Table of Contents

Preface xiii

Chapter 1. Introduction to EU Privacy and Data Protection 1
I. Relevant Legislative Instruments and Treaties 1
   A. Privacy and Data Protection as Fundamental Rights 1
   B. Convention 108 2
   C. OECD Guidelines 3
   D. EU Directive 4
II. Key Terms and Definitions 5
   A. Personal Data 5
      1. “Any Information” 6
      2. “Relating to” 7
      3. “An Identified or Identifiable” 7
      4. “Natural Persons” 8
   B. Data Subject 9
   C. Processing of Personal Data 9
   D. Personal Data Filing System 9
   E. Controller and Processor 10
      1. Controller 11
         a. “Determines the purposes and means of the processing of personal data” 12
         b. “Natural person, legal person or any legal body” 14
         c. “Alone or jointly with others” 14
      2. Processor 15
III. General Principles of Privacy 16
   A. Purpose Limitation (Finality) Principle 17
   B. Data Quality and Legitimacy 18
      1. Legal Basis for Processing (Legitimacy) 18
      2. Data Quality 19
         a. Fair and Lawful Processing 19
         b. Proportionality Principle 19
         c. Accuracy and Retention of Data 20
   C. Individual Rights of Data Subjects (Transparency Principle) 20
      1. Information (Notice) Requirement 20
      2. Access, Correction, and Deletion 21
      3. Remedies and Liabilities 22
   D. Security Principle 23
   E. Restrictions on Transfers 24
   F. Restrictions on Special Categories of Data (Sensitive Data) 24
Navigating EU Privacy and Data Protection Laws

Chapter 2. What Do EU Data Protection Rules Mean in Practice

I. Applicability of the Directive—Does the Directive Apply to My Company or Activities?
   A. Note on the Legislative Intent and Historical Context of the Applicability Provisions
   B. Does the Directive Apply to Me?
      1. Controllers with EU/European Economic Area (EEA) Establishment(s)—Article 4(1)(a)
         a. Establishment
         b. Processing in the Context of Activities
      2. Non-EU/EEA Controllers Processing Data in the EU/EEA—Article 4(1)(c)
         a. Use of Equipment Situated on EU Territory
         b. “In Transit” Exemption
         c. Appointment of a Representative
      3. Other Circumstances in Which EU Data Protection Law Applies

Practical Tips

IV. Do I Have a Sufficient Legal Basis for Processing?
   A. Unambiguous Consent of the Data Subject
   B. Processing Is Necessary for the Performance of a Contract or for Actions to Be Carried Out at the Request of the Data Subject That Are Necessary for the Conclusion of a Contract
   C. Processing Is Necessary to Comply with a Legal Obligation to Which the Controller is Subject
   D. Processing Is Necessary to Uphold the Legitimate Interests of the Controller or of a Third Party to Whom the Data are Supplied
   E. Summary

Chapter 3. Practical Compliance Steps

I. Interactions with DPAs
   A. Notifications to DPAs
      1. Timing of Notifications—Prior to Processing
      2. Exemptions from Notification
Practical Tips 47

3. Notification Procedure 47
4. Maintenance of Notifications 48

Practical Tips 48

How Do You File Notifications? 48
How Many Notifications Must You Submit? 49
B. Prior Checks—Authorization by DPAs 49
C. DPOs 50
1. Timing of Your Interactions with the DPAs and Risks Associated with Notifications 50

II. Internal Documents 54

A. Notice Requirement (Information to Individuals) 54
1. Timing 55
2. Means of Providing Notice 55
B. Notices, Privacy Policies 55
1. Websites 56
C. Consent 58
1. Informed Consent 58
2. “Unambiguous” Consent 58
3. Cookies 58
D. Notice 59

Practical Tips 59
1. Translations 60
2. Employee Representatives or Works Councils 60

E. Privacy and Data Impact Assessments 61

III. International Data Transfers 65

A. Adequacy Determination 66
1. Factors for a Determination of Adequacy 67
2. Procedure for Determining Adequacy 68
3. Countries Benefiting from Adequacy Determinations 68
4. Safe Harbor Framework (Transfers to the United States) 69
   a. Recent Developments Concerning Safe Harbor 69
5. PNR Data 71
B. Other Safeguards 71
1. Model Contracts 71
   a. Contractual Provisions 72
   b. Practical Considerations of Model Contract Use 72
2. BCRs 73
3. Industry Codes of Conduct 75
4. Ad Hoc Data Transfer Agreements 76
C. Article 26(1) Exemptions 76
   1. Interpretation of the Article 26(1) Exemptions 77
   2. Best Practice 79
   3. Consent 80
   4. Necessary for the Performance of a Contract 80
   5. Necessary for Contracts 81
   6. Public Interest Grounds and Legal Claims 82
   7. Data Subject’s Vital Interest 83
   8. Public Register 83

IV. Use of Processors (Independent Contractors and Vendors) 86
   A. Processor Obligations 87
      1. Data Security 87
      2. Confidentiality 88
   B. Contract between the Controller and the Processor 89
      1. France 91
      2. Norway 92
      3. Spain 93
      4. United Kingdom 94

Chapter 4. Human Resources 97
I. General Provisions Relating to Human Resources 97
   A. Records in the Employment Context 98
   B. Lawfulness of the Personal Data Processing 99
   C. Applicability of Data Subject Rights and Data Protection Principles in the Employment Context 100
      1. Notice/Privacy Policy 100
      2. Right of Access 100
      3. Other Individual Rights 101
      4. Data Quality 101
      5. Technical and Organizational Measures—Security 101
   D. International Transfers 101

II. Technology and Employee Relationships 104
   A. E-mail and Internet Use 104
      1. Working Party Guidelines for the Implementation of E-mail Monitoring 105
      2. Transparency and Notice to Employees 105
      3. Application of Data Protection Principles 108
         a. Necessity 108
         b. Finality 109
         c. Transparency 109
         d. Legitimacy 109
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>e. Proportionality</td>
<td>109</td>
</tr>
<tr>
<td>f. Accuracy and Retention of Data</td>
<td>110</td>
</tr>
<tr>
<td>g. Security</td>
<td>110</td>
</tr>
<tr>
<td>4. Working Party Guidance on Employer E-mail Policies</td>
<td>111</td>
</tr>
<tr>
<td>5. Consideration of e-Communication Laws</td>
<td>111</td>
</tr>
<tr>
<td>a. Belgium</td>
<td>112</td>
</tr>
<tr>
<td>b. France</td>
<td>112</td>
</tr>
<tr>
<td>c. Germany</td>
<td>114</td>
</tr>
<tr>
<td>Practical Tips</td>
<td>114</td>
</tr>
<tr>
<td>B. Video Surveillance</td>
<td>114</td>
</tr>
<tr>
<td>C. Social Networking</td>
<td>117</td>
</tr>
<tr>
<td>1. Potential Employer Liability and Risks</td>
<td>117</td>
</tr>
<tr>
<td>Related to Employees Using SNS</td>
<td>117</td>
</tr>
<tr>
<td>2. Employer Monitoring of the Use of SNS by Employees</td>
<td>118</td>
</tr>
<tr>
<td>Regarding Sanctioning Employees for SNS Use</td>
<td>119</td>
</tr>
<tr>
<td>D. Bring Your Own Device</td>
<td>119</td>
</tr>
<tr>
<td>E. Geolocation and Biometrics</td>
<td>120</td>
</tr>
<tr>
<td>1. Geolocation Technology</td>
<td>121</td>
</tr>
<tr>
<td>2. Biometrics</td>
<td>122</td>
</tr>
<tr>
<td>III. Sensitive Data</td>
<td>123</td>
</tr>
<tr>
<td>1. Varying Categories and Treatment in Member States</td>
<td>124</td>
</tr>
<tr>
<td>2. Preconditions for Processing</td>
<td>125</td>
</tr>
<tr>
<td>B. Particular Consideration of Certain Sensitive Data in the Employment Context</td>
<td>126</td>
</tr>
<tr>
<td>1. Health</td>
<td>126</td>
</tr>
<tr>
<td>2. Background Checks—Criminal Data</td>
<td>127</td>
</tr>
<tr>
<td>3. Social Security and National Identity Numbers</td>
<td>128</td>
</tr>
<tr>
<td>Chapter 5. Privacy and Company Compliance</td>
<td>131</td>
</tr>
<tr>
<td>I. Whistle-Blowing Hotlines</td>
<td>131</td>
</tr>
<tr>
<td>A. Cultural and Employment Concerns</td>
<td>131</td>
</tr>
<tr>
<td>B. Legal Basis for Hotlines</td>
<td>133</td>
</tr>
<tr>
<td>C. Proportionality and Data Quality: Limiting the Scope of the Hotline</td>
<td>133</td>
</tr>
<tr>
<td>1. A Limit on the Number (Type) of People Who Are Able to Use the Hotline to Submit a Report</td>
<td>134</td>
</tr>
<tr>
<td>2. A Limit on the Number (Type) of People Who May Be Incriminated via the Hotline</td>
<td>134</td>
</tr>
</tbody>
</table>
3. Preference for Identified versus Anonymous Reports and Promoting Confidentiality of a Hotline 134
4. Scope of Reporting: Proportionality and Accuracy within Hotline 135
5. Data Retention 136
D. Transparency and Notice 136
E. Rights of Implicated Persons 136
1. Notice—Communication about Implication in Report 137
F. Right of Access 137
G. Confidentiality and Information Security Measures 137
H. Management of Hotlines and Internal Handling 138
I. External Hotline Providers 138
J. Preference for EU Treatment of Investigations 139
K. Transfers 139

II. Audits and Foreign Corrupt Practices Act (and Other Anti-bribery/Anticorruption Legislation) 140
A. Background on Corruption Compliance and Data Protection 140
B. A Short Overview of ACB and AML Laws 141
C. How Personal Data Fits In 143
1. Risk Assessments 143
2. Due Diligence 144
D. Data Protection Issues 145
1. Legal Basis for Processing 145
2. Controller/Processor Determinations 146
3. Notices 146
4. Proportionality and Purpose Limitation 147
5. Retention Policies 148
6. Data Transfers 148
E. Summary 148

Chapter 6. Customers and Marketing 151
I. Direct Electronic Marketing and the e-Privacy Directive 151
A. Privacy, e-Marketing, and the e-Privacy Directive 152
1. An Opt-in Requirement to Receive Commercial Communications and the Concept of Prior Consent 152
2. The Existing Customer Exception 154
3. Recent Guidance on the Existing Customer Exception 155
4. Notice/Transparency 155
5. Protections 156
   a. Protection of the “Legitimate Interests” of Legal Persons 156
   b. Opt-out Registers 156
   c. Certain Exclusions 157
**Table of Contents**

B. A Sectoral Code of Conduct in the Direct Marketing Area:  
The FEDMA Code of Conduct and Annex 157

II. Behavioral Marketing and Cookies 158  
A. Terms Used 158  
B. Applicable Law 159  
C. Cookies under EU Privacy and Data Protection Law 160  
   2. UK ICO Guidance on the Use of Cookies 161  
D. Online Behavioral Advertising 164  
   1. Introduction 164  
   2. Application of the e-Privacy Directive 165  
   3. Responsibilities of the Various Actors in Behavioral Advertising and Guidance 166  
      a. Summary of Responsibilities of Behavioral Advertising Actors 166  
      b. Guidance on Consent for Ad Networks 167  
      c. Guidance on Information and Other Requirements for Ad Networks 167  
      d. Guidance on Sensitive Data 168  
   4. EASA/IAB Code—Best Practice Recommendation on Online Behavioural Advertising 169  
      a. Use of Opt-out Cookie System and JavaScript 170  
      b. Other Areas of Concern 170  
      c. Alternatives to Pop-up Screens for Obtaining Consent 170  
   5. UK CAP Rules on Online Behavioral Advertising 171  
E. Relationship with the GDPR 171

Chapter 7. Development of New Technologies 173  
I. Biometrics and Facial Recognition 173  
A. Working Party Guidance 174  
B. Complying with the Directive 175  
   1. Proportionality and Purpose Limitation 175  
   2. Legal Grounds for Processing 175  
      a. Performance of a Contract 175  
      b. Controller’s Legitimate Interest 175  
      c. Individual’s Consent 176  
   3. Security Measures—Technical and Organizational Measures to Protect Personal Data 176  
   4. Privacy by Design and Privacy Impact Assessments 177
Table of Contents

E. UK ICO Guidance on Anonymization of Data
   1. Discussion of UK Data Protection Law 201
   2. Guidance on Whether Data Can Be Anonymized 201
   3. Guidance Concerning Governance 202
F. Need for International Cooperation 202
V. The Internet of Things 204

Chapter 8. What Is on the Horizon? 207
   I. Current and Future Legislative Process 207
   II. Key Amendments to the GDPR in the European Parliament 210
      A. Territorial Scope 210
      B. Right to Be Forgotten and Right to Erasure 210
      C. Designation of the Data Protection Officer 210
      D. Administrative Sanctions 211
      E. Points of Divergence between the European Parliament and the Council 211
   III. The Right to Be Forgotten 211
   IV. Conclusion 212

Appendixes 213
   Appendix A. Notification/Registration on DPA Websites 213
   Appendix C. Glossary of Terms and Abbreviations Used 221

Bibliography 231

Index 247