DIN 66398:2016-05 (D)

Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten

Inhalt

Seite

Vorwort 5

Einleitung 6

1 Anwendungsbereich 9

2 Begriffe 9

3 Abkürzungen 13

4 Grundlagen eines Löschkonzepts 13
4.1 Allgemeines 13
4.2 Anwendung einschlägiger datenschutzrechtlicher Vorschriften 15
4.3 Was bedeutet „Löschen“? 16
4.4 Für jede Datenart eine Löschregel 16
4.4.1 Datenarten 16
4.4.2 Löschregeln 16
4.4.3 Vorhaltefrist und Regellöschfrist 17
4.4.4 Behandlung nicht-produktiver Datenbestände: Archive und Sicherungskopien 19
4.4.5 Standardlöschfristen, Startzeitpunkte, Löschregeln und Löschklassen 19
4.4.6 Löschen in Sondersituationen 20
4.5 Dokumentenstruktur im Löschkonzept 20

5 Datenarten bilden 21
5.1 Datenbestände, Zwecke und Datenarten 21
5.2 Datenarten systematisch erfassen 22
5.3 Gestaltungskriterien für die Bildung von Datenarten 22
5.3.1 Hinweise aus der Praxis 22
5.3.2 Orientierung an Rechtsvorgaben 22
5.3.3 Orientierung an Betroffenen 22
5.3.4 Orientierung an Verwendungszwecken 23
5.3.5 Orientierung an der Sensitivität von Daten 23

6 Löschfristen festlegen 23
6.1 Standardlöschfristen verwenden 23
6.2 Fristfestlegungen 24
6.2.1 Vorgehensweise und Standardlöschfristen 24
6.2.2 Verfahren zur Fristableitung 26
6.2.3 Katalog von Standardlöschfristen festlegen 27
6.3 Besonderheiten für Fristfestlegungen 27
6.3.1 Regellöschfristen und Abweichungen 27
6.3.2 Friständerungen durch Verdichtung mit Wechsel der Datenart 27
6.3.3 Wechsel der Datenart für Sonderfälle mit längerer Verwendung 28
6.3.4 Ausnahmen von Regelprozessen: Aussetzung der Löschung 28
6.3.5 Abweichungen von Standardlöschfristen für Sicherungskopien 28

7 Löschklassen 29
7.1 Abstrakte Startzeitpunkte – abstrakte Löschregeln 29
7.2 Matrix der Löschklassen 30
7.3 Datenarten, Löschklassen und Löschregeln 30

8 Vorgaben für die Umsetzung von Löschregeln 32

8.1 Struktur und Inhalte der Umsetzungsvorgaben 32
8.1.1 Verhältnis zwischen dem Dokument „Löschregeln“ und Umsetzungsvorgaben 32
8.1.2 Inhalt von Umsetzungsvorgaben 33
8.2 Umsetzungsvorgaben für Querschnittsbereiche 34
8.3 Umsetzungsvorgaben für einzelne IT-Systeme 36
8.4 Einzelmaßnahmen zur Löschung von Datenbeständen 38
8.4.1 Allgemeine Hinweise zu Umsetzungsvorgaben für Einzelmaßnahmen 38
8.4.2 Umsetzungsvorgaben für Datenobjekte im Arbeitsalltag 38
8.4.3 Umsetzungsvorgaben für Datenbestände in regelmäßigen manuellen Prozessen 39
8.4.4 Umsetzungsvorgaben für Kopien personenbezogener Daten für Sonderverwendungen 40
8.4.5 Umsetzungsvorgaben für Restbestände in IT-Systemen 41
8.4.6 Umsetzungsvorgaben für unzulässige Bestände mit personenbezogenen Daten 42
8.5 Umsetzungsvorgaben für Dienstleister 43

9 Aufbau- und Ablauforganisation: Verantwortung und Prozesse für das Löschen von personenbezogenen Daten 44
9.1 Organisatorische Einbettung 44
9.2 Leitung der Organisation 44
9.3 Rolle des Ansprechpartners für Datenschutz 45
9.3.1 Pflegeverantwortung für Dokumente 45
9.3.2 Prozesse beim Ansprechpartner für Datenschutz 45
9.3.3 Freigabe-Beteiligungen 45
9.4 Verantwortung für Umsetzungsvorgaben 46
9.4.1 Organisationseinheiten mit Verantwortung für Bestände mit personenbezogenen Daten 46
9.4.2 Weitere Aufgaben im Zusammenhang mit Umsetzungsvorgaben 47
9.4.3 Organisationseinheit Change-Management 48
9.4.4 Organisationseinheiten mit Verantwortung zur Steuerung von Dienstleistern 48
9.5 Allgemeine Meldepflichten 49

Anhang A (informativ) Hinweise für ein Projekt „Löschkonzept“ 50

Anhang B (informativ) Hinweise zur Anonymisierung personenbezogener Daten 53

Anhang C (informativ) Hinweise zu Vorgaben für die Sicherheit von Löschmechanismen 55

Anhang D (informativ) Hinweise zur Sperrung von Datenbeständen 57

Literaturhinweise 59

Tabellen

Tabelle 1 — Verwendete Abkürzungen 13

Tabelle 2 — Empfehlungen für die Pflegeverantwortung und Freigaberegeln des Dokuments „Löschregeln“ 31

Tabelle 3 — Empfehlungen für Pflegeverantwortung und Freigaberegeln der „Umsetzungsvorgaben für Querschnittsbereiche“ 36

Tabelle 4 — Empfehlungen für Pflegeverantwortung „Bestandsverzeichnis der Datenträger“ 36

Tabelle 5 — Empfehlungen für die Pflegeverantwortung und Freigaberegeln der „Umsetzungsvorgaben für einzelne IT-Systeme“ 38

Tabelle 6 — Empfehlungen für die Pflegeverantwortung und Freigaberegeln der „Umsetzungsvorgaben für Datenobjekte im Arbeitsalltag 39

Tabelle 7 — Empfehlungen für Pflegeverantwortung und Freigaberegeln „Umsetzungsvorgaben für Datenbestände in regelmäßigen manuellen Prozessen 39

Tabelle 8 — Empfehlungen für Pflegeverantwortung und Freigaberegeln „Umsetzungsvorgaben für Kopien personenbezogener Daten für Sonderverwendungen“ 40

Tabelle 9 — Empfehlungen für Pflegeverantwortung und Freigaberegeln „Übersicht über Ausnahmeregelungen“ 41

Tabelle 10 — Empfehlungen für Pflegeverantwortung und Freigaberegeln „Umsetzungsvorgaben für Restbestände in IT-Systemen“ 42

Tabelle 11 — Empfehlungen für die Pflegeverantwortung und Freigaberegeln der „Umsetzungsvorgaben für unzulässige Bestände mit personenbezogenen Daten“ 43

Tabelle 12 — Empfehlungen für die Pflegeverantwortung und Freigaberegeln der „Umsetzungsvorgaben für Dienstleister“ 44

Tabelle 13 — Empfehlungen für die Pflegeverantwortung der „Übersicht über IT-Systeme und andere Bestände mit pbD“ 47

Tabelle 14 — Empfehlungen für die Pflegeverantwortung der „Handlungsbedarfe aus Umsetzungsvorgaben" 48

Bilder

Bild 1 — Beispiel für Fristabschnitte für einen ‚Auftrag‘ im Löschkonzept 18

Bild 2 — Mögliche Standardlöschfristen eines TK-Dienstleisters 27

Bild 3 — Beispielhafte Matrix von Löschklassen für einen TK-Dienstleister 30

Bild 4 — Verhältnis zwischen Dokument „Löschregeln“ und Umsetzungsvorgaben 32

Bild A.1 — Aufteilung in Projektphasen 51