Inhalt

11 **Vorwort UNIQA Insurance Group AG**

14 **Vorwort Österreichische Post AG**

15 **Vorwort der Herausgeber**

19 **1 Einleitung**
19 1.1 Warum Datenschutz?
21 1.2 Verwendung des Werkes

23 **2 Einführung in die DSGVO**
23 2.1 Was ist die DSGVO?
24 2.2 Begriffsbestimmungen
24 2.2.1 Personenbezogene Daten
25 2.2.2 Pseudonyme bzw. pseudonymisierte Daten
25 2.2.3 Anonyme bzw. anonymisierte Daten
25 2.2.4 Besondere Kategorien personenbezogener Daten
25 2.2.5 Strafrechtsbezogene Daten
26 2.2.6 Betroffene Person
26 2.2.7 Verantwortlicher
26 2.2.8 Auftragsverarbeiter
26 2.2.9 Verarbeitung
27 2.3 Anwendungsbereich
27 2.3.1 Sachlicher Anwendungsbereich
27 2.3.2 Räumlicher Anwendungsbereich
28 2.4 Grundsätze der Verarbeitung
28 2.4.1 Die fünf Grundsätze
30 2.4.2 Die Rechenschaftspflicht („Accountability")
31 2.5 Rechtmäßigkeit der Verarbeitung
31 2.5.1 Allgemeine Kategorie
33 2.5.2 Besondere Kategorien personenbezogener Daten
34 2.5.3 Strafrechtsbezogene Daten
34 2.6 Datenübermittlung

37 **3 Das Datenschutzprojekt**
37 3.1 Einführung
37 3.2 Projektmanagement
37 3.2.1 Ressourcen
38 3.2.2 Projektorganisation (Rollen und Aufgaben)
40 3.2.3 Projektplanung
42 3.3 Datenschutzorganisation
42 3.3.1 Zielsetzungen
42 3.3.2 Berichtswesen etablieren
42 3.3.3 Rollen und Verantwortlichkeiten
45 3.3.4 Training und Awareness
45 3.3.5 Datenschutz-Betriebshandbuch
45 3.3.6 Überführung in den Regelbetrieb

47 **4 Arbeitspaket 1: Erstellung eines initialen Datenschutzrisikoprofils und Erhebung des aktuellen Datenschutzniveaus**
47 4.1 Einführung
49 4.2 Erstellung eines initialen Datenschutzrisikoprofils
50 4.3 Erhebung des aktuellen Datenschutzniveaus
51 4.4 Management Summary

55 **5 Arbeitspaket 2: Verzeichnis der Verarbeitungstätigkeiten**
55 5.1 Einführung
55 5.2 Pflicht zur Führung eines VdV
56 5.3 Grundlagen des VdV
57 5.4 Struktur und Inhalt des VdV
58 5.4.1 Grunddaten
58 5.4.2 Zu dokumentierende Daten pro Verarbeitungstätigkeit
59 5.4.3 Übergreifende technische und organisatorische Maßnahmen (TOMs)
61 5.5 SONDERFORM: Das VdV in der Rolle des Auftragsverarbeiters
61 5.5.1 Grundlagen
61 5.5.2 Struktur und Inhalt
61 5.6 Good Practice-Vorgehensweise zur Einführung des VdV
62 5.6.1 Umsetzung/Implementierung
63 5.6.2 Definition „Verarbeitungstätigkeit“

64 5.7 Prozess zur Erhebung der Verarbeitungstätigkeiten
64 5.7.1 Vorbereitungsphase
66 5.7.2 Erhebungsphase
67 5.7.3 Wartungsphase

69 **6 Arbeitspaket 3: Datenschutz-Folgenabschätzung**
70 6.1 DSFA-Methodik
70 6.1.1 Voraussetzungen prüfen
74 6.1.2 Datenerhebung
74 6.1.3 Schutzziele
74 6.1.4 Risikoanalyse
76 6.1.5 Identifizierung von Maßnahmen

81 **7 Arbeitspaket 4: Privacy by Design & Default**
81 7.1 Privacy by Design
82 7.1.1 Sicherung von Gebäuden
83 7.1.2 Sicherung von Büros
83 7.1.3 Sicherung von Servern
84 7.1.4 Sicherung von Desktops und Laptops
84 7.1.5 Sicherung auf Datenebene
85 7.1.6 Personelle Sicherheit
86 7.1.7 Maßnahmentracking
86 7.1.8 Regelmäßige Prüfung
86 7.2 Privacy by Default
86 7.2.1 Menge der erhobenen Daten und Umfang ihrer Verarbeitung
88 7.2.2 Speicherfrist
88 7.2.3 Zugänglichkeit
89 7.3 Umsetzung in der Praxis
90 7.4 Privacy by Design & Default durch Hersteller
90 7.5 Nachweise

93 **8 Arbeitspaket 5: Datenschutz in Vereinbarungen**
93 8.1 Einführung
94 8.2 Informationspflichten
95 8.3 Einwilligung
97 8.4 Kreise betroffener Personen
97 8.4.1 Kunden
97 8.4.2 Mitarbeiter
98 8.4.3 Lieferanten

98 8.4.4 Auftragsverarbeiter
101 8.5 SONDERFORM: Gemeinsame Verarbeitung
101 8.5.1 Allgemeines
102 8.5.2 Schriftliche Vereinbarung
103 8.5.3 Verantwortung und zentrale Anlaufstelle
103 8.5.4 Offenlegung der wesentlichen Punkte der Vereinbarung

105 **9 Arbeitspaket 6: Betroffenenrechte**
105 9.1 Einführung
107 9.2 Grundlagen zu Betroffenenrechten
108 9.3 Umsetzung in der Praxis

113 **10 Arbeitspaket 7: Umgang mit Datenschutzverletzungen**
113 10.1 Einführung
113 10.1.1 Meldepflichten
116 10.1.2 Dokumentationspflichten
116 10.2 Vorbereitungstätigkeiten
119 10.3 Data-Breach-Prozess

123 **11 Ausblick**
123 11.1 Kontinuierliche Verbesserung
124 11.2 Rechtslage

127 **12 Literatur- und Normenverzeichnis**
127 12.1 Literatur
128 12.2 Verzeichnis der wichtigsten referenzierten Normen

131 **13 Die Autoren**

135 **14 Danksagung**