

Inhaltsverzeichnis

| | |
|---|------|
| Verzeichnis der Muster | XIII |
| Abkürzungsverzeichnis | XV |
| Die praktische Umsetzung der DSGVO | 1 |
| Schritt 1: Unterstützung aus dem Management sichern | 3 |
| Schritt 2: Datenschutzbeauftragten bzw -manager ernennen und Zuständigkeiten klären | 4 |
| Schritt 3: Ersten Überblick verschaffen..... | 6 |
| Schritt 4: Ziele des Datenschutzmanagements in einer Unternehmens- richtlinie definieren | 9 |
| Schritt 5: Passende IT-Tools für das Datenschutz-Management auswählen..... | 11 |
| Schritt 6: Informationen über alle Datenverarbeitungsprozesse erheben | 13 |
| Schritt 7: Verzeichnis der Verarbeitungstätigkeiten erstellen | 14 |
| Schritt 8: Rechtmäßigkeit der Verarbeitungstätigkeiten absichern | 14 |
| Schritt 9: Datenschutz-Folgenabschätzungen durchführen | 21 |
| Schritt 10: Datenschutzrelevante Unternehmensrichtlinien erstellen.... | 22 |
| Schritt 11: Konzept für unternehmensinterne Informationsmaßnahmen und Schulungen erstellen..... | 24 |
| Schritt 12: Datenschutz im täglichen Betrieb aufrechterhalten | 24 |
| 100 Praxisfragen und Antworten zur DSGVO | 27 |
| A. Der Datenschutzbeauftragte..... | 29 |
| 1. Wann muss eine Organisation einen Datenschutzbeauftragten bestellen?..... | 29 |
| 2. Wann ist eine Organisation eine „Behörde oder öffentliche Stelle“ und muss aus diesem Grund einen Datenschutz- beauftragten bestellen? | 31 |
| 3. Welche Stellung hat der Datenschutzbeauftragte in der Organisation? | 32 |

| | |
|--|----|
| 4. Welche Pflichten hat der Datenschutzbeauftragte? | 33 |
| 5. Welches Haftungsrisiko hat der Datenschutzbeauftragte? | 35 |
| 6. Genießt ein Datenschutzbeauftragter Kündigungsschutz?..... | 36 |
| 7. Welche Ausbildung und Fähigkeiten muss ein Datenschutz- beauftragter haben?..... | 38 |
| 8. Kann ein Datenschutzbeauftragter auch andere Aufgaben wahrnehmen oder in Teilzeit bestellt werden?..... | 40 |
| 9. Kann der Leiter der IT-Abteilung als Datenschutzbeauftragter bestellt werden?..... | 40 |
| 10. Muss der Name des Datenschutzbeauftragten veröffentlicht werden?..... | 42 |
| 11. Wie lange ist die Funktionsperiode eines Datenschutz- beauftragten? | 43 |
| 12. Kann auch ein Externer als Datenschutzbeauftragter fungieren? | 44 |
| 13. Welche Vor- und Nachteile hat ein externer Datenschutz- beauftragter? | 44 |
| B. Das Verzeichnis der Verarbeitungstätigkeiten | 47 |
| 14. Ein Unternehmen hat weniger als 250 Mitarbeiter – Muss trotzdem ein Verzeichnis der Verarbeitungstätigkeiten geführt werden?..... | 47 |
| 15. Was muss im Verzeichnis der Verarbeitungstätigkeiten jeden- falls dokumentiert werden? | 48 |
| 16. Muss auch ein Auftragsverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten führen? | 53 |
| 17. Soll mehr als das Minimum im Verzeichnis der Verarbeitungs- tätigkeiten dokumentiert werden? | 54 |
| 18. Müssen auch Verarbeitungstätigkeiten dokumentiert werden, die ohnedies bereits in DVR-Online gemeldet wurden? | 55 |
| 19. Ist der Datenschutzbeauftragte für die Führung des Verzeich- nisses der Verarbeitungstätigkeiten verantwortlich? | 56 |
| 20. Kann das Verzeichnis der Verarbeitungstätigkeiten auch elektronisch geführt werden? Sollen spezielle Softwarelösungen verwendet werden?..... | 57 |
| 21. Kann das Verzeichnis der Verarbeitungstätigkeiten auch auf Englisch geführt werden? | 59 |
| C. Datenschutz-Folgenabschätzungen | 61 |
| 22. Was ist eine Datenschutz-Folgenabschätzung eigentlich? | 61 |
| 23. Wann muss eine Datenschutz-Folgenabschätzung durchgeführt werden?..... | 62 |
| 24. Wie lautet die Faustregel der Artikel-29-Datenschutzgruppe zur Notwendigkeit einer Datenschutz-Folgenabschätzung? | 65 |

| | |
|--|-----|
| 25. Muss eine Datenschutz-Folgenabschätzung auch für alte Datenanwendungen durchgeführt werden, die es bereits vor Geltungsbeginn der DSGVO gab? | 66 |
| 26. Wie soll eine Datenschutz-Folgenabschätzung durchgeführt werden?..... | 67 |
| 27. Wer ist für die Datenschutz-Folgenabschätzung verantwortlich? | 74 |
| 28. Was sind mögliche Risikominderungsmaßnahmen? | 75 |
| 29. Ist eine Datenschutz-Folgenabschätzung eine einmalige Angelegenheit?..... | 77 |
| 30. In welchen Fällen ist eine Konsultation mit der Datenschutzbehörde durchzuführen?..... | 77 |
| D. Datenschutzmitteilungen und Betroffenenrechte..... | 79 |
| 31. Muss die Verarbeitung gegenüber den Betroffenen offengelegt werden?..... | 79 |
| 32. Wann und wie sind die Betroffenen zu informieren?..... | 83 |
| 33. Was ist vom Recht auf Auskunft umfasst? | 85 |
| 34. Hat der Betroffene bei einem Auskunftsbegehren eine Mitwirkungspflicht?..... | 86 |
| 35. Muss eine Person ihre Identität nachweisen, um ihre Betroffenenrechte geltend zu machen?..... | 86 |
| 36. Hat der Betroffene immer ein Recht auf Datenübertragbarkeit? | 89 |
| 37. In welchem Format müssen Daten übergeben werden, wenn der Betroffene Datenübertragbarkeit fordert?..... | 90 |
| 38. Können Betroffene immer einen Widerspruch erheben?..... | 91 |
| 39. Kann das Recht auf Vergessenwerden immer geltend gemacht werden?..... | 93 |
| 40. Wie schnell muss man reagieren, wenn Betroffene ihre Rechte geltend machen?..... | 94 |
| 41. Haben auch juristische Personen Betroffenenrechte?..... | 94 |
| 42. Sind bei Ausübung des Lösungsrechts auch Daten von Backups zu löschen?..... | 95 |
| E. IP-Adressen, Cookies und Social Media Plugins | 97 |
| 43. Sind IP-Adressen personenbezogene Daten? | 97 |
| 44. Welche Daten dürfen wir am Webserver protokollieren?..... | 98 |
| 45. Ist eine Einwilligung für Cookies erforderlich? | 99 |
| 46. Wie soll die Datenschutzmitteilung auf einer Website aussehen? | 99 |
| 47. Dürfen wir auf unserer Website Google Analytics verwenden? .. | 103 |
| 48. Ist es zulässig, auf der eigenen Website Social Media Plugins zu verwenden?..... | 106 |
| F. E-Mails | 109 |
| 49. Wie lange sollen E-Mails aufbewahrt werden? | 109 |

| | |
|--|-----|
| 50. Dürfen eingehende und ausgehende E-Mails gespiegelt werden? | 110 |
| 51. Darf man auf den E-Mail-Account eines Mitarbeiters zugreifen, der auf Urlaub ist oder das Unternehmen verlassen hat?..... | 111 |
| G. Kundendatenschutz..... | 113 |
| 52. Ich habe nur Geschäftskunden – gilt die DSGVO überhaupt? | 113 |
| 53. Müssen Kunden in die Verarbeitung ihrer Daten einwilligen?..... | 114 |
| 54. Ist eine Einwilligung für einen E-Mail-Newsletter erforderlich? | 115 |
| 55. Was ist bei Kunden-Profilung zu beachten?..... | 117 |
| 56. Ist eine Einwilligungserklärung in AGB zulässig?..... | 119 |
| 57. Sind separate Einwilligungen für unterschiedliche Verarbeitungszwecke erforderlich?..... | 119 |
| 58. Gelten alte Einwilligungen, die vor Geltungsbeginn der DSGVO erteilt wurden, fort?..... | 121 |
| 59. Ab welchem Alter ist eine Einwilligung von Minderjährigen wirksam?..... | 121 |
| 60. Darf man das Angebot von Waren und Dienstleistungen von der Erteilung einer Einwilligung abhängig machen (Koppelungsverbot)..... | 122 |
| 61. Wie umgeht man das Koppelungsverbot? | 123 |
| H. Mitarbeiterdatenschutz | 125 |
| 62. Von welchen IT-Systemen muss der Betriebsrat informiert werden?..... | 125 |
| 63. In welchen Fällen ist eine Betriebsvereinbarung erforderlich?..... | 126 |
| 64. Droht eine Geldbuße, wenn eine Betriebsvereinbarung fehlt?..... | 127 |
| 65. Was ist notwendiger Inhalt einer Betriebsvereinbarung?..... | 127 |
| 66. Darf der Betriebsrat in alle Mitarbeiterdaten Einsicht nehmen?.. | 129 |
| 67. Wie lange dürfen Mitarbeiterdaten aufbewahrt werden?..... | 130 |
| 68. Ist eine Mitarbeitererlaubnis wirksam? | 131 |
| 69. Ist die Überwachung des Internetverkehrs der Mitarbeiter zulässig? Einschließlich Aufbrechen der SSL/TLS-Verschlüsselung?.. | 131 |
| I. Outsourcing | 135 |
| 70. Muss der Verantwortliche mit jedem Dienstleister einen Vertrag abschließen? Wie muss dieser aussehen?..... | 135 |
| 71. Der Dienstleister versichert, dass er ohnedies nie auf die Daten zugreifen wird – reicht das? | 140 |
| 72. Darf sich ein Auftragsverarbeiter vertraglich vorbehalten, Sub-Auftragsverarbeiter einzusetzen? | 140 |
| 73. Darf man einen Auftragsverarbeiter mit Sitz in den USA einsetzen?..... | 141 |
| 74. Sind Abweichungen von den Standardvertragsklauseln zulässig oder sogar notwendig?..... | 142 |

| | |
|---|-----|
| 75. Haftet ein IT-Dienstleister, wenn er rechtswidrige Anweisungen seiner Kunden befolgt? | 145 |
| J. Fotos und Videoüberwachung | 147 |
| 76. Zu welchen Zwecken dürfen Foto- oder Videoaufnahmen gemacht werden? | 147 |
| 77. Wie lange dürfen Foto- und Videoaufnahmen gespeichert werden? | 149 |
| 78. Wann dürfen Aufzeichnungen einer Videoüberwachung ausgewertet werden? | 149 |
| 79. Ist eine Betriebsvereinbarung oder die Zustimmung der Arbeitnehmer für eine Videoüberwachung notwendig? | 150 |
| K. Whistleblowing und interne Compliance-Untersuchungen..... | 153 |
| 80. Ist eine Betriebsvereinbarung für eine Whistleblowing-Hotline notwendig? | 153 |
| 81. Welche Arten von Rechtsverstößen können über eine Whistleblowing-Hotline gemeldet werden?..... | 154 |
| 82. Es gibt keinen Betriebsrat: Müssen die Mitarbeiter der Whistleblowing-Hotline zustimmen?..... | 155 |
| 83. Über welche Personen darf eine Whistleblowing-Meldung erstattet werden? | 156 |
| 84. Wann darf man E-Mails verdächtiger Mitarbeiter auswerten? | 157 |
| 85. Können datenschutzrechtswidrig erlangte Beweise verwertet werden? | 158 |
| L. Datensicherheit & Sicherheitsverletzungen | 159 |
| 86. Wie sicher ist sicher genug?..... | 159 |
| 87. An welchen technischen Sicherheitsstandards kann man sich orientieren? | 160 |
| 88. Ist eine Zertifizierung nach ISO 27001 erforderlich? Was sagt sie aus? | 162 |
| 89. Wie kann man ein Sicherheitskonzept leicht überprüfen? | 163 |
| 90. Was sind die gefährlichsten Sicherheitslücken? | 164 |
| 91. Sind Penetrationstests zwingend erforderlich? | 166 |
| 92. Wann muss die Datenschutzbehörde und wann müssen die Betroffenen von einer Sicherheitsverletzung informiert werden? | 167 |
| 93. In welcher Form sind Sicherheitsverletzungen zu dokumentieren? | 171 |
| M. Geldbußen und Haftung..... | 173 |
| 94. Wie hoch können die Geldbußen für Datenschutzverstöße sein? | 173 |
| 95. Wann haftet das Management, wann das Unternehmen für Geldbußen?..... | 174 |
| 96. Haftet die Konzernmutter für die Tochter? | 175 |

| | |
|--|-----|
| 97. Haftet der Leiter der öffentlichen Stelle für die öffentliche Stelle?..... | 175 |
| 98. Wie weit reicht der Schadenersatzanspruch der Betroffenen?..... | 176 |
| 99. Wird es in Österreich Sammelklagen geben?..... | 177 |
| 100. Wie kann man vorsorgen, um sich in einem Schadenersatzprozess freibeweisen zu können? | 178 |
| Datenschutzwörterbuch | 181 |
| Stichwortverzeichnis..... | 201 |