

# Contents

Acknowledgements	9
Liability and legal disclaimer	10
List of abbreviations	11
<b>Preface</b>	<b>13</b>
<b>Introduction</b>	<b>17</b>
Background	17
Structure	18
Method	20
Bringing in added value	21
Target audience	21
<b>1. Navigating support</b>	<b>23</b>
1.1. National and regional Data Protection Authorities (DPAs)	24
1.2. The European Data Protection Board (EDPB)	26
1.3. The European Data Protection Supervisor (EDPS)	27
1.4. The European Union Agency for Cybersecurity (ENISA)	28
1.5. The European Union Agency for Fundamental Rights (FRA)	28
1.6. The EU funded initiatives	29
1.7. The International Association of Privacy Professionals (IAPP)	30
<b>2. Personal data protection basics</b>	<b>31</b>
2.1. What is personal data and its processing?	31
2.2. What are the possible roles for an SME in the processing operations?	41

2.3. What are the principles applicable to the processing of personal data?	49
2.4. What are the possible legal bases for personal data processing?	51
2.4.1. Background	51
2.4.2. How to choose among different legal bases?	52
Consent	52
Contractual relationship	56
Compliance with a legal obligation	57
Vital interests of data subjects or of another person	58
Public interest or exercise of an official authority vested in the data controller	58
Legitimate interests pursued by the data controller	59
2.5. What are the data subjects' rights?	62
2.5.1. Background	62
2.5.2. What are data subjects' requests, and how can these be fulfilled?	64
Right to transparency and information	64
Right to access	66
Right to rectification	69
Right to erasure, a.k.a. right to be forgotten (right to de-listing)	69
Right to restriction of processing	71
Right to data portability	72
Right to object	73
Right to not be subject to a decision based solely on automated decision-making (or profiling)	74
2.6. The obligation to appoint a Data Protection Officer (DPO)	75
2.6.1. Background	75
2.6.2. Is the appointment of a DPO mandatory for SMEs?	75
2.6.3. Who should be a DPO?	79
2.6.4. What tasks can be assigned to a DPO working for an SME?	80
2.6.5. Can an SME share a DPO with other organizations?	83
2.6.6. What should be considered before appointing a DPO?	83

<b>3. The theory and practice of a risk-based approach</b>	<b>85</b>
3.1. Background	85
3.2. What is a risk in the GDPR?	86
3.3. What does cause risks?	87
3.4. How can risks under the GDPR be evaluated?	89
3.5. What are the provisions embedding a risk-based approach in the GDPR?	95
3.6. How can a risk-based approach benefit SMEs?	96
3.7. A risk-based approach in practice	97
3.7.1. Responsibility of the controller and the principle of accountability	97
Background	97
What does an SME need to do to be accountable?	98
What are the other examples of accountability measures?	99
What are the advantages of accountability for an SME?	100
3.7.2. Data protection by design and data protection by default	101
Background	101
What does data protection by design entail?	102
How to evaluate the appropriateness and effectiveness of data protection by design measures?	105
What does data protection by default entail?	107
What are some examples of measures implementing data protection by default?	107
3.7.3. Records of processing activities and other documentation	110
Background	110
What does documentation require?	110
What are the other types of documentation required by the GDPR?	114
3.7.4. Security of processing	116
Background	116
How is the security obligation related to other provisions?	116
What organizational security measures can an SME take?	117

What technical security measures can an SME take?	118
What level of security is required?	119
<b>3.7.5. Personal data breach notification</b>	<b>120</b>
Background	120
Under what conditions is a notification to the DPA required?	122
What documentation could help an SME to prepare for a data breach?	123
Under what conditions is a notification to affected individuals required?	124
<b>3.7.6. Data protection impact assessment (DPIA) and prior consultation</b>	<b>128</b>
Background	128
Who has to perform a DPIA?	129
When is a DPIA mandatory?	130
When is a DPIA not required?	135
When is a new (revised) DPIA required?	136
How should a DPIA be conducted?	137
<b>3.7.7. Codes of conduct</b>	<b>144</b>
Background	144
What are the advantages of codes of conduct?	146
How to select the appropriate code of conduct?	146
<b>3.7.8. Certification</b>	<b>147</b>
Background	147
What are the advantages of certifications for SMEs?	148
How should you choose between different certifications?	149
<b>4. SMEs and employees' data</b>	<b>151</b>
4.1. What are the possible legal bases for processing the personal data of employees?	152
4.2. When and what monitoring activities are permissible?	154
<b>Annex I – National laws</b>	<b>157</b>
<b>About the editors</b>	<b>169</b>