Đorđe Krivokapić
Dunja Tasić Krivokapić
Jelena Adamović
Andrea Nikolić

PERSONAL DATA PROTECTION IN BUSINESS

Prof. Dr. Đorđe Krivokapić
Jelena Adamović
Dunja Tasić Krivokapić
Andrea Nikolić

HANDBOOK: PERSONAL DATA PROTECTION IN BUSINESS

HANDBOOK: PERSONAL DATA PROTECTION IN BUSINESS

Prof. Dr. Đorđe Krivokapić
Jelena Adamović
Dunja Tasić Krivokapić
Andrea Nikolić

Reviews

Milan Marinović
Prof. Dr. Hrvoje Lisičar
Dr. Nasir Muftić

Art direction

Kristina Pavlak

Translation

Milica Jovanović

Layout

Miodrag Panić

Design

Goran Ratković

Printed by Službeni Glasnik

Number of copies: 150

Published by the Faculty of Organizational Sciences, Belgrade, 2023.

Prof. Dr. Đorđe Krivokapić
Jelena Adamović
Dunja Tasić Krivokapić
Andrea Nikolić

HANDBOOK:
Personal data protection in business

Publication “HANDBOOK: PERSONAL DATA PROTECTION IN BUSINESS” was created as a result of the Author’s activities within the project “Greater Internet Freedom” realized by the Author with the support of Internews and the United States Agency for International Development USAID. The views expressed in this publication/book do not reflect necessarily the views of Internews and the United States Agency for International Development USAID or the Government of the United States of America.

© Fakultet organizacionih nauka, Univerzitet u Beogradu
http://www.fon.bg.ac.rs

CONTENT

1. FOREWORD 11
   1.1. Commissioner's foreword 11
   1.2. Greater Internet Freedom Serbia Project foreword 13

2. GLOSSARY AND ABBREVIATIONS 15
   2.1. Legal glossary 15
   2.2. Technical glossary 18
   2.3. Abbreviations 19

3. PREFACE 21

4. LEGAL FRAMEWORK 25
   4.1. International system 25
   4.2. European Union 26
      4.2.1. GDPR 26
      4.2.2. Police directive 27
      4.2.3. National legislation 27
      4.2.4. European Data Protection Board opinions 28
      4.2.5. Opinions and decisions of independent supervisors 29
      4.2.6. Decisions of the Court of Justice of the European Union 34
      4.2.7. National court practice 34
      4.2.8. Additional support 35
   4.3. Serbia 37
      4.3.1. Personal Data Protection Law 37
      4.3.2. Secondary legislation 38
      4.3.3. Practice 39
         4.3.3.1 Court decisions 41
         4.3.3.2. Decisions of the Commissioner 41

4.3.3.3. Opinions of the Commissioner 42
4.4. Commissioner for Information of Public Importance and Personal Data Protection 43
4.4.1. History and status 43
4.4.2. Commissioner's powers 45
4.5. Broader regulatory framework 45
4.5.1. Information security 45
4.5.2. E-commerce, advertising law, and intermediary liability 47
4.5.3. Law of obligations 49
4.5.4. Cybercrime 49
4.5.5. Free access to information of public importance and open data 50
4.5.6. Sectoral legislation 51
4.5.7. Self-regulation 51
4.5.7.1. Code of conduct 52
4.5.7.2. Certification 53
4.5.7.3. Binding corporate rules 55
4.5.7.4. Ethical guidelines for the development a nd application of reliable and responsible artificial intelligence 56

5. SCOPE OF APPLICATION 57
5.1. Material application 57
5.1.1. Automated processing and data collections 57
5.1.2. Personal or household exemption 58
5.2. Territorial application 60

6. BASIC CONCEPTS 67
6.1. Personal data 67
6.2. Data subject 72
6.3. Special categories of personal data 73
6.4. Data processing 77
6.4.1. Automated decision-making and profiling 80

7. KEY ROLES 87
7.1. Data controller 90

7.2. Joint controllers 95
7.3. Data processor 98
7.4. Data recipient 100
7.5. Third party 101

8. PRINCIPLES OF DATA PROCESSING 103
8.1. Importance of principles 103
8.2. Lawfulness, fairness, and transparency 104
8.3. Purpose limitation 110
8.4. Data minimisation 115
8.5. Accuracy 119
8.6. Storage limitation 122
8.7. Integrity and confidentiality 125
8.8. Accountability 127

9. LAWFULNESS 131
9.1. When is processing lawful? 131
9.2. Conclusion and execution of contracts 134
9.3. Compliance with legal obligations 138
9.4. Legitimate interests 140
9.5. Consent 147
9.5.1. Consent of minors 151
9.6. Protection of vital interests 153
9.7. Execution of public authority 154
9.8. Lawfulness of processing special categories of data 157

10. RESPONSIBILITY AND COMPLIANCE 161
10.1. Key obligations 161
10.1.1. Joint controller agreement 163
10.1.2. Controller and processor relationship 166
10.2. Documentation 169
10.2.1. Mapping processing activities 170
10.2.2. Records of processing activities 171
10.2.2.1. Controller's records 172
10.2.2.2. Processor's records 173
10.2.3. Policies and templates 173

10.3. Data Protection Impact Assessment 174
10.4. Privacy by Design and by Default 182
10.5. Data processing security 187
10.5.1. Risk Assessment 188
10.5.2. Security measures 190
10.5.2.1. Access control 191
10.5.2.2. Encryption 192
10.5.2.3. Pseudonymisation, tokenisation, and anonymisation 193
10.5.2.4. Data loss prevention 195
10.6. Incident Response 196
10.6.1. Incident management 196
10.6.2. Incident management policy 201
10.6.3. Notifying the Commissioner 202
10.6.4. Notifying data subjects 204
10.7. Data transfers 204
10.7.1. General rule for transfers 206
10.7.2. Transfers based on an adequate level of protection 206
10.7.3. Transfer with appropriate safeguards 210
10.7.4. Transfers in special situations 213
10.7.5. Data import into Serbia from the EU 214
10.8. Representative 216
10.8.1. Representative of a foreign controller or processor in Serbia 216
10.8.2. Representative of a Serbian controller or processor in the EU 218
10.8.3. Representative of a Serbian controller or processor in third countries 220
10.9. Allocation of roles in the organization 221
10.9.1. Managing the protection of personal data in the organization 222
10.9.2. Management 224
10.9.3. Data Protection Officer 226
10.9.3.1. When is there an obligation to appoint a Data Protection Officer? 226
10.9.3.2. Data Protection Officer status 229
10.9.3.3. Data Protection Officer duties 231

10.10. Employees 231
10.11. Organizational and personnel measures 234
10.12. Continuous internal education 236
10.13. Service providers 237
10.13.1. Software Services 237
10.13.2. Storage and maintenance services 238
10.13.3. E-commerce services 239
10.13.4. Professional management and consulting services 239
10.14. Cooperation with the Commissioner 241

11. CITIZENS' RIGHTS 245
11.1. Exercising rights and Transparency 245
11.2. The right to information 247
11.3. Right of access 252
11.4. Right to rectification and completion 255
11.5. Right to erasure 256
11.6. Right to restriction of processing 260
11.7. Right to data portability 262
11.8. Right to object 264
11.9. Right to legal remedy 265
11.10. Rights regarding automated decisions and profiling 266
11.11. Restriction of rights 269
11.12. Citizen requests 269

12. TYPICAL SITUATIONS 271
12.1. Recruitment process 271
12.2. Required personnel records 276
12.3. Video surveillance of employees 280
12.4. Employee productivity monitoring 284
12.5. Direct marketing 289
12.6. Mobile application 294
12.7. Online market and loyalty program 298
12.8. Big data 302

13. SPECIAL CASES OF PROCESSING 307
13.1. Freedom of expression and information 307

13.2. Free access to information of public importance 310
13.3. Processing of the national identification number 310
13.4. Processing in the field of labour and employment..... 311
13.5. Processing for archiving, research, and statistics 311
13.6. Processing by churches and religious communities 312
13.7. Processing for humanitarian purposes by authorities 312

14. SANCTIONS 313
14.1. Misdemeanour penalties 313
14.2. Nonmonetary liabilities 316
14.3. Compensatory damages 317
14.4. Reputational risk 318
14.5. Criminal liability 319

AUTHORS' BIOGRAPHIES 323