
CONTENT

CONTRIBUTORS.....	17
PREFACE	20
I. COMPARATIVE REPORT ON THE REGULATION OF WORKPLACE PRIVACY IN HUNGARY AND GERMANY	25
1. INTRODUCTION AND BACKGROUND	27
1.1. Purpose and methodology	27
1.2. Overview of the relevant legal sources	28
1.2.1. International and EU sources	28
1.2.1.1. The ILO code of practice	28
1.2.1.1.1. Approach and guiding principles of ILOC	28
1.2.1.1.2. Rules of ILOC related to monitoring and surveillance.....	29
1.2.1.2. The Council of Europe's approach	30
1.2.1.3. Charter of Fundamental Rights of the European Union.....	30
1.2.1.4. EU initiatives.....	30
1.2.1.5. Opinions and working papers of the Article 29 Data Protection Working Party	32
1.2.1.5.1. Opinion on Employee Evaluation Data.....	32
1.2.1.5.2. Opinion on the processing of personal data in the employment context.....	32
1.2.1.5.3. Working document on the surveillance of electronic communications in the workplace.....	33
1.2.1.5.4. Opinion on the Processing of Personal Data by means of Video Surveillance	33
1.2.1.5.5. The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data	34
1.2.1.5.6. Opinion on the Industry Proposal for Privacy and Data Protection Impact Assessment Framework for RFID Applications.....	34

1.2.1.5.7.	Monitoring and surveillance related rules	34
1.2.2.	The basic concept of privacy protection and the detailed legal framework in Hungary	36
1.2.2.1.	Constitutional background	37
1.2.2.2.	General and sector-specific data protection regulation and regulation of other privacy rights	38
1.2.2.3.	The basic concept of the Data Protection Act.	38
1.2.2.3.1.	The definition of personal data	38
1.2.2.3.2.	Data processing, data controller, data processor.	39
1.2.2.3.3.	The legal basis of data processing.	40
1.2.2.3.4.	Consent to data processing	42
1.2.2.3.5.	Other rules of data processing.	46
1.2.2.4.	The special role of the Data Protection Commissioner in case law. . .	48
1.2.2.5.	Definitions of the area – basic background information regarding the issue of privacy in the workplace	48
1.2.2.5.1.	Different regulation of the public and private sectors.	48
1.2.2.5.2.	The employers' interest in monitoring the employee	48
1.2.2.5.3.	Data protection provisions in the Labour Codes.	49
1.2.3.	Basic concept of data protection in Germany and the dogmatic bases of the general protection of personality rights.	51
1.2.3.1.	Taking stock of protection of personality rights at the workplace. . .	51
1.2.3.1.1.	The needs of the employee in respect of personality rights	52
1.2.3.1.2.	Limitations of the personality rights of the employee.	56
1.2.4.	Legal sources of national data protection law in Germany.	58
1.2.4.1.	BDSG and field-specific data protection regulations	58
1.2.4.2.	Data protection in scope of the federal data protection law	59
1.2.4.2.1.	§ 32 of the BDSG as the basic regulation for employee data protection.	59
1.2.4.2.2.	Fundamental facts, and § 32 par. 1 s. 1. of BDSG.	59
1.2.4.2.3.	Identification of offences, § 32 par. 1 s. 2 BDSG	60
1.2.4.2.4.	§ 32 par. 2 BDSG as extension for manual data processing	61
1.2.4.2.5.	Competition with § 28 of Federal Data Protection Act[1].	61
1.2.4.3.	Outlook: Revision of employee data protection, §§ 32-32l in the new BDSG.	62
1.2.5.	Self-regulation in Hungary	63
1.2.6.	The concept of self-regulation in Germany	65

1.3.	Mutual dependence	66
1.3.1.	The dependent position of the employee: can his consent be regarded as voluntary consent?	66
1.3.2.	The 'dependent' employer: Can the employer prevent an employee from stealing valuable data without strong monitoring?	68
2.	THE LEGAL REGULATION CONCERNING SELECTED MONITORING MEASURES.	69
2.1.	The regulation of correspondence monitoring	69
2.1.1.	Hungarian regulation.	69
2.1.1.1.	Legislation	69
2.1.1.2.	Case law of the Data Protection Commissioner	70
2.1.1.3.	Judicial case law	71
2.1.1.4.	Academic papers, scientific opinions	71
2.1.2.	German regulation.	71
2.1.2.1.	Legislation	71
2.1.2.2.	Cases from the jurisdiction	71
2.1.2.3.	Academic debate	72
2.1.3.	Conclusion	72
2.2.	The monitoring of the use of computer, Internet and email in the workplace.	72
2.2.1.	Hungarian regulation.	73
2.2.1.1.	Legislation	73
2.2.1.2.	Case law of the Data Protection Commissioner	74
2.2.1.2.1.	Cases on the monitoring of computers	74
2.2.1.2.2.	Cases on the monitoring of Internet use by the employer.	75
2.2.1.2.3.	Cases on the monitoring of emails	76
2.2.1.3.	Judicial case law	77
2.2.1.4.	Academic papers, scientific opinions	77
2.2.1.4.1.	Issues connected to the monitoring of computers.	77
2.2.1.4.2.	Issues connected to the monitoring of Internet use by the employees	77
2.2.1.4.3.	Issues connected to the monitoring of email communications.	78
2.2.2.	German regulation.	79
2.2.2.1.	The employer's right to monitor personal computers or notebooks, internet and email usage	79
2.2.2.2.	Cases from the jurisdiction	81
2.2.2.3.	Academic debate	81

2.2.2.3.1.	In the absence of an explicit regulation the private use is not allowed	81
2.2.2.3.2.	Explicit and implied regulations of use	82
2.2.2.3.3.	Operational practice	82
2.2.2.3.4.	Restriction and withdrawal of permission	83
2.2.2.3.5.	Allowed extent of monitoring e-mails and internet use	84
2.2.3.	Conclusion	89
2.3.	Regulation of social networks.	89
2.3.1.	On the nature and functioning of social networks	90
2.3.2.	The importance of social networks in the digitized world of work	91
2.3.3.	Hungarian regulation.	91
2.3.3.1.	Legislation	91
2.3.3.2.	Case law of the Data Protection Commissioner	91
2.3.4.	German regulation.	92
2.3.4.1.	Cases from the jurisdiction	92
2.3.4.2.	Academic debate	92
2.3.4.2.1.	Right to manage regarding self-presentation in private social networks	92
2.3.4.2.2.	Right to manage regarding self-presentation in professional social networks	93
2.3.4.2.3.	Requirements of the right to manage in terms of content.	93
2.3.4.2.4.	Dealing with employee data on termination of employment	94
2.3.5.	Conclusion	95
2.4.	Monitoring of telephone calls.	95
2.4.1.	Hungarian regulation.	96
2.4.1.1.	Legislation	96
2.4.1.2.	Case law of the Data Protection Commissioner	96
2.4.1.3.	Judicial case law	97
2.4.1.4.	Academic debate	97
2.4.2.	German regulation.	98
2.4.2.1.	Cases from the jurisdiction	98
2.4.2.2.	Academic debate	98
2.4.2.2.1.	Permitted private use.	98
2.4.2.2.2.	Exclusive official use.	99
2.4.3.	Conclusions	101

2.5.	Video surveillance	101
2.5.1.	Hungarian regulation.	102
2.5.1.1.	Legislation	102
2.5.1.2.	Judicial case law	102
2.5.1.3.	Case law of the Data Protection Commissioner	103
2.5.1.4.	Academic papers, scientific opinions	103
2.5.1.5.	Self-regulation	104
2.5.2.	German regulation.	104
2.5.2.1.	Cases from the jurisdiction	104
2.5.2.2.	Academic debate	105
2.5.2.2.1.	Video surveillance in publicly accessible areas, § 6b of the Federal Data Protection Act	105
2.5.2.2.2.	Video surveillance of publicly inaccessible areas.	115
2.5.3.	Conclusion on the use of CCTV systems	117
2.6.	Regulations for using GPS and GSM technology for tracking the location of employees	117
2.6.1.	GPS location	118
2.6.2.	GSM location.	118
2.6.3.	Hungarian regulation.	119
2.6.3.1.	Legislation	119
2.6.3.2.	Case law of the Data Protection Commissioner	119
2.6.3.3.	Judicial case law	120
2.6.3.4.	Academic papers, scientific opinions	120
2.6.4.	German regulation.	121
2.6.4.1.	Cases from the jurisdiction	121
2.6.4.2.	Academic debate	121
2.6.4.2.1.	GPS tracking of company vehicles	121
2.6.4.2.2.	Privacy in telecommunication.	123
2.6.5.	Conclusion.	124
2.7.	Regulation of transponder-based and biometric identification systems	124
2.7.1.	Description of commonly used systems	125
2.7.1.1.	Transponder-based systems.	125
2.7.1.2.	The use of biometric systems	125
2.7.2.	Hungarian regulation.	126

2.7.2.1.	Legislation	126
2.7.2.2.	Case law of the Data Protection Commissioner	127
2.7.2.3.	Judicial case law	127
2.7.2.4.	Academic papers, scientific opinions	127
2.7.3.	German regulation.	127
2.7.3.1.	Cases from the jurisdiction	127
2.7.3.2.	Academic debate	128
2.7.4.	Conclusion.	129
2.8.	Regulation of RFID usage	129
2.8.1.	Hungarian regulation.	130
2.8.1.1.	Legislation	130
2.8.1.2.	Case law of the Data Protection Commissioner	130
2.8.1.3.	Judicial case law	131
2.8.1.4.	Academic papers, scientific opinions	131
2.8.2.	German regulation.	131
2.8.2.1.	Cases from the jurisdiction	131
2.8.2.2.	Academic debate	131
2.8.3.	Conclusion.	132
3.	SUPERVISION REGIME AND SANCTIONS IN THE FIELD OF PRIVACY AT WORKPLACES	133
3.1.	Hungarian regulation	133
3.1.1.	Sanctions according to Data Protection Law	133
3.1.1.1.	Court action.	133
3.1.1.2.	The Data Protection Commissioner and the National Data Protection and Freedom of Information Authority	133
3.1.1.2.1.	The Data Protection Commissioner	133
3.1.1.2.2.	National Data Protection and Freedom of Information Authority	134
3.1.2.	Sanctions based on the Labour Code	135
3.1.3.	Other sanctions	136
3.1.3.1.	Sanctions based on the Civil Code	136
3.1.3.2.	Sanctions based on the Criminal Code	136
3.2.	German regulation	137
3.2.1.	Sanctions in the field of data protection	137

3.2.2.	Sanctions in the field of Labour Law	138
3.2.3.	Other sanctions	139
3.3.	Conclusion	140
4.	LITERATURE AND REFERENCES	141
4.1.	Books, essays and articles	141
4.2.	Bundestag printed matters	157
4.3.	Other printed matter	158
4.4.	Cases of the Hungarian Data Protection Commissioner	158
4.5.	Court cases	160
4.5.1.	Cases of the ECJ	160
4.5.2.	Hungarian court cases	160
4.5.3.	Decisions of German High Courts	160
4.6.	Other documents	161
II.	SURVEY REPORT ON PRIVACY IN THE WORKPLACE IN HUNGARY AND GERMANY	163
	SUMMARY	165
	The extent of IT equipment use for private purposes at the workplace ...	165
	Private use of workplace equipment from the perspective of employers ...	166
	Data processing practices at the workplace	166
	The level of privacy regulation	167
	Information on privacy issues at the workplace	167
	Remedies	167
	Data protection awareness	168
	Attitudes to data protection	168
	Notes on methodology	168
	THE USE OF WORKPLACE COMMUNICATION AND IT EQUIPMENT FOR PRIVATE PURPOSES	172
	Frequency of private use	172
	Socio-demographic correlations	176
	Employers' assessment of the use of workplace equipment for private purposes	177
	Justified sanctions for unauthorized use of workplace equipment as perceived by employer representatives	184

DATA PRACTICES AT THE WORKPLACE	185
Monitoring communication and IT equipment at the workplace	185
Workplace characteristics in terms of privacy and data protection	188
The level of privacy regulation at the workplace	191
Information on privacy issues at the workplace	195
Remedies	198
DATA PROTECTION AWARENESS	203
ATTITUDES TO DATA PROTECTION	211
LIST OF DIAGRAMS AND TABLES	219
III. CODES OF CONDUCT	223
UNIVERSAL CODE ON THE PROTECTION OF PERSONAL DATA ACQUIRED THROUGH MONITORING IN EMPLOYMENT RELATIONSHIPS	225
Part I	225
1. Purpose and scope	225
2. Definitions and interpretation	226
3. Principles	226
Part II	227
4. Legal basis of monitoring	227
5. Purpose of monitoring and retention of data acquired through monitoring ..	227
6. Informing workers in advance	228
7. Additional requirements for secret monitoring	229
8. Security aspects	229
9. Co-operation between employers and employees	230
10. Training of staff	230
11. Documentation of data processing	230
Part III	230
12. Specification of requirements	230
13. Compliance assessment and certification	231
Annex I. Applicability statement	232
Annex II. Accredited jurisdiction or sector specific codes of conduct	236
Annex III. Commentary on the Universal code on the protection of personal data acquired through monitoring in employment relationships	237
Introduction	237
Part I	237

1.	Purpose and scope.....	237
1.1.	Purpose of the Code	237
1.2.	Scope of the Code	238
1.3.	Structure of the Code	238
2.	Definitions and interpretation.....	238
2.1.	Definitions given by the Code.....	238
2.2.	References to jurisdiction specific regulations	239
3.	Principles.....	239
3.1.	Finality.....	240
3.2.	Proportionality	240
3.3.	Transparency.....	241
3.4.	Accuracy, security and confidentiality	241
3.5.	Partnership and co-operation	242
3.6.	No waiver for privacy rights	242
Part II		242
4.	Legal basis of monitoring	242
5.	Purpose of monitoring and retention of data acquired through monitoring.....	243
6.	Informing workers in advance	243
7.	Additional requirements for secret monitoring.....	243
8.	Security aspects.....	244
9.	Co-operation between employers and employees.....	244
10.	Training of staff.....	245
11.	Documentation of data processing	245
Part III		245
12.	Specification of requirements	245
13.	Compliance assessment and certification	246
HUNGARIAN JURISDICTION SPECIFIC IMPLEMENTATION OF THE UNIVERSAL CODE ON THE PROTECTION OF PERSONAL DATA ACQUIRED THROUGH MONITORING IN EMPLOYMENT RELATIONSHIPS.....		247
Part I		247
1.	Purpose and scope.....	247
2.	Definitions and interpretation	248
3.	Principles.....	249
Part II		250
4.	Legal basis of monitoring	250
5.	Purpose of monitoring and retention of data acquired through monitoring.....	251

6.	Informing workers in advance	253
7.	Additional requirements for secret monitoring	254
8.	Security aspects	254
9.	Co-operation between employers and employees	256
10.	Training of staff	257
11.	Documentation of data processing	257
Part III		258
12.	Specification of requirements	258
13.	Compliance assessment and certification	258
Annex I Applicability statement.		260
Annex II References.		261
Laws and regulations		261
Decisions of the Data Protection Commissioner		261
RECOMMENDATIONS ON THE REGULATION OF TECHNICAL CONTROL AND SURVEILLANCE IN THE EMPLOYMENT CONTEXT IN GERMANY		263
1.	Background, Objectives of the Agreement	264
2.	Scope of application	265
2.1.	Territorial scope	265
2.2.	Material scope	265
2.3.	Personal scope	265
3.	Definitions	265
4.	General Principles	265
5.	The legal basis for the processing of employees' personal data; special categories of personal data; Distribution of the burden of proof	266
6.	Special requirements for the consent of the employee	267
7.	The purpose of the processing of data	267
8.	Principle of narrow interpretation of the purpose limitation	269
9.	Change of purpose	269
10.	Separation rule	269
11.	Obligation to provide information	270
12.	Covert measures (secret surveillance)	271
13.	Security aspects	272
14.	Data secrecy, education and training	273
15.	Documentation of the data processing and use	274
16.	Audit	275
17.	Rights of the employees	275
18.	Participation right of the works council	276
19.	Infringements, interpretation of the Agreement	276
20.	Severability Clause	277
21.	Entry into force, termination, validity, written form, Annexes	277

Annex I Definitions	279
Annex II Explanation of the general data protection principles, ensuring the comprehensive employee of data protection	280
1. General data protection principles	280
2. Ensuring comprehensive employee data protection	281
Annex III Purpose	282
IV. IMPLEMENTING AND AUDIT OF THE CODES OF CONDUCT	285
1. SELF-REGULATION, AUDIT AND CERTIFICATION SCHEMES IN THE FIELD OF DATA PROTECTION.....	287
1.1. Endeavours toward Self-Regulation	287
1.2. Self-regulation in the framework of the new European data protection regime.	289
1.2.1. Obligations imposed on data controllers and data processors	289
1.2.2. Elaboration of codes of conduct and certification.....	293
1.3. Data Protection Audit and Certification.....	293
1.3.1. Definition of data protection audit and certification.....	293
1.3.2. Types of audit/certification	294
1.3.2.1. Instrument audit and system audit	294
1.3.2.2. Internal, supplier and external audit	295
1.3.2.3. Adequacy audit and compliance audit.	295
1.3.3. Advantages and disadvantages of data protection audit – the motivation of the organizations concerned.....	296
1.3.4. The Regulation of Data Protection Audit in Hungary	297
2. METHODOLOGY TO IMPLEMENT AND AUDIT OF A PRIVACY MANAGEMENT SYSTEM CONCERNING MONITORING IN EMPLOYMENT RELATIONSHIPS.....	301
2.1. The concept of the Code of Conduct	301
2.1.1. The general or the specific nature of the Code	301
2.1.2. The wide scope of applicability of the Code.....	301
2.1.3. Approach based on “management system”.....	302
2.1.4. Applicability and certifiability	303

2.2.	The implementation of the Code: establishing a data protection management system.	303
2.2.1.	Collecting the binding rules	304
2.2.2.	Preparing the appropriate internal documentation	304
2.2.2.1.	Applicability Statement.	304
2.2.2.2.	Privacy Policy	305
2.2.2.3.	Information documents	305
2.2.2.4.	Account of security measures	305
2.2.3.	Adjusting the actual operation of the organisation to the documentation	305
2.3.	Audit and certification of data protection management systems	306
2.3.1.	The provisions of the Code of Conduct on auditing	308
2.3.2.	The point(s) of reference for compliance.	308
2.3.3.	The audit process.	309
2.3.3.1.	Principles.	309
2.3.3.2.	Defining the scope.	309
2.3.3.3.	Making and implementing an audit plan.	309
2.3.3.4.	Findings of the audit	310
2.3.3.5.	Preparing an audit report.	310
2.3.4.	Certification.	310
3.	THE ROLE OF THE TECHNOLOGY – AUDITING AND CERTIFICATION IN THE FIELD OF DATA SECURITY	311
3.1.	Technologies of workplace surveillance.	311
3.1.1.	Camera surveillance	311
3.1.2.	Access control systems	313
3.1.3.	The application of ICT devices	317
3.2.	Privacy enhancing technologies	323
3.3.	The accountability of data protection requirements	325
3.4.	Aligning the requirements of data security	329
3.4.1.	Using best practice	330
3.4.2.	COBIT	332
3.4.3.	ISO/IEC 27001	334
	LITERATURE AND REFERENCES	339