

Informations-sicherheit und Datenschutz

Handbuch für Praktiker
und Begleitbuch zum T.I.S.P.

dpunkt.verlag

Inhalt

Cover

Titel

Impressum

Vorwort des TeleTrusT Deutschland e.V.

Vorwort zur vierten Auflage

Inhaltsübersicht

Inhaltsverzeichnis

1 Aufgaben und Ziele der Informationssicherheit

Einleitung

1.1 Aufgaben und Anforderungen eines ISMS

1.1.1 Risikomanagement

1.1.2 Gefährdungen erkennen und bewerten

1.1.3 Angreifermodelle betrachten

1.1.4 Hauptursachen für Sicherheitsprobleme identifizieren

1.1.5 Sicherheitskonzept erstellen

1.1.6 Sicherheitsmaßnahmen überprüfen

1.2 Generische Sicherheitsziele

1.2.1 Vertraulichkeit

1.2.2 Integrität

1.2.3 Verfügbarkeit

1.2.4 Authentizität

1.2.5 Sicherheitsziele und Sicherheitskonzept

Zusammenfassung

Literatur

2 Betriebswirtschaftliche Aspekte der Informationssicherheit

Einleitung
2.1 Risikomanagement
2.2 Quantitative Modelle
2.2.1 Kosten von Risiken
2.2.2 Kosten von Sicherheitsvorfällen
2.2.3 Kosten von Sicherheitsmaßnahmen
2.2.4 Das ROSI-Modell
2.2.5 Grenzen des ROSI-Ansatzes
2.2.6 Alternative quantitative Modelle
2.3 Qualitative Betrachtungen
2.3.1 Grenzen betriebswirtschaftlicher Betrachtungen
2.3.2 Wirtschaftlichkeit von Investitionsentscheidungen
2.3.3 Risikomatrix
2.3.4 Pareto-Prinzip
2.3.5 Erfahrungswerte – Best Practice
Zusammenfassung
Literatur
3 Informationssicherheit und rechtliche Anforderungen
Einleitung
3.1 Informationssicherheit und Recht im Überblick
3.1.1 Risikomanagement als rechtliche Anforderung
3.1.2 Anforderungen aus dem Gesellschaftsrecht
3.1.3 Anforderungen aus dem Bankenrecht
3.1.4 Anforderungen aus dem Steuer- und Handelsrecht
3.1.5 Informationssicherheit für Kritische Infrastrukturen
3.2 Telekommunikationsrecht

3.2.1 Grundlagen zur Informationssicherheit im Telekommunikationsrecht

3.2.2 Anforderungen an Informationssicherheit im Telekommunikationsrecht

3.2.3 Durchsetzung von Informationssicherheit im Telekommunikationsrecht

3.3 Strafrecht

3.4 Verträge und Vertragsrecht

3.4.1 Anforderungen an Informationssicherheit in Verträgen und im Vertragsrecht

3.4.2 Durchsetzung von Informationssicherheit in Verträgen und im Vertragsrecht

3.5 Arbeitsrecht

3.5.1 Arbeitsrecht als Gestaltungsmittel der Informationssicherheit

3.5.2 Regelungen im Arbeitsverhältnis

3.5.3 Regelungen durch Betriebsvereinbarung

3.6 Regulierte Infrastrukturen

3.6.1 eIDAS-Verordnung

3.6.2 Rolle und Anforderungen an Vertrauensdiensteanbieter

3.6.3 Arten von elektronischen Signaturen

3.6.4 Anforderungen an die Erstellung qualifizierter Zertifikate

3.6.5 Rechtsfolgen und Beweisrecht beim Einsatz von Vertrauensdiensten

3.7 Rechtliche Grenzen für Sicherheitsmaßnahmen

3.7.1 Datenschutzrecht

3.7.2 Telekommunikationsrecht

3.7.3 Telemedienrecht

3.7.4 Betriebliche Mitbestimmung

Zusammenfassung

Literatur

4 Datenschutzrecht

Einleitung

4.1 Ziele des Datenschutzrechts

4.1.1 Entwicklung des Datenschutzrechts

4.1.2 Anwendungsbereich und Begriffsbestimmungen

4.1.3 Sachlicher Anwendungsbereich

4.1.4 Personenbezogene Daten

4.1.5 Verarbeitung von Daten

4.1.6 Räumlicher Anwendungsbereich

4.1.7 Weitere Begriffsbestimmungen

4.1.8 Rechtsrahmen und Umsetzungsvorgaben

4.1.9 Datenschutzrechtliche Grundprinzipien

4.1.10 Datenschutzleitlinie

4.1.11 Zweck und Geltungsbereich

4.1.12 Datenschutzrichtlinie

4.1.13 Richtlinie zur Privatnutzung des betrieblichen Internets und E-Mail

4.1.14 Richtlinie für datenschutzrechtliche Anforderungen an IT-Projekte

4.1.15 Datenschutzimplementierung/Datenschutzmanagementsystem (DSMS)

4.1.16 Datenschutzrichtlinien und arbeitsanweisungen

4.1.17 Datenschutzorganisation

4.1.18 Datenschutzkonzept

4.2 Verarbeitungstätigkeiten

4.2.1 Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

4.2.2 Rollen-Berechtigungskonzept

4.2.3 Informationspflichten

4.2.4 Auftragsverarbeitung

4.2.5 Auftragsverarbeitungsvertrag

4.2.6 Grenzen der Auftragsverarbeitung

4.2.7 Technische und organisatorische Maßnahmen (TOM)

4.2.8 Gemeinsame Verantwortlichkeit

4.2.9 Drittstaatentransfer von personenbezogenen Daten

4.2.10 Angemessenheitsbeschluss (Art. 45 DSGVO)

4.2.11 Vorliegen geeigneter Garantien (Art. 46 DSGVO)

4.2.12 Standarddatenschutzklauseln der Kommission oder einer Aufsichtsbehörde

4.2.13 Löschregeln

4.3 Datenschutz-Vorgänge

4.3.1 Datenschutzverpflichtung

4.3.2 Datenschutzschulung

4.3.3 Betroffenenrechte

4.3.4 Auskunft

4.3.5 Auskunftsersuchen von Betroffenen

4.3.6 Auskunftsersuchen von Dritten sowie von Ämtern und Ermittlungsbehörden

4.3.7 Berichtigung

4.3.8 Löschung

4.3.9 Einschränkung

4.3.10 Datenübertragung

4.3.11 Widerspruch

4.3.12 Datenschutzvorfälle

4.3.13 Whistleblower-Richtlinie

4.3.14 Benennung des Datenschutzbeauftragten

4.3.15 Audits

4.3.16 Kontinuierliche Umsetzungsverpflichtung der Sicherheit der Verarbeitung

4.3.17 Datenschutzaudit

4.3.18 Self Assessment

4.3.19 Zertifizierung

4.4 Gesetz über digitale Dienste

4.5 Sicherheit der Verarbeitung zur Gewährleistung der Informationssicherheit

4.5.1 Durchsetzung von Informationssicherheit im Datenschutzrecht

4.6 Telemedien-Datenschutzrecht

4.6.1 Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG)

4.6.2 Grundlagen zum Telemedien-Datenschutzrecht

4.6.3 Anforderungen an Datenschutz im Telemedienrecht

4.6.4 Durchsetzung von Datenschutz im Telemedienrecht

4.6.5 Cookie-Banner

4.6.6 Einwilligung nach § 25 TTDSG/Art. 6 Abs. 1 lit. a DSGVO

4.6.7 Nudging und Dark Pattern

4.7 Telekommunikations-Datenschutzrecht

4.7.1 Anforderungen an Datenschutz im Telekommunikationsrecht

4.7.2 Durchsetzung von Datenschutz im Telekommunikationsrecht

4.8 Strafrecht

4.8.1 Grundlagen zu Datenschutz und Informationssicherheit im Strafrecht

4.8.2 Anforderungen an Informationssicherheit und Datenschutz im Strafrecht

4.8.3 Durchsetzung von Datenschutz und Informationssicherheit im Strafrecht

4.8.4 Schutz der Informations- und Datenverarbeitung durch Strafrecht

4.9 Arbeitsrecht

4.9.1 Regelungen im Arbeitsverhältnis

4.9.2 Datenschutz im Homeoffice

4.9.3 Durchsetzung von Datenschutzmaßnahmen im Arbeitsverhältnis

4.9.4 Haftung der Arbeitnehmer

4.9.5 Regelungen durch Betriebsvereinbarung

Zusammenfassung

5 Hackermethoden

Einleitung

5.1 Begriffsdefinition »Hacker«

5.2 Ursachen von Sicherheitsproblemen

5.2.1 SQL-Injection

5.2.2 Buffer Overflows

5.2.3 Motivation eines Angreifers

5.3 Vorgehensweise bei Penetrationstests

5.3.1 Informationsbeschaffung

5.3.2 Portscans

5.3.3 Automatische Überprüfungen

5.3.4 Manuelle Untersuchungen

5.3.5 Anwendung von Exploits

5.3.6 Schwachstellenverkettung und Lateral Movement

5.3.7 Social Engineering

5.4 Angriffswerkzeuge

5.4.1 Rootkits

5.4.2 Virus Construction Kits

5.4.3 Trojaner und Kryptotrojaner

5.4.4 PowerShell

Zusammenfassung

Literatur

6 ISO 27001 und ISO 27002

Einleitung

6.1 Entstehungsgeschichte

6.2 Die Familie der ISO-27000-Standards

6.3 ISO 27001

6.3.1 Vorgehensweise und Anwendungen

6.3.2 Inhaltliche Elemente der ISO 27001

6.3.3 Notwendige Dokumentation

6.3.4 Prüfungs- und Zertifizierungsprozess

6.4 ISO 27002

Zusammenfassung

Literatur

7 IT-Grundschutz

Einleitung

7.1 Historie

7.2 IT-Grundschutz – der Ansatz

7.3 IT-Grundschutz-Dokumente

7.3.1 BSI-Standard 200-1: Managementsysteme für Informationssicherheit

7.3.2 BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise

7.3.3 BSI-Standard 200-3: Risikomanagement

7.3.4 BSI-Standard 100-4: Notfallmanagement

7.3.5 IT-Grundschutz-Kompendium

7.4 Tool-Unterstützung

7.5 ISO 27001-Zertifizierung auf Basis von IT-Grundschutz

Zusammenfassung

Literatur

8 Sicherheitskonzept

Einleitung

8.1 Ziele eines Sicherheitskonzepts

8.2 Zentrale Aufgaben im Sicherheitskonzept

8.2.1 Berechtigte und Unberechtigte

8.2.2 Schwachstellen vermeiden

8.2.3 Identifikation von Unregelmäßigkeiten

8.2.4 Reaktionen auf Störfälle

Zusammenfassung

Literatur

9 Datenschutzkonzept

Einleitung

9.1 Ziele des Datenschutzkonzepts

9.2 Zentrale Elemente eines Datenschutzkonzepts

9.2.1 Organisation

9.2.2 Regelungen

9.2.3 Prozesse

9.2.4 Verträge

9.2.5 Audits

9.2.6 Dokumentation

9.2.7 Vorlagen

9.3 Regelmäßige Überarbeitung

Zusammenfassung

10 Physische Sicherheit

Einleitung

10.1 Bedrohungen
10.2 Erhöhung der Gebäudesicherheit
10.2.1 Bewusste Standortwahl
10.2.2 Sichere bauliche Gestaltung
10.2.3 Schutzzonen
10.2.4 Rettungs- und Fluchtwege
10.3 Angemessene Überwachung
10.4 Monitoring und automatisierte Maßnahmensteuerung
10.5 Wirksamer Brandschutz
10.6 Stromversorgung
10.7 Physische Schutzmaßnahmen in externen Bereichen
10.7.1 Mobile Endgeräte
10.7.2 Häuslicher Arbeitsplatz
10.7.3 Datenträger
Zusammenfassung
Literatur
11 Grundlagen der Netzwerksicherheit
Einleitung
11.1 Das OSI-Modell
11.1.1 Protokolle, Adressen und Ports
11.1.2 Bedrohungen
11.2 Das Internet Protocol
11.3 IPv4
11.3.1 Address Resolution Protocol – ARP
11.3.2 Bedrohungen gegen IPv4
11.4 IPv6
11.4.1 Unterschiede zwischen IPv6 und IPv4

11.4.2 Neighbor Discovery

11.4.3 Header-Erweiterungen

11.4.4 Fragmentierung

11.4.5 Privatsphäre

11.4.6 Netzwerk-Scans

11.4.7 Produkte und Implementierungen

11.4.8 Besonderheiten zur Tunnelung von IPv6

11.5 Multiprotocol Label Switching – MPLS

11.6 Transportprotokolle

11.6.1 Sicherheitsmechanismen in Transportprotokollen

11.6.2 Übersicht über verschiedene Transportprotokolle

11.7 Netzwerkmanagementprotokolle

11.7.1 Konfigurationsprotokolle

11.7.2 Auskunftsdienst DNS

11.7.3 Routing-Protokolle

11.7.4 Anmerkung zu verschiedenen Sicherheitsmechanismen der Protokolle

11.8 Sicherheitsmechanismen für Netzwerke

11.8.1 IEEE 802.1X

11.8.2 IPsec

11.8.3 SSL/TLS

11.8.4 Datagram Transport Layer Security – DTLS

11.8.5 Secure Shell – SSH

11.8.6 Überwachung des Netzwerkverkehrs

11.9 Netzarchitektur

11.9.1 Einteilung des Netzes in Zonen

11.9.2 Zugriffskontrolle auf Switchen

11.9.3 Virtuelle LANs
11.9.4 Network Address Translation
11.9.5 Software Defined Networking (SDN)
Zusammenfassung
Literatur
12 Firewalls
Einleitung
12.1 Grundlagen von Firewalls
12.1.1 Absicherung von Firewalls
12.1.2 Regelwerk
12.2 Firewall-Typen
12.2.1 Paketfilter
12.2.2 Application Level Gateway
12.2.3 Stealth Gateway
12.2.4 Unified Threat Management (UTM)/Next-Generation Firewalls
12.3 Firewall-Architekturen
12.3.1 Einstufige Paketfilter-Architektur
12.3.2 Multi-Homed-Architektur
12.3.3 Demilitarisierte Zone
12.3.4 PAP-Firewall-Architekturen
12.4 Firewall-Konzepte
12.4.1 Anforderungsanalyse für den Firewall-Einsatz
12.4.2 Betriebliche Anforderungen für die Firewall-Konzeption
12.5 Grenzen von Firewalls
Zusammenfassung
Literatur
13 Kryptografie

Einleitung
13.1 Vorgehensweise
13.2 Begriffsklärung
13.3 Angriffs- und Sicherheitsziele
13.3.1 Lesen von Daten – Vertraulichkeit
13.3.2 Ändern von Daten – Integrität
13.3.3 Wiedereinspielen von Daten – Frische
13.3.4 Vortäuschen einer Identität – Urheber-Authentizität
13.3.5 Abstreiten der Verantwortung – Nicht-Abstreitbarkeit
13.3.6 Weitere Angriffs- und Sicherheitsziele
13.4 Grundsätzliche Angriffsszenarien
13.5 Sichere Kanäle
13.5.1 Verschlüsselung
13.5.2 Chiffrierverfahren
13.5.3 Betriebsmodi
13.5.4 Integrität
13.5.5 Authentisierte Verschlüsselung
13.6 Herausforderung Schlüsselverteilung
13.6.1 Der direkte Weg
13.6.2 Indirekt über vertrauenswürdige Dritte
13.7 Asymmetrische Verfahren zur Schlüsselverteilung
13.7.1 Grundprinzipien asymmetrischer Verfahren
13.7.2 Schlüsseltransport
13.7.3 Schlüsselaustausch
13.8 Digitale Signaturen
13.8.1 Grundprinzipien digitaler Signaturen
13.8.2 Digitale Signaturen für die Nicht-Abstreitbarkeit

13.8.3 Digitale Signaturen für Zertifikate
13.9 Praktischer Einsatz
13.9.1 Schlüssel- und Hash-Wert-Längen
13.9.2 Proprietäre Verfahren
13.9.3 Proprietäre Implementierungen
13.9.4 Erzeugung von Zufallszahlen
Zusammenfassung
Literatur
14 Vertrauensmodelle und PKI-Komponenten
Einleitung
14.1 Vertrauensmodelle
14.1.1 Web of Trust
14.1.2 Zentrales Modell der Public-Key-Infrastruktur
14.2 Public-Key-Infrastruktur
14.2.1 Zertifikate und CRLs
14.2.2 Zertifizierungshierarchien
14.2.3 Verifikation einer digitalen Signatur
14.2.4 Komponenten und Prozesse einer PKI
14.2.5 Policies für Public-Key-Infrastrukturen
14.3 Standards im Bereich PKI
14.3.1 X.509-Standard
14.3.2 PKIX-Standards
14.3.3 PKCS-Standards
14.3.4 Common-PKI-Spezifikationen
14.4 Verknüpfung von Public-Key-Infrastrukturen
14.5 Langzeitarchivierung
Zusammenfassung

Literatur

15 Virtual Private Networks

Einleitung

15.1 VPN-Szenarien

15.1.1 Site-to-Site-VPN

15.1.2 End-to-Site-VPN

15.1.3 End-to-End-VPN

15.1.4 Protokollebenen von VPN und VPN-Tunnel

15.2 Technische Realisierung von VPNs

15.2.1 PPP, L2F und PPTP

15.2.2 Layer 2 Tunneling Protocol – L2TP

15.2.3 IP Security – IPsec

15.2.4 OpenVPN

15.2.5 WireGuard

15.3 Spezielle Risiken von VPNs

Zusammenfassung

Literatur

16 Sicherheit in mobilen Netzen

Einleitung

16.1 Bedrohungen in mobilen Netzen

16.2 Wireless LAN

16.2.1 Entwicklung und Standardisierung

16.2.2 Netzarchitektur und Netzkomponenten

16.2.3 Sicherheitsverfahren

16.2.4 Empfohlene Sicherheitsmaßnahmen

16.3 Bluetooth

16.3.1 Entwicklung und Standardisierung

16.3.2 Netzarchitektur und -komponenten

16.3.3 Sicherheitsverfahren in Bluetooth

16.3.4 Bluetooth-Sicherheitsmechanismen im Detail

16.3.5 Bewertung der Sicherheitsmaßnahmen

16.4 Mobilfunk

16.4.1 GSM

16.4.2 GPRS

16.4.3 UMTS

16.4.4 LTE

Zusammenfassung

Literatur

17 Authentifizierung und Berechtigungsmanagement

Einleitung

17.1 Benutzer

17.2 Identität

17.3 Identifizierung

17.4 Authentifizierung

17.4.1 Authentifizierung durch Wissen

17.4.2 Authentifizierung durch Besitz

17.4.3 Authentifizierung durch Biometrie

17.4.4 Authentifizierung in verteilten Systemen

17.5 Autorisierung und Zugriffskontrolle

17.5.1 Zugriffsrechtematrix

17.5.2 Zugriffskontrolllisten

17.5.3 Capabilities

17.5.4 Rollenbasierte Zugriffskontrolle

17.5.5 Nachteile von Zugriffskontrollstrategien

17.6 Identitäts- und Berechtigungsmanagement
17.7 Single Sign-On
17.7.1 Unternehmensweites Single Sign-On
17.7.2 SSO für Web-Services
17.7.3 OpenID
17.7.4 OAuth 2.0
17.7.5 OpenID-Connect
17.7.6 SAML
17.7.7 Mozilla Persona
17.7.8 Sicherheit von SAML, OpenID, OAuth und Mozilla Persona
Zusammenfassung
Literatur
18 Betriebssystemsicherheit
Einleitung
18.1 Identität und Autorisierung
18.1.1 Benutzer, Benutzergruppen und Rollen
18.1.2 Ressourcen
18.1.3 Zugriffsrechte
18.1.4 Erweiterung von Rechten – privilegierte Aktionen
18.2 Systemzugang und Authentisierung
18.2.1 Sicherer lokaler Zugang
18.2.2 Sicherer Fernzugang
18.2.3 Session-Sicherheit
18.3 Schutz der Anwenderdaten
18.3.1 Ablage auf Speichermedien
18.3.2 Verarbeitung im Speicher
18.3.3 Transit über ein Netzwerk

18.4 Konfigurationsmanagement
18.5 Protokollierung und Überwachung
18.5.1 Protokollierung und Auswertung
18.5.2 Überwachung im laufenden Betrieb
18.6 Selbstschutz und Härtung des Betriebssystems
18.6.1 Härtung gegen spezifische Bedrohungen
18.6.2 Malwareschutz
18.6.3 Boot-Schutz
18.6.4 Verwaltung angeschlossener Geräte und Speichermedien
18.6.5 Reduktion der Angriffsoberfläche
18.6.6 Einschränkung des zulässigen Netzwerkverkehrs
Zusammenfassung
Literatur
19 Windows-Sicherheit
Einleitung
19.1 Identifizierung und Autorisierung
19.1.1 Benutzer, Benutzergruppen und Rollen
19.1.2 Ressourcen
19.1.3 Zugriffsrechte
19.1.4 Erweiterung von Rechten – privilegierte Aktionen
19.2 Systemzugang und Authentisierung
19.2.1 Sicherer lokaler Zugang
19.2.2 Sicherer Fernzugang
19.2.3 Session-Sicherheit
19.3 Schutz der Anwenderdaten
19.3.1 Ablage auf Speichermedien
19.3.2 Verarbeitung im Speicher

19.3.3 Transit über ein Netzwerk
19.4 Konfigurationsmanagement
19.4.1 Die Registry
19.4.2 Active Directory Domain Services
19.4.3 Gruppenrichtlinien
19.4.4 Management-Werkzeuge
19.5 Protokollierung und Überwachung
19.5.1 Protokollierung und Auswertung der Protokollierung
19.5.2 Überwachung im laufenden Betrieb
19.6 Selbstschutz und Härtung des Betriebssystems
19.6.1 Härtung gegen spezifische Bedrohungen
19.6.2 Malwareschutz
19.6.3 Bootschutz
19.6.4 Verwaltung angeschlossener Geräte und Speichermedien
19.6.5 Reduktion der Angriffsoberfläche
19.6.6 Einschränkung des zulässigen Netzwerkverkehrs
Zusammenfassung
Literatur
20 Unix-Sicherheit
Einleitung
20.1 Identität und Autorisierung
20.1.1 Benutzer, Benutzergruppen und Rollen
20.1.2 Ressourcen
20.1.3 Zugriffsrechte
20.1.4 Erweiterung von Rechten – privilegierte Aktionen
20.2 Systemzugang und Authentisierung
20.2.1 Sicherer lokaler Zugang

20.2.2 Sicherer Fernzugang
20.2.3 Session-Sicherheit
20.3 Schutz der Anwenderdaten
20.3.1 Ablage auf Speichermedien
20.3.2 Verarbeitung im Speicher
20.3.3 Transit über ein Netzwerk
20.4 Konfigurationsmanagement
20.5 Protokollierung und Überwachung
20.5.1 Protokollierung und Auswertung
20.5.2 Überwachung im laufenden Betrieb
20.6 Selbstschutz des Betriebssystems
20.6.1 Härtung gegen spezifische Bedrohungen
20.6.2 Malwareschutz
20.6.3 Boot-Schutz
20.6.4 Verwaltung angeschlossener Geräte und Speichermedien
20.6.5 Reduktion der Angriffsoberfläche
20.6.6 Einschränkung des zulässigen Netzwerkverkehrs
Zusammenfassung
Literatur
21 Virtualisierung
Einleitung
21.1 Vorteile von Virtualisierungslösungen
21.2 Nachteile von Virtualisierungslösungen
21.3 Servervirtualisierung
21.4 Plattformvirtualisierung (Container)
21.5 Speichervirtualisierung (SAN)
21.6 Clientvirtualisierung (VDI)

21.7 Netzwerkvirtualisierung

21.8 Grundsätzliche Sicherheitsmaßnahmen

21.9 Abhängigkeiten und neue Angriffswege/Fehlkonfigurationen berücksichtigen

Zusammenfassung

Literatur

22 Sicherheit von mobilen Endgeräten

Einleitung und Überblick

22.1 Herausforderungen

22.2 Generelle Security-Architekturen mobiler Systeme

22.3 Bindung an Hersteller/Store und Eingriffsmöglichkeiten des Benutzers

22.4 Bring your own Device

22.5 Mobile Device Management

Zusammenfassung

23 Anwendungssicherheit

Einleitung

Definition gängiger Begriffe

Das Sicherheitsdilemma

23.1 Secure Software Development Lifecycle

23.1.1 Phasen der Softwareentwicklung

23.1.2 Besonderheiten der »Supply Chain«

23.2 Schwachstellen in Anwendungen

23.3 Reifegradmodelle

23.4 Threat Modeling und Security Requirements

23.5 Secure Design

23.6 Kryptografie

23.7 Secure Coding

23.8 Verifikation und Audit

Zusammenfassung

Literatur

24 Technisches Löschen und Vernichten

Einleitung

24.1 Anforderungen zum Löschen und Entsorgen

24.2 Realisierung durch ein Lösch- und Entsorgungskonzept

24.3 Speicherorte

24.4 Technische Löschmaßnahmen

24.4.1 Drei Schritte in Löschläufen

24.4.2 Anforderungen an Löschmechanismen

24.4.3 Grenzen des einfachen Löschens

24.4.4 Sicheres Löschen durch Überschreiben

24.4.5 Verschlüsselung und Löschen

24.4.6 Löschen auf USB-Sticks und anderen Flash-Medien

24.4.7 Vernichten und Entsorgen

24.4.8 Integration in den Arbeitsalltag

Zusammenfassung

Literatur

25 Datenschutzrechtliches Löschkonzept

Einleitung

25.1 Vorgaben der DSGVO zum Löschen personenbezogener Daten

25.2 Vorgehensweise nach DIN 66398

25.3 Der Regelkatalog

25.3.1 Datenarten und Löschregeln

25.3.2 Verbindlichkeit des Regelkatalogs

25.3.3 Pflegeprozess für den Regelkatalog

25.4 Umsetzung

25.4.1 Löschmaßnahmen

25.4.2 Umsetzungsbereiche

25.4.3 Spezielle Aufgaben für die Umsetzung

25.4.4 Umsetzungsdefizite

25.5 Nutzen …

Zusammenfassung

Literatur

26 Awareness

Einleitung

26.1 »Risikofaktor« Mensch

26.1.1 Zur Wahrnehmung von Informationssicherheit

26.1.2 Randbedingungen und Konsequenzen

26.2 Durchführung von Awareness-Kampagnen

26.2.1 Kampagnen-Problematiken

26.2.2 Zielsetzung einer Awareness-Kampagne

26.3 Awareness in der Praxis

26.3.1 Erfolgsfaktoren

26.3.2 Beteiligte

26.3.3 Das Vier-Phasen-Konzept einer Awareness-Kampagne

26.3.4 Gamification

26.3.5 Erfolgsmessung

Zusammenfassung

Literatur

27 Malware und Content Security

Einleitung und Historie

27.1 Historie

27.2 Technische Verbreitungswege und Funktionen

27.2.1 Ablauf einer Infektion

27.2.2 Verbreitungswege

27.2.3 Mobile Datenträger

27.3 Geschäftsmodelle und Auswirkungen

27.3.1 Motivation der Angreifer

27.3.2 Geschäftsmodelle

27.3.3 Auswirkungen von Schadsoftware

27.4 Gegenmaßnahmen

27.4.1 Abschottung von Systemen

27.4.2 Content-Analyse

27.4.3 Erfassung des Netzwerkverkehrs

27.4.4 Dekomposition der Inhalte und Header-Analyse

27.4.5 Klassifikation von Inhalten

27.4.6 Ergebnisgesteuerte Aktionen

27.4.7 Besonderheiten bei der Nutzung eines Content-Filters für Anti-Spam-Maßnahmen

27.4.8 Content-Filter und verschlüsselte Inhalte

27.4.9 Verhaltensanalyse

27.4.10 Mikrovirtualisierung

Literatur

28 Intrusion Detection

Einleitung

28.1 Einordnung und Definitionen

28.2 Architektur und Komponenten von Intrusion-Detection-Systemen

28.3 Grundproblem der Analyse – oder »der Schein trügt«

28.4 Typen von Intrusion-Detection-Systemen

28.4.1 Host-based Intrusion-Detection-Systeme
28.4.2 Network-based Intrusion-Detection-System
28.4.3 Hybride Intrusion-Detection-Systeme
28.5 Komponenten von Intrusion-Detection-Systemen
28.5.1 Hostsensoren
28.5.2 Netzsensoren
28.5.3 Datenbankkomponenten
28.5.4 Managementstation
28.5.5 Auswertungsstation
28.6 Methoden der Angriffserkennung
28.6.1 Erkennen von Angriffsmustern
28.6.2 Anomalieerkennung
28.6.3 Korrelation von Ereignisdaten
28.7 Das Intrusion-Detection-Dilemma
28.8 Ausblick und Vorgaben für IDS
28.8.1 Anforderungen an die Sicherheitsadministration
28.8.2 Auswahl und Test eines IDS
Zusammenfassung
Literatur
29 Datensicherung
Einleitung
29.1 Zwecke der Datensicherung
29.2 Strategien der Datensicherung
29.3 Technische Mechanismen
29.4 Backups von vertraulichen Daten
29.5 Backup-Medien
29.6 Datensicherung in der Cloud

29.7 Erfolgsfaktoren für Recovery

29.7.1 Physische Verfügbarkeit

29.7.2 Betriebliche Voraussetzungen für Recovery

29.7.3 Recovery-Fähigkeit überprüfen

29.8 Datensicherungskonzept

Zusammenfassung

Literatur

30 Incident-Management und Computer-Emergency-Response-Teams

Einleitung

30.1 Ziel und Aufgaben des Incident-Managements

30.2 Der Aufbau des CERT

30.3 Regelmäßige Aufgaben des CERT

30.3.1 Überwachen der Informationsströme – Erkennen von Incidents

30.3.2 Aufbau- und Pflegearbeiten

30.4 Der Incident-Prozess

30.4.1 Phase 1: Analysieren

30.4.2 Phase 2: Reagieren

30.4.3 Phase 3: Nachbereitung

Zusammenfassung

Literatur

Übersicht über CERT-Organisationen

31 Business-Continuity-Management

Einleitung

31.1 Business Continuity

31.1.1 Hohe Verfügbarkeit erreichen und schwere Störfälle beherrschen

31.1.2 Business-Impact-Analyse

31.1.3 Verantwortung für Business Continuity

31.2 Business Continuity vorbereiten

31.2.1 Notfall-Teams und Krisenstab etablieren

31.2.2 Störfalleskalationswege aufbauen

31.2.3 Notfallhandbuch bereitstellen

31.2.4 Notfallvorsorge

31.2.5 Krisenkommunikation vorbereiten

31.2.6 BC-Training, BC-Awareness und BC-Kultur

31.3 BCM etablieren

31.3.1 Das BCM-Team

31.3.2 Initialisierung des Business-Continuity-Managements

31.3.3 BCM-Planungsphase

31.3.4 Umsetzungsphase

31.3.5 Überwachung

31.3.6 Weiterentwicklung

31.4 Standards für BCM

31.4.1 ISO 22301

31.4.2 ISO 22313

31.4.3 ISO/IEC 27031

31.4.4 BSI-Standard 100-4 Notfallmanagement

31.4.5 BCI Good Practice Guidelines

Zusammenfassung

Literatur

32 Cloud Security

Einleitung

32.1 Cloud-Modelle und Cloud-Angebote

32.2 Gefahren der Cloud-Nutzung

32.3 Identitäts- und Berechtigungsmanagement

32.4 Verschlüsselung

32.5 Konfigurationsmanagement

32.6 Weitere Sicherheitsaspekte Cloud Security

Zusammenfassung

Literatur

Anhang

Übersicht zu Standards der Informationssicherheit

Index

Abkürzungen und Glossar

4 Datenschutzrecht

Einleitung

Dem Datenschutzrecht kommt im Rechtsrahmen der Informationssicherheit eine besondere Rolle zu. Zum einen, da es in vielen Fällen der Ursprung von Sicherheitsanforderungen ist, zum anderen, da viele Maßnahmen zur Informationssicherheit ihrerseits am Datenschutzrecht zu messen sind. Dieser Abschnitt vermittelt einen Überblick über die Grundzüge des Datenschutzrechts.

Die Darstellung des Datenschutzrechts beschränkt sich jedoch auf die Darstellung der Ziele des Datenschutzes, in welchem rechtlichen Rahmen sich Verantwortliche zu bewegen haben und wie diese rechtlichen Vorgaben umzusetzen sind. Dabei wird einerseits ein Blick auf einzelne Verarbeitungstätigkeiten geworfen sowie andererseits die sich aus der Datenschutz-Grundverordnung (DSGVO) ergebenden Rechte und Pflichten erläutert. Zum Schluss wird ein Blick auf den spezifischen Datenschutz im Bereich der Telemedien und Telekommunikation sowie weitere Rechtsvorschriften geworfen, die datenschutzrechtliche Regelungen enthalten.

4.1 Ziele des Datenschutzrechts

Das Datenschutzrecht dient dem Schutz des Einzelnen vor Beeinträchtigungen seines Persönlichkeitsrechts durch den Umgang mit seinen personenbezogenen Daten (vgl. Art. 1 Abs. 2 DSGVO). Das heißt, dass jede natürliche Person selbst bestimmen kann, wer, wie, wann und welche personenbezogenen Daten über einen selbst verarbeiten darf. Dies bedeutet auch, dass Daten jeglicher Art gegen Bedrohungen, Manipulation, unberechtigten Zugriff oder Kenntnisnahme abgesichert werden müssen.

Darüber hinaus schützt das Datenschutzrecht auch den freien Verkehr personenbezogener Daten innerhalb der Union, sodass dieser aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden darf (vgl. Art. 1 Abs. 3 DSGVO).

4.1.1 Entwicklung des Datenschutzrechts

Um das System des Datenschutzrechts und seine Wirkungsweise zu verstehen, ist ein Blick auf die Geschichte des Datenschutzes hilfreich. Das weltweit erste Datenschutzgesetz wurde 1970 in Hessen verabschiedet. Weitere Bundesländer folgten und 1977 erließ auch der Bund ein Datenschutzgesetz, das Bundesdatenschutzgesetz (BDSG).

Begleitet wurde die Datenschutzgesetzgebung durch die Rechtsprechung des Bundesverfassungsgerichts. Bis heute prägende Bedeutung hat vor allem das Volkszählungsurteil vom 15.12.1983,[1] in dem mit dem *Recht auf informationelle Selbstbestimmung* eine Ausprägung des allgemeinen Persönlichkeitsrechts geschaffen wurde. Das Recht auf informationelle Selbstbestimmung ist bis heute aus deutscher Sicht das grundrechtliche Fundament des Datenschutzes. Daneben haben die meisten Landesverfassungen das Recht auf informationelle Selbstbestimmung in ihren Grundrechtskatalog aufgenommen.

Auch Art. 8 der Charta der Grundrechte der Europäischen Union (GRCh) enthält seit dem Jahr 2000 eine Grundrechtsbestimmung zum Datenschutz. Art. 8 GRCh regelt das verfassungsrechtliche Fundament des europäischen Datenschutzes. Die dortige Regelung enthält eine Beschränkung der Verarbeitung personenbezogener Daten, wonach diese nur unter Voraussetzung einer gesetzlich geregelten Erlaubnisgrundlage oder auf Grundlage einer Einwilligung verarbeitet werden dürfen. Auch werden dort die Zweckbindung, das individuelle Auskunftsrecht und die dort verankerte Überwachung zur Einhaltung dieser Vorschrift durch unabhängige Stellen begründet. Im europäischen Kontext ist das Recht auf informationelle Selbstbestimmung nicht als Freiheitsrecht, sondern als Recht auf staatlichen Schutz formuliert ist. Dennoch spielt die Selbstbestimmungsmöglichkeit des Einzelnen auch in der Datenschutz-Grundverordnung eine große Rolle, was an den gestärkten Betroffenen- und Transparenzrechten deutlich wird.

Die Datenschutz-Grundverordnung trat am 25.05.2016 in Kraft und gilt als Verordnung unmittelbar ohne weiteren Umsetzungsakt in allen Mitgliedstaaten. Das BDSG alter Fassung wurde mit Geltung der Grundverordnung zum 25.05.2018 aufgehoben und durch ein neues Bundesdatenschutzgesetz ersetzt.[2]

Wie sich aus der Bezeichnung der Datenschutz-*Grund*verordnung bereits ergibt, regelt diese lediglich die Grundlagen des Datenschutzrechts. Daneben enthält sie sog. *Öffnungsklauseln*, die den Mitgliedstaaten ermöglichen, die Datenschutz-Grundverordnung zu konkretisieren und zu ergänzen. Das »neue« Bundesdatenschutzgesetz enthält daher nur noch eine Reihe von Konkretisierungen zur Datenschutz-Grundverordnung. Dazu gehören

Regelungen des Beschäftigtendatenschutzes und ansonsten Umsetzungsbestimmungen u. a. zum Aufbau der Datenschutzaufsicht. Neben dem Bundesdatenschutzgesetz hat der deutsche Gesetzgeber in weiteren Spezialgesetzen wie dem Handelsgesetzbuch, der Abgabenordnung, dem 10. Sozialgesetzbuch und dem Einkommensteuergesetz von den Öffnungsklauseln Gebrauch gemacht.

Daneben wurde die Interpretation der Datenschutz-Grundverordnung durch die Rechtsprechung des Europäischen Gerichtshofs wesentlich mitgestaltet. So wirken sich insbesondere die sog. »Schrems-Urteile«[3] wesentlich aus. Die Urteile haben für den Datentransfer in unsichere Drittländer weitreichende Folgen. Bei Drittländern handelt es sich um Länder, bei denen die Europäische Kommission per Angemessenheitsbeschluss kein angemessenes Datenschutzniveau bestätigt hat. Im Wege der »Schrems-Urteile« hatte der Europäische Gerichtshof zwischenstaatliche Vereinbarungen einer genauen Prüfung unterzogen und daraufhin (insbesondere das Safe-Harbour-Abkommen und das EU-US Privacy Shield zwischen den USA und der Europäischen Union) untersagt. Infolgedessen sind Datenübermittlungen in Drittstaaten immer dann erschwert, wenn die Drittstaaten kein anerkanntes, ähnliches Datenschutzniveau wie die EU aufweisen.

4.1.2 Anwendungsbereich und Begriffsbestimmungen

Bei der Anwendung des Datenschutzrechts ist entscheidend, in welchem Anwendungsfall welches Gesetz zur Anwendung kommt sowie wo welches Gesetz räumlich Anwendung findet. Dabei ist zwischen dem räumlichen und sachlichen Anwendungsbereich zu unterscheiden.

4.1.3 Sachlicher Anwendungsbereich

Der sachliche Anwendungsbereich der Datenschutz-Grundverordnung umfasst gemäß Art. 2 Abs. 1 DSGVO »die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen«. Die Grenzen des sachlichen Anwendungsbereichs regelt Art. 2 Abs. 2 DSGVO. Darunter fällt bspw. die Verarbeitung personenbezogener Daten für ausschließlich persönliche oder familiäre Tätigkeiten (Art. 2 Abs. 2 lit. c DSGVO).

Eine Besonderheit des Datenschutzes ist insbesondere bei nicht personenbezogenen Daten zu beachten, die aber aufgrund anderer Umstände als besonders sensibel betrachtet werden. Zwar fallen diese nicht in den

sachlichen Anwendungsbereich der Datenschutz-Grundverordnung. Jedoch greift gegebenenfalls in diesem Fall der Schutz durch das Geschäftsgeheimnisgesetz.

4.1.4 Personenbezogene Daten

Das Verständnis von Datenschutz ist unmittelbar an den Begriff der personenbezogenen Daten geknüpft. Art. 4 Nr. 1 DSGVO definiert personenbezogene Daten als »alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen«. Im zweiten Halbsatz wird dann die Identifizierbarkeit, also der Personenbezug als Möglichkeit, eine Person direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung oder zu besonderen Merkmalen, zu identifizieren, erläutert. Erfasst sind damit sämtliche Informationen, die auf eine konkrete Person bezogen werden können, unabhängig von deren Bedeutung für den Betroffenen. Die bloße Möglichkeit des Personenbezugs kann jedoch zu Abgrenzungsschwierigkeiten führen. Pseudonymisierte Daten (Art. 4 Nr. 5 DSGVO), bei denen definitionsgemäß der Name oder andere Identifikationsmerkmale der Bezugsperson durch ein Kennzeichen ersetzt werden, um die direkte Bestimmung bspw. für Gruppen von Anwendern auszuschließen oder wesentlich zu erschweren, gelten als personenbeziehbar, da das Kennzeichen die Zuordnung weiter erlaubt. Sie unterfallen damit weiterhin dem Datenschutzrecht.

Anders sieht es hingegen bei anonymisierten Daten aus, die grundsätzlich keine personenbezogenen Daten darstellen (vgl. ErwG 26). Wann Daten als anonym einzustufen sind, ist unter Umständen aber schwer zu beurteilen – eine tiefere Analyse von Datenbeständen führt immer wieder zu überraschenden Erkenntnissen. Beispielsweise können Angaben zu einer Person auch ohne bestimmte Identifikationsmerkmale personenbeziehbar werden, wenn die Angaben in ihrer Konstellation und Menge lediglich eine einzige Person zutreffend beschreiben. So kann die Kombination der besuchten Schule, des Geburtsjahrgangs, des Berufs und eines bestimmten Hobbys bereits ausreichen, um eine Person zu bestimmen. Ein Personenbezug liegt bspw. bei dynamischen IP-Adressen vor.[4] Neben anonymisierten Daten gibt es auch synthetische Daten. Dabei handelt es sich um Daten, bei denen durch künstliche Intelligenz völlig neue künstliche Daten generiert werden, die keinen Personenbezug haben. Da der Algorithmus der künstlichen Intelligenz jedoch in der Regel durch personenbezogene Daten trainiert wird, kommt es im Zweifel auf eine Einschätzung im Einzelfall an, ob die synthetisch generierten Daten tatsächlich keinen Personenbezug aufweisen.

4.1.5 Verarbeitung von Daten

Die entscheidende Tätigkeit für die sachliche Anwendung der Datenschutz-Grundverordnung ist die Verarbeitung der personenbezogenen Daten. Die Verarbeitung umfasst dabei das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreiten oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder das Vernichten (Art. 4 Nr. 2 DSGVO). Der Begriff des Offenlegens macht deutlich, dass der Verarbeitungsbegriff nicht auf die gezielte Übermittlung beschränkt bleibt, sondern dass bereits die Einblicksmöglichkeit Dritter zur Verarbeitung führt.

4.1.6 Räumlicher Anwendungsbereich

Bei dem räumlichen Anwendungsbereich des Datenschutzrechts ist zwischen deutschen Vorschriften und der sowohl in Deutschland als auch in den übrigen Mitgliedsstaaten der Europäischen Union direkt geltenden Datenschutz-Grundverordnung zu unterscheiden. Deutsche Datenschutzvorschriften erfassen in der Regel jegliche Datenerhebung, -verarbeitung oder -nutzung in Deutschland, es sei denn, die verantwortliche Stelle hat ihren Sitz in einem anderen Staat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum. Die Datenschutz-Grundverordnung knüpft zum einen an die Tätigkeit eines Verantwortlichen oder eines Auftragsverarbeiters mit Niederlassung in der Europäischen Union an. Zum anderen ist die Datenschutz-Grundverordnung auf Verarbeitungstätigkeiten anzuwenden, die von Verantwortlichen außerhalb der Union ausgehen, aber im Zusammenhang mit Angeboten an betroffene Personen in der Union stehen, oder die der Verhaltensbeobachtung zu betroffenen Personen dienen, die sich in der Union befinden.

4.1.7 Weitere Begriffsbestimmungen

Neben den personenbezogenen Daten und der Verarbeitung enthält die Datenschutz-Grundverordnung eine Vielzahl von weiteren Begrifflichkeiten, die in Art. 4 DSGVO legaldefiniert sind. Im Folgenden werden einige Begrifflichkeiten erläutert.

- **Adressat des Datenschutzrechts**

  Adressaten des Datenschutzrechts sind Verantwortliche und Auftragsverarbeiter.

- **Verantwortlicher** (Art. 4 Nr. 7 DSGVO)

Der Verantwortliche entscheidet allein oder gemeinsam mit weiteren Verantwortlichen über Zwecke und Mittel der Verarbeitung. Verantwortliche können natürliche und juristische Personen, Behörden oder andere Stellen sein.

- **Auftragsverarbeiter** (Art. 4 Nr. 8 DSGVO)

  Auftragsverarbeiter verarbeiten personenbezogene Daten im Auftrag des Verantwortlichen, unterliegen dabei jedoch eigenen Datenschutzpflichten. Sie sind streng den Weisungen des Verantwortlichen unterworfen.

  Verbindungen von juristischen Personen untereinander, etwa eine Konzernzugehörigkeit oder ein mehrheitlicher Anteilsbesitz an einer anderen juristischen Person, haben keine Bedeutung – es existiert im Datenschutzrecht kein Konzernprivileg. Daran hat auch die Datenschutz-Grundverordnung im Grundsatz nichts geändert.

- **Betroffene Person** (Art. 4 Nr. 1 DSGVO)

  Die natürliche Person, auf die sich die personenbezogenen Daten beziehen, ist die betroffene Person.

- **Dritte** (Art. 4 Nr. 10 DSGVO)

  Alle Personen oder Stellen außerhalb der verantwortlichen Stellen der Betroffenen und des Auftragsverarbeiters sind sogenannte Dritte.

4.1.8 Rechtsrahmen und Umsetzungsvorgaben

Das Grundrecht auf informationelle Selbstbestimmung macht deutlich, dass die Verwendung personenbezogener Daten zu Eingriffen in die Grundrechte des Betroffenen führt. Hieraus leitet sich ein tragendes Grundprinzip des Datenschutzrechts ab: Eine Verarbeitung (z. B. Erheben, Verarbeiten oder Nutzen) von personenbezogenen Daten darf nur auf Grundlage einer rechtlichen Erlaubnisnorm stattfinden und ist ansonsten verboten. Dieser Grundsatz wird auch als *Verbot mit Erlaubnisvorbehalt* bezeichnet. Als Bestandteil des Art. 8 Abs. 2 der Charta der Grundrechte und konkretisiert durch Art. 6 Abs. 1 DSGVO besteht dieser Grundsatz weiterhin. Der Grundsatz darf jedoch nicht darüber hinwegtäuschen, dass die Datenschutz-Grundverordnung sehr weite allgemeine Erlaubnisnormen enthält, vor allem die Verarbeitung auf Grundlage des berechtigten Interesses, Art. 6 Abs. 1 lit. f DSGVO. Die speziellen Regelungen des Bundesdatenschutzgesetzes etwa zur Verarbeitung zu Werbezwecken existieren nicht mehr. Stattdessen enthält Art. 6 Abs. 1 DSGVO die wesentlichen Erlaubnisnormen:

- Die Verarbeitung kann auf die Einwilligung des Betroffenen gestützt werden (Art. 6 Abs. 1 lit. a DSGVO).
- Die Verarbeitung von personenbezogenen Daten ist für die Begründung, Durchführung oder Beendigung eines Vertrags oder eines vorvertraglichen Rechtsverhältnisses erforderlich (Art. 6 Abs. 1 lit. b DSGVO). Ein wichtiger Unterfall ist hier das Beschäftigtenverhältnis, bei dem die Verarbeitung jedoch auf § 26 BDSG gestützt wird.
- Die Datenverarbeitung wird durch rechtliche Verpflichtungen des Verantwortlichen erforderlich (Art. 6 Abs. 1 lit. c DSGVO).
- Die Verarbeitung ist zum Schutz lebenswichtiger Interessen erforderlich (Art. 6 Abs. 1 lit. d DSGVO).
- Schließlich besteht ein Auffangtatbestand mit der Erlaubnis, personenbezogene Daten zur Wahrung berechtigter Interessen der verantwortlichen Stelle zu verwenden. In diesem Fall ist jedoch eine Abwägung mit anzunehmenden bzw. offensichtlich überwiegenden schutzwürdigen Interessen der Betroffenen durchzuführen (Art. 6 Abs. 1 lit. f DSGVO).

Die oben genannten rechtlichen Verpflichtungen finden sich in einer Unzahl von Spezialgesetzen, von den Sozialgesetzbüchern bis hin zu öffentlich-rechtlichen Gesetzen wie den Melde- oder Polizeigesetzen. Ausführlichere Datenschutzregeln in nationalen Gesetzen werden jedoch je nach Regelungsinhalt durch die Datenschutz-Grundverordnung als höherrangiges Recht verdrängt, soweit diese keine Öffnungsklausel enthält und den Regelungsgegenstand grundsätzlich umfasst.

Neben dem fortbestehenden Verbot mit Erlaubnisvorbehalt und den Erlaubnistatbeständen des Art. 6 Abs. 1 DSGVO sieht die Datenschutz-Grundverordnung ergänzend die Grundsätze der Verarbeitung nach Treu und Glauben und der Verarbeitung in einer für den Betroffenen nachvollziehbaren Weise vor, d. h., dass bei der Prüfung der Rechtmäßigkeit und der Anwendung der Erlaubnisse aus Art. 6 Abs. 1 DSGVO auch die Perspektive des Betroffenen zu berücksichtigen ist.

4.1.9 Datenschutzrechtliche Grundprinzipien

Neben diesem die Struktur des Datenschutzrechts prägenden ersten Grundprinzip stehen weitere Grundprinzipien, die in Art. 5 Abs. 1 DSGVO niedergelegt sind: die Zweckbindung, die Datenminimierung und Speicherbegrenzung, das Transparenzgebot, das sich ebenfalls aus der Nachvollziehbarkeit für den Betroffenen ableitet, die Richtigkeit der verarbeiteten personenbezogenen Daten und deren Integrität und

Vertraulichkeit in Form der angemessenen Sicherheit durch technische und organisatorische Maßnahmen (sog. TOM).

Die **Zweckbindung** personenbezogener Daten ist auch eine wesentliche Forderung des Volkszählungsurteils. Die Datenschutz-Grundverordnung hat dieses Kernprinzip im Grundsatz nicht angetastet. Demnach dürfen personenbezogene Daten grundsätzlich nur für den vorab festzulegenden Zweck verwendet werden, für den sie erhoben oder übermittelt worden sind. Der Zweck muss dabei nach einer der oben genannten Alternativen rechtlich zulässig sein. Ist später eine Verwendung der Daten für andere Zwecke beabsichtigt, bedarf es einer neuen Rechtsgrundlage oder einer Abwägung nach den Kriterien des Art. 6 Abs. 4 DSGVO, der dem Verantwortlichen in einem engen Rahmen die Verarbeitung zu einem nicht ursprünglich vorgesehenen Zweck gestattet.

Eine weitere Grenze der Datenverwendung wird durch das **Erforderlichkeitsprinzip** gezogen. In der Datenschutz-Grundverordnung wird dieses zusammenfassende Prinzip durch die Grundsätze der Datenminimierung und der Speicherbegrenzung repräsentiert. Der Wortlaut von Art. 5 Abs. 1 lit. c DSGVO (Datenminimierung) lautet: »Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.« Die verantwortliche Stelle darf demnach nur die personenbezogenen Daten erheben und verarbeiten, die für den festgelegten Zweck benötigt werden. Die Erforderlichkeit begrenzt auch die Dauer der Verarbeitung. Ist der Zweck erfüllt und bestehen keine Aufbewahrungspflichten mehr (etwa steuerlicher Natur oder aufgrund gesetzlicher Dokumentationspflichten), sind die personenbezogenen Daten zu löschen oder zu anonymisieren. Dieser Aspekt des Erforderlichkeitsprinzips wird in der Datenschutz-Grundverordnung als Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO) gesondert hervorgehoben. Für die Umsetzung der IT-Sicherheit hat dieses Prinzip besondere Bedeutung, wie im Folgenden noch dargestellt wird, denn es begrenzt bspw. auch die Dauer, über die Sicherheitsprotokollierungen aufbewahrt werden dürfen, und zwingt, den Auswertungszeitraum zu begründen.

Schließlich gilt das Grundprinzip der **Transparenz**. Der Betroffene soll einschätzen können, was Dritte über ihn wissen (so verkürzt das Volkszählungsurteil). Die Erwägungsgründe der Datenschutz-Grundverordnung lauten hierzu: »Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und in klarer und einfacher Sprache abgefasst sind.« (ErwG 39 S. 3 f.). Dieser Grundsatz wird durch die Art. 12 ff. DSGVO konkretisiert. Angesichts der steigenden Komplexität vieler Datenverarbeitungen stellt die

Umsetzung dieses Grundsatzes und die Anforderung der Verständlichkeit eine wesentliche Herausforderung bei der Umsetzung der Datenschutz-Grundverordnung dar. Ergänzend dienen individuelle Auskunftsansprüche gegen verantwortliche Stellen (Art. 15 DSGVO) und Benachrichtigungspflichten (bspw. in Art. 19, 21 DSGVO oder Art. 34 DSGVO im Fall von Datenschutzvorfällen) der Transparenz.

Der Grundsatz der **Richtigkeit** der Daten (Art. 5 Abs. 1 lit. d DSGVO) bezieht sich auf die Verpflichtung zur Aktualität und zur selbstständigen Berichtigung von, bezogen auf den Zweck, unrichtigen personenbezogenen Daten. Die Verpflichtung zur fortlaufenden Kontrolle wird auf die Erforderlichkeit und auf angemessene Maßnahmen begrenzt. Konkretisiert wird der Grundsatz vor allem durch das Betroffenenrecht auf Berichtigung, Art. 16 DSGVO, oder Löschung, Art. 17 DSGVO, die allerdings eine aktive Rolle des Betroffenen vorsehen.

Für die Informationssicherheit besonders bedeutsam sind die Hervorhebung von **Integrität und Vertraulichkeit** sowie die **Gewährleistung einer angemessenen Sicherheit** der personenbezogenen Daten als Grundsatz in Art. 5 Abs. 1 lit. f DSGVO. Die Konkretisierung erfolgt durch Art. 24, 32 DSGVO durch die Schaffung geeigneter technischer und organisatorischer Maßnahmen sowie durch die Pflicht zu Datenschutz mittels Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO, sogenanntes Privacy by Design und Privacy by Default).

Für die Praxis zusätzlich bedeutsam ist die in Art. 5 Abs. 2 DSGVO geregelte **Nachweis- oder Rechenschaftspflicht**, die dem Verantwortlichen auferlegt, seine Maßnahmen zur Einhaltung der Anforderungen aus der Datenschutz-Grundverordnung nachweisen zu können. Hieraus ergibt sich eine umfassende Dokumentationspflicht, die zwar in Bezug auf ihre Wahrnehmung nicht näher ausgestaltet ist, jedoch absehbar einen höheren Dokumentationsaufwand für die Verantwortlichen erzeugt. Diese Nachweispflicht umfasst auch die ergriffenen technischen und organisatorischen Maßnahmen sowie die Begründung ihrer Auswahl in Bezug auf die Einschätzung der bestehenden Risiken. Somit wird insbesondere der Bereich der Informationssicherheit durch diesen Grundsatz berührt.

4.1.10 Datenschutzleitlinie

Eine **Datenschutzleitlinie** ist eine Zusammenführung von internen Datenschutzthemen, die der Unterweisung und Orientierung aller Mitarbeiter eines Unternehmens dient. Inhaltlich handelt es sich um einseitige Vorgaben des Arbeitgebers und Verantwortlichen an die Arbeitnehmer zu übergreifenden

datenschutzrechtlichen Vorgaben, die den Datenschutz sowohl regeln als auch organisieren.

4.1.11 Zweck und Geltungsbereich

Für eine wirksame Umsetzung des Datenschutzes innerhalb eines Unternehmens empfiehlt sich eine Dokumentenstruktur mit unterschiedlichen datenschutzbezogenen Dokumenten. Dies kann wie folgt aussehen:

1. Als übergeordnetes Dokument gilt die Datenschutzleitlinie, die grundsätzliche Vorgaben an den Datenschutz definiert.
2. Das Datenschutzkonzept beschreibt die Datenschutz-Organisation auf Prozessebene, das Datenschutzmanagement (DSMS) mit den relevanten Datenschutzprozessen sowie die Einhaltung der Schutzziele und Datenschutz-Anforderungen.
3. Die von der Datenschutz-Grundverordnung definierten Schutzziele umfassen die Integrität, Vertraulichkeit und Verfügbarkeit (inkl. Belastbarkeit). Diese werden durch definierte und den jeweiligen Schutzzielen zugewiesene Sicherheitsmaßnahmen umgesetzt und regelmäßig überprüft.

Der Geltungsbereich der Datenschutzleitlinie und des DSMS innerhalb mehrerer Standorte muss eindeutig festgelegt werden. So können sie bspw. für alle nationalen Standorte oder internationale Standorte gelten, es können aber auch einzelne internationale Standorte ausgeschlossen werden. Sie sind für alle Mitarbeiter (Festangestellte, Teilzeitmitarbeitende, Auszubildende, Freelancer etc.) verbindlich und sollten ihnen über ein internes Portal zugänglich gemacht werden. Bei Bedarf können sie Dritten (Externen) zur Verfügung gestellt werden. Einer Bewilligung durch die Geschäftsführung bedarf es hierfür nicht.

Die Datenschutzleitlinie und das DSMS sollten regelmäßig, mindestens jedoch einmal pro Jahr überprüft sowie bei Bedarf überarbeitet werden.

4.1.12 Datenschutzrichtlinie

Mit der Datenschutzrichtlinie soll sichergestellt werden, dass sich auch Mitarbeiter eines Verantwortlichen ihrer Verantwortung und Aufgaben bewusst sind, die mit dem Umgang mit personenbezogenen Daten verbunden sind. Es soll weiter sichergestellt werden, dass alle gesetzlichen Vorschriften im Zusammenhang mit der betrieblichen Nutzung dieser Daten verstanden und beachtet werden.

Mit Hilfe der Datenschutzrichtlinie sollen unternehmensinterne Daten und personenbezogene Daten vor unberechtigtem Zugriff geschützt werden und dafür gesorgt werden, dass für und durch Systeme und ein Unternehmen insgesamt kein Schaden durch unsachgemäße oder unberechtigte Benutzung entsteht.

Die Datenschutzrichtlinie gilt als Arbeits- und Handlungsanweisung für alle Mitarbeiterinnen und Mitarbeiter des Verantwortlichen. Sie regelt den Umgang mit personenbezogenen Daten gemäß der Datenschutz-Grundverordnung bzw. weiteren einschlägigen Datenschutzgesetzen sowie mit sonstigen betrieblichen Daten. Diese Richtlinie wird allen Mitarbeitern bei Beginn des Arbeitsverhältnisses ausgehändigt und gilt stets in der aktuellen Fassung.

4.1.13 Richtlinie zur Privatnutzung des betrieblichen Internets und E-Mail

Grundsätzlich steht es einem Unternehmen frei, ob es die private Nutzung des betrieblichen Internets und der betrieblichen E-Mail-Adresse erlauben möchte oder nicht. Dies gilt auch unabhängig davon, ob im Unternehmen ein Betriebsrat besteht (vgl. § 87 Abs. 1 Nr. 1 und 10 BetrVG).

Allerdings ist der Arbeitgeber auch nach der Einführung des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) gem. § 3 Abs. 3 TTDSG gegenüber seinen Beschäftigten als Telekommunikationsanbieter anzusehen, der das Fernmeldegeheimnis einzuhalten hat. Da die Vorschrift inhaltlich vollständig aus dem alten § 88 TKG übernommen wurde, besteht nach wie vor Streitigkeit über die private Nutzung des betrieblichen Internets und E-Mail. So listet § 3 Abs. 2 Nr. 2 TTDSG weiterhin die »Anbieter von ganz oder teilweise geschäftsmäßig angebotenen Telekommunikationsdiensten« auf. Dabei reicht bereits das bloße »Mitwirken«, wodurch die Privatnutzung von betrieblichem Internet und E-Mail unter das Fernmeldegeheimnis fällt, sobald eine Datenübertragung über das Internet stattfindet.

Solange diese Frage nicht durch den Gesetzgeber und der höchstrichterlichen Rechtsprechung geklärt ist, ist umstritten, ob das Fernmeldegeheimnis in diesem Fall tatsächlich zu beachten ist. Arbeitgeber sollten jedoch zur Vermeidung etwaiger Strafbarkeit davon ausgehen, dass sie Telekommunikationsanbieter sind und entweder die private Nutzung verbieten oder die Mitarbeiter zur Wahrung des Fernmeldegeheimnisses zu verpflichten.

4.1.14 Richtlinie für datenschutzrechtliche Anforderungen an IT-Projekte

Die Datenschutz-Grundverordnung fordert, dass Verarbeitungstätigkeiten datenschutzgerecht gestaltet werden. Dazu gehört, dass angemessene technisch-organisatorische Maßnahmen zum Schutz der Daten ergriffen werden (Art. 24 und 32 DSGVO) und die Prinzipien des Privacy by Design und Privacy by Default (Art. 25 DSGVO) angewandt werden. Dies ist mit vertretbarem Aufwand nur möglich, wenn die entsprechenden Anforderungen bereits sehr früh in IT-Projekten festgelegt werden. Deswegen sollten Verantwortliche Richtlinien für datenschutzrechtliche Anforderungen an IT-Projekten festlegen. Dies betrifft sowohl Entwicklungsprojekte als auch Beschaffungsprojekte.

Im Projektprozess wird sichergestellt, dass die Anforderungen an die datenschutzgerechte Gestaltung von IT-Systemen und die datenschutzgerechte Projektabwicklung erfüllt werden.

Dazu wird geprüft,

- ob der Anforderungskatalog die datenschutzrechtlich geforderten Angaben enthält und
- ob im Projektplan datenschutzrechtlich relevante Aktivitäten enthalten sind und ob diese in einer angemessenen Weise geplant sind. So ist die »Richtlinie Produktivdaten in Test- und Entwicklungssystemen« einzuhalten, wenn entsprechende Aktivitäten geplant sind.

Der Datenschutzbeauftragte ist an der Freigabe der Prozessschritte zu beteiligen.

Es sollte ein Anforderungskatalog mit folgenden Punkten erstellt werden:

- Ein datenschutzrechtlich freigegebenes Rollen- und Berechtigungskonzept.
- Eine Übersicht über Datenarten und Löschregeln, die dem Katalog der Löschregeln entspricht. Es ist sicheres Löschen zu fordern.
- Die Anforderungen sollen in Form einer Umsetzungsvorgabe beschrieben sein. Neue Löschregeln sind vor der Aufnahme mit dem Datenschutzbeauftragten abzustimmen und begleitend zum Projekt in den Katalog der Löschregeln einzupflegen (Antrag an den Verantwortlichen für die Verarbeitungsübersicht).

Wenn die Anforderungen zum Prozessschritt nicht abschließend formuliert werden können, können sie nach Zustimmung des Datenschutzbeauftragten projektbegleitend weiterentwickelt werden.

Der Projektplan muss ausweisen, ob Produktionsdaten im Projekt auf Test- und Entwicklungssystemen eingesetzt werden sollen. So wird sichergestellt,

dass gegebenenfalls personenbezogene (Kunden-)Daten nicht versehentlich bei der Entwicklung von IT-Projekten zum Einsatz kommen und dabei für einen illegitimen Zweck eingesetzt werden.

4.1.15 Datenschutzimplementierung/Datenschutzmanagementsystem (DSMS)

Der Datenschutzimplementierung durch dokumentierte, verbindliche Prozesse wird ein hoher Stellenwert beigemessen. Sie ist u. a. von Relevanz hinsichtlich eines DSMS. Unter einem DSMS sind alle Prozesse, internen Standards, Regeln und Vorgaben zur Erfüllung der gesetzlichen Vorgaben an die Verarbeitung personenbezogener Daten zu verstehen. Diese Prozesse begleiten den gesamten Lebenszyklus automatisierter Verfahren – von der Konzeption über die Implementierung und den Betrieb bis zur Außerbetriebnahme.

4.1.16 Datenschutzrichtlinien und Arbeitsanweisungen

Die Aufrechterhaltung eines angemessenen Datenschutzniveaus ist ohne aktive Einbindung der Mitarbeiter und Regelung spezifischer Prozesse nicht möglich. Hierzu sind weitere detaillierte Richtlinien und Arbeitsanweisungen zum Datenschutz erforderlich. Die durch das Unternehmen festgelegten Verhaltenspflichten dienen als Orientierung für die Mitarbeiter (z. B. Datenschutzkonzept, Schulungsunterlagen, Verzeichnis von Verarbeitungstätigkeiten). Das Verzeichnis von Verarbeitungstätigkeiten ist zudem eine gesetzliche Unternehmenspflicht aus Art. 30 DSGVO, soweit die Voraussetzungen vorliegen. Darüber hinaus dient es der Dokumentation der Umsetzung von Datenschutzgrundsätzen und bestimmter Datenschutzpflichten. Durch die Erfassung von Verarbeitungstätigkeiten kann zugleich deren Prüfung auf Zulässigkeit und Anforderungskonformität nachgewiesen werden. Das Verzeichnis stellt einen tragenden Dokumentationsbestandteil dar.

4.1.17 Datenschutzorganisation

Damit die Grundsätze eines DSGVO-konformen Umgangs mit personenbezogenen Daten im operativen Betrieb umgesetzt werden können, bedarf es einer übersichtlich strukturierten Datenschutzorganisation mit klarer Zuweisung der jeweiligen Aufgaben, Kompetenzen und Verantwortlichkeiten. Eine dokumentierte und damit nachweisbare Datenschutzorganisation dient zudem der Erfüllung der in Art. 5 Abs. 2 DSGVO geregelten Rechenschaftspflicht. Die Regelung fester Prozesse zur Erfüllung und Umsetzung der Datenschutzanforderungen setzt zudem die Organisationspflichten des Unternehmens und Verantwortlichen um. Die Umsetzung einer

Datenschutzorganisation besteht daher größtenteils aus dem Etablieren und Dokumentieren von Prozessen durch Richtlinien und Arbeitsanweisungen sowie aus der Organisation und Bereitstellung der erforderlichen Hilfsmittel und Informationen.

Die Datenschutzorganisation umfasst zum einen den personellen Aufbau des Datenschutzes, also die konkrete Benennung von den zur Regelung des Datenschutzes eingebundenen Personen und die rollenbasierte Zuweisung von internen Verantwortlichkeiten. Weiter betrifft die Organisation die Dokumentation und das Berichtswesen über den Datenschutz sowie den Umgang mit datenschutzrelevanten Ereignissen. Ebenso umfasst sie die Beschreibung, wie Datenschutzpflichten erfüllt und die Rechtmäßigkeit der Verarbeitungstätigkeiten geprüft werden.

4.1.18 Datenschutzkonzept

Sämtliche datenschutzrelevanten Prozesse sind im Datenschutzkonzept aufgeführt. Die konkreten Umsetzungsvorgaben sind in den jeweiligen Anweisungen beschrieben. Die Steuerung der Datenschutzdokumentation im Sinne der Überarbeitungen und regelmäßigen Umsetzungsüberprüfungen sind ebenfalls im Konzept oder auf der jeweiligen Prozessebene erläutert und in den Anweisungen konkret vorgegeben. Speziell erwähnt sei hier das Verzeichnis von Verarbeitungstätigkeiten, das zum Nachweis der Einhaltung der Vorgaben aus der Datenschutz-Grundverordnung dient. Es gilt als eine der essenziellen Datenschutz-Dokumentationen und beinhaltet sämtliche unternehmensinternen personenbezogenen Verarbeitungsvorgänge. Das Datenschutzkonzept dient der allgemeinen Verantwortungszuweisung und Rollenbeschreibung, der Zieldefinition und der Festlegung des organisatorischen Rahmens (u. a. der Weiterentwicklung) des Datenschutz-Managements.

4.2 Verarbeitungstätigkeiten

Art. 30 Abs. 1 DSGVO verlangt, dass die verantwortliche Stelle ein Verzeichnis aller Verarbeitungstätigkeiten zu führen hat. Zwar findet sich in der Datenschutz-Grundverordnung keine Legaldefinition der Verarbeitungstätigkeit. Die deutschen Aufsichtsbehörden definieren die Verarbeitungstätigkeit jedoch wie folgt: Als Verarbeitungstätigkeit wird im Allgemeinen ein Geschäftsprozess auf geeignetem Abstraktionsniveau verstanden. Es ist ein strenger Maßstab anzulegen, sodass jeder neue Zweck der Verarbeitung eine eigene Verarbeitungstätigkeit darstellt.[5] Was konkret eine Verarbeitungstätigkeit ist,

hängt vom jeweiligen Unternehmen ab. In einem kleinen Unternehmen mit wenigen Mitarbeitern kann z. B. die gesamte Personalverwaltung (inkl. Bewerbungsverfahren und Lohnabrechnung) als eine einzige Verarbeitungstätigkeit gesehen werden. Bei einem mittleren Unternehmen sollte eine stärkere Untergliederung stattfinden, z. B. in Personalgewinnung, Personaleinstellung, Verwaltung des aktuellen Personals, Beendigung der Arbeitsverhältnisse und ähnliche Verarbeitungstätigkeiten.[6]

4.2.1 Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

Führt eine Verarbeitungstätigkeit voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen, ist gem. Art. 35 Abs. 1, 3 DSGVO eine Datenschutz-Folgenabschätzung (DSFA oder auch PIA (privacy impact assessment)) durchzuführen. Gem. Art. 35 Abs. 3 DSGVO ist eine Datenschutz-Folgenabschätzung insbesondere in folgenden Fällen erforderlich:

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, einschließlich Profiling
- umfangreiche Verarbeitung sensibler Daten
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

Darüber hinaus haben die Aufsichtsbehörden durch sogenannte »Blacklisten« Verarbeitungstätigkeiten aufgelistet, in denen ebenfalls immer eine Datenschutz-Folgenabschätzung durchzuführen ist.

Durch die Durchführung einer DSFA können sich Grenzen für die Verwendung von personenbezogenen Daten oder auch die Anpassung oder Ergänzung von Sicherheitsmaßnahmen ergeben. Die DSFA ist vor Beginn der Verarbeitung der personenbezogenen Daten durchzuführen und zu dokumentieren.

In der DSFA ist die Einhaltung der datenschutzrechtlichen Bestimmungen zu überprüfen. Dazu gehören: das Vorliegen einer Rechtsgrundlage, die Erfüllung von deren Tatbestandsvoraussetzungen, das Vorhandensein angemessener technischer und organisatorischer Maßnahmen zum Schutz der Daten, die Einhaltung von Mitbestimmungsrechten, das Vorliegen einer ausreichenden Dokumentation und das Treffen von Vorkehrungen zur Herstellung von Transparenz und zur Gewährleistung von Betroffenenrechten, z. B. das Erteilen von Auskünften nach Art. 15 DSGVO. Insbesondere sind die Risiken für die Betroffenen, die mit der Datenverarbeitung einhergehen, systematisch abzuschätzen und darzustellen. Darzustellen ist auch, welche Maßnahmen ergriffen werden, um die möglichen Risiken, in der Regel durch technische und

organisatorische Maßnahmen, abzustellen oder abzumildern. Das Ergebnis ist zu dokumentieren.

4.2.2 Rollen-Berechtigungskonzept

Da die Verarbeitung personenbezogener Daten in einem Unternehmen kaum vermieden werden kann, bedarf es in IT-Systemen der Vergabe von Zugriffsrechten durch ein Berechtigungskonzept mit Rollenverteilung. Hierdurch wird sichergestellt, dass nur befugte Personen Zugriff auf personenbezogene Daten erhalten. Im Umkehrschluss wird dadurch auch der Zugriff unbefugter Personen verhindert.

Die rechtlichen Voraussetzungen hierfür ergeben sich einerseits aus dem Grundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DSGVO), wonach eine angemessene Sicherheit für personenbezogene Daten geschaffen werden muss, um diese vor unbefugter oder unrechtmäßiger Verarbeitung zu schützen. Andererseits werden Verantwortliche und Auftragsverarbeiter explizit zum Treffen geeigneter technischer und organisatorischer Maßnahmen verpflichtet, um den Schutz personenbezogener Daten während der Datenverarbeitung zu gewährleisten (Art. 32 Abs. 1 lit. b DSGVO). Gleichzeitig werden hierdurch auch die Rechenschafts- und Nachweispflichten (Art. 5 Abs. 2 DSGVO) gewahrt.

Für den Aufbau eines Berechtigungskonzepts eignet sich die Bildung von Rollen und Identitäten. Dazu sind zunächst geeignete Rollen zu definieren, die aus den Nutzungsvorgängen und Prozessen abzuleiten sind. Diesen Rollen sind wiederum Rechte nach dem »Need-to-know«-Prinzip zuzuordnen: Die jeweilige Berechtigung muss erforderlich sein, um die mit der Rolle verbundene Aufgabe erfüllen zu können. Dabei sind insbesondere Lese- und Schreibberechtigungen zu unterscheiden.

Rollen und Berechtigungen sind für jedes betroffene IT-System in einem Rollen- und Berechtigungskonzept zu dokumentieren. Sie sind die Vorgabe (Soll-Definition) für die Umsetzung in dem jeweiligen IT-System und die Vorgabe für Audits. Die Erstellung des Rollen- und Berechtigungskonzepts liegt in der Verantwortung des Verarbeitungs-Verantwortlichen, der das IT-System nutzt. Die Freigabe erfolgt durch den Datenschutzbeauftragten.

Das Rollen- und Berechtigungskonzept muss die folgenden Regelungen und Festlegungen umfassen:

- Berechtigungsvergabe
    - Wer ist zuständig für die Wahl der für eine Rolle erforderlichen Berechtigungen?

        - Wer ist verantwortlich für den Entzug von einer Rolle zugewiesenen Berechtigungen?
        - Wer ist berechtigt, über abweichende Ausnahmeregelungen (zusätzliche Berechtigungen, die einer Person, nicht einer Rolle zugewiesen werden) zu entscheiden?
        - Wie lange sind Ausnahmeregelungen maximal gültig?
        - Wo werden Ausnahmeregelungen nachweisbar dokumentiert?
    - Rollenzuordnung
        - Wer ist zuständig für die Zuweisung von Personen zu einer Rolle?
        - Wie und wo wird die Rollenzuweisung (mit Datum, Rolle, Person) dokumentiert?
        - Wer ist verantwortlich für die Änderung der Rollenzuweisung bei Änderung der Betriebszugehörigkeit oder der innerbetrieblichen Zuständigkeit?
        - In welchem Zeitraum erfolgt spätestens eine ggf. erforderliche Anpassung der Rollenzuweisung?

Rollen- und Berechtigungskonzepte sind für das betroffene IT-System bindend; alle Änderungen sind vom Datenschutzbeauftragten freizugeben. In den Freigabeprozess ist ggf. auch der Betriebsrat einzubinden.

Rollen- und Berechtigungskonzepte werden mindestens einmal jährlich durch den Verarbeitungsverantwortlichen auf fortgeltende Eignung überprüft.

4.2.3 Informationspflichten

Jeder Verantwortliche ist verpflichtet, für die Verarbeitung personenbezogener Daten geeignete Maßnahmen zu ergreifen, um die betroffenen Personen über die Verarbeitungen, deren Rahmen und Zwecke sowie über ihre Rechte zu informieren. Die diesbezüglichen Anforderungen an die Informationspflichten sind in den Art. 12, 13 und 14 DSGVO geregelt. Informationspflichten bestehen dabei regelmäßig gegenüber Websitebesuchern, Kunden, Lieferanten, Dienstleistern, Beschäftigten und Interessenten.

Der Umfang der Informationspflicht unterscheidet sich geringfügig danach, ob die personenbezogenen Daten direkt von dem Betroffenen erhoben werden (Art. 13 DSGVO) oder ob eine Erhebung über Dritte oder anderweitig bestehende gespeicherte Daten erfolgt (Art. 14 DSGVO). Die zu erteilenden Informationen umfassen dabei:

- den Namen und die Kontaktdaten des Verantwortlichen

- die Kontaktdaten des Datenschutzbeauftragten
- die Zwecke der Verarbeitung
- die Rechtsgrundlage der Verarbeitung
- das berechtigte Interesse im Falle von Art. 6 Abs. 1 S. 1 lit. f DSGVO
- die Empfänger (oder Kategorien von Empfängern)
- die beabsichtigte Drittlandübermittlungen sowie die zugehörigen Garantien und deren Einsehbarkeit
- die geplante Dauer der Verarbeitung
- die Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung und ggf. Widerspruch)
- das Beschwerderecht
- die verarbeiteten Kategorien von Daten (sobald nicht bei dem Betroffenen direkt erhoben wird, Art. 14 DSGVO)
- die Herkunft dieser Daten (sobald nicht bei dem Betroffenen direkt erhoben wird, Art. 14 DSGVO)

Die jeweiligen Betroffeneninformationen können anhand einer Vorlage erstellt und erfasst werden. Als gesonderte Information ist die Datenschutzerklärung der Website erfasst. Die Pflege der Informationen ist eine kontinuierliche Aufgabe, da Verarbeitungsvorgänge regelmäßig Veränderungen unterliegen. Die Verarbeitungsverantwortlichen haben daher regelmäßig die ihnen zugeordneten Informationen zu überprüfen.

Neben den separaten Betroffeneninformationen können Verweise auf die Betroffeneninformationen oder gezielte Informationen zu einer bestimmten Verarbeitung Bestandteil von AGB (Allgemeinen Geschäftsbedingungen), Angebotstexten oder Nutzungshinweisen sein. Diese werden von den Verarbeitungsverantwortlichen in Verantwortung der jeweils zuständigen Unternehmensbereiche gepflegt und nicht im DSMS erfasst. Diesbezügliche Abstimmungen und Vorgänge können jedoch von den Datenschutzbeauftragten oder Datenschutzkoordinatoren unter den Datenschutzvorgängen erfasst werden.

4.2.4 Auftragsverarbeitung

Die Datenverarbeitung erfolgt heute zunehmend nicht mehr allein durch die verantwortliche Stelle. Vielfach werden Verarbeitungsprozesse an Dritte als Dienstleister ausgelagert. Innerhalb von Konzernen werden häufig Tochtergesellschaften mit der zentralen IT-Betreuung und -Bereitstellung, der Personalverwaltung, Buchhaltung, Marketingaktivitäten oder Logistik für die gesamte Konzerngruppe beauftragt. Der aktuelle Trend zur Auslagerung von IT-Aufgaben wird durch die Public Cloud markiert. Eine solche Verlagerung von

Infrastruktur bis hin zu Software-as-a-Service-Angeboten betrifft häufig auch die Verarbeitung personenbezogener Daten. Die Daten sollen aber bei ausgelagerter Verarbeitung genauso geschützt werden, wie dies bei der verantwortlichen Stelle gefordert ist.

Das Datenschutzrecht hat diesen Umstand durch die Regelung der Auftragsverarbeitung (ehemals in Deutschland unter dem Begriff der Auftragsdatenverarbeitung bekannt) in Art. 28 DSGVO geregelt. Dabei nimmt die Datenschutz-Grundverordnung den Auftragsverarbeiter stärker in die Pflicht, als es noch beim früheren Bundesdatenschutzgesetz der Fall war. Eine Auftragsverarbeitung liegt vor, wenn der Auftragsverarbeiter im Auftrag des Verantwortlichen personenbezogene Daten verarbeitet und dabei weisungsgebunden ist. Auftragsverarbeitungen sind sowohl außerhalb des eigenen Unternehmens als auch zwischen den verschiedenen rechtlichen Einheiten eines Konzerns möglich. Dabei ist der Auftragsverarbeiter und Auftragnehmer unabhängig vom Auftraggeber und dessen Auftrag, Datenschutzpflichten zu erfüllen (bspw. eigenes Verarbeitungsverzeichnis, eigene Pflichten und Verantwortung bei der Unterbeauftragung). Bei der Auftragsverarbeitung bleibt der Auftraggeber Verantwortlicher für den gesamten Verarbeitungsprozess – auch für die beim Auftragnehmer verarbeiteten Daten. Voraussetzung hierfür ist, dass der Auftragnehmer die Daten nicht für eigene Zwecke verarbeitet und einer engen Weisungsbindung des Auftraggebers unterliegt. Die Rechte des Betroffenen, bspw. auf Auskunft, Berichtigung oder Löschung, richten sich weiter gegen den Auftraggeber und Verantwortlichen. Der Auftragsverarbeiter gilt nicht als Dritter, sondern als Teil der verantwortlichen Stelle (Art. 4 Nr. 10 DSGVO). Die Vorschriften zur Auftragsverarbeitung gelten nicht nur innerhalb der Europäischen Union, sondern bereits, wenn die Verarbeitung einen Zusammenhang mit Tätigkeiten einer Niederlassung in der Europäischen Union aufweist. Nach der in Deutschland vorherrschenden Auffassung benötigt die verantwortliche Stelle keine weitere Rechtsgrundlage, um die personenbezogenen Daten an den Auftragsverarbeiter weiterzugeben.

4.2.5 Auftragsverarbeitungsvertrag

Grundsätzlich hat die Verarbeitung durch den Auftragsverarbeiter gem. Art. 28 Abs. 3 DSGVO auf Grundlage eines Vertrags (sog. Auftragsverarbeitungsvertrag) oder eines anderen Rechtsinstruments zu erfolgen […]. Darüber hinaus regelt Art. 28 Abs. 3 DSGVO die dafür erforderlichen Mindestvoraussetzungen. Enthalten sein müssen Gegenstand und Dauer, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen. Dazu gehören unter anderem das Weisungsrecht des Auftraggebers, die Verpflichtung, bearbeitende Personen

zur Vertraulichkeit zu verpflichten, die Umsetzung der Betroffenenrechte, Unterauftragsverhältnisse, Nachweis-, Kontroll- und Besichtigungsrechte des Auftraggebers und die Abwicklung bei Vertragsende (vgl. Art. 28 Abs. 3 S. 2 DSGVO). Gegenstand des Vertrags hat somit die Verpflichtung des Auftragverarbeiters zum Ergreifen angemessener technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO zu sein (vgl. Art. 28 Abs. 1 DSGVO), genauso wie die vertragsgemäße Unterstützung des Verantwortlichen bei dessen Einhaltung der Verpflichtung zu Umsetzung technischer und organisatorischer Maßnahmen sowie zur Behandlung von Datenschutzvorfällen.

Der Anwendungsbereich der Auftragsverarbeitung schließt auch Unterauftragnehmer ein. Dabei handelt es sich üblicherweise um Subunternehmer des Auftragsverarbeiters. Der Unterschied zum Auftragsverarbeiter besteht darin, dass zwischen dem Verantwortlichen und dem Unterauftragnehmer kein Vertragsverhältnis besteht. Unter Dienstleistungen von Unterauftragnehmern fallen bspw. Fernwartungen und sämtliche Formen der Systembetreuung vor Ort. Auch wenn hierbei Daten nur beiläufig zur Kenntnis genommen und nicht aktiv verarbeitet werden, bestehen Gefährdungen und sind datenschutzrechtliche Schutzmaßnahmen umzusetzen.

Im Auftragsverarbeitungsvertrag sind für die Tätigkeiten vor Ort technische und organisatorische Maßnahmen zu vereinbaren, die für die Systeme in der Hand des Dienstleisters gelten, mit denen ein Zugriff erfolgt. Diese zu dokumentieren, ist eine eigenständige Verpflichtung aus Art. 5 Abs. 2 (Rechenschaftspflicht) und Art. 32 DSGVO. Um als Verantwortlicher seine DSGVO-Erfüllung bei der Auftragsverarbeitung nachweisen zu können, ist eine Aufnahme wesentlicher Maßnahmen in den Vertrag dennoch wie bislang zu empfehlen. Solche Vereinbarungen, bspw. zum Zugangs- und Zugriffsschutz, beziehen sich dann u. a. auf Notebooks oder Datenspeicher, die der Dienstleister für seine Arbeiten mitbringt. Selbstverständlich müssen auch von der verantwortlichen Stelle Sicherheitsmaßnahmen gegenüber den Wartungstechnikern ergriffen werden. Der Zugriff auf Bestände mit personenbezogenen Daten ist nach Möglichkeit zu entziehen oder mindestens nach dem Need-to-know-Prinzip zu begrenzen. Werden Remote-Zugriffe verwendet, ist festzulegen, mit welchen Systemen über welche Schnittstellen zugegriffen wird und wie der Transfer geschützt wird. Besondere Bedeutung hat die Kontrolle und Nachvollziehbarkeit der Remote-Zugriffe. Regelmäßig ist eine Freigabe durch den Auftraggeber pro Zugriff und eine möglichst revisionssichere Protokollierung der Tätigkeit, wenigstens aber eine Vereinbarung zur Dokumentation der Zugriffe zu fordern.

4.2.6 Grenzen der Auftragsverarbeitung

Eine Grenze findet die Anwendung der Auftragsverarbeitung, wenn Teile der Verarbeitung durch den Dienstleister für dessen eigene Interessen stattfinden, bspw. bei konzernweiten Auswertungen der von den Tochtergesellschaften weitergegebenen personenbezogenen Daten. In diesem Fall findet neben der Auftragsverarbeitung eine Übermittlung statt. Die Übermittlung darf aber nur erfolgen, wenn sie datenschutzrechtlich zulässig ist, bspw. als im Rahmen der Arbeitsaufgaben des betroffenen Mitarbeiters erforderliche Übermittlung. Kritisch ist eine Auftragsverarbeitung zu bewerten, wenn Träger von Berufsgeheimnissen dadurch geschützte Informationen Dritten offenbaren (§ 203 StGB). Hier hat sich die Rechtslage durch die Ergänzung des § 203 StGB in Absatz 3 und 4 ebenfalls im Jahr 2018 geändert. Existierte zuvor ein erhebliches Rechtsrisiko und wenigstens eine ausgeprägte Grauzone bei der Auslagerung, sind nun Voraussetzungen für die Beauftragung von Dienstleistern mit möglichem Einblick geregelt, und diese ist nun rechtskonform möglich. Der Dienstleister wird durch die Gesetzesänderung jedoch in die Strafbarkeit nach § 203 StGB mit einbezogen, das Zeugnisverweigerungsrecht und damit ebenfalls die Abwehr von Beschlagnahmungen von Daten werden auch auf ihn erstreckt.

4.2.7 Technische und organisatorische Maßnahmen (TOM)

Um den Anforderungen der Datenschutz-Grundverordnung zu entsprechen, haben verantwortliche Stellen und Auftragsverarbeiter für ihre Datenverarbeitungen gemäß Erwägungsgrund 78 der DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen zum Schutz der Rechte und Freiheiten der Betroffenen zu treffen. Um Nachweispflichten nachzukommen, sollten interne Strategien festgelegt und Maßnahmen ergriffen werden, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) entsprechen. Zentrale Vorschrift ist Art. 32 DSGVO, der die individuelle Abwägung des Verantwortlichen und deren Nachvollziehbarkeit in den Vordergrund stellt. Unter dem Gesichtspunkt der Maßnahmen beschränkt sich die Datenschutz-Grundverordnung darauf, einige Maßnahmenarten und Mittel exemplarisch hervorzuheben. Dies betrifft die Pseudonymisierung und Verschlüsselung sowie den Verfügbarkeitsschutz im Sinne einer schnellen Wiederherstellbarkeit von Daten nach Zwischenfällen. Im Übrigen haben sich die Maßnahmen an der Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und Dienste zu orientieren. Es wird also auf die klassischen Informationssicherheitsziele Bezug genommen.

Als Ergänzung fordert Art. 32 DSGVO ein Verfahren zur regelmäßigen Evaluierung der getroffenen Maßnahmen. Hinsichtlich der tatsächlich zu erfüllenden Anforderungen ist die Datenschutz-Grundverordnung damit deutlich weniger konkret gestaltet worden. Aus diesem Grund bietet sich weiterhin die Orientierung an den bisherigen Anforderungsinhalten an, die durch § 9 BDSG a. F. und seine Anlage etabliert wurden.

Es haben sich die folgenden Maßnahmen etabliert, welche die verantwortlichen Stellen und Auftragsverarbeiter ergreifen sollten:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Zweckbindung durch Datentrennung

Die **Zutrittskontrolle** soll Unbefugten den »physischen« Zutritt zu den Datenverarbeitungsanlagen verwehren. Da zu den Datenverarbeitungsanlagen nicht nur die Server des Unternehmens gehören, sondern auch die einzelnen Clients und Terminals, ist nicht nur für den Zutrittsschutz des Serverraums zu sorgen, sondern auch sicherzustellen, dass Rechnerarbeitsplätze innerhalb der verantwortlichen Stelle nicht durch Unbefugte erreicht werden können. Ein weiterer Aspekt der Zutrittskontrolle ist die Einblicksverhinderung, sodass Unbefugte oder Dritte Bildschirme von Rechnerarbeitsplätzen nicht beobachten können.

Die **Zugangskontrolle** soll die unbefugte Nutzung der Datenverarbeitungsanlagen verhindern. Im Rahmen der Zugangskontrolle ist der Zugang zu Arbeitsplatzrechnern, Mobilgeräten und Datenträgern an die Identifikation zugelassener Nutzer zu knüpfen. Teil der Sicherheitsanforderungen ist es, den Zugriff auf personenbezogene Daten auf denjenigen Personenkreis einer verantwortlichen Stelle zu beschränken, dessen Aufgaben den Zugriff erfordern. So muss bspw. in praktisch jeder verantwortlichen Stelle der Zugriff auf die Daten der Personalverwaltung so beschränkt werden, dass er nur den Mitarbeitern der Personalabteilung möglich ist.

Die **Zugriffskontrolle** dient dazu, Berechtigungen und Berechtigungsgrenzen zu definieren, umzusetzen und zu kontrollieren. Besonderes Augenmerk gebührt hierbei der Archivierung personenbezogener Daten, etwa zur Erfüllung von

Aufbewahrungs- und Dokumentationspflichten, bspw. nach den Regeln der AO. Nach § 35 Abs. 3 BDSG sind diese Daten zu sperren, sobald sie für ihre anderen Verarbeitungszwecke nicht mehr erforderlich sind und nur noch aufbewahrt werden müssen. Die Sperrung bedeutet, dass die weitere Verwendung nur noch für solche Personen möglich sein darf, die Aufgaben mit Archivbeständen erfüllen, sie also z. B. steuerlich prüfen. Zur Zugriffskontrolle gehört auch der allgemeine Schutz vor unbefugtem Lesen, Kopieren, Ändern oder Entfernen der personenbezogenen Daten, also bspw. der Schutz vor Hackern.

Die **Weitergabekontrolle** hat zum einen den Schutz der Daten bei jeder Form des Datentransports vor unbefugten Zugriffen zu gewährleisten, sowohl intern als auch an Dritte oder Auftragnehmer. Zum anderen ist sicherzustellen, dass jederzeit geprüft werden kann, an welche Stellen Übermittlungen vorgesehen sind. Die Weitergabekontrolle ist nicht auf die automatisierte Datenverarbeitung beschränkt, sondern fordert auch den Schutz anderer Medien, bspw. Papierakten. Vor allem bezüglich des internen Austauschs personenbezogener Daten ergeben sich zwangsläufig Überschneidungen mit Zielen und Maßnahmen der Zugriffskontrolle, da hier lediglich der Ausgangspunkt unterschiedlich ist: Für die Zugriffskontrolle steht die Authentifizierung und Berechtigung im Vordergrund, für die Weitergabekontrolle der Schutz bei Transport und Übertragung.

Die **Eingabekontrolle** soll die Nachvollziehbarkeit der Eingabe, Veränderung oder Entfernung personenbezogener Daten in den Datenverarbeitungssystemen gewährleisten. Sie bedingt damit eine Protokollierung der Änderungen an personenbezogenen Daten. Diese Protokolleinträge enthalten in der Regel nicht nur personenbezogene Daten der Betroffenen, deren Daten geändert werden, sondern auch über die Benutzer, die Aktionen durchgeführt oder Ereignisse ausgelöst haben. Handelt es sich dabei um Beschäftigte einer verantwortlichen Stelle, sind solche Daten häufig zur Überwachung von Mitarbeitern oder zu Leistungskontrollen geeignet. Damit unterliegen die Aufzeichnungen der Mitbestimmung (§ 87 Abs. 1 BetrVG[7]). Gleichzeitig sind auch die einschlägigen Datenschutzvorschriften anzuwenden. Dies gilt insbesondere für den Grundsatz der Zweckbindung, Datenminimierung und Speicherbegrenzung. Für Protokolle ist daher in besonderem Maße Datensparsamkeit und eine kurzfristige Auswertung geboten. Die Kriterien der Auswertung ergeben sich aus den vor der Aufzeichnung bestimmten Zwecken. Aus den zulässigen Auswertungszielen ergeben sich der notwendige Umfang der Protokollierung, der Rhythmus der Auswertung und die Speicherdauer für Protokolldaten ohne Auffälligkeiten. Ein Aufzeichnen ohne solche Vorgaben ist in der Regel als Vorratsdatenspeicherung zu qualifizieren und nach BDSG nicht zulässig. Der Umfang der Protokolldaten muss auch verhältnismäßig zum Auswertungsziel sein. Daher ist eine

umfassende Protokollierung oder eine lange Speicherdauer mit der Begründung, man wolle Unregelmäßigkeiten aufklären können, kritisch zu hinterfragen. In der Regel bietet es sich an, den Umfang der Protokollierung mit dem betrieblichen Datenschutzbeauftragten und der Beschäftigtenvertretung abzustimmen und zu dokumentieren.

Die **Auftragskontrolle** folgt als Pflicht direkt aus Art. 28 DSGVO. Dieser erfordert, dass die personenbezogenen Daten beim Auftragnehmer nur den Anweisungen entsprechend verarbeitet werden können. Es ist also sicherzustellen, dass die Weisungsbindung sowohl technisch als auch organisatorisch abgesichert ist.

Die **Verfügbarkeitskontrolle** beinhaltet die Forderung, eine angemessene Datensicherung sicherzustellen, um die Daten gegen zufällige Zerstörung oder Verlust zu schützen.

Ziele der **zweckorientierten Datentrennung** sind im Falle der Auftragsverarbeitung die Trennung von Daten verschiedener Auftraggeber bei einem Auftragnehmer. Nur dadurch können Weisungen jeweils unabhängig von den Weisungen anderer Auftraggeber umgesetzt werden. Außerdem müssen Einblicke der Auftraggeber in die jeweils anderen Datenbestände wirksam verhindert werden. Die Forderung ist ebenso auf die interne Verarbeitung anzuwenden. Sie fordert die Trennung von Daten verschiedener interner Verfahren, die unterschiedlichen Zwecken dienen und daher u. a. auch unterschiedlichen Berechtigungen unterliegen. Maßnahmen zu dieser Forderung sind gegebenenfalls auch beim Auftragnehmer zu realisieren.

Zusammengefasst bilden die Vorgaben des Anhangs zu § 9 BDSG a. F. die wohl am weitesten ins Detail gehende gesetzliche Regelung zu Informationssicherheitspflichten. Es handelt sich dabei aber nicht um eine abschließende Liste, mit der sämtlichen Pflichten Rechnung getragen wird. Spezifische Aspekte der Datenverarbeitung, bspw. besondere Risiken, können weitere Maßnahmen außerhalb des Katalogs erfordern. So könnten bspw. auf die Mitarbeiter gerichtete Sicherheitsmaßnahmen notwendig oder der Verzicht auf Auftragsverarbeitung angebracht sein. Die Forderungen im Anhang bestimmen auch keine tatsächlich zu ergreifenden Maßnahmen und deren Angemessenheit. Hierfür ist auf die gängigen technischen Standards oder Best-Practice-Lösungen der Informationssicherheit zurückzugreifen.

Neben den technischen und organisatorischen Maßnahmen hat die Meldung und Aufklärung von Datenschutzvorfällen durch Art. 33 DSGVO an Bedeutung gewonnen. Dieser regelt eine innerhalb von 72 Stunden zu erfüllende Meldepflicht an die Aufsichtsbehörde, soweit die Verletzung des Schutzes der personenbezogenen Daten ein hohes Risiko für den Betroffenen zur Folge hat.

Zu melden sind eine Beschreibung des Ereignisses, insbesondere der betroffenen personenbezogenen Daten, die Zahl der Betroffenen und die der Datensätze. Die wahrscheinlichen Folgen sind darzustellen, ebenso die ergriffenen und vorgeschlagenen Maßnahmen zur Schadensbegrenzung. Durch die enge Meldefrist von 72 Stunden bleibt dem Verantwortlichen wenig Zeit zur Vorfallsanalyse, geregelte Melde- und Analyseprozesse sind hier praktisch zwingend erforderlich.

4.2.8 Gemeinsame Verantwortlichkeit

Die gemeinsame Verantwortlichkeit für die (Daten-)Verarbeitung ist die rechtliche Bezeichnung für »digitale Arbeitsteilung«, die keine Auftragsverarbeitung ist. Im Gegensatz zur Auftragsverarbeitung sind bei der gemeinsamen Verantwortlichkeit mindestens zwei oder mehr Verantwortliche für die Festlegung der Zwecke und Mittel der Verarbeitungstätigkeit zuständig (Art. 26 Abs. 1 S. 1, Art. 4 Abs. 7 DSGVO).

Hintergrund der Regelungen nach Art. 26 DSGVO ist, dass es für Betroffene und Aufsichtsbehörden auf einen Blick klar sein soll, wer Verantwortlicher ist. Sind nämlich mehrere Stellen gemeinsam für die Verarbeitung verantwortlich, müssen die Ausgestaltung und die Rechtsfolgen für die gemeinsame Verantwortlichkeit festgelegt sein.

Die beteiligten Verantwortlichen legen miteinander die Zwecke und Mittel der Verarbeitung fest und werden dadurch zu gemeinsam Verantwortlichen, sogenannten »joint controllers«. Ausreichend für die gemeinsame Verantwortlichkeit ist nicht, dass sie gemeinsam nur ein Mittel festlegen. Die beteiligten Verantwortlichen haben in einer Vereinbarung festzuhalten, welcher der an der Verarbeitungstätigkeit Beteiligten welchen Verpflichtungen aus der Datenschutz-Grundverordnung nachkommt; dies gilt insbesondere für die Wahrnehmung der Betroffenenrechte.

4.2.9 Drittstaatentransfer von personenbezogenen Daten

Besondere Probleme wirft die Beauftragung von Dienstleistern (Auftragsverarbeiter) außerhalb der Europäischen Union und außerhalb der Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum auf. Der Auftraggeber oder der Verantwortliche einer Übermittlung hat hierbei ein angemessenes Datenschutzniveau sicherzustellen.

Es gibt verschiedene Möglichkeiten, das angemessene Datenschutzniveau durch den Datenexporteur sicherzustellen.

4.2.10 Angemessenheitsbeschluss (Art. 45 DSGVO)

Die einfachste Möglichkeit ist gegeben, wenn für den Drittstaat ein sog. Angemessenheitsbeschluss der Europäischen Kommission gem. Art. 45 DSGVO existiert.

Derzeit existieren Angemessenheitsbeschlüsse für die Übermittlung personenbezogener Daten in folgende Drittländer:

- Andorra
- Argentinien
- Kanada
- Färöerinseln
- Guernsey
- Israel
- Isle of Man
- Japan
- Jersey
- Neuseeland
- Republik Korea (Südkorea)
- Schweiz
- Uruguay
- Vereinigtes Königreich

4.2.11 Vorliegen geeigneter Garantien (Art. 46 DSGVO)

Datenübermittlungen in Drittstaaten sind auch dann zulässig, wenn der Verantwortliche oder der Auftragsverarbeiter für geeignete Garantien zur Gewährleistung des angemessenen Datenschutzniveaus gesorgt hat. Dafür kommen die folgenden Möglichkeiten in Betracht:

Verbindliche interne Datenschutzvorschriften, auch Binding Corporate Rules (BCR) genannt, gem. Art. 46 Abs. 2 lit. b, Art. 47 DSGVO, sind vor allem bei international agierenden Konzernen relevant, wenn innerhalb des Konzerns Drittstaaten-Übermittlungen stattfinden. Das Unternehmen legt die Regelungen für den Umgang mit personenbezogenen Daten selbst fest und gewährleistet durch diese Regeln ein Datenschutzniveau, das dem der Datenschutz-Grundverordnung entspricht. Der Mindestinhalt hierfür wird in Art. 47 Abs. 2 DSGVO festgelegt. Betroffene Personen müssen ihre Rechte gegenüber dem Verantwortlichen durchsetzen können. Die BCR werden in einem Kohärenzverfahren nach Art. 47 Abs. 1 DSGVO durch die zuständige

Aufsichtsbehörde genehmigt, sodass nicht mehr die einzelnen Übermittlungen genehmigt werden müssen.

4.2.12 Standarddatenschutzklauseln der Kommission oder einer Aufsichtsbehörde

Bei den Standardvertragsklauseln (Art. 46 Abs. 2 lit. c und d DSGVO) handelt es sich um von der Europäischen Kommission verabschiedete Vertragsmuster. Durch die Verwendung dieser Vertragsklauseln zwischen dem Datenexporteur und dem Datenimporteur wird der europäische Datenschutzstandard vereinbart und sichergestellt. Diese Möglichkeit gab es auch schon vor dem Inkrafttreten der DSGVO, sie wurden jedoch durch das sog. Schrems-II-Urteil (Rechtssache C-311/18) des Europäischen Gerichtshofs vom 16.07.2020[8] ganz erheblich verschärft.

Exkurs: Das Schrems-II-Urteil

Mit dem Schrems-II-Urteil hat der Europäische Gerichtshof (EuGH) den Durchführungsbeschluss zum EU-US Privacy Shield am 16.07.2020 für unwirksam erklärt. Dies hatte zur Folge, dass Datenübermittlungen in die USA nicht mehr durch den Angemessenheitsbeschluss erfolgen konnten und folglich auf andere geeignete Garantien gestützt werden müssen. Hinsichtlich der Verwendung von Standardvertragsklauseln hatte der EuGH entschieden, dass dies zwar weiterhin möglich ist, der Verantwortliche aber zu prüfen hat, ob sichergestellt ist, dass im Drittstaat ein gleichwertiges (Daten-)Schutzniveau gewährleistet ist, damit die Rechte der betroffenen Personen ausreichend geschützt werden. Ist dies nicht der Fall, hat der Verantwortliche zu prüfen, welche zusätzlichen vertraglichen, technischen und organisatorischen Maßnahmen zu ergreifen sind, um ein »im Wesentlichen gleichwertiges Schutzniveau« sicherzustellen. Dabei muss jedoch sichergestellt sein, dass diese Maßnahmen nicht durch die Rechtsordnung des Drittstaates in ihrer Wirksamkeit beeinträchtigt werden. Führen die Schutzmaßnahmen nicht zum gewünschten Erfolg, hat der Datenexporteur von der Datenübermittlung Abstand zu nehmen.

Der Europäische Datenschutzausschuss hat mit den Empfehlungen 01/2020 (Version 2.0 vom 18.06.2021) eine Arbeitshilfe für Verantwortliche und Auftragsverarbeiter mit Beispielen für zusätzliche vertragliche, technische und organisatorische Maßnahmen veröffentlicht.

Im Juni 2021 hat die EU-Kommission dann neue Standardvertragsklauseln veröffentlicht,[9] welche die Rechtsprechung des EuGH berücksichtigen.

Diese modular aufgebauten Standardvertragsklauseln können in den folgenden Konstellationen eingesetzt werden:

- Verantwortlicher an Verantwortlichen
- Verantwortlicher an Auftragsverarbeiter
- Auftragsverarbeiter an (Unter-)Auftragsverarbeiter

- Rückübermittlung des Auftragsverarbeiters in der EU an einen Verantwortlichen im Drittland

Im Falle von Drittstaatentransfers deckt Klausel 14 die Anforderungen des EuGH aus dem Schrems-II-Urteil ab. Der Datenexporteur muss aber dennoch die Rechtslage und Rechtspraxis im Drittstaat prüfen und falls erforderlich zusätzliche Schutzmaßnahmen ergreifen.

Soweit die Standardvertragsklauseln unverändert übernommen werden, muss der Datenexporteur die Datenverarbeitung nicht mehr gesondert genehmigen lassen. Die Vertragspartner können die Standardvertragsklauseln auch in (eigene) umfangreichere Vertragswerke mitaufnehmen. Die weiteren Regelungen dürfen aber weder unmittelbar noch mittelbar im Widerspruch zu den Standardvertragsklauseln stehen und die Grundfreiheiten der Betroffenen nicht beschneiden. Unproblematisch ist es, wenn weitere Module hinzugefügt oder Ergänzungen oder Aktualisierung von Informationen in Anlagen vorgenommen werden. Für weitere Informationen zur Datenschutz-Folgenabschätzung siehe Abschnitt 4.2.1.

4.2.13 Löschregeln

Der Verantwortliche hat dafür Sorge zu tragen, dass die verarbeiteten Daten nach Erreichung des Zwecks gelöscht oder anderweitig vernichtet werden. Zu den rechtlichen Vorgaben für die Löschung und zum Vorgehen bei der Definition von Löschregeln siehe Kapitel 25. Die Umsetzung von Löschmaßnahmen führt Kapitel 24 zum technischen Löschen und Vernichten aus.

4.3 Datenschutz-Vorgänge

Die Datenschutz-Vorgänge beschreiben Abläufe und Verfahren des DSMS, die für die Einhaltung der datenschutzrechtlichen Vorschriften erforderlich sind.

4.3.1 Datenschutzverpflichtung

Grundsätzlich sind alle Beschäftigten einer verantwortlichen Stelle, die personenbezogene Daten verarbeiten, auf Vertraulichkeit zu verpflichten (Art. 28 Abs. 3 lit. b DSGVO). Dabei bleibt die Verpflichtung über die Dauer der Tätigkeit im Unternehmen hinaus bestehen. Wirken Beschäftigte an der Erbringung von Telekommunikationsdienstleistungen mit, sind sie zusätzlich auf das Telekommunikationsgeheimnis zu verpflichten.[10] Ein unterzeichnetes Exemplar der jeweiligen Verpflichtung ist in die jeweilige Personalakte aufzunehmen.

4.3.2 Datenschutzschulung

Neu angestellte Beschäftigte sowie Auszubildende, in deren Aufgabenbereich die Verarbeitung personenbezogener Daten fällt, sollten vor Tätigkeitsbeginn von der Personalabteilung auf das Datengeheimnis verpflichtet werden. Die unterzeichnete Verpflichtungserklärung ist anschließend zur Dokumentation in die Personalakte zu übernehmen. Zudem sollte ihnen die im Unternehmen geltende Datenschutzrichtlinie sowie das Handout zur Datenschutzschulung als schriftliche Unterweisung ausgehändigt werden.

Innerhalb des ersten Jahres ihrer Tätigkeit sollten alle Mitarbeiterinnen und Mitarbeiter, die personenbezogene Daten verarbeiten, an einer Datenschutzschulung teilnehmen. Über eine Teilnahmeliste ist die Anwesenheit der Beschäftigten zu dokumentieren. Die Kenntnisse im Datenschutz sollten spätestens alle drei Jahre durch eine erneute Schulungsteilnahme aufgefrischt werden. Die Schulungen werden in der Regel vom Datenschutzbeauftragten (oder einem von ihm benannten Vertreter) durchgeführt und dokumentiert.

Die verwendeten Schulungsunterlagen und das zugehörige Handout sollten jährlich vom Datenschutzbeauftragten geprüft und erforderlichenfalls aktualisiert werden.

4.3.3 Betroffenenrechte

Die Datenschutz-Grundverordnung gewährt betroffenen Personen gegenüber der verantwortlichen Stelle bestimmte Rechte (sog. Betroffenenrechte). Hierunter fallen:

- Recht auf Auskunft (Art. 15 DSGVO)
- Recht auf Berichtigung (Art. 16 DSGVO)
- Recht auf Löschung (Art. 17 DSGVO)
- Recht auf Einschränkung (Art. 18 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
- Recht auf Widerspruch (Art. 21 DSGVO)
- Recht auf Widerruf der Einwilligung (Art. 7 Abs. 3 DSGVO)
- Recht, keiner automatisierten Entscheidung unterworfen zu werden (Art. 22 DSGVO)
- Beschwerderecht bei der Aufsichtsbehörde (Art. 77 DSGVO i. V. m. § 19 BDSG)

Falls die von den betroffenen Personen angegebenen Daten für eine zuverlässige Identifizierung unzureichend sind, kann die betroffene Stelle von den Betroffenen zusätzliche Nachweise einfordern, die eine Identifizierung

ermöglichen. Dies sollte im Bedarfsfall vor der Beantwortung des entsprechenden Betroffenenersuchens geschehen. Können keine zusätzlichen Nachweise beschafft werden, sollte für die Auskunftserteilung nur eine bereits hinterlegte Adresse verwendet werden. Sofern betroffene Personen einen Antrag elektronisch stellen, ist dieser Form bei der Beantwortung ebenfalls zu entsprechen, sofern dies nicht anders gefordert wird. In Abhängigkeit vom Inhalt der Auskunftserteilung sollte dies jedoch nur nach vorheriger Abstimmung mit dem Betroffenen erfolgen, wenn die elektronische Kommunikation (bspw. E-Mail) nur eine eingeschränkte Kommunikationssicherheit garantieren kann. Für die Beantwortung von Betroffenenersuchen gelten die Fristen nach Art. 12 DSGVO, d. h., die Beantwortung erfolgt grundsätzlich unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang. Falls eine mögliche Fristverlängerung von bis zu zwei weiteren Monaten beansprucht wird – z. B. aufgrund der Komplexität oder des Umfangs der Bearbeitung –, sind die betroffenen Personen darüber inkl. Begründung zu unterrichten.

In den folgenden Unterkapiteln werden die jeweiligen eingehenden Betroffenenrechte näher erläutert.

4.3.4 Auskunft

Bei Auskunftsersuchen ist zwischen Ersuchen der Betroffenen selbst und Ersuchen von Dritten wie bspw. von Familienmitgliedern, Ämtern und Ermittlungsbehörden zu unterscheiden.

4.3.5 Auskunftsersuchen von Betroffenen

Art. 15 DSGVO sieht ein zweistufiges Auskunftsrecht für den Betroffenen vor. Zuerst kann er von der verantwortlichen Stelle eine Bestätigung darüber verlangen, ob personenbezogene Daten zu seiner Person verarbeitet werden. Anschließend hat er das Recht auf Auskunft über diese Daten und diesbezüglich weiterführende Informationen. Zu den Daten sind nach Art. 15 Abs. 1 lit. a – h DSGVO der Zweck, die Datenkategorien, die Empfänger oder Empfänger-Kategorien, die Speicherdauer oder Kriterien zu ihrer Festlegung, die Rechte des Betroffenen (Berichtigung, Löschung, Einschränkung, Beschwerderecht bei einer Aufsichtsbehörde), bei Dritterhebung die Datenquelle sowie ggf. automatisierte Entscheidungsfindungen anzugeben. Werden Daten in Drittstaaten übermittelt, ist das von der Datenschutz-Grundverordnung geforderte Schutzniveau durch geeignete Garantien für einen gleichwertigen Datenschutz nach Art. 44 ff. DSGVO anzugeben. Vorhandene personenbezogene Daten sind als Kopie bereitzustellen. Bei elektronischen Anfragen erfolgt die Beantwortung auch elektronisch, außer der Betroffene wünscht einen anderen

Kommunikationskanal. Wird eine große Datenmenge über den Betroffenen verarbeitet oder erstreckt sich die Datenverarbeitung über einen längeren Zeitraum, müssen nicht sämtliche Daten als Kopien bereitgestellt werden. Vielmehr kann die verantwortliche Stelle eine Präzisierung des Auskunftsersuchens verlangen. Eine Kopie der erteilten Auskunft ist grundsätzlich für zwei Jahre zu Nachweiszwecken aufzubewahren.

4.3.6 Auskunftsersuchen von Dritten sowie von Ämtern und Ermittlungsbehörden

Auskunftsersuchen von privaten Dritten (z. B. Familienangehörigen, Vermietern) dürfen nur beantwortet werden, wenn eine entsprechende Vollmacht des Betroffenen vorliegt. In diesem Fall werden Daten nach dem gleichen Verfahren zur Verfügung gestellt, wie wenn der Betroffene direkt anfragt.

Auskunftsersuchen von Ämtern zu einem Kunden oder Mitarbeiter bzw. dessen Daten dürfen nur nach schriftlicher Anfrage mit Angabe der Rechtsgrundlage für das Auskunftsersuchen beantwortet werden. Ist der Auskunftsanspruch berechtigt, werden die angefragten Daten zusammengestellt und per Brief oder durch verschlüsselte elektronische Kommunikationswege an die anfragende Stelle gesendet. Wird der Auskunftsanspruch als unberechtigt bewertet, wird dies dem Auskunftsersuchenden ebenfalls mitgeteilt.

Auskunftsersuchen der Polizei und der Staatsanwaltschaften können auf die allgemeine Ermittlungsbefugnis nach § 163 StPO und ggf. weitere speziellere Rechtsgrundlagen gestützt werden. Für den Verantwortlichen ergibt sich in diesem Fall die Übermittlungsbefugnis durch das Vorliegen einer rechtlichen Pflicht nach Art. 6 Abs. 1 lit. c DSGVO. In jedem Fall ist aber eine Begründung für das Vorliegen der Rechtsgrundlage zu verlangen und vor Erteilung der Auskunft auf das formelle Ausreichen zu prüfen. Liegt eine benannte Rechtsgrundlage samt plausibler Begründung für Polizei oder Staatsanwaltschaft vor, dann ist die Auskunft zu erteilen. Eine Ausnahme stellen Auskunftsgegenstände dar, die Berufsgeheimnissen wie bspw. der ärztlichen Schweigepflicht unterfallen (§ 203 StGB). In diesen Fällen kann eine Herausgabe nicht verlangt werden; sie bedürfen einer Schweigepflichtentbindung des Betroffenen. Die Entscheidung hat der Berufsgeheimnisträger zu treffen. Etwas anders liegt der Fall, wenn Polizei und Staatsanwaltschaft lediglich informell auf Grundlage ihrer allgemeinen Ermittlungsbefugnis Anfragen stellen, ohne einen Auskunftsanspruch zu haben. Für den Verantwortlichen besteht hier keine rechtliche Pflicht zur Herausgabe der Daten, sodass er eine Auskunft nur auf Grundlage des berechtigten Interesses eines Dritten nach Art. 6 Abs. 1 lit. f DSGVO erteilen kann. Da es sich in diesem Fall lediglich um ein informelles

Ersuchen handelt, muss dieses nicht beantwortet werden. Unabhängig von der Entscheidung werden die Anfrage und Entscheidung immer dokumentiert.

Wird eine Anfrage an eine verantwortliche Stelle als Auftragsverarbeiterin gestellt, so ist der Verantwortliche umgehend über das Ersuchen zu informieren, es sei denn, die verantwortliche Stelle ist selbst Gegenstand der Ermittlungen.

4.3.7 Berichtigung

Gemäß Art. 16 DSGVO können Betroffene von der verantwortlichen Stelle verlangen, die dort verarbeiteten personenbezogenen Daten zu berichtigen, wenn sie unrichtig sind, oder unvollständige Daten zu ergänzen. Sofern eine Berichtigung nicht möglich ist, sind die unrichtigen Informationen zu löschen.

4.3.8 Löschung

Die Datenschutz-Grundverordnung sieht in Art. 17 DSGVO ein Recht auf Löschung für den Betroffenen vor. Der Anspruch auf Löschen kann geltend gemacht werden, wenn einer der in Art. 17 Abs. 1 lit a – f DSGVO genannten Gründe zutrifft:

1. Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
2. Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Art. 6 Abs. 1 lit a oder Art. 9 Abs. 2 lit. a DSGVO stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
3. Die betroffene Person legt gemäß Art. 21 Abs. 1 DSGVO Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor oder die betroffene Person legt gemäß Art. 21 Abs. 2 DSGVO Widerspruch gegen die Verarbeitung ein.
4. Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
5. Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
6. Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DSGVO erhoben.

Die verantwortliche Stelle kann jedoch die Löschung aus den in Art. 17 Abs. 3 lit. a – e DSGVO genannten fünf Gründen verweigern. Denn der Anspruch auf

Löschung gem. Art. 17 Abs. 1 und Abs. 2 DSGVO gilt nicht, soweit die Verarbeitung erforderlich ist

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
- zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem EU-Recht, dem die verantwortliche Stelle unterliegt, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, oder in Ausübung öffentlicher Gewalt, die der verantwortlichen Stelle übertragen wurde;
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Art. 9 Abs. 2 lit. h und i sowie Art. 9 Abs. 3 DSGVO;
- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Art. 39 Abs. 1 DSGVO, soweit das in Abs. 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Hat die verantwortliche Stelle die Daten an Dritte weitergegeben, so hat sie die Empfänger über den geltend gemachten Löschanspruch zu informieren, damit auch diese der Pflicht zur Löschung der Daten nachkommen können.

4.3.9 Einschränkung

Nach Art. 18 DSGVO hat die betroffene Person das Recht, von der verantwortlichen Stelle die Einschränkung der Verarbeitung ihrer personenbezogenen Daten zu verlangen, sofern einer der folgenden vier Gründe zutrifft:

- Die Datenrichtigkeit wird von der betroffenen Person bestritten, die Daten werden so lange gesperrt, bis deren Richtigkeit überprüft werden konnte.
- Die Verarbeitung ist unrechtmäßig erfolgt, jedoch lehnt die betroffene Person eine Löschung ab und fordert stattdessen die Sperrung der Daten.
- Die verantwortliche Stelle benötigt die Daten nicht mehr, jedoch benötigt die betroffene Person diese zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
- Die betroffene Person legt Widerspruch nach Art. 21 DSGVO ein und es ist noch nicht festgestellt, ob die berechtigten Gründe von der

verantwortlichen Stelle gegenüber denen der betroffenen Person überwiegen.

Die verantwortliche Stelle unterrichtet die betroffene Person, bevor die Einschränkung aufgehoben wird.

4.3.10 Datenübertragung

Das Recht des Betroffenen auf Datenübertragbarkeit ergibt sich aus Art. 20 DSGVO. Es besteht bei Vorliegen einer der drei Rechtsgrundlagen für die Verarbeitung, der Einwilligung, bei Vertrag oder bei automatisierten Verfahrungen zur Verarbeitung. Es müssen sämtliche vom Betroffenen selbst für einen Dienst bei der verantwortlichen Stelle bereitgestellten personenbezogenen Daten übertragen werden. In der Regel sind damit die sog. Stammdaten erfasst. Hinzukommen können nach Ausgestaltung des Einzelfalls noch Bestelldaten oder auch Inhaltsdaten bei Cloud-Diensten sowie ggfs. indirekt bereitgestellte Daten, sog. beobachtete Daten, also z. B. Playlists, Werte von (Fitness-)Trackern, Suchlauf, Verkehrsdaten, Standortdaten. Also alle Daten, die wissentlich und willentlich mit bewusstem Zutun der betroffenen Person verarbeitet werden.

Nicht übertragen werden müssen aus Rückschlüssen erzeugte und abgeleitete Daten sowie die Daten Dritter, sog. Drittdaten.

Die Übertragung muss in einem strukturierten, gängigen, maschinenlesbaren Format erfolgen, z. B. CSV, XML, HTML, ODF. Wie für alle anderen Betroffenenrechte gilt auch hier, dass die verantwortliche Stelle keinen Entgeltanspruch gegenüber dem Betroffenen hat, wenn dieser seine Rechte ausübt (Art. 12 Abs. 5 S. 1 DSGVO).

4.3.11 Widerspruch

Betroffene besitzen auch ein Widerspruchsrecht (Art. 21 DSGVO) hinsichtlich der Verarbeitung ihrer personenbezogenen Daten auf der Rechtsgrundlage nach Art. 6 Abs. 1 lit. e DSGVO (Wahrnehmung einer öffentlichen Aufgabe) und lit. f DSGVO (berechtigte Interessen des Verantwortlichen). Dies bedeutet, dass der Betroffene einer solchen Verarbeitung seiner personenbezogenen Daten jederzeit widersprechen kann und der Verantwortliche diese Daten dann nicht bzw. nicht mehr verarbeiten darf.

Ausnahme hiervon ist, dass der Verantwortliche zwingende schutzwürdige Gründe geltend machen kann, die gegenüber dem Interesse der betroffenen Person überwiegen. Bei der vorzunehmenden Interessenabwägung hat der

Verantwortliche auch immer die konkrete Situation der betroffenen Person zu berücksichtigen.

4.3.12 Datenschutzvorfälle

Gemäß Art. 33 DSGVO sind Vorfälle, bei denen es zu einer Verletzung des Schutzes personenbezogener Daten gekommen ist, binnen 72 Stunden unverzüglich nach Bekanntwerden von der verantwortlichen Stelle an die zuständige Aufsichtsbehörde zu melden, es sei denn, die Verletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen. Die Meldung muss eine Beschreibung der Art der Verletzung, der ungefähren Zahl der Betroffenen, die Kontaktdaten des DSB, eine Beschreibung der wahrscheinlichen Folgen und der von der verantwortlichen Stelle ergriffenen Maßnahmen zur Behebung der Verletzung bzw. zur Minderung der nachteiligen Auswirkungen umfassen.

Sofern bei einer Verletzung des Schutzes personenbezogener Daten für den Betroffenen voraussichtlich ein hohes Risiko für seine persönlichen Rechte und Freiheiten entsteht, benachrichtigt der Verantwortliche den Betroffenen unverzüglich von der eingetretenen Verletzung. Eine Benachrichtigung kann entfallen, wenn eine der Bedingungen nach Art. 34 Abs. 3 DSGVO erfüllt ist:

- Es wurden durch den Verantwortlichen geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen, die auf die Verletzung angewendet wurden (insbes. das Unzugänglichmachen, etwa durch Verschlüsselung).
- Der Verantwortliche hat durch nachfolgende Maßnahmen sichergestellt, dass das hohe Risiko für die betroffene Person nach Art. 34 Abs. 1 DSGVO nicht mehr besteht.
- Sie wäre mit einem unverhältnismäßigen Aufwand verbunden. In diesem Fall hat eine öffentliche Bekanntmachung oder vergleichbare Maßnahme zu erfolgen, um der Benachrichtigung nachzukommen.

Nach erfolgter Risikobetrachtung mit Entscheid »hohes Risiko« und, sofern kein Grund zur Nicht-Benachrichtigung nach Art. 34 Abs. 3 DSGVO vorliegt, erfolgt die Benachrichtigung des Betroffenen. Die hier abrufbare Vorlage beinhaltet ein Schreiben nach Art. 34 Abs. 2 DSGVO.

Die folgenden Seiten enthalten die Dokumentation aller erfassten (und ggf. an die Aufsichtsbehörde gemeldeten) Datenschutzvorfälle sowie die zugehörige Kommunikation mit der Aufsichtsbehörde.

4.3.13 Whistleblower-Richtlinie

Nach den Vorgaben der EU-Kommission hätte durch den deutschen Gesetzgeber die sog. Whistleblower-Richtlinie[11] zum 17.12.2021 in deutsches Recht umgesetzt werden müssen. Anders als EU-Verordnungen, die unmittelbar anwendbar sind, müssen EU-Richtlinien in der Regel durch einen Rechtssetzungsakt der nationalen Gesetzgeber in nationales Gesetz umgesetzt werden. Hier konnten sich die im Bundestag vertretenen Parteien nicht auf ein Gesetz zur Umsetzung einigen, was dazu führte, dass die Richtlinie schlicht nicht umgesetzt wurde[12].

Gemäß der EU-Richtlinie werden Personen geschützt, die Verstöße gegen das Unionsrecht in bestimmten Bereichen melden. Dafür müss(t)en die Arbeitgeber, d. h. die Unternehmen oder öffentliche Stellen, soweit sie durch die Richtlinie erfasst werden, Meldewege einrichten, sodass die in der Richtlinie genannten Missstände durch Mitarbeiter gemeldet werden können. Kernelement der Regelungen soll die Schaffung eines antidiskriminierungsrechtlichen Schutzsystems für hinweisgebende und weitere Personen werden, die auch anonyme Meldungen ermöglichen. Dabei soll es sowohl (Unternehmens-) interne als auch staatliche, d. h. externe Meldestellen geben, die die Meldungen dann vertraulich entgegennehmen und angemessene Folgemaßnahmen einleiten. Dabei darf allerdings nicht derjenige außer Acht gelassen werden, der durch eine Meldung betroffen ist, d. h., Meldungen müssen gutgläubig erfolgen. Der Hinweisgebende muss nach Art. 6 Abs. 1 lit. a der Richtlinie hinreichend Grund zur Annahme gehabt haben, dass die gemeldeten Informationen über die Verstöße zum Zeitpunkt der Meldung der Wahrheit entsprochen haben und dass die Informationen auch in den sachlichen Anwendungsbereich der Richtlinie fielen. Dadurch sollen Whistleblower einerseits geschützt, aber andererseits auch die Interessen der betroffenen Personen zum Ausgleich gebracht werden. Hier spielt dann der Datenschutz eine Rolle, nämlich wenn es um die Mitteilung der personenbezogenen Daten der Betroffenen einerseits und andererseits um die Mitteilung personenbezogener Daten von Hinweisgebenden geht, die die Betroffenen fordern könnten, um sich gegen möglicherweise falsche oder böswillige Beschuldigungen, d. h. missbräuchliche Meldungen zur Wehr zu setzen. Dabei hat der Gesetzgeber mit Art. 23 Abs. 1 und 2 DSGVO einen Rahmen erhalten, innerhalb dessen er sich bewegen kann, um dafür Sorge zu tragen, dass die Ziele der Whistleblower-Richtlinie angemessen umgesetzt werden, damit der Schutz der Whistleblower einerseits nicht durch die Ausübung von Informations- und Auskunftsansprüchen gem. Art. 12 ff. DSGVO unterlaufen wird, andererseits aber Betroffenen nicht die Möglichkeit genommen wird, sich gegen falsche Behauptungen zu wehren.

4.3.14 Benennung des Datenschutzbeauftragten

Die Datenschutz-Grundverordnung sieht die Benennung eines Datenschutzbeauftragten vor. Nach Art. 37 Abs. 1 lit. b und c DSGVO muss für nicht öffentliche Stellen ein Datenschutzbeauftragter benannt werden, wenn die Kerntätigkeit des Unternehmens in

- der Durchführung von Verarbeitungen besteht, die eine umfangreiche regelmäßige und systematische Überwachung von Betroffenen erfordern oder
- einer umfangreichen Verarbeitung besonderer personenbezogener Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen bzw. Straftaten besteht.

Darüber hinaus besteht eine Öffnungsklausel in Art. 37 Abs. 54 DSGVO, in denen die Mitgliedstaaten die Möglichkeit haben, die Ausgestaltung der Benennung zu ergänzen. Der deutsche Gesetzgeber hat hiervon mit § 38 BDSG Gebrauch gemacht. Demnach ist die Benennung eines Datenschutzbeauftragten erforderlich, wenn

- i. d. R. mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind und
- unabhängig von der Anzahl mit der Verarbeitung personenbezogener Daten beschäftigter Mitarbeiter
    - Verarbeitungen vorgenommen werden, die einer Datenschutz-Folgenabschätzung unterliegen oder
    - personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- und Meinungsforschung verarbeitet werden.

Die Schriftlichkeit der Benennung ist nach der Datenschutz-Grundverordnung nicht gefordert; sie dient allerdings der Erfüllung der Nachweispflichten nach Art. 24 DSGVO.

Der Datenschutzbeauftragte hat die Aufgabe, die Rechtskonformität der im Unternehmen stattfindenden Verwendung personenbezogener Daten zu überwachen. Er berät die Geschäftsführung in Datenschutzfragen, sensibilisiert die Beschäftigten in Datenschutzfragen und wirkt bei der datenschutzkonformen, datensparsamen Gestaltung neuer Verfahren der automatisierten Datenverarbeitung mit. Der Datenschutzbeauftragte ist in seiner Tätigkeit weisungsfrei und zur Verschwiegenheit verpflichtet (Art. 37 ff. DSGVO, §§ 5 f., 38 BDSG). Er ist dem Leiter der verantwortlichen Stelle unmittelbar zu

unterstellen und genießt dank §§ 38 Abs. 2, 6 Abs. 4 BDSG nach deutschem Recht auch weiterhin Kündigungsschutz.

Die Pflicht zur schriftlichen Bestellung des Datenschutzbeauftragten knüpft in Deutschland für nicht öffentliche Stellen nach wie vor an die Beschäftigtenzahl an. Die Pflicht besteht, sobald mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten befasst sind oder sobald eine verantwortliche Stelle personenbezogene Daten in einer besondere Risiken für die Betroffenen begründenden Art und Weise verarbeitet.

Damit der Datenschutzbeauftragte seine Aufgaben wahrnehmen kann, muss die verantwortliche Stelle ihn ausreichend mit Ressourcen ausstatten. Sie muss ihm ein Verzeichnis der Verfahren zur Verfügung stellen, in denen personenbezogene Daten verwendet werden. Der Datenschutzbeauftragte muss derart in die Prozesse der Stelle eingebunden sein, dass er geeignet auf die Einhaltung von Datenschutzvorschriften hinwirken kann. Beispielsweise muss er dazu rechtzeitig in Prozesse zur Systementwicklung eingebunden werden. Sinnvoll ist in der Regel auch, dass der Datenschutzbeauftragte an der Beantwortung von Auskunftsersuchen beteiligt wird.

Während der Informationssicherheitsbeauftragte lediglich in verschiedenen Standards, vgl. hierzu Kapitel 7 zum IT-Grundschutz, Erwähnung findet, hat der betriebliche Datenschutzbeauftragte mit Art. 37 ff. DSGVO eine gesetzliche Arbeitsgrundlage. Zwischen dem betrieblichen Datenschutzbeauftragten und dem Informationssicherheitsbeauftragten kann Personalunion bestehen,[13] vorausgesetzt die Gestaltung der Funktionen bedingt nicht, dass der Betreffende in einer der beiden Funktionen seine eigene Tätigkeit in der jeweils anderen Funktion zu überwachen hat. Wie im weiteren Verlauf des Kapitels gezeigt wird, bestehen aber durchaus Zielkonflikte zwischen Maßnahmen für Datenschutz und Informationssicherheit. Daher scheint eine Rollentrennung grundsätzlich geboten.

4.3.15 Audits

Die Durchführung von Audits soll die Umsetzung der datenschutzrechtlichen Vorgaben und die Wirksamkeit und Effizienz von Datenschutzmanagementsystemen (DSMS) sicherstellen. Dabei ermittelt der Auditor den Ist-Zustand und vergleicht diesen mit dem zuvor definierten Soll-Zustand. Der Soll-Zustand kann sich dabei sowohl aus gesetzlichen Vorgaben wie der Datenschutz-Grundverordnung ableiten oder direkt aus dem Gesetz resultieren. Werden nach der Durchführung des Audits Abweichungen des Ist-Zustands vom Soll-Zustand festgestellt, so kann der Auditor Abhilfemaßnahmen vorschlagen.

Auch bei der Einführung bzw. dem Aufbau eines DSMS muss der Ist-Zustand des Datenschutzes in einem Unternehmen, praktisch als Bestandsaufnahme, evaluiert werden. Hierdurch kann sich der Verantwortliche den notwendigen Überblick über stattfindende Datenverarbeitungen verschaffen und geschaffene Datenschutzkonzepte zur Umsetzung bringen.

In der Datenschutz-Grundverordnung findet sich dieser Ansatz allerdings nicht unmittelbar wieder, sondern ergibt sich aus der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO. Der Verantwortliche hat die Einhaltung der Datenschutz-Grundsätze gem. Art. 5 Abs. 1 DSGVO nachzuweisen. Auch an anderen Stellen in der DSGVO finden sich noch Nachweispflichten, insbesondere bei der Erfüllung von Datenschutzsicherheitsmaßnahmen.

4.3.16 Kontinuierliche Umsetzungsverpflichtung der Sicherheit der Verarbeitung

Mit den Anforderungen aus Art. 32 DSGVO zur Sicherheit der Verarbeitung ergibt sich eine kontinuierliche Umsetzungsverpflichtung der Sicherheit der Verarbeitung, d. h. der regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung dieser. Zur Überprüfung der technischen und organisatorischen Maßnahmen gehört auch der Nachweis für die Compliance des Verantwortlichen im Sinne von Art. 24 Abs. 3 DSGVO und des Auftragsverarbeiters gemäß Art. 28 Abs. 5 DSGVO. Verantwortliche und Auftragsverarbeiter müssen dafür Sorge tragen, dass das angemessene Sicherheitsniveau ständig gewährleistet wird. Hierzu sind Verfahren zu etablieren, die dies sicherstellen. Dabei bestehen sehr starke Überschneidungen zu den Informationssicherheitsmanagementsystemen.

Es gibt in der Datenschutz-Grundverordnung keine vorgegebenen Zeitintervalle, nach denen Audits durchzuführen sind. Es muss jedoch sichergestellt sein, dass der Nachweis (Art. 5 Abs. 2 DSGVO) der Erfüllung des Art. 32 DSGVO gelingt. Folglich bestimmen sich die Häufigkeit und der Detaillierungsgrad der Überprüfung nach der Höhe des Risikos und der Höhe des angemessenen Schutzniveaus.

4.3.17 Datenschutzaudit

Bei einem Datenschutzaudit handelt es sich um eine freiwillige Analyse und Prüfung bzgl. der Einhaltung des Datenschutzes innerhalb eines Unternehmens. Prüfungsgegenstand können dabei das Datenschutzmanagementsystem (DSMS), die datenverarbeitenden Vorgänge, interne Richtlinien,

Betriebsvereinbarungen und Verträge darstellen. Das Audit dient als Grundlage für die Schaffung und Entwicklung langfristiger Datenschutzstrategien. Es kann sowohl zur Verbesserung des Datenschutzmanagements als auch bestehender Betriebsabläufe beitragen.

Vorgaben, wie Datenschutz-Audits abzulaufen haben, macht die Datenschutz-Grundverordnung nicht. Es ist Sache des Verantwortlichen, seiner Rechenschaftspflicht nachzukommen, bspw. durch interne oder externe Audits. Das Datenschutzaudit kann deshalb sowohl intern als auch extern stattfinden, d. h., der Verantwortliche kann auch einen externen Auditor beauftragen, ein Datenschutzaudit durchzuführen. Im Bereich der Informationssicherheit sind solche Audits längst etabliert, weshalb es naheliegt, sich hier an diesen etablierten Mechanismen zu orientieren, vgl. hierzu Kapitel 3 zu Informationssicherheit und rechtliche Anforderungen.

Bei internen Audits bietet es sich an, dass der Datenschutzbeauftragte die Rolle des Auditors übernimmt, da er in gewissem Maße über die notwendige Unabhängigkeit und das notwendige Fachwissen verfügt.

4.3.18 Self Assessment

In Abgrenzung zu den internen Audits sind sog. Self Assessments Überprüfungen, die die jeweiligen Fachabteilungen selbst durchführen.[14] Die Fachabteilungen prüfen die im vorigen Abschnitt genannten Datenschutzgrundsätze anhand von Fragebögen oder Checklisten, die ihnen bspw. durch das Datenschutzmanagementsystem bei der Einführung neuer Verarbeitungen zur Verfügung gestellt werden. Sie geben anschließend eine Selbsteinschätzung und Selbsterklärung ab, bei der sie beurteilen, ob die betroffene Datenverarbeitung den für das Unternehmen festgelegten Datenschutzkonzepten und den Ansprüchen der DSGVO genügt. Unerlässlich dafür ist, dass die Mitarbeitenden eines Unternehmens gut über die Datenschutzgrundsätze informiert und regelmäßig geschult und sensibilisiert werden. Der Erfolg oder Misserfolg und damit auch das Datenschutzniveau sind davon in hohem Maße abhängig, weshalb es sinnvoll ist, solche Self Assessments mindestens durch interne Audits stichprobenhaft zu überprüfen. Zu beachten ist ferner, dass auch bei Self Assessments eine gute Dokumentation notwendig ist, damit der Verantwortliche seiner Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO gerecht wird.

4.3.19 Zertifizierung

Die Datenschutz-Grundverordnung sieht in Art. 42 DSGVO die Einführung von datenschutzspezifischen Zertifizierungsverfahren vor, die dazu dienen nachzuweisen, dass die Datenschutz-Grundverordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Die Zertifizierung kann gem. Art. 43 Abs. 5 DSGVO ausschließlich durch eine akkreditierte Zertifizierungsstelle oder durch eine Datenschutz-Aufsichtsbehörde durchgeführt werden. Zwar werden die Zertifizierungen durch Dritte erbracht, dies befreit gem. Art. 42 Abs. 5 DSGVO den Verantwortlichen allerdings nicht von der Verantwortung für die Einhaltung der Datenschutz-Grundverordnung. Die Zertifizierung muss dabei gem. Art. 42 Abs. 3 DSGVO freiwillig und über ein transparentes Verfahren zugänglich sein.

Mit Zertifizierungen gemäß Art. 42 DSGVO können Nachweise über die Einhaltung der DSGVO in folgenden Bereichen erbracht werden:

- Erfüllung der Pflichten des Verantwortlichen gem. Art. 24 Abs. 3 DSGVO
- Erfüllung der Anforderungen an Technikgestaltung und Datenschutz-freundliche Voreinstellungen gem. Art. 25 Abs. 1 und 2 DSGVO
- Garantien des Auftragsverarbeiters nach Art. 28 DSGVO
- Sicherheit der Verarbeitung i.S.v. Art. 32 Abs. 3 DSGVO
- Datenübermittlung an ein Drittland nach Art. 46 Abs. 2 lit. f DSGVO
- Datenschutz-Folgenabschätzung, vgl. Erwägungsgrund 90

Zwar sind mit der Datenschutz-Grundverordnung die Regelungen zur Akkreditierung und Zertifizierung in Kraft getreten, doch noch fehlt es an Akkreditierungen von Zertifizierungsstellen in Europa. Inzwischen wurden aber die notwendigen Voraussetzungen beim Europäischen Datenschutzausschuss geschaffen, sodass erste Verfahren zur Genehmigung von Kriterienkatalogen als Voraussetzung für Akkreditierungen gestartet wurden. Dabei leitet das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) den Arbeitskreis Zertifizierung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK). Während die Aufsichtsbehörden die Genehmigung von Kriterienkatalogen vornehmen, betreibt die Deutsche Akkreditierungsstelle GmbH (DAkkS) das eigentliche Akkreditierungsverfahren in Kooperation mit den Datenschutzaufsichtsbehörden.[15]

4.4 Gesetz über digitale Dienste

Das Gesetz über digitale Dienste, engl. Digital Services Act (DSA) wurde am 27. Oktober 2022 bekannt gegeben und ist seit dem 17.02.2023 vollständig anwendbar. Es bildet zusammen mit dem Gesetz über digitale Märkte ein umfassendes Regulierungspaket für Vermittlungsdienste (Art. 3 lit. g DSA).

Das Gesetz über digitale Dienste ergänzt und aktualisiert Teile der inzwischen 20 Jahre alten E-Commerce-Richtlinie. Ziel dieser Verordnung ist es, gem. Art. 1 Abs. 1 DSA einheitliche horizontale Regeln zu Sorgfaltspflichten und Haftungsausschlüssen für Vermittlungsdienste (wie etwa Online-Plattformen) zu schaffen und damit zu einem sicheren, vorhersehbaren und vertrauenswürdigen Online-Umfeld und einem reibungslosen Funktionieren des EU-Binnenmarkts für Vermittlungsdienste beizutragen. Damit ist der Datenschutz nicht das zentrale Thema des Gesetzes über digitale Dienste, dennoch wird das Schutzniveau von Betroffenen verbessert.

So stellt die Verordnung bestimmte Anforderungen an Online-Plattformen. Dazu gehören Gestaltungsanforderungen an sog. Online-Schnittstellen, die nicht so zu konzipieren, organisieren oder betreiben sind, dass Nutzer getäuscht, manipuliert oder anderweitig in ihrer Fähigkeit, freie und informierte Entscheidungen zu treffen, maßgeblich beeinträchtigt oder behindert werden (sog. Dark Pattern). Art. 25 Abs. 1 DSA. Art. 2 lit. m DSA legaldefiniert die Online-Schnittstelle als Software, darunter auch Websites oder Teile davon (bspw. Cookie-Banner) sowie Anwendungen einschließlich Mobile-Apps. Abs. 3 nennt beispielhaft drei Praktiken, in denen die Voraussetzungen des Abs. 1 vorliegen können. Der Anwendungsbereich des Art. 25 Abs. 1 DSA ist jedoch nach Abs. 2 beschränkt, da die UPG-Richtlinie und die DSGVO vorrangig anzuwenden sind.[16]

4.5 Sicherheit der Verarbeitung zur Gewährleistung der Informationssicherheit

Aus dem Datenschutzrecht resultieren verschiedene Pflichten zur Gewährleistung von Informationssicherheit bezüglich personenbezogener Daten. Sicherheitsmaßnahmen sind grundsätzlich zu treffen, damit die Grundsätze der Zweckbindung, der Integrität und Vertraulichkeit sowie der Transparenz umgesetzt werden: Wären Daten nicht gegen die Verwendung durch Unberechtigte geschützt, könnten sie für beliebige Zwecke und damit unrechtmäßig verwendet werden. Außerdem könnte die verantwortliche Stelle nicht mehr nachvollziehen, wofür die Daten verwendet werden, und damit dem Betroffenen auch nicht mehr korrekt Auskunft erteilen.

Eine direkte gesetzliche Pflicht, die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um eine gesetzeskonforme Datenverwendung sicherzustellen, ergibt sich aus Art. 24 Abs. 1 und 32 DSGVO. Ergänzend ist mit Art. 25 DSGVO dem Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen noch die Verpflichtung hinzugetreten, nachvollziehbar bereits bei der Gestaltung und Planung von Verarbeitungen Risikofolgen abzuschätzen und zur Umsetzung der Datenschutz-Grundverordnung geeignete technische und organisatorische Maßnahmen zu ergreifen.

Zu ergreifen sind die jeweiligen Maßnahmen allerdings nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Anhaltspunkte zur Angemessenheit von Maßnahmen können die technischen Standards zur Informationssicherheit geben. Der Verhältnismäßigkeitsvorbehalt bedeutet zudem nicht, dass die verantwortliche Stelle auf die Maßnahmen bei geringem Schutzbedarf gänzlich verzichten kann: Unter Vorbehalt steht vorrangig das »Wie« der Maßnahmen, nicht das »Ob«. Auf der anderen Seite ist der Maßstab des Art. 32 DSGVO die Berücksichtigung der generellen Verarbeitungszwecke und -umstände, des Verarbeitungsumfangs und der unterschiedlichen Eintrittswahrscheinlichkeit sowie der Schwere des Risikos für die Betroffenen. Auch hier gilt, dass die Vorschrift zusammen mit der Rechenschaftspflicht zu lesen ist. Somit hat der Verantwortliche sich dokumentiert mit den möglichen Risiken seiner Datenverarbeitung für die Betroffenen und einer Einschätzung des Schutzbedarfs auseinanderzusetzen. Die Vorgängerregelung des § 9 BDSG zu technischen und organisatorischen Maßnahmen ist nicht mehr in Kraft. Für die Praxis spielt sie dennoch bezüglich der Darstellung und der inhaltlichen Anforderungen an die Maßnahmen eine Rolle. Die zugehörige Anlage führte acht Anforderungen (Kontrollen) an die interne Organisation auf. Wie oben dargestellt bilden diese nach wie vor für die Praxis ein Grundgerüst für die Darstellung der technischen und organisatorischen Maßnahmen. Dies gilt vor allem für die im Rahmen der Auftragsverarbeitung erforderliche Darstellung der getroffenen Maßnahmen oder für die nach Art. 30 Abs. 1 lit. g DSGVO erforderliche Darstellung der technischen und organisatorischen Maßnahmen im Rahmen des Verzeichnisses der Verarbeitungstätigkeiten. Ein solches Verzeichnis über die einzelnen Verarbeitungsverfahren haben Unternehmen über einer Mitarbeiterschwelle von 250 Beschäftigten zu führen. Es ist jedoch darüber hinaus sinnvoll, ein solches Verzeichnis auch mit Blick auf die Rechenschaftspflicht und den Nachweis der Rechtmäßigkeitsprüfung der einzelnen Verarbeitungen zu führen.

4.5.1 Durchsetzung von Informationssicherheit im Datenschutzrecht

Zur Durchsetzung der im Datenschutzrecht geforderten angemessenen Informationssicherheit hat der Gesetzgeber mit der Datenschutz-Grundverordnung eine Reihe von Druckmitteln und Sanktionen vorgesehen.

Die Verletzung der Pflicht zu technischen und organisatorischen Maßnahmen ist ebenso erfasst wie eine unzureichende Berücksichtigung der Gestaltungsmöglichkeiten im Einführungsstadium der Verarbeitung. Auch eine mangelnde Datenschutzdokumentation stellt einen Bußgeldtatbestand dar, ebenso wie das Versäumnis, einen Vorfall zu melden.

Die Sanktionshöhe ist durch die Datenschutz-Grundverordnung erheblich verschärft. Im Gegensatz zu 50.000 Euro Bußgeldrahmen des BDSG a. F. für einfache Verstöße und 300.000 Euro für schwere Verstöße setzt die Datenschutz-Grundverordnung in Art. 83 DSGVO Rahmen von 10.000.000 Euro oder 2 % des weltweit erzielten Jahresumsatzes für Verstöße an, für schwere Verstöße erfolgt nochmals eine Verdoppelung, d. h. 4 % des weltweit erzielten Jahresumsatzes oder 20.000.000 Euro.[17]

Eine unbefugte Offenbarung oder Übermittlung, etwa durch unzureichende Schutzmaßnahmen, fällt ebenso unter die zweite Kategorie wie die Nicht-Befolgung von Anweisungen der Aufsichtsbehörde.

Art. 84 DSGVO gibt den Mitgliedstaaten zudem vor, auch nicht bußgeldbewehrte Verstöße innerstaatlich mit wirksamen, verhältnismäßigen und abschreckenden Sanktionen zu belegen. Hierunter fällt etwa der Straftatbestand des § 42 BDSG, der Freiheitsstrafen bis zu drei Jahren bei unbefugten Übermittlungen oder anderweitigen gewerbsmäßigen unbefugten Offenlegungen und bis zu zwei Jahren bei dem Erschleichen von Daten oder unberechtigter Verarbeitung gegen Entgelt vorsieht.

Die Aufsichtsbehörden haben außerdem die Möglichkeit, **Vor-Ort-Kontrollen** der verantwortlichen Stellen vorzunehmen und Anordnungen zur Beseitigung festgestellter Verstöße oder von Mängeln bei den technischen und organisatorischen Maßnahmen zu erlassen (Art. 58 DSGVO). Werden die Anordnungen nicht in angemessener Zeit befolgt, kann die Aufsichtsbehörde den Betrieb der mängelbehafteten Verfahren untersagen und z. B. IT-Anwendungen stilllegen lassen.

Dem Betroffenen steht zudem ein eigener **Schadensersatzanspruch** zu, falls ihm Schäden aus einer unzulässigen Datenverwendung entstehen, die auf einer Sorgfaltspflichtverletzung der verantwortlichen Stelle beruht (Art. 82 DSGVO).

4.6 Telemedien-Datenschutzrecht

Die im Telemediengesetz geregelten datenschutzrechtlichen Vorschriften zu Telemedien wurden in das Telekommunikations-Telemedien-Datenschutz-Gesetz überführt. Zu den Telemedien zählt ein Großteil der Angebote im Internet, z. B. Web-Auftritte von Organisationen und Privaten, Web-Shops, Online-Auktionshäuser, Suchmaschinen, Web-E-Mail-Dienste, Informationsdienste (Wetter, Verkehrshinweise usw.), Chatrooms und soziale Netzwerke. Abzugrenzen sind die Telemedien zu den Telekommunikationsdiensten (s. Abschnitt 4.7).

Aufgrund der unterschiedlichen Gesetzgebungskompetenzen hatten Bund und Länder den weder technisch noch inhaltlich oder funktional eindeutig zu trennenden Regelungsbereich der Multımediadienste 1997 in »Teledienste« und »Mediendienste« unterteilt. Für Teledienste galt das Teledienstegesetz (TDG) des Bundes und für Mediendienste der Mediendienste-Staatsvertrag (MDStV) der Länder. Seit dem 01.03.2007 sind beide Gesetze aufgehoben und durch das Telemediengesetz (TMG) und den neuen Abschnitt VI des Rundfunkstaatsvertrags (RStV) ersetzt worden. Im Telemediengesetz regelt nun der Bund die wirtschaftsbezogenen Aspekte der Telemedien, während im Rundfunkstaatsvertrag die Länder inhaltsbezogene Vorgaben für presse- und rundfunknahe Telemedien regeln. Die datenschutzrechtlichen Regelungen finden sich seit dem 01.12.2022 im Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG).

Das Telemediengesetz definiert in § 1 Abs. 1 TTDSG »Telemedien« als Restgröße. Erfasst sind alle Informations- und Kommunikationsdienste, die nicht Telekommunikation (überwiegende Signalübertragung) oder Rundfunk sind. »Informations- und Kommunikationsdienste« ist damit der Oberbegriff für alle Dienste, die elektronisch Text-, Bild- oder Toninhalte anbieten. Unter »Rundfunk« nach § 2 RStV versteht man dagegen alle für die Allgemeinheit bestimmten Veranstaltungen und Verbreitungen von Darbietungen aller Art unter Benutzungen elektromagnetischer Schwingungen ohne Verbindungsleitung oder längs oder mittels eines Leiters. Hierzu sollen neben dem herkömmlichen Rundfunk unter anderem auch Live-Streaming und Web-Casting gehören. Dagegen sollen Tele- und Radiotext sowie Teleshopping und Video-on-Demand Telemedien sein. Da das Telemedienrecht einen bedeutenden Teil der Informations- und Kommunikationstechnik regelt, liegt ein Einfluss auch auf Fragen des Datenschutzrechts in diesem Bereich nahe und wurde vom Gesetzgeber durch die Schaffung des TTDSG als solcher auch erkannt.

Im TTDSG geregelt sind daneben aber auch die Regelungen des Datenschutzes und der Privatsphäre in der Telekommunikation, die früher im TKG geregelt waren.

4.6.1 Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG)

Anfang Dezember 2021 löste das Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) die datenschutzrechtlichen Vorschriften aus Telekommunikations- (TKG) und Telemediengesetz (TMG) ab und setzt damit die EU-Kodex-Richtlinie um.

So brachte das Telekommunikations-Telemedien-Datenschutz-Gesetz Änderungen im Bereich der Einwilligungen beim Speichern und dem Zugriff auf Informationen in der Endeinrichtung des Endnutzers. Daneben sieht das TTDSG auch den Einsatz von sog. Personal-Information-Management-Systemen (PIMS) vor, um den Endnutzern mehr Kontrolle über ihre Daten zu geben. Mit Hilfe von PIMS lässt sich einstellen, welche Daten mit wem geteilt werden oder eben nicht. Daneben enthält das TTDSG aber auch noch weniger beachtete Regelungen für den Bereich der Telekommunikation, die zur Folge haben, dass reine Videokonferenzdienste nunmehr als Telekommunikation gelten.[18] Dies führt dazu, dass für diese Dienste keine Auftragsverarbeitungsverträge mehr abgeschlossen werden müssen.

4.6.2 Grundlagen zum Telemedien-Datenschutzrecht

Die Regelungen zum speziellen Telemediendatenschutzrecht finden sich in Teil 3 des Telekommunikations-Telemedien-Datenschutz-Gesetzes. Hier finden sich Regelungen zu technischen und organisatorischen Vorkehrungen sowie Regelungen zur Verarbeitung von Daten zum Zweck des Jugendschutzes und zur Auskunftserteilung. Grundsätzlich gelten aber in diesem Bereich die Regelungen der Datenschutz-Grundverordnung.

Wie im allgemeinen Datenschutzrecht stellt das TTDSG die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für Telemedien unter einen Erlaubnisvorbehalt. Nach § 25 TTDSG sind diese Tätigkeiten nur zulässig, wenn der Nutzer eingewilligt hat oder eine Rechtsvorschrift sie ausdrücklich erlaubt.

Die zulässig erhobenen Daten unterliegen einer strengen Zweckbindung und dürfen nur für die Umsetzung des Angebots von Telemedien verwendet werden.

§ 21 TTDSG regelt, in welchen Fällen und für wen ein Auskunftsanspruch gegenüber dem Anbieter von Telemedien für Bestandsdaten besteht, der

Anspruch löst den aus § 14 TMG a. F. ab. In § 23 TTDSG wird der Anbieter von geschäftsmäßigen Telemediendiensten unter besonderen Voraussetzungen verpflichtet, bei Erfüllung der Voraussetzungen Informationen, Passwörter oder Zugangsdaten für Webseiten an Strafverfolgungsbehörden und die Polizei weiterzugeben. § 24 TTDSG regelt den Auskunftsanspruch für Nutzungsdaten, zu denen auch die IP-Adresse als personenbezogenes Datum gehört. Dieser Auskunftsanspruch wurde durch die Reform auf die in § 24 Abs. 3 TTDSG genannten Behörden beschränkt, sodass die betroffene Person hier keinen eigenen Anspruch aus dem Telemedienrecht gegenüber den Anbietern von Telemedien mehr hat.

Für eigene Informationen sind Anbieter voll verantwortlich. Für fremde Informationen, die sie nur in einem Kommunikationsnetz übermitteln oder zu denen sie nur den Zugang zur Nutzung vermitteln, tragen sie keine Verantwortung. Sie tragen auch keine Verantwortung, wenn sie Informationen nur automatisch und zeitlich begrenzt zwischenspeichern und die Informationen unverzüglich entfernen oder sperren, sobald sie erfahren, dass sie am Ursprungsort entfernt oder gesperrt wurden. Gleiches gilt bei einer gerichtlichen Anordnung. Soweit Anbieter fremde Informationen für einen Nutzer speichern, trifft sie keine Mitverantwortung, wenn sie keine Kenntnis vom rechtswidrigen Inhalt dieser Informationen haben oder sie nach Kenntniserlangung die Informationen unverzüglich sperren oder entfernen. Die Anbieter sind nach dem TTDSG nicht verpflichtet, die Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen, derartige Pflichten richten sich für die Betreiber sozialer Netzwerke nach dem Netzwerkdurchsetzungsgesetz.

Diese Verantwortungsregeln sind auch für die Verantwortlichen nach der Datenschutz-Grundverordnung relevant, vor allem wenn ein Unternehmen ein Gästenetz für den Internetzugang betreibt. Nach der Verantwortung bestimmt sich die rechtliche Erforderlichkeit von Filter- und Kontrollmaßnahmen, um Eingriffe in das Recht auf informationelle Selbstbestimmung zu verhindern.

Nur für Telemedien mit journalistisch-redaktionell gestalteten Angeboten, in denen vollständig oder teilweise Inhalte periodischer Druckerzeugnisse in Text oder Bild wiedergegeben werden, und für Anbieter von vergleichbaren Telemedien sind zusätzlich zu den Vorgaben des TMG die inhaltsbezogenen Anforderungen der §§ 55 ff. RStV zu beachten.

4.6.3 Anforderungen an Datenschutz im Telemedienrecht

Das TTDSG fördert Konzepte zum Selbst- und System-Datenschutz. Diese sind vor allem in § 19 TTDSG umgesetzt. Danach hat der Anbieter durch technische

und organisatorische Vorkehrungen sicherzustellen, dass die Datenschutzanforderungen umgesetzt werden: Der Nutzer muss die Nutzung des Diensts jederzeit beenden können. Die Protokollierung des Nutzerverhaltens ist nur sehr eingeschränkt erlaubt, denn Daten über den Ablauf des Zugriffs und Nutzungsdaten müssen unmittelbar nach Beendigung des Diensts gelöscht bzw. gesperrt werden. Das Telekommunikations-Telemedien-Datenschutz-Gesetz schreibt dem Anbieter zudem vor, dass er die Daten des Nutzers vor der Kenntnisnahme durch Dritte zu schützen hat. Diese Vorschrift lässt einen breiten Interpretationsspielraum und ist gleichzeitig eine sehr weit reichende Verpflichtung für den Anbieter von Telemedien, den Schutz der Privatsphäre zu gewährleisten. Der Anbieter ist für die Sicherheit des Dienstes verantwortlich. Für die Ausgestaltung trifft das Telekommunikations-Telemedien-Datenschutz-Gesetz keine konkreten Vorgaben. Erwartet wird, dass die Sicherheitsmaßnahmen dem aktuellen Stand der Technik entsprechen. Außerdem sollten sich die Anbieter bei der Verwendung personenbezogener Daten an den technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO orientieren.

Ein Ziel des Telekommunikations-Telemedien-Datenschutz-Gesetzes ist es, die anonyme oder pseudonyme Nutzung des Internets zu ermöglichen. Dies ist z. B. sinnvoll, weil zwischen Anbietern und Nutzern von Telemedien oftmals kein Vertragsverhältnis entsteht, z. B. beim einfachen Besuch einer Webseite. In vielen Fällen ist die Identifikation des Surfers deshalb nicht erforderlich. Dem Prinzip der Datenvermeidung und Datensparsamkeit gem. Art. 5 Abs. 1 lit. c und e DSGVO folgend, dürfen Anbieter keine oder nur möglichst wenige Daten erheben. Der Anbieter hat nach § 19 Abs. 2 TTDSG den Nutzern die Inanspruchnahme und Bezahlung von Telemedien anonym oder unter Pseudonym zu ermöglichen.[19] Nutzungsprofile sind nach § 25 TTDSG nur bei Vorliegen einer wirksam erteilten Einwilligung zulässig. Sie dürfen ohne Einwilligung nicht mit Daten des Trägers des Pseudonyms zusammengeführt werden.

Die Anbieter sollen durch technische und organisatorische Maßnahmen im Rahmen der wirtschaftlichen Zumutbarkeit sicherstellen, dass keine unerlaubten Zugriffe auf die für die Telemediendienste genutzten technischen Einrichtungen möglich sind (§ 19 Abs. 4 TTDSG). Die Schutzpflicht soll sich insbesondere auch auf Störungen durch äußere Angriffe beziehen. Maßstab der Maßnahmen ist erneut der Stand der Technik, eine gesetzlich erwähnte Maßnahme ist die Verwendung eines als sicher anerkannten Verschlüsselungsverfahrens.

4.6.4 Durchsetzung von Datenschutz im Telemedienrecht

Telemedien sind im Rahmen der Gesetze zulassungs- und anmeldefrei. Eine Prüfung der technischen Umsetzung oder der Erfüllung der gesetzlichen Anforderungen findet daher nicht statt.

Im Falle einer unrechtmäßiger Kenntniserlangung von Bestands- oder Nutzungsdaten trifft den Diensteanbieter eine Informationspflicht nach den Regelungen der Datenschutz-Grundverordnung: Wenn schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Nutzers drohen, hat der Diensteanbieter dies unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen (Art. 33, 34 DSGVO). Konkret bedeutet dies, dass z. B. der Betreiber einer »gehackten« Webseite, auf der personenbezogene Daten erhoben werden, sich nicht nur um die Behebung der Sicherheitslücke kümmern muss – er muss vielmehr auch für die Information der Betroffenen sorgen.

Da es sich bei vielen Regelungen des Telekommunikations-Telemedien-Datenschutz-Gesetzes um Ausprägungen des Datenschutzrechts handelt, überwacht der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit als Aufsichtsbehörde die Einhaltung der Vorschriften des TTDSG. Verstöße können damit auch zu entsprechenden Bußgeldern führen.

Strittig ist derzeit, inwiefern Verstöße gegen Datenschutz- und Telemedienrecht als Verstöße gegen Wettbewerbsrecht, also das Gesetz gegen den unlauteren Wettbewerb (UWG) anzusehen sind. Bei Art. 13 DSGVO handelt es sich nach überwiegend vertretener Auffassung um eine gesetzliche Vorschrift im Sinne von § 3a UWG, die auch dazu bestimmt ist, im Interesse der Marktteilnehmer das Marktverhalten zu regeln. Indem der Verstoß gegen Art. 13 DSGVO geeignet ist, vor allem die Interessen von Verbrauchern und Mitbewerbern spürbar zu beeinträchtigen, wird der Tatbestand des Rechtsbruchs gemäß § 3a UWG erfüllt. Folglich können derartige Verstöße auch wettbewerbsrechtlich abgemahnt werden. Die aufgrund von § 3a UWG unlautere geschäftliche Handlung ist unzulässig (§ 3 Abs. 1 UWG) und begründet einen Anspruch auf Unterlassung gemäß § 8 Abs. 1 S. 1 UWG. Wenn Gerichte dies so sehen, dann können bspw. Mitbewerber durch Abmahnungen auf die Einhaltung von Vorgaben der Datenschutz-Grundverordnung bzw. TTDSG hinwirken.

Aus Berlin und Hamburg gibt es OLG-Entscheidungen zu der Frage, ob mangelhafte Datenschutzbestimmungen, die sich auf einer Website befinden (noch zu § 13 Abs. 1 TMG a. F.), abmahnfähig sind. Das OLG Hamburg sieht in seiner Entscheidung (Urteil vom 27.06.2013 – 3 U 26/12) einen Wettbewerbsbezug des § 13 Abs. 1 TMG. Das Berliner Kammergericht vertritt dagegen die Auffassung (Urteil vom 29.04.2011 – 5 W 88/11, CR 2011, 468), dass

ein Wettbewerbsbezug allenfalls in Betracht kommt, wenn die Gefahr unerwünschter Werbung besteht – was sich nur selten aus Mängeln von Datenschutzbestimmungen ergeben dürfte.[20] Am BGH ist ein Verfahren anhängig, in dem es um die Abmahn- und Klagebefugnis von Wettbewerbern wegen Verstößen gegen die Datenschutz-Grundverordnung geht (BGH Aktenzeichen I ZR 222/19 u. BGH Aktenzeichen I ZR 223/19), das im Januar 2023 entschieden werden sollte, aber bis zur Entscheidung des EuGH in der Rechtssache C-21/23 ausgesetzt ist.

4.6.5 Cookie-Banner

Auf heutigen Webseiten sind Consent Layer (dt. Einverständniserklärung), auch als sog. Cookie-Banner bekannt, allgegenwärtig. Für eine datenschutzgerechte Datenverarbeitung muss, wenn auf der Endeinrichtung des Endnutzers Informationen gespeichert oder darauf zugegriffen werden sollen, mittels Cookie-Banner darüber informiert werden, welche Informationen das sind, wer sie nutzt, für welchen Zweck sie genutzt werden und wie lange die Informationen verarbeitet bzw. gespeichert werden. Das Wort »Cookies« umfasst in diesem Zusammenhang nicht nur die klassischen kleinen Textdateien, sondern auch andere neuere Technologien, mittels derer Informationen über den Endnutzer gesammelt und verarbeitet werden. Eine Ausnahme gibt es für Informationen, deren alleiniger Zweck die Speicherung von in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen oder die Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist, oder wenn die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen unbedingt erforderlich ist, damit der Anbieter eines Telemediendienstes dem Nutzer den von diesem gewünschten Dienst zur Verfügung stellen kann (Art. 25 Abs. 2 TTDSG). Verwendet der Anbieter ohnehin nur solche »technisch notwendigen« Cookies, dann benötigt er keinen Cookie-Banner. Cookie-Banner gibt es in zwei Formen. Es gibt zum einen die klassischen Banner, die zum Teil recht unscheinbar sind und eine Nutzung der Webseite zulassen, ohne dass eine weitere Handlung erforderlich ist. Hier ist darauf zu achten, dass keine Cookies gesetzt werden dürfen, ohne dass eine Einwilligung vorliegt. Zum anderen gibt es sogenannte Cookie-Walls, die eine Entscheidung des Nutzers erzwingen, weil die Webseite ohne eine Entscheidung des Nutzers nicht betrachtet werden kann. Dies ist inzwischen insbesondere bei den Anbietern redaktioneller Inhalte auf werbefinanzierten Webseiten gang und gäbe. Der Nutzer muss sich hier entscheiden, ob er für die vom Anbieter gelieferten Inhalte mit seinen Daten

»bezahlt« oder ob er die Datennutzung durch eine Geldzahlung für die Inhalte vermeidet. Hier gab es hinsichtlich der Zulässigkeit EU-übergreifende Diskussionen.[21] Problematisch ist insbesondere die Frage der Freiwilligkeit der erteilten Einwilligung, welche häufig in Zweifel gezogen werden kann. Andererseits wurde durch neue EU-Vorschriften zum Verbraucherschutz auch in Deutschland die Form des »Bezahlens mit Daten« Anfang 2022 eingeführt, was für einen Cookie-Wall sprechen könnte. Dies setzt aber voraus, dass es sich um einen angemessenen Preis handelt. Hier bleibt abzuwarten, was dann zukünftig als angemessen betrachtet wird, sei es bei der Menge der verarbeiteten Daten, sei es bei dem alternativ zu bezahlenden Preis in Euro.

4.6.6 Einwilligung nach § 25 TTDSG/Art. 6 Abs. 1 lit. a DSGVO

Gem. § 25 Abs. 1 TTDSG muss eine Einwilligung des Nutzers eingeholt werden, wenn nicht der Ausnahmetatbestand des Abs. 2 greift. In der Vergangenheit sah dies oft so aus, dass entweder davon ausgegangen wurde, dass die weitere Nutzung der Webseite als Einwilligung gewertet wurde oder das ein entsprechendes Kästchen vorangekreuzt war. Dies hat sich durch die sog. Planet-49/Cookie-II-Urteile des EuGH[22] bzw. BGH[23] geändert. Danach war die E-Privacy-Richtlinie 2002/58/EU so auszulegen, dass eine Einwilligung aktiv erteilt werden muss. Die Möglichkeit des Abwählens zur Verweigerung seiner Einwilligung (sog. Opt-Out) reicht nicht aus, um eine Einwilligung wirksam zu erteilen. Eine Einwilligung setzt zudem voraus, dass der Nutzer ausführlich und verständlich über die Cookies informiert wird, d. h. auch, dass Angaben zur Funktionsdauer der Cookies und Angaben zum Zugriff Dritter auf die Cookies gemacht werden müssen. Die Ausgangsregelung im TMG musste danach so ausgelegt werden, dass das Wort »Widerspruch« als »Einwilligung« zu lesen war. Mit der neuen Regelung hat sich dieser Zustand geändert. Die Anforderungen an die Einwilligung gemäß TTDSG ergeben sich aus den Anforderungen der Einwilligung gem. Art. 6 Abs. 1 S. 1. lit. a DSGVO. Sie wurden seit Inkrafttreten des Gesetzes durch die Aufsichtsbehörden EU-weit sowie national durch entsprechende Handreichungen[24] und Leitlinien[25] dargelegt.

Zusammengefasst muss eine Einwilligung:

- informiert,
- separat von anderen Erklärungen,
- durch eine eindeutige bestätigende Handlung, d. h. aktiv
- und freiwillig

erfolgen. Es muss möglich sein, die Einwilligung abzulehnen. Der Widerruf der Einwilligung muss jederzeit und genauso einfach wie die Erteilung der

Einwilligung möglich sein.

Informiert bedeutet dabei, dass bestimmte Mindestinformationen angegeben werden müssen: Diese sind die Identität des Verantwortlichen, die Verarbeitungszwecke, die verarbeiteten Daten an sich, die Absicht einer ausschließlich automatisierten Entscheidung (Art. 22 Abs. 2 lit. c DSGVO) und die Absicht einer Datenübermittlung in Drittländer (Art. 49 Abs. 1 S. 1 lit. a DSGVO).

Der Zweck der Datenverarbeitung muss dabei bereits vor der Datenverarbeitung feststehen und darf nicht im Nachhinein durch andere Zwecke ergänzt werden.

Die Informationen zur Einwilligung müssen von anderen Informationen abgegrenzt erfolgen.

4.6.7 Nudging und Dark Pattern

Problematisch im Bereich der Cookie-Banner und der einzuholenden Einwilligung ist, dass die Anbieter oftmals versuchen, die Nutzer durch die Gestaltung der Consent Layer zu einer Einwilligung zu bewegen. Die Webseiten-Besucher werden durch Tricks bei der Gestaltung dieser Banner dazu bewegt, doch eine entgegen ihres eigentlichen Willens stehende Einwilligung abzugeben. Diese Taktik wird als »Nudging«[26] und die dahinter stehenden grafischen Gestaltungen als »Dark Pattern« bezeichnet. So werden die Nutzer durch die Verwendung von Farben oder Gestaltung von Schaltflächen zur Erteilung von Einwilligungen verleitet, wie die nachfolgende Grafik veranschaulicht:

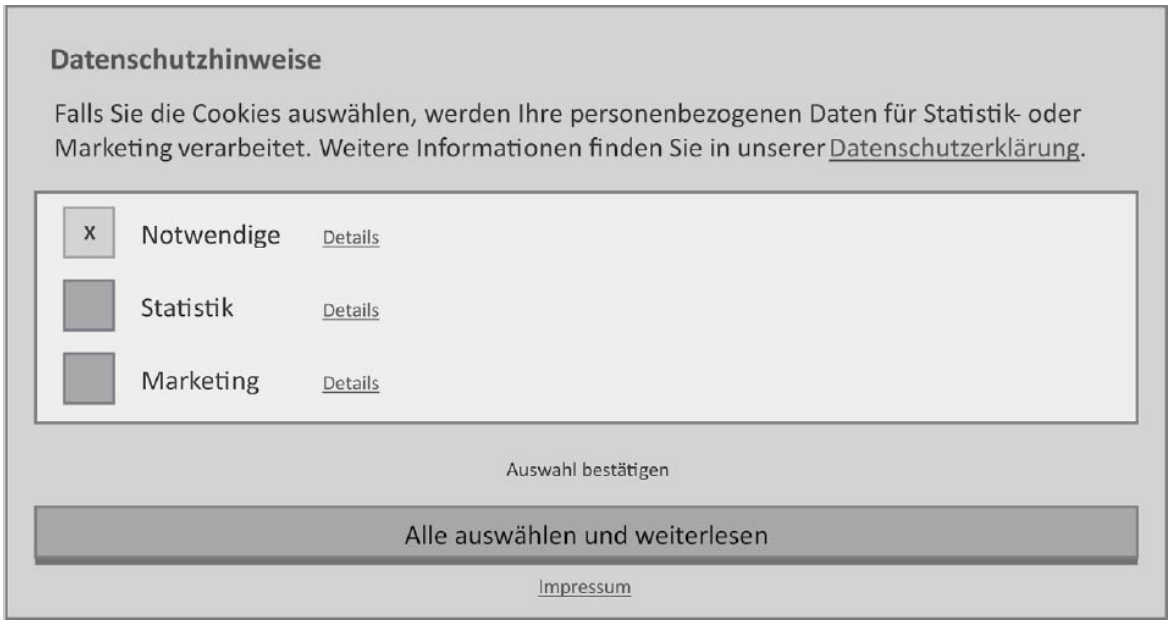
Daneben wird auch versucht, durch eine Vielzahl an Einstellungsmöglichkeiten Verwirrung zu stiften, denn die Nutzer werden regelmäßig den Aufwand der Auswahl scheuen und deshalb den Button »Einwilligung« ohne vorherige Information über die Details betätigen. Dadurch wird aber keine wirksame Einwilligung erteilt, weil die im vorstehenden Abschnitt genannten Anforderungen nicht erfüllt werden.

Die Aufsichtsbehörden haben diese Problematik erkannt und deshalb Überprüfungen von Webauftritten von Anbietern eingeleitet.

Kritisiert wird dabei auch, dass vielfach Einwilligungen, die bereits verweigert wurden, durch sich ständig wiederholende Abfragen doch noch erreicht werden sollen. Hier zeigt sich, dass die Consent Layer dem Zweck des Datenschutzes eigentlich zuwiderlaufen. Ansätze für eine Verbesserung sind möglicherweise die Einführung eines »Alles ablehnen«-Buttons, der aber so keine gesetzliche Grundlage hat, oder die Verwendung von Browser-Plug-ins wie dem »Nervenschoner« der Verbraucherzentrale Bayern[27], der für ungestörtes Surfen

sorgen soll. Hier werden die Banner und Cookie-Walls von vornherein ausgeblendet und Einwilligungen automatisch verweigert, sodass der Nutzer dadurch nicht mehr belästigt wird. Allerdings erfolgt hier das Einschreiten durch den Nutzer und nicht durch den Anbieter, der eigentlich als Verantwortlicher durch datenschutzfreundliche Voreinstellungen dafür zu sorgen hat, dass die Zwecke des Datenschutzes erreicht werden (Art. 25 DSGVO). Die Einstellungen bei den Consent Layern müssen dem Betroffenen dienen, nicht der Gewinnerzielungsabsicht des Seitenbetreibers/Verantwortlichen.

Abbildung 4.1: Negativbeispiel eines Datenschutzhinweises einer Webseite unter Ausnutzung von Dark Pattern.



Die Ablehnungsmöglichkeit »Auswahl bestätigen« lässt sich gestalterisch nicht als Auswahlmöglichkeit erkennen Neben der verringerten Schriftgröße lässt sich nicht einmal erkennen, dass es sich überhaupt um eine Schaltfläche handelt. Wohingegen die Schaltfläche »Alles auswählen und weiterlesen« dominant hervorgehoben wurde und darüber täuscht, dass eine Datenverarbeitung für Statistik- & Marketingzwecke stattfindet, obwohl diese im Auswahlbereich darüber überhaupt nicht ausgewählt waren.

4.7 Telekommunikations-Datenschutzrecht

Das Telekommunikationsrecht hat neben der Wettbewerbsregulierung das Ziel, die Nutzerinteressen und das Fernmeldegeheimnis zu schützen (§§ 1, 2 Abs. 2 TKG). Gegenstand des Telekommunikationsrechts ist die Telekommunikation, d. h. der technische Vorgang des Aussendens, Übermittelns, Vermittelns und Empfangens von Nachrichten in Form von elektromagnetischen oder optischen Signalen mittels technischer Einrichtungen (§ 3 Nr. 22, 23 TKG). Zentraler

Ansatzpunkt sind außerdem Telekommunikationsdienste: Dabei handelt es sich um in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen. Mittels dieser Dienstdefinition wird die Abgrenzung zu den Telemediendiensten erreicht (zu Letzteren siehe Abschnitt 4.6.1). Der Datenschutz wurde ebenso wie im Telemedienrecht aus dem TKG herausgelöst und in das TTDSG überführt. Dort finden sich nun in § 3 TTDSG die Regelungen zum Fernmeldegeheimnis, also dem Schutz der Vertraulichkeit der Kommunikation.

Das Thema Telekommunikationsrecht setzt aber auch spezifische rechtliche Grenzen für Sicherheitsmaßnahmen. Die aus dem Telekommunikationsverhalten entstehenden Daten, u. a. Standortdaten, bieten besonders umfangreiche Möglichkeiten zur Profilbildung. Betriebliche Sicherheitsmaßnahmen unter Rückgriff auf TK-Daten, vor allem bei einer erlaubten privaten Nutzung, können daher besonders leicht rechtliche Grenzen überschreiten.

Die datenschutzrechtlichen Grundsätze zur Auftragsverarbeitung finden in allgemeiner Form Anwendung (§ 109 Abs. 2 S. 5 TKG). Das bedeutet, dass unabhängig von personenbezogenen Daten bei der Beauftragung externer Dienstleister auch zum Schutz der Verfügbarkeit der Dienste und des Fernmeldegeheimnisses die Weisungsbindung und Zuverlässigkeit zu vereinbaren bzw. sicherzustellen sind.

Während die »Cookie-Vorschriften« der §§ 25 f. TTDSG in den Medien und in der Literatur viel Beachtung erfahren haben, wurden die neuen Vorschriften des Telekommunikationsrechts weitestgehend vernachlässigt. Da diese Vorschriften grundlegende Änderungen für sogenannte nummernunabhängige interpersonelle Telekommunikationsdienste zur Folge haben, sollen die wichtigsten Änderungen an dieser Stelle erwähnt werden. Hinter diesem Begriff verbergen sich wichtige Anwendungen wie Instant-Messenger, E-Mail-Dienste und Videokonferenzsysteme.

Bedeutsam ist die Erweiterung der Anwendung des TKG auf sog. Over-The-Top-Dienste als Telekommunikationsdienste insbesondere für die Verantwortlichkeit der Anbieter von Videokonferenzsystemen nach der DSGVO.

Bislang waren Anbieter von Videokonferenzsystemen nach Ansicht der Datenschutzkonferenz abhängig von ihrem Betriebsmodell als Verantwortliche oder als Auftragsverarbeiter zu qualifizieren. Im praktisch relevantesten Betriebsmodell des Videokonferenzsystems als Online-Dienst galt, dass der Nutzer eines Videokonferenzsystems Verantwortlicher und der Anbieter grundsätzlich als Auftragsverarbeiter anzusehen war. Im Falle einer Verarbeitung der Daten durch den Anbieter zu eigenen oder gemeinsamen Zwecken war aber

auch eine Übermittlung zwischen zwei Verantwortlichen oder eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO denkbar. Durch die Einstufung als Kommunikationsdienst ist nun ein Auftragsverarbeitungsvertrag für reine Videokonferenzdienste nicht mehr erforderlich. Abzuwarten bleibt, wie die Beurteilung von überschießenden Services dieser Dienste zukünftig beurteilt wird, sodass, wenn derartige Zusatzdienste verwendet werden, dennoch ein Auftragsverarbeitungsvertrag abgeschlossen werden muss.

Aufsichtsbehörde ist hier der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.

4.7.1 Anforderungen an Datenschutz im Telekommunikationsrecht

Am Anfang der Anforderungen zum Schutz des Fernmeldegeheimnisses stehen allgemeine Datenschutzprinzipien wie die Einhaltung von »Datensparsamkeit« und gesetzlichen Löschfristen. Zur Ergänzung von Zutritts-, Zugangs- und Zugriffsschutzmaßnahmen sollen geeignete Verschlüsselungsverfahren zur Anwendung gebracht werden. Die Zuteilung von Zugriffsrechten soll sich am Need-to-know-Prinzip orientieren, zur Entdeckung widerrechtlicher Zugriffe soll ein Monitoring angewendet werden. Der Umgang mit dem Telekommunikationsgeheimnis unterliegenden Daten ist durch Verfahrensanweisungen zu regeln, eine entsprechende Schulung der Beschäftigten wird empfohlen.

Im Weiteren werden generelle Maßnahmen von der Mitarbeitersensibilisierung über den Zutritts-, Zugangs- und Zugriffsschutz, etwa durch Verwendung eines Rollenkonzepts oder die Festlegung von Verfahren für Datenübermittlungen aufgeführt. Externe Fernwartungszugänge sollen mit Schutzmechanismen versehen werden, die automatisch den unberechtigten Zugriff auf die Datenverarbeitungsanlage verweigern. Gefordert wird auch, dass Datenveränderungen oder -löschungen durch entsprechende Protokollierungsmechanismen nachvollziehbar sind.

4.7.2 Durchsetzung von Datenschutz im Telekommunikationsrecht

Die Aufsicht über Telekommunikationsdiensteanbieter liegt bei der Bundesnetzagentur soweit nicht gem. § 29 TTDSG der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit als Aufsichtsbehörde benannt ist. Deren Befugnisse zur Durchsetzung der Verpflichtungen regelt § 30 TTDSG. Aus § 30 Abs. 2 TTDSG ergeben sich zudem umfangreiche Auskunftsrechte der Bundesnetzagentur gegenüber den Unternehmen. Zur Überprüfung von Beschwerden oder bei Annahme von Pflichtverstößen kann die Bundesnetzagentur gezielt Auskunftsverlangen

stellen. Die Bundesnetzagentur kann zur Überprüfung die Geschäfts- und Betriebsräume während der Geschäftszeiten betreten und besichtigen.

Zur Durchsetzung der Behebung festgestellter Verstöße kann die Bundesnetzagentur Zwangsgelder von bis zu 1.000.000 Euro festsetzen. Führen mildere Maßnahmen nicht zum Ziel, steht der Bundesnetzagentur auch das Mittel der teilweisen oder vollständigen Betriebsuntersagung zur Verfügung (§ 30 Abs. 3 und 4 TTDSG).

Eine Benachrichtigung der Bundesnetzagentur und des Bundesdatenschutzbeauftragten, wenn der Schutz personenbezogener Daten verletzt wird, richtet sich nach Art. 33 DSGVO. Drohen den Betroffenen schwerwiegende Beeinträchtigungen, sind sie ebenfalls zu benachrichtigen. Eine Ausnahme hiervon gilt nur, wenn durch das Sicherheitskonzept ein geeigneter Schutz der betroffenen personenbezogenen Daten nachgewiesen werden kann. Die Bundesnetzagentur kann als Aufsichtsbehörde allerdings auch dann unter Berücksichtigung der möglichen Folgen für die Betroffenen deren Benachrichtigung anordnen. Trifft den Diensteanbieter die Pflicht, die Betroffenen zu benachrichtigen, hat er mindestens über die Art der Schutzverletzung, die Möglichkeit, weitere Informationen zu erhalten, und Empfehlungen zu Maßnahmen, um mögliche Schäden zu verhindern oder zu begrenzen, zu informieren (Art. 34 Abs. 2 DSGVO).

4.8 Strafrecht

Auch das Strafrecht enthält Anforderungen und Durchsetzungsmechanismen für die Informationssicherheit und das Datenschutzrecht. Strafbar machen kann sich ein Unternehmen als solches nicht. Nur natürliche Personen, d. h. Menschen wie die Mitarbeiter oder Leiter des Unternehmens, sind Adressaten von Strafrechtsnormen und Strafen. Für das Unternehmen sind daher Fälle relevant, in denen ein Mitarbeiter die Unternehmens-IT missbraucht oder in denen ein externer Angreifer seine Aktionen mithilfe der Unternehmens-IT durchführt. Das Unternehmen und seine Infrastruktur können in diesen Fällen Ziel oder Gegenstand von Ermittlungsmaßnahmen werden, die unter Umständen zu Funktionseinschränkungen führen können. Unternehmen sind daher gut beraten, wenn sie durch Maßnahmen der Informationssicherheit bzw. des Datenschutzes den Missbrauch der IT verhindern oder wenigstens nachvollziehbar machen und damit strafrechtliche Ermittlungen, die den IT-Betrieb beeinträchtigen, vermeiden. Insofern ist die Motivation für Sicherheitsmaßnahmen aus dem Strafrecht indirekt.

Bestimmte Verhaltensweisen, z. B. das Ausforschen des Netzwerkverkehrs oder das Brechen von Passwörtern mit dem Ziel unbefugten Datenzugriffs, verstoßen gegen Strafvorschriften. Solche Maßnahmen werden auch – mit berechtigtem Interesse – zur Überprüfung des Sicherheitsniveaus im Unternehmen selbst eingesetzt. Daraus ergibt sich im Bereich des Strafrechts ein grundsätzlicher Konflikt zwischen dem Sicherheitsziel der Rechtsvorschriften und den Maßnahmen, die zur Absicherung von IT-Infrastrukturen eingesetzt werden. Um diesen Zielkonflikt aufzulösen, müssen im Unternehmen geeignete Regelungen für den Einsatz der Werkzeuge getroffen werden.

Bestimmte Sicherheitsmaßnahmen können außerdem ihrerseits zu Verstößen gegen Strafrechtsnormen führen, z. B. können bestimmte Überwachungen des Internetverkehrs in einem Unternehmen gegen das Fernmeldegeheimnis verstoßen. Deshalb werden Strafrechtsnormen mit Telekommunikationsbezug in Abschnitt 4.8.4 unter dem Aspekt der rechtlichen Grenze für IT-Sicherheitsmaßnahmen nochmals aufgegriffen. Im Mittelpunkt stehen dort Straftatbestände, die Geheimnisse oder Persönlichkeitsrechte schützen.

Die originäre Funktion des Strafrechts ist jedoch das Verbot von Handlungen oder Angriffen, die sich direkt gegen die Informationssicherheit oder geschützte Rechtsgüter richten. Das strafrechtliche Verbot unterstützt aus dieser Perspektive die Informationssicherheit. Die wichtigsten Tatbestände werden im Weiteren vorgestellt.

4.8.1 Grundlagen zu Datenschutz und Informationssicherheit im Strafrecht

Das Strafgesetzbuch (StGB) als zentrale Quelle strafrechtlicher Verbote enthält eine Reihe spezieller *Computertatbestände*, die als Reaktion auf die sogenannte Computerkriminalität geschaffen wurden, nicht zuletzt auf Grundlage internationaler Vereinbarungen.[28] Grund hierfür ist auch das strikte Analogieverbot des Strafrechts. Dieses schließt aus, dass Straftatbestände, wie etwa die Beschädigung von körperlichen Gegenständen durch »Sachbeschädigung« auf das mutwillige Beschädigen von (unkörperlichen) Softwareinstallationen übertragen werden. Aus diesem Grund war für eine Reihe von vorhandenen Deliktstatbeständen eine »virtuelle« Variante einzuführen. Für das Verständnis dieser Tatbestände kann der Vergleich mit der herkömmlichen Variante aber hilfreich sein. Weitere spezielle Tatbestände sind im sogenannten Nebenstrafrecht, Strafrechtsbestimmungen in Spezialgesetzen wie dem Urhebergesetz, dem Telekommunikationsgesetz oder in den Datenschutzgesetzen entstanden.

Es sind jedoch weniger diese speziellen Tatbestände zum Schutz der IT-Infrastruktur oder von IT-Verfahren als eine Vielzahl von Straftatbeständen, die mittels der IT-Infrastruktur eines Unternehmens begangen werden können, die die Unternehmen zu Sicherheitsmaßnahmen zwingen. Der Handlungsdruck entsteht dabei weniger durch die Gefahr, sich als Unternehmensleitung strafbar zu machen, als durch die Folgen gegebenenfalls ausgelöster strafrechtlicher Ermittlungen. Gehen von der Unternehmens-IT-Infrastruktur massive Strafrechtsverletzungen aus, werden die Server, Clients, Sicherungen oder andere Komponenten je nach Verdachtslage zu Untersuchungsgegenständen und Beweismitteln. Sie können dann nach § 94 Abs. 1 Strafprozessordnung (StPO) beschlagnahmt werden. Doch selbst wenn dieses Worst-Case-Szenario ausbleibt, können Ermittlungen größere Störungen des Betriebsablaufs verursachen.

Eine Pflicht, über die Unternehmens-IT begangene Straftaten anzuzeigen, besteht jedoch nicht. § 138 StGB stellt lediglich die Nichtanzeige eines Katalogs *geplanter Straftaten* unter Strafe. Entscheidend dafür ist, ob das Vorhaben oder die Ausführung zu einem Zeitpunkt bekannt war, als die Ausführung oder der Taterfolg noch hätte abgewendet werden können. Erfasst sind ausschließlich schwere Straftaten wie Mord, Totschlag, Raub, gemeingefährliche Straftaten, aber auch Hoch- und Landesverrat sowie Geldfälschung. Dennoch kann eine Strafanzeige für die Unternehmensleitung auch bei vollendeten und geringeren Delikten aus verschiedenen Gründen geboten sein, z. B. um weiteren Schaden zu vermeiden, den Verdacht der Beihilfe auszuschließen oder durch staatsanwaltschaftliche Ermittlungen eine bessere Beweislage bezüglich eigener Ansprüche zu gewinnen.

Die Liste sämtlicher Straftatbestände, die heute digital begangen werden können, würde den Rahmen dieses Kapitels sprengen. Daher soll nur auf einige häufige Tatbestände eingegangen werden.

Nach der Häufigkeit stehen mit an erster Stelle die **Urheberrechtsverletzungen**. § 106 Abs. 1 UrhG[29] stellt die Vervielfältigung, Verbreitung oder öffentliche Wiedergabe ohne Einwilligung des Rechteinhabers unter Strafe. Ein urheberrechtlich geschütztes Werk kann nach § 2 Abs. 2 UrhG sowohl ein Sprachwerk als auch ein Werk der bildenden Kunst oder ein Foto, ein Film, ein Musikstück, eine technische Zeichnung, ein Plan oder eine plastische Darstellung sein. Unter Sprachwerke werden auch Computerprogramme gefasst. § 4 Abs. 2 UrhG regelt die Datenbankwerke. Dabei ist zu beachten, dass das zur Schaffung des Datenbankwerks oder zur Ermöglichung des Zugangs zu dessen Elementen verwendete Computerprogramm nicht Bestandteil des Datenbankwerks ist, vgl. § 4 Abs. 3 UrhG.

Rechtswidrige Downloads können über die Unternehmensinfrastruktur und den Internetzugang des Unternehmens angeboten werden. Die einzelnen Handlungen beim Urheberrechtsverstoß werden in der Rechtsordnung unterschiedlich erfasst. Das Erstellen einer lokalen Kopie (Download) wird durch das *Vervielfältigen* erfasst, das Anbieten von Dateien oder Dateiteilen durch die *öffentliche Wiedergabe*. Gesetzlich zugelassene und damit nicht strafbare Fälle sind bspw. vorübergehende Vervielfältigungshandlungen (§ 44a UrhG), etwa in Form eines kurzfristigen Zwischenspeicherns beim Streaming, oder aber Vervielfältigungen zum privaten oder sonstigen eigenen Gebrauch (§ 53 UrhG). Letztere dürfen jedoch nicht auf einer Vorlage beruhen, bei der die fehlende Berechtigung offensichtlich ist.

Urheberrechtsverstöße können auch von der Staatsanwaltschaft verfolgt werden. Eine ein Unternehmen beeinträchtigende Ermittlung wird allerdings erst bei einem hohen Aufkommen von rechtswidrig verbreiteten Inhalten stattfinden.

Einige Straftatbestände können zu Imageschäden für Unternehmen führen, z. B. §§ 184 ff. StGB. Dazu gehören die Verbreitung pornografischer Schriften und die Verbreitung von Schriften, die Gewalttätigkeiten zum Inhalt haben. § 184d Abs. 1 StGB stellt die Verbreitung pornografischer Inhalte durch Telemediendienste, also über Angebote im Internet, unter Strafe, sofern nicht durch technische oder sonstige Vorkehrungen ein Zugangs-Ausschluss von unter 18-Jährigen sichergestellt ist. § 11 Abs. 3 StGB stellt den Schriften Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen gleich, sodass durch den Begriff Schriften auch Filme oder Zeichnungen erfasst sind. Handelt es sich um kinder- oder jugendpornografisches Material, ist sogar die Handlung des Sich-Besitz-Verschaffens, des Beziehens und Vorrätig-Haltens strafbar. Im Rahmen ihrer Sicherheitsmaßnahmen können Unternehmen versuchen, ihre Unternehmensinfrastruktur vor solchen Delikten zu schützen. Ein weiterer Bereich sind Äußerungen, die ausgehend von der Unternehmensinfrastruktur im Internet publik gemacht werden. Hier können **Beleidigungstatbestände** (§§ 185 ff. StGB), **Volksverhetzung** (§ 130 StGB) oder die **Anleitung zu Straftaten** (§ 130a StGB) eine Rolle spielen. Besonders in diesem Bereich ist die Vielfalt möglicher Straftaten kaum überschaubar. Im Rahmen der Regelungen für Prozesse, bspw. im Bereich Außenkommunikation, und durch Sicherheitsmaßnahmen können Vorkehrungen getroffen werden, um Imageverlust und Aufwand in Ermittlungsverfahren zu vermeiden.

Auch eine Reihe von computerspezifischen Delikten können aus dieser Perspektive, dem Begehen der Straftat mithilfe der Unternehmens-IT, eine Rolle spielen. Beispielsweise können die Tatbestände der Datenveränderung (§ 303a StGB) und der Computersabotage (§ 303b StGB) von Tätern mithilfe der

Unternehmens-IT gegenüber Dritten begangen werden. Die **Datenveränderung** erfasst das Löschen, Unterdrücken oder Unbrauchbarmachen von Daten. Daten sind nach § 202a StGB in dem hier gebrauchten Begriffsverständnis nur Daten, die elektronisch, magnetisch oder sonst nicht unmittelbar, d. h. ohne technische Hilfsmittel, wahrnehmbar gespeichert sind oder übermittelt werden. Unter Löschen ist das unwiederbringliche Vernichten der Daten durch die physische Zerstörung des Datenträgers oder durch Überschreiben zu verstehen. Unterdrücken wird als das Entziehen des Zugriffs gegenüber dem Berechtigten für einen nicht unerheblichen Zeitraum definiert, z. B. durch das unberechtigte Einrichten eines Passwortschutzes. Unbrauchbar werden Daten, wenn sie für ihren bestimmungsgemäßen Zweck nicht mehr verwendet werden können, z. B. weil weitere Daten nicht nachvollziehbar hinzugefügt wurden. Das Verändern schließlich umfasst jegliche Form der inhaltlichen Umgestaltung der Daten.

Die **Computersabotage** dagegen erfasst das Stören einer Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist. Als Tathandlungen werden die Datenveränderung, die Eingabe oder Übermittlung von Daten mit Schädigungsabsicht und das Zerstören, Beschädigen oder Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers aufgeführt. Im Unterschied zur Datenveränderung wird der Schutzbereich der Computersabotage auf den inhaltlich schwer zu bestimmenden Prozess der Datenverarbeitung ausgedehnt, sodass die Ausführung von Programmen und der gesamte Umgang mit Daten umfasst werden. Beispiele sind sowohl die Zerstörung der Verarbeitungshardware als auch die Störung durch Denial-of-Service-Attacken (DoS-Attacken).

Um derartige DoS-Attacken abzuwehren und zu analysieren, werden auch sogenannte Honeypots eingesetzt. Dabei handelt es sich um Computersysteme, die gezielt Angriffe anlocken, um Angreifer in die Irre zu führen, sie vom eigentlichen Angriffsziel abzulenken, ihre Angriffsmethodik zu untersuchen und dadurch die Angreifer zu identifizieren. Das Betreiben eines solchen Honeypots kann eine Beihilfe zur Computersabotage (§§ 303b Abs. 1 Nr. 2, 27 StGB) darstellen und damit (solange keine Zustimmung des Angegriffenen vorliegt) aus rechtlicher Sicht problematisch sein.[30]

Der Strafrahmen für Computersabotage liegt bei einer Freiheitsstrafe bis zu fünf Jahren, bei der Datenveränderung bei einer Freiheitsstrafe bis zu zwei Jahren oder jeweils einer Geldstrafe.

Weitere Straftatbestände, bei denen die Gefahr besteht, dass sie unter Nutzung von Unternehmensmitteln begangen werden, ergeben sich aus dem sogenannten Nebenstrafrecht. Dies sind Straftatbestände, die in Spezialgesetzen

wie den § 42 – 44 Bundesdatenschutzgesetz neue Fassung (BDSG) kodifiziert sind.

4.8.2 Anforderungen an Informationssicherheit und Datenschutz im Strafrecht

Das Strafrecht stellt lediglich bestimmte sozial schädliche Verhaltensweisen unter Strafe. Konkrete Vorgaben für Maßnahmen zur Verhinderung der Begehung werden nicht formuliert.

Zunächst ist jede Organisation aufgefordert, mit ihren Geschäftsprozessen nicht gegen das Strafrecht zu verstoßen. Daher können die zuständigen Fachabteilungen, z. B. für Recht, Compliance oder die Revision, darauf hinwirken, dass Sicherheitsmaßnahmen ergriffen und bestimmte Verhaltensweisen durch organisatorische Maßnahmen unterbunden werden.

Unternehmen können aber ein großes Interesse haben, die indirekten Folgen von Straftaten zu vermeiden. Außerdem besteht die Gefahr, dass die Organisation durch das missbräuchliche Handeln einzelner Mitarbeiter zum Gegenstand von Ermittlungen wird. Da diese den (IT-)Betrieb stören oder auch zu erheblichen Imageschäden führen können, können Maßnahmen zur Überwachung der IT-Infrastruktur auf missbräuchliche Nutzungen und zur Aufklärung solcher Fälle geboten sein. Die Straftatbestände können so zu Sorgfaltspflichten der Unternehmensleitung führen. In welcher Form sie diese erfüllt, bleibt jedoch völlig offen.

Oben wurde der Zielkonflikt angesprochen, der sich vor allem aus § 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten) ergibt. Er entsteht aus der Strafbarkeit von Maßnahmen, die für die Überprüfung des Sicherheitsniveaus oder zur Analyse von Störfällen eingesetzt werden sollen, und trifft die Mitarbeiter im Bereich IT-Sicherheit unmittelbar. Das Unternehmen kann den Zielkonflikt auflösen, indem es klare Regeln für den Einsatz der Tools festlegt. Dies ist durch die Fürsorgepflicht für die Mitarbeiter auch rechtlich geboten. Das Regelwerk im Bereich Informationssicherheit muss also die Befugnisse und Vorgehensweisen für solche Aufzeichnungen, Tests und Analysen umfassen.

4.8.3 Durchsetzung von Datenschutz und Informationssicherheit im Strafrecht

Dementsprechend ergibt sich die Durchsetzung oder die Motivation entsprechender Maßnahmen aus dem Strafrecht nur indirekt. Bereits angesprochen wurde die Gefahr von Beschlagnahmen nach §§ 94 ff. StPO. EDV-

Anlagen werden hier zunächst als Sachgesamtheit angesehen, d. h., ein Ausbau der relevanten Datenspeicher braucht nicht stattzufinden. Das Erstellen lediglich einer forensischen Kopie, ohne die Datenträger zu beschlagnahmen, ist ebenfalls nicht vorgesehen. Dennoch kann die Beschlagnahme unter Verhältnismäßigkeitsgesichtspunkten auf eine Kopie beschränkt werden.

Für die Unternehmensleitung besteht eine vage Gefahr auch darin, zum strafrechtlichen Unterlassungstäter zu werden oder Beihilfe zu Straftaten zu leisten. Unterlassung bezieht sich auf die Möglichkeit, strafbare Handlungen anderer zu verhindern. Die *strafbare Unterlassung* setzt allerdings voraus, dass der Vorstand aus Gesetz, aus bestehenden Verkehrssicherungspflichten oder weil er die Gefahrenlage erst herbeigeführt hat, verpflichtet ist, den Taterfolg zu verhindern (Garantenstellung). Ein Beispiel könnte ein manipulierter Webshop sein, über den ein externer Angreifer Bankverbindungen sammelt und anschließend missbraucht. Wird der Unternehmensleitung dies klar und trifft sie keine wirksamen Gegenmaßnahmen, könnte der Tatbestand der unbefugten Datenverarbeitung (§ 42 BDSG) erfüllt sein. Die Geschäftsführung trifft jedoch keine generelle Garantenpflicht, Straftaten der Unternehmensmitarbeiter zu verhindern. Diese tritt erst ein, wenn die Straftat in Ausführung von Arbeitsleistungen begangen wird, sich auch auf die Unternehmenstätigkeit bezieht (bspw. mittels Bestechungen oder Betrugshandlungen) und die Unternehmensleitung davon Kenntnis gewinnt (§ 13 StGB »Begehen durch Unterlassen«, § 43 GmbH-Gesetz »Haftung der Geschäftsführer«, § 93 Aktiengesetz »Sorgfaltspflicht und Verantwortlichkeit der Vorstandsmitglieder«). Dann muss sie einschreiten, weil sie mit ihrer Organisationsmacht den Zustand abstellen kann. *Beihilfe zu Straftaten* läge dann vor, wenn die Unternehmensleitung der Straftat zustimmt und sie gegebenenfalls noch fördert.

4.8.4 Schutz der Informations- und Datenverarbeitung durch Strafrecht

Aus den speziellen Tatbeständen des Computerstrafrechts ergibt sich allerdings ein zusätzlicher Schutz der Informationssicherheit, da bestimmte Angriffe auf die Daten, Geheimnisse und die IT-Infrastruktur der Unternehmen unter Strafe gestellt werden [GeBr 2009]. Dies soll von solchen Taten abschrecken. Für Unternehmen können sich hier Anforderungen ergeben, wenn sie den zusätzlichen Schutz durch Strafvorschriften herbeiführen wollen, die das Außerkraftsetzen von Sicherheitsmaßnahmen voraussetzen (bspw. das Überwinden einer zunächst zu schaffenden Zugangssicherung, § 202a StGB).

Die Tatbestände der **Datenveränderung** und der **Computersabotage** (§§ 303a, 303b StGB) wurden oben bereits dargestellt. Diese können natürlich auch gegen das Unternehmen gerichtet sein. In diesem Fall besteht für das Unternehmen jedoch die Möglichkeit, die eigenen Abwehr- oder Aufklärungsmaßnahmen durch eine Anzeige und daraufhin eingeleitete staatsanwaltschaftliche Ermittlungen zu unterstützen. Vor dem Einschalten der Ermittlungsbehörden kann eine Prüfung sinnvoll sein, ob die Ermittlungen die eigene IT-Infrastruktur in größerem Umfang betreffen würden und ob dies vermieden werden kann.

Schutzgut der §§ 202a bis 202c StGB ist der **persönliche Lebens- und Geheimbereich**. Darunter fallen bspw. Informationen aus der Privatsphäre sowie aus beruflichen Tätigkeiten. Das Ausspähen von Daten (§ 202a StGB) bezieht sich auf das Überwinden einer Zugangssicherung, um sich oder anderen Zugang zu Daten zu verschaffen, die nicht für den Täter bestimmt und gegen unberechtigte Zugriffe besonders gesichert sind. Eine besondere Sicherung liegt dann vor, wenn der Zugang erheblich erschwert oder sogar ausgeschlossen wird. Sperren, die für jeden Interessierten leicht zu überwinden sind, werden von der Regelung nicht erfasst. Die Sicherung muss aber auch kein sehr hohes Sicherheitsniveau aufweisen. Ein einfaches Passwort stellt bspw. einen Zugangsschutz im Sinne der Vorschrift dar. Somit würde bspw. das Sich-Verschaffen ungesicherter Passwörter nicht unter § 202a StGB fallen, wohl aber die Nutzung des Passworts, um sich Zugang auf die geschützten Daten zu verschaffen.

Der Straftatbestand **Abfangen von Daten** (§ 202b StGB) schützt die nicht öffentliche Datenübermittlung. Er stellt auch die missbräuchliche Nutzung von elektromagnetischen Abstrahlungen der Datenverarbeitungsanlagen unter Strafe. Eine besondere Sicherung der Datenübermittlung ist nicht erforderlich. Mit nicht öffentlicher Übertragung ist jede Übertragung gemeint, die nicht an die Allgemeinheit gerichtet ist. Auch die Übermittlung von E-Mails über das Internet oder die Nutzung von Diensten wie Skype stellt eine nicht öffentliche Übertragung dar. Technische Mittel zum Abfangen können nach der Gesetzesbegründung[31] sowohl Hardware zum Empfangen der Übermittlung als auch die eingesetzte Software sein. Weder ein Abfangen noch ein Ausspähen von Daten stellt das sogenannte Schwarzsurfen dar, d. h. der Internetzugriff über das unverschlüsselte WLAN eines Dritten.[32] Selbst bei unterdrückter SSID liegt weder eine nicht öffentliche Übertragung noch eine besondere Sicherheitsmaßnahme vor.

Der Tatbestand des **Vorbereitens des Ausspähens und Abfangens von Daten** (§ 202c StGB) dient der Kriminalisierung der Verbreitung der

Tatwerkzeuge, also der teilweise frei verfügbaren Hard- und Software zur Begehung der oben genannten Straftaten. Hierzu wird das Herstellen, Verschaffen, Verkaufen, Überlassen, Verbreiten und Zugänglichmachen von Passwörtern, sonstigen Sicherungscodes und Computerprogrammen unter Strafe gestellt, deren Zweck die Begehung von Straftaten nach §§ 202a,b, 303a,b StGB, also des Ausspähens oder Abfangens von Daten ist. Auf die strafbare Datenveränderung und Computerveränderung sowie die diesbezüglichen Tatmittel findet § 202c StGB entsprechende Anwendung (s. § 303a Abs. 3, 303b Abs. 5 StGB). Von dem erforderlichen Vorsatz muss wenigstens die Inkaufnahme der Nutzung zu einer der genannten Straftaten erfasst sein. Sowohl der Vorsatz als auch der hierauf gerichtete Zweck der Software soll nicht vorliegen, wenn die Software zur Verwendung von legitimen Sicherheitstests hergestellt wird. Das Bundesverfassungsgericht hat 2009 die Verfassungsbeschwerde eines Informationssicherheitsdienstleisters, der befürchtete, sich durch die Verwendung von Hackertools zu Penetrationstests strafbar zu machen, nicht zur Entscheidung angenommen.[33] Es sei durch die Entstehungsgeschichte des Gesetzes und den Gesetzeswortlaut sichergestellt, dass eine Dual-Use-Software nicht aufgrund ihrer bloßen Eignung zur Begehung von Straftaten unter die erfassten Tatwerkzeuge falle. Bei der Nutzung zum Zweck abgestimmter Penetrationstests fehle es zudem an der Vorbereitung von Straftaten. Folglich laufe der Beschwerdeführer nicht Gefahr, nach § 202c StGB für die Benutzung von Hackertools belangt zu werden. Bislang sind zu § 202c StGB lediglich Selbstanzeigen von Journalisten und Verwendern bekannt, die allesamt nicht zur Verfahrenseröffnung geführt haben.[34] Auch nach der höchstrichterlichen Klarstellung steht § 202c StGB wegen seiner unklaren Fassung des Schutzguts und der Tatbestandsmerkmale zu Recht in der Kritik.

Durch § 263a StGB wurde ein auf die Manipulation von computergestützten Verarbeitungsvorgängen bezogener Tatbestand eingeführt, der **Computerbetrug**. Ein Betrug setzt eine Täuschung des Opfers voraus. Durch diese wird beim Opfer ein Irrtum erzeugt oder aufrechterhalten, aufgrund dessen das Opfer eine Vermögensverfügung vornimmt, durch die es sich selbst schädigt. Die Täuschungshandlung muss in der Absicht erfolgen, sich oder einem Dritten einen Vermögensvorteil zu verschaffen. Der Computerbetrug entspricht diesem Aufbau. Allerdings ist das Ziel kein Irrtum und das Objekt der »Täuschung« kein Mensch, sondern es soll das Ergebnis eines Datenverarbeitungsvorgangs manipuliert werden. Die Täuschung kann durch die unrichtige Gestaltung eines Programms, das Verwenden unrichtiger oder unvollständiger Daten, das unbefugte Verwenden von Daten, z. B. einer gestohlenen oder kopierten EC-Karte samt PIN, oder ein sonstiges unbefugtes Einwirken auf den IT-Prozess ausgelöst werden. In der Statistik der IuK-Delikte

von 2012 nimmt der Computerbetrug mit beinahe 25.000 erfassten Fällen eine deutliche Führung ein, hauptsächlich weil darunter auch die Manipulation von Spielautomaten und der Kreditkartenbetrug gefasst werden.[35] Unter den Computerbetrug fallen auch direkte Manipulationen von Programmabläufen oder Hardwaremanipulationen, wenn sie zu einem ungewollten Vermögensabfluss zugunsten des Täters oder eines Dritten führen.

4.9 Arbeitsrecht

Auch im Arbeitsrecht hat der Datenschutz eine hohe Relevanz für die Unternehmen. Entsprechende Pflichten leiten sich bspw. bezüglich des Schutzes von Beschäftigtendaten aus der DSGVO, dem BDSG oder den Sozialgesetzbüchern ab.

Anders als in den vorangegangenen Rechtsgebieten, in denen das Recht Maßnahmen von der Unternehmensleitung fordert, ist das Arbeitsrecht für die Umsetzung von Maßnahmen im Innenverhältnis zwischen Arbeitgeber und Arbeitnehmer relevant. Die Arbeitnehmer wirken in aller Regel bei der Umsetzung von Datenschutzmaßnahmen mit: Sie sind Adressaten organisatorischer Maßnahmen und auch potenzielle Vorfallsverursacher oder Bedrohungen des Datenschutzes und der Datensicherheit.

Grundlage für das Erteilen von Weisungen, den Erlass von Richtlinien und von Sanktionen für datenschutzbezogenes Fehlverhalten ist das sich aus dem Arbeitsvertrag ergebende Arbeitsverhältnis wurden bereits in Abschnitt 3.4.2 dargelegt, hier ergeben sich für den Datenschutz keine Änderungen.

Der Arbeitgeber gestaltet Prozesse und Abläufe zur Erfüllung von Datenschutzzielen, z. B. durch die Etablierung von technischen Abläufen oder Weisungen im Bereich der technischen und organisatorischen Maßnahmen. Viele Datenschutzmaßnahmen betreffen die Festlegung von Verhaltensregeln von Arbeitsprozessen oder bedingen Anweisungen an die Arbeitnehmer als Nutzer der Unternehmens-IT durch den Arbeitgeber als Verantwortlichen (s. o. Abschnitt 3.5.2 und 3.5.3). Das Arbeitsrecht im Sinne des durch im Arbeitsverhältnis geschaffenen Rechts ist daher ein Gestaltungsmittel, um betrieblichen Datenschutz zu erreichen. Bestimmte Maßnahmen des Datenschutzes unterliegen dabei der betrieblichen Mitbestimmung. Diese legt Rechtspflichten des Arbeitgebers vor allem gegenüber dem Betriebsrat bei der Umsetzung von Datenschutz fest. Regeln hierzu stellt bisher § 26 BDSG auf.[36]

Die weitaus meisten der dem Datenschutz dienenden Verhaltensregeln werden jedoch nicht in Arbeitsverträgen, sondern in Richtlinien oder

Arbeitsanweisungen oder Verfahrensanweisungen ausgestaltet.

4.9.1 Regelungen im Arbeitsverhältnis

Wie bereits bei der Informationssicherheit, sind bestimmte Aspekte des Datenschutzes bei der Gestaltung des Arbeitsvertrags zu berücksichtigen. Je nach Position und Aufgabe eines Mitarbeiters ist die Aufnahme einer Verschwiegenheits- oder Geheimhaltungsklausel sowie eine Verpflichtung gem. § 203 StGB bereits in den Arbeitsvertrag, wenn nicht verpflichtend, dann zumindest empfehlenswert. In Bezug auf die Inhalte und Ausgestaltung solcher Klauseln ist hier auf die Ausführungen unter 3.5.2 zu verweisen, wesentliche Unterschiede im Bereich des Datenschutzes gibt es hier nicht.

4.9.2 Datenschutz im Homeoffice

Pandemiebedingt hat sich innerhalb der letzten Jahre Arbeit vom Büro ins Homeoffice verlagert. Der Arbeitnehmer verrichtet seine Arbeit von zu Hause aus, womit unweigerlich auch die Verarbeitung von Daten einhergeht. Der Arbeitgeber hat ein Interesse daran zu wissen, was der Arbeitnehmer zu Hause innerhalb seiner Arbeitszeit tut, das heißt, ob er seinen arbeitsvertraglichen Verpflichtungen vertragsgemäß nachkommt. Überwachungsmaßnahmen steht dabei regelmäßig das allgemeine Persönlichkeitsrecht entgegen. Gegenüber Kunden ist der Arbeitgeber aber innerhalb von Vertragsverhältnissen regelmäßig dazu verpflichtet, für den Schutz der personenbezogenen Daten seiner Kunden auch im Rahmen von Homeoffice-Tätigkeiten zu sorgen. Der Arbeitgeber muss deshalb insbesondere eine sichere, d. h. in der Regel verschlüsselte Kommunikation ermöglichen. Durch ein Datenschutzkonzept für Homeoffice und entsprechende Richtlinien zur Umsetzung sowie den Abschluss einer Homeoffice-Vereinbarung mit dem Arbeitnehmer hat der Arbeitgeber hier wichtige Regelungsinstrumente an der Hand. Inwieweit der Arbeitnehmer auch nur stichprobenartige Kontrollen bei sich zu Hause zulassen muss, ist umstritten.[37] Diese Fragestellung kann in der Homeoffice-Vereinbarung auf freiwilliger Basis geregelt werden, damit zumindest für Zeiten, in denen es keine gesetzliche Homeoffice-Pflicht gibt, eine wirksame Regelung getroffen werden kann. In letzterem Fall ist der Arbeitnehmer zu verpflichten, sich an die vom Arbeitgeber aufgestellten Sicherheits- und Schutzmaßnahmen zu halten, da er hier keine Wahlmöglichkeit bezüglich seines Arbeitsplatzes hat.

4.9.3 Durchsetzung von Datenschutzmaßnahmen im Arbeitsverhältnis

Ergänzend zu den Ausführungen unter 3.5.2 ist hier noch folgendes zu ergänzen. Erlangt der Arbeitgeber von Richtlinienverstößen Kenntnis, ist ein Einschreiten wenigstens mittels Ermahnungen erforderlich, um den Anforderungen aus der DSGVO gerecht zu werden. Ansonsten riskiert die Geschäftsleitung außerdem, dass jene zur Erfüllung von Organisationspflichten erlassenen Richtlinien durch eine gegenläufige betriebliche Übung aufgehoben werden.[38]

4.9.4 Haftung der Arbeitnehmer

Auch die Regeln der Arbeitnehmerhaftung können zur Durchsetzung des Datenschutzes beitragen.

Die DSGVO hat mit Art. 82 DSGVO auch noch eine eigene deliktische Haftungsgrundlage. Da die praktische Umsetzung des Datenschutzes zu wesentlichen Teilen in den Händen der Arbeitnehmer liegt und von ihrem Verhalten abhängt, stellt sich nämlich die Frage nach der Haftung für die Folgen von Fehlverhalten. Grundsätzlich haftet ein Arbeitnehmer gegenüber dem Arbeitgeber nach den gleichen Regeln wie auch andere Vertragspartner, nämlich für vorsätzliche oder fahrlässige Verstöße gegen Vertragspflichten. Bereits Anfang des letzten Jahrhunderts erkannte aber die Rechtsprechung, dass für das Arbeitsverhältnis Begrenzungen angemessen waren. Für Arbeitnehmer steht häufig das Schadensrisiko nicht selbstbestimmter Tätigkeit außer Verhältnis zur vertraglichen Gegenleistung, dem Lohn. Daher wird dem Arbeitgeber grundsätzlich die Sach- oder Betriebsgefahr zugerechnet. Für die Haftungsverteilung wird zwischen deren Realisierung und dem Grad des Verschuldens des Arbeitnehmers abgewogen.

Diese greift in der Regel aber gegenüber dem Arbeitnehmer nur dann, wenn es sich um einen sog. Mitarbeiterexzess handelt, da Verantwortlicher in der Regel immer der Arbeitgeber ist. Ein Mitarbeiterexzess liegt vor, wenn der Arbeitnehmer bspw. personenbezogene Daten über seine berufliche Tätigkeit hinaus und privat nutzt.

Regelmäßig haftet der Arbeitnehmer voll bei Vorsatz und grober Fahrlässigkeit, bei mittlerer Fahrlässigkeit kommt es zu einer Verteilung nach Quoten und bei leichter Fahrlässigkeit hat der Arbeitgeber den Schaden voll zu tragen. Abweichungen sind nach den Umständen des Einzelfalls aber möglich. Grobe Fahrlässigkeit liegt vor, wenn selbst einfachste, jedem einleuchtende Überlegungen zu den eigenen Sorgfaltspflichten außer Acht gelassen werden. Unter leichte Fahrlässigkeit fallen dagegen leicht entschuldbare

Pflichtwidrigkeiten, die im Laufe der Zeit jedem passieren können, oder kurze, nur momentane Unaufmerksamkeiten. Für den Bereich der Informationssicherheit werden Pflichtverletzungen wie das vergessene Sperren des Bildschirms bei kurzer Abwesenheit, verpasste Softwareupdates, unsichere Passwörter und Ähnliches als leichte Fahrlässigkeit gelten können. Der bewusste Verstoß gegen Richtlinien nach Aufklärung über dadurch entstehende Risiken dagegen kann eine grobe Fahrlässigkeit darstellen. Bei der Abwägung werden auch die Stellung und die Pflichten des Arbeitnehmers sowie die Awareness-Maßnahmen des Arbeitgebers berücksichtigt. Sind relevante Sicherheitsanweisungen des Arbeitgebers unzureichend, fehlerhaft oder unverständlich, geht dies zulasten des Arbeitgebers. Dies gilt auch, wenn die tatsächlichen Arbeitsbedingungen verhindern, dass ansonsten wichtige Regelungen zur Informationssicherheit umgesetzt werden können.

Gegenüber Dritten haftet der Arbeitnehmer unbeschränkt. Wird nicht der Arbeitgeber geschädigt, sondern ein Dritter infolge der Pflichtwidrigkeit des Arbeitnehmers, so kann sich der Dritte also gleichermaßen an Arbeitgeber und Arbeitnehmer halten. Ein Arbeitnehmer hat jedoch im Fall seiner Inanspruchnahme einen Erstattungsanspruch gegen den Arbeitgeber in Höhe des Schadens, der bei einer Haftung im Arbeitsverhältnis vom Arbeitgeber zu tragen gewesen wäre. Eine Absicherung des Arbeitnehmers durch seine private Haftpflichtversicherung besteht in der Regel nicht, da Schäden aus der Berufstätigkeit durch die Versicherungsbedingungen gewöhnlich ausgeschlossen werden.

Die bestehenden Haftungsrisiken sollten für Arbeitnehmer ein guter Grund sein, Anweisungen mit Sicherheitsrelevanz zu beachten.

4.9.5 Regelungen durch Betriebsvereinbarung

Die betriebliche Mitbestimmung hat mehrere Schnittstellen zum Datenschutz. Sie kann zum einen die Einführung von Datenschutzmaßnahmen und deren Ausgestaltung betreffen. Daneben können aus Betriebsvereinbarungen Verpflichtungen für den Arbeitgeber zu Maßnahmen des Datenschutzes entstehen, wenn mitbestimmungspflichtige Verfahren eingeführt werden, die personenbezogene Daten der Beschäftigten betreffen. Nicht zuletzt können organisatorische Regelungen wie Sicherheits- oder Verhaltensrichtlinien der Mitbestimmung unterliegen. Diese Aspekte der betrieblichen Mitbestimmung werden im Weiteren kurz dargestellt. Sie gelten entsprechend im öffentlich-rechtlichen Bereich für die Mitbestimmung im Rahmen der Personalvertretungsgesetze des Bundes und der Länder. Ein echtes Beschäftigtendatenschutzrecht, wie es seit Längerem geplant ist, ist innerhalb

der Bundesrepublik nicht umgesetzt, auch nicht durch die DSGVO. Die einzige Regelung, die einen ausdrücklichen Anhaltspunkt enthält, findet sich in § 26 BDSG.

Bei der Umsetzung oder Planung von Datenschutzmaßnahmen ist daher stets zu prüfen, ob bereits in Betriebsvereinbarungen einschlägige Regelungen getroffen worden sind oder ob ein erst noch Mitbestimmungsverfahren einzuleiten ist.

Zusammenfassung

Die Regelungen der DSGVO und weitere rechtliche Regelungen verpflichten Unternehmensleitungen auf vielfältige Weise zur Umsetzung der dort niedergelegten Vorgaben. Zur Durchsetzung der Vorgaben greift der Gesetzgeber auf die Aufsichtsbehörden, Bußgelder, Benachrichtigungs- und Veröffentlichungspflichten bei Datenschutzvorfällen, Straftatbestände oder – im Verhältnis zwischen privaten Akteuren – auf Haftungsregelungen sowie Schadensersatzansprüche der Betroffenen zurück. Durch die Vielfalt der Regelungen, die für die Praxis meist konkretisierungsbedürftig sind, ist der Bereich des Datenschutzes trotz der gesetzlichen Vorgaben noch nicht abschließend geklärt und bedarf der Klärung durch die nationalen Gerichte und den Europäischen Gerichtshof. Auch fehlt es teilweise an der notwendigen Regelungsschärfe.

Die Vorgaben für die technischen und organisatorischen Maßnahmen sind durch die DSGVO bewusst technikoffen gefasst. Durch dieses Vorgehen des Gesetzgebers wird sowohl der Vielfalt an Datenverarbeitungen in den Unternehmen wie auch der Dynamik der Entwicklungen in technischer Hinsicht Rechnung getragen. Die Unternehmen müssen daher ihre Datenschutz- und Datensicherheitskonzepte und -maßnahmen entsprechend ihren Gegebenheiten und den für sie einschlägigen Rechtsvorschriften ausgestalten, umsetzen und dokumentieren.

Das Datenschutzrecht ist von allen Unternehmen umzusetzen. Art. 32 DSGVO entfaltet daher eine flächendeckende Wirkung. Unterstützung finden Verantwortliche bei den Aufsichtsbehörden, die neben ihrer Aufsichtsfunktion häufig beratend aktiv sind. Daneben sind es die internen und externen Datenschutzbeauftragten, die einerseits die Einhaltung der datenschutzrechtlichen Vorgaben überwachen, andererseits bei Umsetzungs- und Anwendungsfragen auch unterstützend beratend tätig sind.

Die Unternehmensleitung als Verantwortliche muss ihre Verantwortlichkeit aktiv wahrnehmen. Andernfalls drohen neben den Schäden aus

Datenschutzvorfällen und der negativen Öffentlichkeitswirkung auch die oben genannten Sanktionen und Schadensersatzansprüche. Die DSGVO und die dazu ergangene Rechtsprechung sind in der Summe geeignet, den Datenschutz im Unternehmen systematisch und angemessen umzusetzen.

Index

Angaben in eckigen Klammern »[nnn]« sind Platzhalter, z. B. für laufende Nummern in Standards. Standards sind unter ihrer Kurzbezeichnung aufgeführt, eine Verweisliste findet sich unter dem Stichwort »Standards«. Die Sortierung der Standards erfolgt anhand der Kurzbezeichnungen. Da sich die Nummernkreise verschiedener Standardgruppen, z. B. DIN und DIN/VDE oder ISO und ISO/IEC überschneiden können, bilden sie auch im Index jeweils eigene Gruppen. Eine zusammenfassende Übersicht zu Standards gibt der Anhang »Übersicht zu Standards der Informationssicherheit«. Die Einträge dieses Anhangs sind ebenfalls im Index ausgewiesen.

Symbole

2-Wege-Authentifikation 373

3-Wege-Authentifikation 373

/etc/group 568

/etc/passwd 566

/etc/shadow 566

A

A3/A8 422, 426, 431

A5 423

- A5/1 312
- A5/3 426, 427
- Schwachstellen 426

AAA-Protokolle 449

Abgabenordnung 48

Abhören 12, 216, 369

- Funkverbindung 393
- Pairing 408, 417

Abhörsicherheit 417

Abschirmung – WLAN 403

Abstrahlung 220

Abstreiten der Verantwortung 306

Access Concentrator – L2TP 374

Access Point 396, 399, 405

Active Directory 263, 265, 363, 507, 508, 517, 526, 530

Acunetix Web Vulnerability Scanner 156

Address Space Layout Randomisation 494, 579

Ad-Hoc-Modus – WLAN 396

Administrator 457, 475

- Berechtigungen 153, 299, 475
- Windows 506, 507, 515

Adresse

- Access Point 397
- Fälschung Geräteadresse 393

Advisory Lock 560

AES 303, 313, 315, 382, 411, 412

- Blocklänge 316
- CBC 307
- CCM 400, 412
- CTR 307
- mit GMAC 827
- Schlüssel 312
- Variante für UMTS 431

Aggressive Mode – IKE 384

Akkreditierung – Certification Body nach 27006 172

Aktenvernichter 634

Aktiengesetz 26, 39, 42

Aktive Inhalte 677

Alarm 223

- Auswertung CERT 737
- Content-Analyse 670
- IDS 699
- Notfalldienste 222, 760, 763

Alarmierung 492

- Netzwerküberwachung 275

Allmende-Dilemma 659

Ändern von Daten – Angriff 234, 305

Android 598, 599

Angemessenheitsbeschluss 111

Angreifer 3, 4, 216

- Know-how 158

- Motivation 153
- Ressourcen 4, 302, 335

Angreifermodell 307

Angreifermodelle 3, 4, 25

Angriffe

- aktive – GSM 422
- Kosten 25
- kryptografische 399
- kryptografisch erfolgreiche 304
- passive 411
- von innen 298
- Zeitfenster – Bluetooth 410

Angriffsmotive 153

- finanzielle 1

Angriffsszenarien 3

- kryptografische 307

Angriffstechniken 158

Angriffstypen 149

Angriffsversuch – manueller 156

Angriffswerkzeuge 158, 159, 403

- Denial of Service 394

Angriffsziele

- Data Recovery 356
- kryptografische Verfahren 304
- Recovery Key 355
- Superuser 475, 545
- Unix-Prozesse 579

Annual Loss Expectancy 18

Anonymität 306

- GSM 418

Anschlagsdynamik 448

ANSI 359 456, 793

Anwendungen – Eingabeüberprüfung 150

Application Level Gateway 289, 290, 296

- TTL 241

Application Protocol Data Unit 353

AppLocker 537

Arbeitsplatz – verlassen 661

Arbeitsrecht 65

Architektur 3, 21

- PAM 569

Archiv 718

- im IDS 702

ARP 236, 243, 245, 275

ARP Cache Poisoning 237

AS 4360 24

ASLR 535

Asset-Management 175, 738, 753

ASVS 615

ATM 375

Audit 7

- als Störungsursache 177
- BMCS 774
- Firewall-Regeln 288
- Information Security Management System 173
- ISO 27001 165, 170
- Soll-Vorgaben 7
- Strafbarkeit 86
- Systembetrieb – ISO 27002 176
- TK-Diensteanbieter nach TKG 59

Audit-Bericht – ISMS-Zertifizierung 173

Aufmerksamkeit – Sicherheitsziel 307

Auftragnehmer – ISO 27002 177

Auftragsdatenverarbeitung

- Datenschutz-Grundverordnung 84
- Kreditwesengesetz 44
- Telekommunikationsgesetz 58

Auftragsverarbeitung 105, 208

Aufwand – Sicherheitsmaßnahmen 16

- Awareness 670
- Best Practice 29
- Gesamtkosten 21
- Wirtschaftlichkeit 27

Auswertung

- CERT 736
- IDS 699
- IDS-Ereignisse 712

Authenticate-and-Encrypt 324

Authenticate-then-Encrypt 324

Authentication and Key Agreement Protocol 431

Authentication Center 419

Authentication Header 380

- Grenzen bei NAT 386

Authentication Server 449

Authentifizierung 200, 437, 485, 902

- Biometrie 448
- Bluetooth 406, 412, 414, 417
- Challenge-Response-Verfahren 441
- durch Besitz 445
- durch Entschlüsselung 443
- durch Signaturerstellung 443
- durch Wissen 438
- GPRS 427
- GSM 418, 420, 422
- in verteilten Systemen 449
- Mehrfaktorauthentifizierung 438
- Netzwerkgerät 399
- NTLM 519
- per PKI-Zertifikat 378
- PPP 378
- über EAP 374
- UMTS 429
- Unix über Netzwerk 568
- VPN 369

Authentifizierung per PKI-Zertifikat 483

Authentifizierungsprotokolle 449

Authentisierung 437, 478

- asymmetrischen Schlüsseltransport 330
- digitale Signatur 331
- fehlende 394
- NFS 572
- Pass-the-Hash 520
- Server per SSL 443
- SSH 480
- Telnet 479
- Unix 565
- Windows 517
- zentraler Dienst 460

Authentizität 11, 306, 334

- mobile Netze 393
- öffentliche Schlüssel 334

Autorisierung 453, 902

- Bluetooth 406, 417
- GSM-Netzzugang 419

Awareness 5, 170, 201, 655

- Business Continuity 766, 774
- CERT 730
- Firewall 299
- Incident-Management 738
- Kampagne 659
- löschen und entsorgen 636
- Verhalten in der Öffentlichkeit 658
- Vier-Phasen-Konzept 665

B

Backup 717

Bankenrecht 42

Basel II 43

Basic NAT 386

Basic Service Set 396

BCI Good Practice Guidelines 777

BCM 177, 202, 751

- BSI 100-4 776
- Good Practice Guidelines 777
- Leitlinie 758, 769, 773
- MaRisk 45
- Standards 772
- Team 768

BCM-Leitlinie 777

Beacon 397

Bedrohungen

- externe 216
- mobile Netze 393
- physische 215
- Unternehmensrisiken 15

Bedrohungslage 159

Benutzer 436, 474

Benutzerkonto 400, 436, 438, 454, 474

- individuelles 459
- nicht benötigtes 288
- sperren 438
- Unix 544, 555, 562, 565
- Web-Service 461
- Windows 504

Benutzername 437

Benutzungsfreundlichkeit 12, 364, 657

- biometrische Merkmale 448

Berechtigungskonzept 457

- DMZ 295

Berechtigungsmanagement 176, 200, 458

Bericht

- an die Unternehmensleitung 669
- BCM 758
- Firewall-Einsatz 299
- IDS-Report 708

Beschaffungsprozess 625

Best Practice

- ISO 27002 173
- Maßnahmen 163
- Netzwerksicherheit 277, 280
- Sicherheitsinvestitionen 29

Best-Practice – BCM 777

Betriebsmodus – authentisierte Verschlüsselung 325

Betriebsrat 670

Betriebssystem 474

Betriebssystemerkennung 156

Betriebssystemsicherheit 201, 473

- Härtung 493

Betriebsverfassungsgesetz 69

Betriebswirtschaftliche Betrachtungen

- qualitative 26
- quantitative 17

Betroffenenrechte 114

- löschen 642

Bewegungsabläufe zur Authentifizierung 448

Bewegungsanalyse 918

Bewegungsmuster 394

Beweissicherung – Incident-Prozess 734, 740, 745

Beweiswert

- Dokumentation 11
- IDS-Protokoll 710

BGP 266

Biometrische Anforderungen 448

Biometrische Merkmale 437

Biometrische Verfahren 448

- Datenschutz 81

BIOS 498

Bitcoin 683

BitLocker 523

Black-Box-Verschlüsselung 309

Black Hat 154

Blackholing 267

Blockchiffrierverfahren 312, 328

- Betriebsmodus 316
- ideales Blockchiffrierverfahren 312
- MAC-Bildung 320, 323

Bluetooth 403

- kryptografische Verfahren 412
- Profilbildung 394
- sicherer Einsatz 417
- Sicherheitsbewertung 416
- Sicherheitsmodus 406
- Sicherheitsverfahren 406
- Standards 403, 795

Bootvorgang

- Schutz 498
- Schutz – Unix 583
- Schutz – Windows 538

Bot-Netz 1, 153

Branch-Office-VPN 371

Brand 3, 220, 222

Brandbekämpfung 222

Brandlast 223

Brandschutz 222, 226, 227

Bridging Loops 267

Bridging – zwischen VLANs 280

British Standards

- BS 7799-1 794
- BS 7799-2 794
- BS 7799-[n] 164
- BS 25999-1 793
- BS 25999-2 793

Brute-Force-Angriff 519

- auf Passwörter 153, 322, 401, 438, 567
- erschweren 414

Brute-Force-Methode 309

BSI-Gesetz 35

BSI Grundschutz-Standards – BSI 100-4 772, 776

BSI-Mindeststandard – Mobile Device Management 604

BSIMM 609

BSI-Standard 200-1 – Managementsysteme für Informationssicherheit 184

BSI-Standard 200-2 – IT-Grundschutz-Vorgehensweise 186

BSI-Standard 200-3 – Risikomanagement 193

BSI-Standards 181, 183

- BSI TL 03305 225, 795
- BSI TR 03125 795

BSI-TR 03125 365

Buffer Overflow 151, 262, 535, 563

- Gegenmaßnahmen 493

Buffer-Overflows 608

Buffer over-read 608

Bugs 605

Build Security In Maturity Model 609

Bundesamt für Sicherheit in der Informationstechnik (BSI) 181, 196

Bürgerliches Gesetzbuch 62, 64, 65, 79

Business Continuity Institute 777

Business-Impact-Analyse 718, 753, 769

Business Judgement Rule 42

C

C4-Modell 610

Canarys 494

Capabilities 456

- Unix 546, 564

CardSpace Identitätsmanagement 463

CBC-MAC 323, 400

CERT 177, 729

- CERT-Organisationen 748
- Incident-Prozess 739
- Informationsströme überwachen 735

Certificate-Management-Protokoll 359

Certificate Policy 357

Certificate Revocation List 346

- Profil 359, 361
- Verifikation 359

Certificate Transparency 356

Certification Request 359

CFB 312, 316

Challenge 373

Challenge-Response-Verfahren 412, 414, 438, 441, 447, 903

- L2TP 376
- NTLMv2 520
- Schwachstelle 426, 519

Change-Management

- BCM 771
- Firewall 298
- Systementwicklung 625

changeroot-Mechanismen 288

Chaos Computer Clubs (CCC) 606

CHAP 373, 452, 525

Chiffrierverfahren 310

Chosen-Ciphertext-Angriff 308

Chosen-Message-Angriff 308

Chosen-Plaintext-Angriff 307

chroot 579

Cipher Block Chaining 316, 317, 323, 325, 338, 382

Ciphering Offset 415

Circle of Trust 462

Claimant – Bluetooth 414

Client

- L2TP 375
- Software für PKI-Funktionen 360

Closed System – WLAN 397

Cloud-Backup – Online-Backup 724

CMAC 323

CMS 359

C-Netz 418

Codebook Attack 438

COF 415

Cold Standby

- Firewall 298
- Rechenzentrum 765

Common Criteria 796

- CEM 796

Common Internet File System 524

Common Intrusion Detection Framework 700

Common PKI 360, 796

Common Weakness Enumeration 609

COMP128 423

- Schwachstelle 426

Container 590

Content Security 201, 297

- Awareness 668
- Filter 30, 290, 371, 403, 657, 668
- Filter im VPN 388
- löschen von Schadsoftware – Recht 85
- unter Unix 583
- unter Windows 536

Control Groups – Unix 582

Countermode 307, 312, 316, 400

Credential 904

Cryptographically Generated Addresses – IPv6 246

Cryptographic Token 360

ctive Directory Domain Services 526

CVE 609

CWC 325

CWE 609

Cyber-Terrorismus 1

Cyber War 1

D

Daemon 389

DAST 607

Data Execution Protection 493

Data Recovery 356

Datei

- Unix-Sperre 560
- Windows 509

Datenart 645, 646

Datenpaket – Verifikation 398

Datenschränke 220

Datenschutz 12, 357

- Datensicherung 718
- Incident-Prozess 734
- Langzeitarchivierung 365
- Log-Protokolle 82
- Löschkonzept 641
- Mozilla Persona 470
- NAT 249
- Privacy Extensions 249
- Probleme mit TPM 487
- SSO für Web Services 470
- Videoüberwachung 221
- Zutrittskontrolle 220

Datenschutzaudits 210

Datenschutzaufsichtsbehörde 203

Datenschutzbeauftragte 205

Datenschutz-Folgenabschätzung 102, 207

Datenschutz-Grundverordnung 636

- Löschkonzept 641

Datenschutzkoordinatoren 205

Datenschutzleitlinie 98

Datenschutzmanagementsystem 204

Datenschutzrecht

- Grenzen 80
- Telekommunikationsgesetz 58

Datenschutzrichtlinie 206

Datenschutzrisikobewertungen 207

Datenschutzvorfälle 118

Datensicherung 157, 202, 717, 765, 766

- Datenschutz 82
- Löschkonzept 625
- Medien 723

Datensicherungskonzept 725

Datensparsamkeit 365

Datenträger

- Backup 723
- Kontrolle durch Betriebssytem 486
- manipulierte 499, 658
- mobile Datenträger 224, 624
- mobile Datenträger – Kontrolle unter Windows 538
- mobile Datenträger zur Datensicherung 722
- physische Sicherheitsmaßnahmen 224
- Verwaltung durch Betriebssystem 499
- Verwaltung Unix 552

DCCP 257

Defects 605

Denial of Service 1, 12, 153, 234, 254, 256, 394, 416, 493, 572, 705, 712

- ARP 237
- DNS 262
- Module 156
- Neighbor Discovery 245
- Netzwerkmanagementprotokolle 259, 263, 264
- PKI 351
- Routing 267
- SNMP 261
- STP 268

DEP 535, 579

DES 313, 315, 374, 519

Destination Options – IPv6 248

DHCP 259, 275

DHCP Starvation 259

DHCPv6 242, 259

Diameter 453

Dictionary Attack 438

Diebstahl 216

Dienste – nicht benötigte 288

Diffie-Hellman 328

- Gruppen 383
- Schlüsselaustausch 384, 411, 414

Digitale Signatur 328, 331, 345

- abstreiten 333
- Angriff auf die Schlüsselverteilung 332
- Angriff Known-Message-Angriff 308
- API 361
- Common PKI 360
- für Zertifikate 334
- IPsec 384
- Umsetzung 332
- Verfahren 331
- Verfahren Sicherheit 322
- Verifikation 333, 341, 348, 358, 359
- Verifikationszeitpunkt 348
- Verwendung von Hash-Werten 322

Digital Rights Management 488

Digital Services Act 124

DIN 4102-1 226, 797

DIN 18095-[n] 226, 797

DIN 18106 226, 797

DIN 18251-[n] 226, 797

DIN 32757-[n] 797

DIN 66398 641, 643

DIN 66399-[n] 634

DIN 66399-[x] 798

DIN 77200 227, 798

DIN EN 356 225, 799

DIN EN 1047-[n] 225, 798

DIN EN 1063 225, 798

DIN EN 1522 225, 799

DIN EN 1523 225, 799

DIN EN 12604 226, 799

DIN EN 15659 226, 799
DIN EN 50131-1 227, 799
DIN VDE 0110 225, 799
DIN VDE 0185 225, 799
DIN VDE 0833-1 226, 799
DIN V ENV 1627 226, 799
Direct Memory Access 499
Direkter Schlüsselaustausch 325
Discretionary Access Control (DAC) 454
DMZ 276, 277, 294, 705
DNA 448
D-Netze 418
DNS 154, 233, 259, 262, 275
DNSSEC 263
DNS-Server 580
Dokumentation
- BMCS 774
- Incident-Prozess 740
- Information Security Management System 170, 171
- nach ISO 9001 172
- Struktur im ISMS 6

Domain Controller 526
Double-Encapsulation 281
Dragonfly 401
Dreiwege-Handshake 156
Drittstaatentransfer 111
DSA 332
- schlechte Zufallserzeugung 338

DSGVO 205
DSL 373, 452
DSMS 204
DTLS 255, 256, 257, 258, 260, 261, 265, 267, 274
DTP 280
Dual-Homed-Host 293
DVD vernichten 635
Dynamic Analysis Security Testing 607

Dynamic Ports 232

E

EA 7/03 172, 800

EAP 269, 374, 385, 399

EAX 325

ECB 316, 319, 338

EC-Diffie-Hellman 412

EC-DSA 332

E-Commerce 201, 605

EDGE 428

Effizienz

- Angriffe gegen Verschlüsselungsverfahren 335
- digitale Signatur 332

EGID 544, 563

E-Government 361

Einbruch 216, 222

Einbruchhemmung 226

Eindeutigkeit – biometrische Merkmale 448

Eingabevalidierung 150

Einschmelzen 634

Einspielen alter PKI-Informationen 351

Einspielen falscher Datenpakete 12, 401

Einweg-Eigenschaft 320, 321

- Hash-Funktion 323

Einwegfunktion – MAC 323

Einweg-Kommunikation – Unix-Prozesse 550

Elektronische Form 79

Elektronische Signatur nach SigG 11, 333, 349, 350, 360

- Langzeitarchivierung 364

Elektronische Wahlen 306

Elementaren Gefährdungen 4

ElGamal 332

Elliptische Kurven 411

E-Mail

- Awareness 668

- gefälschte 658

Encapsulating Security Payload 381

- mit Authentisierung 324

Encrypted File System 523

Encrypt-then-Authenticate 324

Ende-zu-Ende-Sicherheit 427, 906

- VPN 370, 371, 377

Ende-zu-Ende-Verschlüsselung 427, 906

End-to-End-VPN 371

End-to-Site-VPN 371

Enhanced Mitigation Experience Toolkit 535

Enigma 313

ENISA 749

Erdbeben 217

Erfolgsmessung

- Awareness 670
- BCMS 774
- CERT 746
- Information Security Management System 166, 170
- Sicherheitsmaßnahmen 23

Erforderlichkeitsprinzip 97

Ersatzkarte 353

Eskalationswege 177, 299, 658, 700, 758, 760, 770, 778

- CERT 733

Ethernet 375, 395

ETSI TS 101 456 800

ETSI TS 102 042 800

EUID 544, 557, 563

European Bridge CA 362

Exploit 26, 154, 157, 159, 605

Explosionen 220

ExpressCard 499

Extended Service Set 396

Extension Header – IPv6 243, 247

Extranet VPN 371

Extremumsprinzip 27

F

Fahrlässigkeit 216

Failover – Firewall 298

Fairness 306

Fälschung

- Datenherkunft 12
- existenzielle Fälschung 332
- Geräteadresse 393

Fälschungssicherheit – biometrische Merkmale 448

False Acceptance 448

False Negative

- Authentifizierung 448
- IDS 709

False Positive

- Authentifizierung 448
- Content-Filter 30
- IDS 710

False Rejection 448

Faradayscher Käfig 417

Federated Identity Management 459

Federated Network Identity 462

Fehlbedienung 3

Feistel-Prinzip 313

Fernmeldegeheimnis 57, 276

Festnetz – Sicherheitsniveau 418

Feuerwehr 223

FIDO 445

FIDO2 445

Fingerabdruck 448

Fingerprint – Hash-Wert 321, 342

- Wurzelzertifikat 363

Fingerprinting 241

FinTS 801, 802

FIPS 46-3 314, 802

FIPS 65 19, 802

FIPS 180-3 322

FIPS 180-4 801

FIPS 186-3 411, 801

FIPS 186-4 332

FIPS 197 315, 802

Firewall 19, 156, 200, 287, 371, 699

- Anforderungsanalyse 298
- Application Level Firewall 390
- Architekturen 292
- automatische Rekonfiguration 703
- betriebliche Anforderungen 299
- Betriebssysteme 501
- Grenzen 299
- Grenzen im VPN 390
- Hybrid-Firewall 289
- Konfigurationsfehler 655
- Personal Firewall 23
- Regelwerk – Policy 287
- Tunneling 390
- Typen 289
- Unix 585
- VPN 388
- Windows 539
- WLAN 403
- Zielkonflikte 298

Firewire 499

Flash-Medien 224, 626

- löschen 631

Flucht- und Rettungswege 219, 221

Forest 526

Fortschreibung von Dokumenten

- BCM 772, 774
- CERT-Organisation 738
- Incident-Prozess 746
- Information Security Management System 171
- Sicherheitskonzept 7, 199

Framecounter 426

Frequency Hopping 404

Frequenzband – 2,4 Ghz 404

Frische von Daten 305, 369

Frische von Nachrichten 307

- UMTS 429

FTP 233, 359, 372, 480, 569

Funkzelle 419

G

Gateway

- NAT 386
- VPN 370

Gateway-to-Gateway-VPN 382

GCM 325

GEAx 427

Gebäude – BCM-Maßnahmen 754

Geburtstags-Paradoxon 336

Gefährdungen 2, 3, 181, 182

- Rootkits 496

Gefahrenmeldeanlagen 226

Gegenseitiges Gewahrsein – Sicherheitsziel 307

Geheimdienste 4

Geräteregister 224

Gerätetreiber – Unix 550

Geschäftsbericht 669

Geschäftsprozess 3, 5, 12, 457

- Abhängigkeit 1, 759
- Kritikalität 753

Gesellschaftsrecht 38

Gesetz über digitale Dienste 124

Gesichtserkennung 448

Gewährleistung einer angemessenen Sicherheit 97

GID 544

GmbH-Gesetz 26

GPRS 427

Grenzen von Sicherheitsmaßnahmen

- Authentication Header 386
- durch Recht 80
- Firewall 299, 390
- Intrusion Detection 705
- Verfügbarkeit 10

Group – Unix 544, 555, 562

Grsecurity 544, 581

Grundprinzip der Erforderlichkeit 81

Gruppe – Windows 504

GSM 418

- Kryptoverfahren 422
- Sicherheitsarchitektur 419
- Sicherheitsniveau 418

Gültigkeitsdauer – PKI-Zertifikat 334

Gültigkeitsmodelle – Zertifikate 348

Gütesiegel

- Common PKI 361
- Entsorger 636
- WebTrust 363

H

Hacker 1, 4, 26, 149

Haftung

- Arbeitnehmer 65, 68
- Unternehmensleitung 41, 46
- Vertragsrecht 64
- Zertifizierungsdiensteanbieter 73

Handelsgesetzbuch 48

Handelsrecht 48

Handshake

- DCCP 257
- SCTP 257
- SSL/TLS 272, 273
- TCP 256

Hardlink 553

- Backup 721

Hardware-Sicherheitsmodul 348, 486, 488, 522, 722, 907

- Trusted Platform Module 487, 498, 524

Hardware-Token 352, 353, 360, 445, 446, 459, 460

- API 360
- PKCS 360
- Reserve-Token 356

Härtung

- Betriebssystem 493
- Firewall 288
- Unix 579

Hash-Funktion 303, 320, 380

- digitale Signaturen 332
- Einweg-Eigenschaft 323
- MAC-Bildung 323
- Schlüsselableitung 330
- Sicherheit 322

Hashtree 364

Hash-Wert 373, 376, 440

- bei NAT 386
- Challenge-Response-Verfahren 441
- Einweg-Eigenschaft 321
- für Zeitstempel 352
- Kollisionsresistenz 321
- Länge 322
- OCSP-Anfragen 352
- Passwort 438
- Schlüsselweitergabe 342
- Schwachstellen LM und NTLM 519
- signierter 322
- verkürzter 380

Heartbleed-Bug 608

Heimarbeitsplatz 224, 667

Helpdesk 354, 761

Hinterlegung von Software 64

Hive 525

HMAC 322, 323, 380, 520

Hochwasser 217

Home Location Register 419, 429

Homeoffice – VPN 369

Honeypot 291

Hop Count 240

Host-based Intrusion-Detection-System 704

Host-System 589

Host-to-Gateway-VPN 371

Host-to-Host-VPN 371

Hot Standby

- Firewall 298
- Rechenzentrum 765, 775

HTTP 233, 252, 290, 359, 372, 462

HTTPS 233, 272, 387

Hybrid Cloud 782

Hyperscaler 787

Hypervisor 589

I

IAM 459

IANA 232

ICMP – echo request 156

ICMPv6 243

ICV 398

Identifizierung 437, 908

Identität 436, 458, 908

- Diebstahl 436
- im Zertifikat 334
- vortäuschen 306

Identitätsmanagement 458

Identity and Access Management 459

Identity-Managementsystem 458

Identity Provider 464

IDS 708

ID-WSF 2.0 462

IEEE 802 395

IEEE 802.1 261

IEEE 802.1AB 261

IEEE 802.1ad 279

IEEE 802.1AE 271, 489, 524

IEEE 802.1D 267

IEEE 802.1Q 279, 280

IEEE 802.1w 267

IEEE 802.1X 246, 269, 271, 278, 280, 399, 452, 524, 572, 802

- WPA 400

IEEE 802.3 261, 395, 803

IEEE 802.5 395, 803
IEEE 802.11 803
IEEE 802.11b/g/n 404
IEEE 802.11i 399, 400
IEEE 802.11[x] 396
IETF 908
IGMP 239, 243
IKE 245, 260, 272, 383
IKEv2 272, 385, 525, 573
IMAPS 272
IMSI 419
- Übermittlung veranlassen – Angriff 422

IMSI-Catcher 425
Incident 729, 775
Incident-Prozess 7, 734, 739, 761
Independent Basic Service Set 396
Industriespionage 4
Informationsabfluss 224
- Betriebssystem 488

Informationsbeschaffung – Angriffe 154
Information Security Management System 1, 163, 167, 198
- Zertifizierung nach ISO 27001 172

Information-Security Management Systems (ISMS) 182
Informationsklassifikation 622
Informationspflichten 104
Informationssicherheit 199
- Organisation 198
- organisatorischer Rahmen 175

Informationssicherheitsmanagementsystem 181
Informationssicherheitsverbund 197
Infrastruktur-Modus – WLAN 396
Infrastruktur – physische Störungsursachen 217
INIT-Flooding 257
Initialisation Key – schwacher 417
Initialisierungsvektor 317, 323, 398, 426, 567

- Länge 400
- vorhersagbarer 338
- Wiederholung 399

inode 553

Integrität 9, 305, 306, 334

- Computer-Grundrecht 35
- Integrity Check Value 398
- kryptografische Integrität 305
- MIC 536
- mobile Netze 393
- Netzwerkkonfiguration 259
- Prüfungen mit Hash-Funktion 322
- Schutz durch Betriebssystem 496
- Softwareschutz 537
- UMTS 429
- Verfahren mit Prüfsumme 320
- VPN 369, 380

Integrität und Vertraulichkeit 97

Internes Kontrollsystem 44

Internet Protocol 234

- IPv4 236
- IPv5 234
- Unterschiede IPv4 und IPv6 234
- Unterschiede zwischen IPv6 und IPv4 241

Intranet-VPN 371

Intrusion Detection 699

Intrusion-Detection-System (IDS) 201, 699, 700

- Angriffsmuster 709
- Architektur 700
- hybrides 705
- Typen 704

iOS 598, 599

IP-Adresse 154, 156, 234, 290, 375, 386

- GPRS 427
- IDS 708
- IPv6 249

IP-Forwarding 293

IP over IP 373

IP-Pakete

- Fragmentierung 239, 244, 248

- gefälschte Adresse 711
- Header-Optionen in IPv4 238
- IPv6-Header 243

IP-Protokoll 232, 372, 379

- Bedrohungen gegen IPv4 236
- Bedrohungen gegen IPv6 236
- IPv4 385
- IPv6 379

IPsec 245, 260, 261, 267, 271, 272, 302, 308, 328, 372, 373, 379, 403, 453, 489, 525, 573, 705

- Konfiguration der Verbindung 382
- L2TP 377
- NAT 282, 385
- Schlüsselaustausch 383
- Transportmodus 381
- Tunnelmodus 381

IPv6 241

- Hop-by-Hop Options 248

Irismuster 448

ISAKMP 383

IS-IS 266

ISIS-MTT 803

ISM-Band 396

ISMS-Bestandteile 184

ISMS-Hilfsmittel 184

ISO 1400[x] 163

ISO 9000 163, 804

ISO 9000-3 804

ISO 9001 172, 805

ISO 9004 805

ISO 14001 803

ISO 27001-Zertifizierung 195

ISO 27031 772

ISO Guide 73 811

ISO/IEC 7498-1 229, 372, 810

ISO/IEC 7816-15 360, 810

ISO/IEC 13335-[x] 805

ISO/IEC 15408-[x] 805

ISO/IEC 17021 806

ISO/IEC 17799 163, 806
ISO/IEC 20000 747, 806
ISO/IEC 24760 807
ISO/IEC 24760-1 435
ISO/IEC 27000 165, 179, 807
- Entstehung 163
ISO/IEC 27001 163, 166, 167, 199, 807
- 2022 166
ISO/IEC 27002 163, 166, 173, 622, 729
ISO/IEC 27003 166, 807
ISO/IEC 27004 166, 808
ISO/IEC 27005 166, 808
ISO/IEC 27006 172, 808
ISO/IEC 27031 775, 809
ISO/IEC 27033 809
ISO/IEC 27034 809
ISO/IEC 27035 747, 809
ISO/IEC 90003 810
ISO/IEC Guide 62 810
ISO/IEC Guide 66 810
ISO/IEC TR 18044 812
IT-Grundschutz 6
- Pareto-Prinzip 29
IT-Grundschutz-Check 191
IT-Grundschutz – der Ansatz 182
IT-Grundschutz-Dokumente 183
IT-Grundschutz-Kataloge 181
IT-Grundschutz-Kompendium 181, 182, 183, 186
ITSEC 163, 812
IT-Sicherheitsbeauftragter – Telekommunikationsgesetz 58
IT-Sicherheitsorganisation – CERT 729
IT-Sicherheitsstrategie 184
IT-Strukturanalyse 189
ITU-T X.200 812
ITU-T X.500 812

ITU-T X.509 346, 358, 813

- v3 358

ITU-T X.520 813

ITU-T X.521 813

J

Jailbreak 600

JavaScript 677

K

Kanal

- Bluetooth 404
- sicherer 308

Kasumi 429, 431

Kerberos 264, 325, 328, 385, 449, 460, 464, 483, 519, 524, 569, 570, 572

Kerkhoffs'sches Prinzip 309

Kernel-Modul 581

Kernel Patch Protection 536

Kettenmodell 349

Key Distribution Center 327

- Kerberos 449

Keylogger 160, 440, 442, 445

Key Server 343

KeyUsage 347, 358

kismet 403

Klimatisierung 217

Known-Message-Angriff 308

Known-Plaintext-Angriff 307, 399

Kollision – Hash-Funktion 320

Kollisionsresistenz 321, 322

- MAC 323

Kommunikation – drahtlose 393

Kommunikationsmatrix 288

Kommunikationsprotokolle 229

- Anomalieerkennung – IDS 709
- Ports 232

Kommunikationswege 170, 177

- Alarmierung Krisenstab 761
- Awareness 662, 665
- CERT-Prozess 732
- Sicherheitsmängel an Unternehmensleitung 46
- Störfall 763, 774

Komplexität 5

- Angriffstechnik 158
- BIA 769
- IDS-Analyse 711
- IT-Sicherheit 659
- Netzwerk 277, 699
- Störfall 760, 762
- VPN 387

Kompromittierende Abstrahlung 220

Konfigurationsmanagement

- Unix 573
- Windows 525

KonTraG 26

Kosten-/Nutzen-Aspekte 7, 16, 18, 27

- Awareness 670
- Entsorgung 635
- Single Sign-On 459
- WLAN 402

Kreditwesengesetz 42

Kriminalitätsrate 217

Krise 759

Krisenbewältigung 754

Krisenkommunikation 766

Krisenmanagementplan 760, 763

Krisenstab 759, 761

Kritikalitätsbewertung von Geschäftsprozessen 753

Kryptanalyse 314, 337

Kryptografie 613

Kryptografische Mechanismen – SSO 460

Kryptografische Primitive 303

Kryptografische Protokolle 302, 303

- Sicherheitsbeweis 337

Kryptografische Schemata 303

Kryptografische Verfahren 200, 301, 303

- asymmetrische Kryptoverfahren 303, 328
- asymmetrische Kryptoverfahren Bluetooth 411
- asymmetrische Kryptoverfahren Challenge Response 443
- Auswahl – Wettbewerb 315
- Common PKI 361
- Effizienz 337
- gebrochene 339
- gebrochene Kryptoverfahren 302
- geheime Kryptoverfahren – Unsicherheit 337
- GSM 422
- Implementierung 337
- Padding 316
- proprietäre Kryptoverfahren 336
- schwache Kryptoverfahren 3
- Schwachstellen 336, 426
- sichere Kanäle 308
- sichere Kryptoverfahren 301
- Sicherheit 335, 337
- symmetrische Kryptoverfahren 303, 309
- zum Schlüsselaustausch 330

Kryptografische Werkzeuge 309

Kryptotrojaner 160

KWG 26

L

L2CAP 405, 406

L2F 373

L2TP 372, 374, 403, 525

- mit IPsec 377

LAC 374

Langzeitarchivierung 302

- elektronische 364

LAN Manager 519

Lastverteilung

- BCM 772
- Firewall 298

Lateral Movement 158

Layer-3-VPN 373

LDAP 351, 359, 569

- Konfigurationsmanagement Unix 573

LDAPS 272

LEAP 399

Lebendigkeit – Sicherheitsziel 307

Legic-Chip 353

Lesen von Daten – Angriff 234, 304, 630

LFSR 415, 424

Liberty Alliance Project 462

Linearität – kryptografische 399

Linux Unified Key Setup 571

LLDP 261

LMP 405, 406

LNS 374

Local Security Authority 505, 518

Lockstep-Ansatz 24

Log-Protokolle 11, 490

- Auswertung 288, 490, 492, 576, 708
- Auswertung durch CERT 736
- Datenschutz 81
- IDS 701, 704, 708
- Netzwerküberwachung 275
- Sudo 546
- Unix 574
- Verfügbarkeit 552

Loose Source and Record Route 238

Löschen und Entsorgen 6, 201, 621

- Crypto-Shredding 631
- Konzept 623, 641
- Maßnahmen 627, 649
- Mitarbeiter einbinden 636
- sicheres 628, 629

Löschregel 646

LTE 432