DIN EN 17799:2024-09 (D)

Anforderungen an den Datenschutz bei Verarbeitungsvorgängen; Deutsche Fassung EN 17799:2023

Inhalt

Seite

Europäisches Vorwort 7

Einleitung 8

1 Anwendungsbereich 9

2 Normative Verweisungen 9

3 Begriffe 9

4 Übersicht 10

5 Planung 10
5.1 Allgemeines 10
5.2 Verstehen der Bedürfnisse und Erwartungen der interessierten Parteien 10
5.3 Umfang der Tätigkeiten zur Verarbeitung personenbezogener Daten 11
5.3.1 Allgemeines 11
5.3.2 Aufzeichnungen über Datenverarbeitungstätigkeiten 11
5.3.3 Ermittlung der Rechtsgrundlage 12
5.3.4 Minimierung der Datenmenge 12
5.3.5 Aufbewahrungsfristen 12
5.4 Richtlinie zum Schutz personenbezogener Daten 12
5.5 Rollen und Verantwortlichkeiten 13
5.5.1 Allgemeines 13
5.5.2 Interne Rollen 14
5.5.3 Externe Rollen 15
5.6 Risikomanagement 16
5.6.1 Allgemeines 16
5.6.2 Datenschutz-Risikobeurteilung und Auswirkungsanalyse 16
5.6.3 Bewertung der Auswirkungen auf den Datenschutz 17
5.6.4 Umgang mit Risiken und Risikobehandlungsplan 17
5.7 Schutz personenbezogener Daten durch Technik und durch datenschutzfreundliche Voreinstellungen 18

6 Operative Tätigkeiten 19
6.1 Allgemeines 19
6.2 Datenschutzerklärung und Einwilligung 19
6.2.1 Datenschutzerklärung 19
6.2.2 Einwilligung 19
6.3 Aktualisierung von Rollen 20
6.4 Schutz personenbezogener Daten 20
6.4.1 Löschung von Daten 20
6.4.2 Umsetzung und Anwendung von Sicherheitsmaßnahmen 20
6.4.3 Umgang mit Verletzungen des Schutzes personenbezogener Daten 21
6.5 Anträge der betroffenen Personen zur Durchsetzung ihrer Rechte 22
6.5.1 Allgemeines 22
6.5.2 Zugang zu Daten 22
6.5.3 Berichtigung 23
6.5.4 Löschung 23
6.5.5 Einschränkung der Verarbeitung 23
6.5.6 Datenübertragbarkeit 24

6.5.7 Widersprüche 24
6.5.8 Automatisierte Entscheidungen, einschließlich Profiling 24
6.5.9 Beschwerden und Einsprüche 24
6.6 Schulung und Sensibilisierung 24
7 Kontrolle 25
7.1 Allgemeines 25
7.2 Interne Audits 25
7.3 Regelmäßiger Bericht 26
7.4 Nichtkonformitäten und Korrekturmaßnahmen 27
Anhang A (informativ) Zuordnung der Anforderungen an Verantwortliche und Auftragsverarbeiter 28
Literaturhinweise 30

Tabellen

Tabelle A.1 — Zuordnung der Anforderungen an Verantwortliche und Auftragsverarbeiter 28