPC, 1092/P/2009 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2009.ZIP, 15.12.2012]
24. DPC, 3362/P/2009 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2009.ZIP, 15.12.2012]
25. DPC, 922/2/2010 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2010.ZIP, 15.12.2012]
26. DPC, 926/H/2010 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2010.ZIP, 15.12.2012]
27. DPC, 1454/K/2010 [http://www.naih.hu/files/ABIWEB--LL-SFOGLAL-SOK_2010.ZIP, 15.12.2012]