DIN EN ISO/IEC 27555:2025-09 (D)

Informationssicherheit, Cybersicherheit und Datenschutz - Leitlinien zur Löschung personenbezogener Daten (ISO/IEC 27555:2021); Deutsche Fassung EN ISO/IEC 27555:2025

Inhalt

Seite

Europäisches Vorwort 7
Vorwort 8
Einleitung 9
1 Anwendungsbereich 10
2 Normative Verweisungen 10
3 Begriffe 10
4 Symbole und Abkürzungen 12
5 Rahmen für die Löschung 12
5.1 Allgemeines 12
5.2 Rahmenbedingungen 13
5.3 Datenarten 13
5.4 Vorhaltefrist und Regellöschfrist 14
5.4.1 Vorhaltefrist 14
5.4.2 Regellöschfrist 14
5.4.3 Zuordnung von Datenarten 15
5.5 Archive und Sicherungskopien (Backup) 15
5.6 Standardlöschfristen, Startzeitpunkte, Löschregeln und Löschklassen 16
5.7 Sondersituationen 16
5.8 Dokumentation des Löschkonzepts 17
6 Datenarten 18
6.1 Allgemeines 18
6.2 Identifikation von Datenarten 19
6.3 Dokumentation von Datenarten 20
7 Festlegung von Löschfristen 20
7.1 Standard- und Regellöschfristen 20
7.2 Ableiten von Regellöschfristen 21
7.3 Identifizieren von Standardlöschfristen 21
7.4 Festlegen von Löschfristen für besondere Situationen 22
7.4.1 Allgemeines 22
7.4.2 Änderung von Datenobjekten 22
7.4.3 Erfordernis zur Verlängerung der aktiven Verwendung 23
7.4.4 Aussetzen der Löschung 23
7.4.5 Sicherungskopien 23
8 Löschklassen 24
8.1 Abstrakte Startzeitpunkte — abstrakte Löschregeln 24
8.2 Matrix der Löschklassen 25
8.3 Einordnung in Löschklassen und Definition von Löschregeln 26
9 Umsetzungsvorgaben 27
9.1 Allgemeines 27
9.2 Bedingungen für Startzeitpunkte außerhalb von IT-Systemen 29
9.3 Umsetzungsvorgaben für organisationsweite Aspekte 29

9.3.1 Allgemeines ... 29
9.3.2 Backup ... 29
9.3.3 Log-Protokolle ... 30
9.3.4 Systeme zur Datenübertragung ... 30
9.3.5 Reparatur, Rückbau und Entsorgung von Systemen und Komponenten ... 30
9.3.6 Arbeitssalltag ... 31
9.4 Umsetzungsvorgaben für einzelne IT-Systeme ... 31
9.5 Löschen in geordneten manuellen Prozessen ... 32
9.6 Umsetzungsvorgaben für Auftragsdatenverarbeiter ... 32
9.7 Steuerung der Löschung in Sonderfällen ... 32
9.7.1 Ausnahmemanagement ... 32
9.7.2 Weitere Bestände personenbezogener Daten ... 33

10 Verantwortlichkeiten ... 34
10.1 Allgemeines ... 34
10.2 Dokumentation ... 35
10.3 Umsetzung ... 36

Literaturhinweise ... 37

Bilder

Bild 1 — Beispiel einer Regellöschfrist für einen Auftrag ... 15

Bild 2 — Beispiel für aus deutschen Rechtsvorschriften abgeleitete Standardlöschfristen ... 22

Bild 3 — Beispielhafte Matrix von Löschklassen für einen TK-Dienstleister ... 26

Bild 4 — Beispiel für eine Dokumentationsstruktur ... 27