

Contents

1	Introduction to EU Data Protection Law	1
1	Introduction	1
2	Revisiting Trust in Data Protection	3
3	Data Protection Directive 1995 and the OECD Guidelines	4
4	Basic Concepts: Data Protection Framework	5
4.1	Data Controller and Processing of Personal Data	5
4.2	Personal Data	17
4.3	Legal Basis of Processing	27
5	ePrivacy Directive	43
5.1	Scope of Article 15(1) of the ePrivacy Directive	43
5.2	ePrivacy vis-à-vis Intellectual Property Infringement	53
	Suggested Readings	56
2	EU Data Protection Law Framework	59
1	Introduction	59
2	Principles of Processing	59
2.1	Purpose Specification and Collection Limitation	60
2.2	Accuracy and the Option to Update Personal Information	61
2.3	Accountability	62
2.4	Limited Storage and Processing	64
3	Consent	70
3.1	Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) Case C—61/19	70
3.2	Bundesverband der Verbraucherzentralen und Verbraucherverbände — verbraucherzentrale Bundesverband eV v Planet49 GmbH Case C-673/17	78
3.3	Dutch Data Protection Authority Decision Against TikTok	82
3.4	Explicit Consent and Ordinary Consent	83

4	Exemptions Under Data Protection Framework	84
4.1	Personal or Household Purposes	84
4.2	Journalistic Purposes	87
	Suggested Readings	94
3	Transparency and Rights of the Data Subject	97
1	Introduction	97
2	The Principle of Transparency	98
2.1	Connecting Transparency with Purpose Limitation Principle	102
3	The Requirement of Transparent Information	103
4	Compliance Example	106
4.1	Transparency and Consent Framework: The Case of Dutch Data Protection Authority and IAB Europe	107
5	Right of Access Under the GDPR	111
5.1	RW v Österreichische Post AG Case C-154/21	113
6	The Right to Erasure (Right to Be Forgotten)	115
6.1	The Idea of the Right to Be Forgotten	115
7	The Right to Data Portability and Right to Object to Processing	137
7.1	The Data Portability Right	137
7.2	Right to Object to Processing	139
8	Compliance Examples	142
8.1	Virgin Media	142
8.2	We Buy Any Car Limited (WBAC)	144
	Suggested Readings	146
4	Duties and Responsibilities of Controller and Processor	149
1	Introduction	149
2	Fashion ID C-40/17	149
3	Design and Default Approach to Protecting the Privacy	155
3.1	Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (DPDD)	158
3.2	Implementing Data Protection Principles in the Processing of Personal Data Using Data Protection by Design and by Default	160
4	Role of Controllers and Processors	162
4.1	Controllers Outside the EU	162
4.2	Mandates Under GDPR for Data Controllers/Processors	163
4.3	Processing Under the Authority of a Data Controller	164
5	Security Standards in Data Protection	166
5.1	Security of Processing	167
5.2	Breach of Security Standards in Personal Data: The ICO Decision in Marriott Hotels	168
5.3	What Is Pseudonymisation?	171

6	Data Protection Impact Assessment (DPIA)	172
6.1	Necessity of a Data Protection Impact Assessment Exercise	173
6.2	The Idea of Data Protection Impact Assessment	174
6.3	European Data Protection Board (EDPB) Guidelines on Data Protection Impact Assessment Adopted on 4 April 2017 (Excerpts from the Guideline)	175
6.4	The Role of a Data Protection Officer (DPO)	177
7	Standardisation of Processes	179
7.1	Drawing up of Codes of Conduct by Organisations and Associations	179
7.2	The Consultation Route in Drawing up Codes	180
7.3	The Overall Exercise of Finalising the Codes	180
7.4	Monitoring of Approved Codes of Conduct	181
7.5	Initiating the Process of Certification	183
7.6	Certification	183
7.7	Certification Bodies	184
	Suggested Readings	185
5	Transfer of Personal Data to Third Countries	187
1	Introduction	187
2	Legal Structure on the Rules of Transfer of Personal Data	187
2.1	Transfers Subject to Appropriate Safeguards	190
2.2	Binding Corporate Rules	191
3	Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for Transfers of Personal Data Between EEA and Non-EEA Public Authorities and Bodies	194
3.1	The Idea of Appropriate Safeguards	194
3.2	Transfer Based on Article 46 GDPR	196
4	Adequacy Through the Lens of Law Enforcement Directive (LED)	197
4.1	Transfers on the Basis of an Adequacy Decision	197
5	EU Standards for Adequacy in the Police Cooperation and Judicial Cooperation in Criminal Matters	199
6	Transatlantic Data Transfer: EU-US Standards	200
6.1	Validity of Safe Harbour Regime	200
6.2	Validity of Privacy Shield Regime	209
6.3	EU-US Privacy Framework Agreement	220
7	Tracking the Development of Standard Contractual Clauses Adopted	222
	Suggested Readings	223
6	Enforceability, Remedies, Liabilities and Penalties	225
1	Introduction	225
2	Supervisory Authority	225
2.1	Structure and Establishment	226

- 2.2 Weltimmo Case, C-230/14 229
- 2.3 European Data Protection Board 232
- 3 Remedies, Liability and Penalties 234
 - 3.1 Enforcing GDPR: Lodging a Complaint 235
 - 3.2 The Issue of Compensation 236
 - 3.3 Guidelines on the Application and Setting
of Administrative Fines for the Purpose of Regulation
2016/679 [Article 29 Data Protection Working Party] 241
- 4 How Are Fines Calculated Under GDPR? 243
 - 4.1 Guidelines 04/2022 on the Calculation of Administrative
Fines 244
- Suggested Readings 251