DIN EN ISO/IEC 29134:2026-08 (D)

Informationstechnik - Sicherheitsverfahren - Leitlinien für die Datenschutz-Folgenabschätzung (ISO/IEC 29134:2023); Deutsche Fassung EN ISO/IEC 29134:2026

Inhalt

Seite

Europäisches Vorwort ... 6

Vorwort ... 7

Einleitung ... 8

1 Anwendungsbereich ... 10

2 Normative Verweisungen ... 10

3 Begriffe ... 10

4 Abkürzungen ... 12

5 Vorbereitung der DSFA ... 13
5.1 Vorteile der Durchführung einer DSFA ... 13
5.2 Zielsetzungen von DSFA-Berichten ... 14
5.3 Verantwortlichkeit für die DSFA-Durchführung ... 15
5.4 Umfang einer DSFA ... 16

6 Prozess-Anleitung für die Durchführung einer DSFA ... 16
6.1 Allgemeines ... 16
6.2 Feststellen, ob eine DSFA erforderlich ist (Schwellenwertanalyse) ... 17
6.3 Vorbereitung der DSFA ... 18
6.3.1 Team für DSFA zusammenstellen und Anweisungen erteilen ... 18
6.3.2 Plan für die DSFA vorbereiten und die notwendigen Ressourcen zur Durchführung bestimmen ... 20
6.3.3 Beschreiben, was untersucht wird ... 21
6.3.4 Einbindung von Stakeholdern ... 23
6.4 Die DSFA durchführen ... 25
6.4.1 Identifizieren der Informationsflüsse personenbezogener Daten ... 25
6.4.2 Analysieren der Auswirkungen des Anwendungsfalles ... 26
6.4.3 Bestimmen der relevanten Datenschutzanforderungen ... 27
6.4.4 Beurteilen der Datenschutzrisiken ... 28
6.4.5 Vorbereitung zum Behandeln der Datenschutzrisiken ... 32
6.5 Folgeaktivitäten zur DSFA ... 38
6.5.1 Bericht erstellen ... 38
6.5.2 Veröffentlichung ... 39
6.5.3 Umsetzen der Behandlungspläne für Datenschutzrisiken ... 39
6.5.4 Überprüfen und/oder Auditieren der DSFA ... 40
6.5.5 Reflektieren von Prozessänderungen ... 41

7 DSFA-Bericht ... 41
7.1 Allgemeines ... 41
7.2 Berichtsstruktur ... 42
7.3 Anwendungsbereich der DSFA ... 43
7.3.1 Zu bewertender Prozess ... 43
7.3.2 Risikokriterien ... 45
7.3.3 Ressourcen und beteiligte Personen ... 45
7.3.4 Konsultation mit Stakeholdern ... 45
7.4 Datenschutzanforderungen ... 45
7.5 Risikobeurteilung ... 46

7.5.1 Risikoquellen 46
7.5.2 Bedrohungen und ihre Eintrittswahrscheinlichkeit 46
7.5.3 Konsequenzen und der Grad ihrer Auswirkung 46
7.5.4 Risikobewertung 46
7.5.5 Compliance-Analyse 46
7.6 Risikobehandlungsplan 46
7.7 Schlussfolgerungen und Entscheidungen 46
7.8 Öffentliche Zusammenfassung der DSFA 47

Anhang A (informativ) Kriterien für das Maß des Auswirkungsgrades und die Eintrittswahrscheinlichkeit 48
A.1 Allgemeines 48
A.2 Einschätzung des Auswirkungsgrades 48
A.3 Einschätzung der Eintrittswahrscheinlichkeit 49

Anhang B (informativ) Generische Bedrohungen 51

Anhang C (informativ) Hinweise zum Verständnis verwendeter Benennungen 57
C.1 Anwendungsbereich der DSFA 57
C.2 Projekt 57
C.3 Prozess 58
C.4 Bedeutung 58
C.5 Überwachung und Überprüfung 59

Anhang D (informativ) Illustrierte Beispiele zur Unterstützung des DSFA-Prozesses 60
D.1 Arbeitsablaufdiagramm für die Verarbeitung personenbezogener Daten 60
D.2 Beispiel einer Datenschutz-Risikomatrix 60

Literaturhinweise 62

Bilder

Bild D.1 — Arbeitsablaufdiagramm für die Verarbeitung personenbezogener Daten 60

Bild D.2 — Beispiel einer Datenschutz-Risikomatrix 61

Tabellen

Tabelle A.1 — Beispiele für den Auswirkungsgrad, basierend auf der Art der personenbezogenen Daten 49

Tabelle B.1 — Generische Bedrohungen 52