

Contents

About the Authors	7
List of Abbreviations	8
Introduction	11
1. Biometric Technology	15
1.1 Purpose and Characteristics of Biometrics	15
1.2 Biometrics and Law in General	18
1.3 Risks Associated with Using Biometrics	20
1.3.1 Risks Related to Design of Biometric Systems	21
1.3.2 Risks Related to Attacks on Biometric Systems	30
1.3.3 Risks Related to Legal Regulation of Biometric Systems	30
2. Biometrics from the Perspective of International and EU Law	33
2.1 International Law	33
2.2 EU Law	35
2.2.1 GDPR and Its Ancestors	35
2.2.2 National Derogations of Selected Member States to the GDPR and the Data Protection Directive for Police and Criminal Justice Authorities with Regard to Biometrics	47
2.2.3 Other EU Legislation	53
2.2.4 EU Policies on Artificial Intelligence and Potential Future Requirements on Processing of Biometric Data	54
3. Czech Legislation on Biometrics	57
3.1 Social and Constitutional Aspects of the Biometrics	57
3.1.1 Introduction	57
3.1.2 An Individual's Biometric Data and Basic Structure of Its Protection	59
3.1.3 Right to Privacy and its Relation to Other Fundamental Rights in the Context of Protection of Biometric Data	60
3.1.4 Risks Related to Processing Biometric Data and their Categorization	66
3.1.5 Social Specifics of Using Biometrics in the Czech Republic – results of statistical research titled 'Biometrics and its Use from the Perspective of the Czechs'	69
3.1.6 Solutions in Constitutional and Human Rights Spheres	71
3.2 Current Czech Personal Data Protection Legislation	76
3.3 Other Legislation with Specific Rules on Biometrics	77
3.3.1 Travel Documents	77

3.3.2	Biometric Data of Foreigners	78
3.3.3	Processing of Biometric Data by the Czech Police	78
3.3.4	Processing of Biometric Data by the Czech Military Police	79
3.3.5	Obligatory Biometric Identification or Authentication	80
3.4	Special Cases of Processing Biometric Data	81
3.4.1	Dynamic Biometric Signature	81
3.4.2	Biometric Data in Health Applications	90
3.4.3	Biometric Data and Neuromarketing	96
3.4.4	Biometric Data and Profiling for the Purpose of Criminal Proceedings and Implications for Human Rights	104
4.	Data Subjects and Their Options with Regard to Protecting Own Biometric Data	119
4.1	Concerns of Data Subjects	119
4.2	Scope of Data Subjects' Autonomy	120
4.2.1	General Remarks on the Principle of Personal Autonomy	120
4.2.2	Instruments of Data Subjects for Exercising Their Right to Autonomy	123
4.2.3	Limitations of Personal Autonomy	126
4.3	Right to Hide	130
5.	Recommendations for Data Controllers	133
5.1	Adhering to Principles of Personal Data Processing	133
5.1.1	Lawfulness, Fairness and Transparency	133
5.1.2	Purpose Limitation	134
5.1.3	Data Minimisation	135
5.1.4	Accuracy	135
5.1.5	Storage Limitation	135
5.1.6	Integrity and Confidentiality	136
5.1.7	Accountability	136
5.2	Respecting Legal Grounds for Processing Biometric Data	136
5.3	Fulfilling Rights of Data Subjects	136
5.3.1	Right to Be Forgotten	137
5.3.2	Right to Data Portability	137
5.3.3	Right not to Be Subject to Automated Decision-Making and Profiling	138
5.4	Specific Obligations	138
5.5	Data Vulnerability and Privacy Policy	139
	Conclusion	141
	List of References	145
	Annex I. Report on Augmented Indicative Values of Biometric Data	167