

Inhaltsverzeichnis

1. Einleitung	5
2. Verantwortung und Accountability	6
3. Datenschutz und Risikomanagement	9
4. Die Aufgaben des Datenschutzbeauftragten	11
5. Zielsetzung und Gegenstand der Überwachung	14
6. Überwachungsinstrumente.	17
6.1 Überwachungsfunktion	17
6.2 Datenschutzkontrollen.	17
6.3 Datenschutzaudits.	18
6.3.1 Begriffsbestimmung und Zielsetzung	18
6.3.2 Durchführung von Datenschutzaudits	18
6.3.3 Arten von Audits	19
6.3.4 Audittypen	20
6.4 Zertifizierung	21
6.5 Sonstige Überwachungsinstrumente.	23
7. Organisatorische Rahmenbedingungen	24
7.1 Voraussetzungen für die Überwachung	24
7.2 Datenschutzleitlinie und -richtlinien.	24
7.3 Datenschutz-Managementsystem.	25
7.4 Datenschutzkontrollen in den Prozessen	26
7.5 Auditfunktion	27
7.6 Datenschutzbeauftragter.	28
7.7 Überwachungskonzept	30
7.8 Zusammenfassung der Aufgaben und Verantwortlichkeiten.	32
8. Datenschutz Audits	34
8.1 Erstellen einer Prüflandkarte.	34
8.2 Risikoorientierte Planung von Datenschutzaudits.	35
8.3 Durchführung.	40
8.4 Maßnahmen-Monitoring	43
8.5 Überwachung von Datenschutz-Audits	43

9. Implementierung von Datenschutzkontrollen	45
9.1 Zielsetzung	45
9.2 Ermittlung der Datenschutzrisiken	45
9.3 Definition von Datenschutzkontrollen	46
9.4 Implementierung der Datenschutzkontrollen	47
9.5 Durchführung der Datenschutzkontrollen	47
10. Überwachung in ausgewählten Bereichen	48
10.1 Abgrenzung der Aufgaben des Datenschutzbeauftragten	48
10.2 Datenschutzorganisation	48
10.3 Datenschutzprozesse	51
10.3.1 Prozess(e) zur Wahrung der Betroffenenrechte	51
10.3.2 Prozess für Datenschutzverletzungen	55
10.3.3 Datenschutz-Folgenabschätzung	58
10.4 Datenschutz in Prozessen	61
10.4.1 Einführung oder Änderung von Verarbeitungen	61
10.4.2 Auftragsverarbeitung	66
10.4.3 Technische und organisatorische Maßnahmen	71
10.4.4 Verzeichnis der Verarbeitungstätigkeiten	73
Abbildungsverzeichnis	79
Stichwortverzeichnis	81

Stichwortverzeichnis

A

Ablauforganisation 7, 15
Accountability 6
Anweisungen 7
Anweisungsverschulden 6
Art. 29 Gruppe 12, 13
Audit 11, 18, 21, 31
 externes 20
 integriertes 20
 internes 20
 joint 20
Auditbericht 19
Auditfunktion 27
Auditprozess 43
Aufbauorganisation 7, 14
Aufgaben und Verantwortlichkeiten 32
Aufgabenverteilung 26, 28, 32
Aufsichtsbehörde 8, 28, 34, 55
Auftragsverarbeitung 66
Auskunftersuchen 14

B

Benennung des DSB 28
Benutzerberechtigungen 17
Beratungsauftrag 12
Berichte 23
Beschwerdemanagement 23
Betriebsrat 8
Betroffene 8, 13
Betroffenenrechte 14, 15, 17
Bewertungsskala 36

C

Compliance 9, 18
Compliance-Abteilung 11
Corporate Governance-Modelle 14

D

Data-Breach-Management 15
Datenschutz in Prozessen 16
Datenschutz in Verarbeitungen/Prozessen 34
Datenschutzablauforganisation 16
Datenschutz-Audit 9, 13, 17, 18, 19, 23, 27, 31, 34, 50, 54
 Überwachung 43
Datenschutzauditoren 19
Datenschutzaufbauorganisation 16, 34

Datenschutzaufsichtsbehörde 18, 21
Datenschutzbeauftragter 8, 9, 12, 28
Datenschutz-Change Management 15
Datenschutz-Folgenabschätzung 15, 18, 29, 30, 32, 49, 58
Datenschutzkontrollen 9, 17, 23, 26, 30, 45, 50
 Implementierung 45
Datenschutzleitlinien 7, 24, 25, 30, 48
Datenschutz-Management 9
Datenschutz-Managementsystem 24, 25
Datenschutz-Organisation 14, 48
Datenschutzpolicies 24
Datenschutzprozesse 7, 15, 34, 51
Datenschutzrichtlinien 7, 9, 15, 24, 30, 48
Datenschutzrisiken 13, 45
Datenschutzverantwortung 14
Datenschutzverletzungen 15, 30, 49, 55
Datenschutzvorfälle 32
Datenschutzvorschriften 24
Datenschutz-Zertifikat 20
Datenschutzziele 24
delegieren 6
DIN EN ISO 19011 11

E

Einführung oder Änderung von Verarbeitungen 61
Eintrittswahrscheinlichkeit 13

F

Fachkunde 12, 19
Fremdkontrolle 8
Funktionen der Internal Governance 9

G

Garantien 23
Geheimhaltungspflichten 28
geringer Risikograd 13

H

Handlungsanweisungen 14
Hinweisgeberverfahren 23

I

Industriestandard 22
Information des Datenschutzbeauftragten 18

Informationssicherheit 21, 26
Informationssicherheitsaudit 31
Informationssicherheitsaudits und IT-Audits 23, 31
Informationssicherheitsmanagement 9, 14, 23
innerbetriebliches Überwachungsorgan 8
Integriertes Audit 20
Interessenkonflikte 17, 18, 28, 30
Interne Revision 9, 18
Internes Kontrollsystem 7, 8, 14, 18
ISO 27000 14
ISO 27001 26
ISO 27701 26
IT-Audit 31
IT-Revision
interne 27

K

Komplexität einer Verarbeitung 36
kontinuierliche Verbesserung 24
kontinuierlicher Verbesserungsprozess 18, 34
Kontrollbeschreibung 47
Kontrolldurchführender 47
Kontrollen 7
aufdeckende 17, 46
automatisierte 17, 46
manuelle 17, 46
vorbeugende 17, 46
Kontrollgegenstand 47
Kontrollnachweis 26, 47
Kontrollvorgehen 47
Kontrollzeitpunkt 47
Kontrollziel 47

L

Leitlinien 14
Löschtermine 18

M

Maßnahmen-Monitoring 31, 43, 69
Meldepflichten 32
Meldung 28
Meldung an die Aufsichtsbehörde 55

N

Normadressat 6

O

Objektivität 17, 18
Organisation des Risikomanagements 9
Organisationsverschulden 6, 11, 12, 49

P

PDCA- Zyklus (Plan, Do, Check, Act) 26
Planung von Datenschutz-Audits 34
Planungsprozess 34
Policy 14
privacy by default 27
privacy by design 27
Prozess für Datenschutzverletzungen 55
Prozess zur Wahrung der Betroffenenrechte 51
Prozessbeteiligte 18, 26
prozessimmanente Risiken 18, 37
Prozessrisiken 46, 49, 52, 56, 59, 63, 68, 72, 75
Prozessunabhängige 17, 18
Prozessverantwortliche 17, 23
Prozessvorgaben 26
Prüfinstanz 27
Prüflandkarte 34
Prüfobjekte 34
Prüfungsbericht 42
Prüfungsdokumentation 43
Prüfungsdurchführung 40, 42
Prüfungsergebnisse 19
Prüfungseröffnungsgespräch 41
Prüfungsgegenstand 39
Prüfungshandlungen 19
Prüfungsinstanz 19
Prüfungsplan 40
Prüfungsschlussgespräch 42
Prüfungsschwerpunkte 40
Prüfungszielsetzung 39

R

Rechenschaftspflicht 6, 11, 14, 48
Rechte der Betroffenen 51
Revision 11
Richtlinien 14
Risiken 11, 13
prozessimmanente 18, 37
Risikobehandlung 32
Risikobewertung 35
Risikoinventar 39

Risikokennziffer 35, 38
 Risikokriterien 35
 Gewichtung 38
 Risikomanagement 9, 23
 Modelle 9
 Risikomanagementsystem 9
 risikoorientiert 12, 27, 30
 Risikoorientierte Planung 35
 Risikoorientierte Überwachung 30, 31

S

Schadenausmaß 13
 Schulung 14
 Schutzbedarf 36
 personenbezogener Daten 30, 36, 38
 Schwellwertanalyse 18, 45, 59
 Selbsteinschätzung 23
 Selbstkontrolle 8
 Selektionsverschulden 6
 Sensibilisierung 14
 Sicherheitsmaßnahmen
 technische und organisatorische 30
 Sicherstellungspflicht 11
 Statistiken 23

T

technischen und organisatorischen
 Maßnahmen (TOM) 12, 14, 18, 21, 49, 71
 Three-Lines-of-Defence-Modell 9

U

Überprüfungen durch den Verantwortlichen
 11
 Überwachung 18, 30
 durch den Datenschutzbeauftragten 11
 ereignisorientierte Überwachung 30, 31
 Gegenstände 14
 Überwachungsansätze 50, 53, 57, 60, 64,
 69, 76
 Überwachungsauftrag 12, 30
 Überwachungsfunktion 17
 Überwachungsinstrumente 17, 18, 23, 30
 Überwachungskonzept 7, 21, 22, 30
 Überwachungspflicht 12
 Überwachungsverschulden 7
 Überwachungsziel 48, 51, 56, 59, 62, 66,
 71, 74
 Unternehmensrisiko 13

V

Verbesserung
 kontinuierliche 24
 Verhaltensregeln 21, 22
 für Auftragsverarbeiter 22
 Verstoß 12
 Verzeichnis der Verarbeitungstätigkeiten
 15, 18, 35, 73

W

Wahrung der Betroffenenrechte 30
 Wirtschaftsprüfungsgesellschaft 18
 WP 243 12

Z

Zeitbudget 28
 Zertifizierung 17, 21, 22
 Instanz 18
 von Datenschutzbeauftragten 22
 Zuständigkeiten 32
 Zutritts- und Zugriffsrechten 28