

# DIN EN ISO/IEC 29134:2020-09 (D)

## Informationstechnik - Sicherheitsverfahren - Leitlinien für die Datenschutz-Folgenabschätzung (ISO/IEC 29134:2017); Deutsche Fassung EN ISO/IEC 29134:2020

---

Inhalt	Seite
Europäisches Vorwort.....	4
Vorwort.....	5
Einleitung.....	6
1 Anwendungsbereich.....	8
2 Normative Verweisungen.....	8
3 Begriffe.....	8
4 Abkürzungen.....	11
5 Grundlagen der DSFA.....	11
5.1 Vorteile der Durchführung einer DSFA.....	11
5.2 Zielsetzungen von DSFA-Berichten.....	12
5.3 Verantwortlichkeit für die DSFA-Durchführung.....	13
5.4 Abstufung einer DSFA.....	14
6 Prozess-Anleitung für die Durchführung einer DSFA.....	14
6.1 Allgemeines.....	14
6.2 Feststellen, ob eine DSFA erforderlich ist (Schwellenwertanalyse).....	15
6.3 Vorbereitung der DSFA.....	16
6.3.1 Team für DSFA zusammenstellen und Anweisungen erteilen.....	16
6.3.2 Plan für die DSFA vorbereiten und die notwendigen Ressourcen zur Durchführung bestimmen.....	18
6.3.3 Beschreiben, was untersucht wird.....	19
6.3.4 Einbindung von Stakeholdern.....	21
6.4 Durchführung der DSFA.....	24
6.4.1 Identifizieren der Informationsflüsse personenbezogener Daten.....	24
6.4.2 Analysieren der Auswirkungen des Anwendungsfalles.....	25
6.4.3 Bestimmen der relevanten Datenschutzanforderungen.....	25
6.4.4 Beurteilen der Datenschutzrisiken.....	26
6.4.5 Vorbereitung zum Behandeln der Datenschutzrisiken.....	30
6.5 Folgeaktivitäten zur DSFA.....	36
6.5.1 Bericht erstellen.....	36
6.5.2 Veröffentlichung.....	37
6.5.3 Umsetzen der Behandlungspläne für Datenschutzrisiken.....	37
6.5.4 Überprüfen und/oder Auditieren der DSFA.....	38
6.5.5 Reflektieren von Prozessänderungen.....	39
7 DSFA-Bericht.....	39
7.1 Allgemeines.....	39
7.2 Berichtsstruktur.....	40
7.3 Anwendungsbereich der DSFA.....	41
7.3.1 Zu bewertender Prozess.....	41
7.3.2 Risikokriterien.....	43
7.3.3 Ressourcen und beteiligte Personen.....	43
7.3.4 Konsultation mit Stakeholdern.....	43
7.4 Datenschutzanforderungen.....	43
7.5 Risikobeurteilung.....	43

7.5.1	Risikoquellen.....	43
7.5.2	Bedrohungen und ihre Eintrittswahrscheinlichkeit .....	44
7.5.3	Konsequenzen und der Grad ihrer Auswirkung .....	44
7.5.4	Risikobewertung .....	44
7.5.5	Compliance-Analyse .....	44
7.6	Plan zur Risikobehandlung.....	44
7.7	Schlussfolgerungen und Entscheidungen.....	44
7.8	Öffentliche Zusammenfassung der DSFA.....	44
<b>Anhang A (informativ) Abstufungskriterien für den Auswirkungsgrad und die</b>		
	<b>Eintrittswahrscheinlichkeit.....</b>	<b>46</b>
A.1	Allgemeines.....	46
A.2	Einschätzung des Auswirkungsgrades .....	46
A.3	Einschätzung der Eintrittswahrscheinlichkeit .....	47
<b>Anhang B (informativ) Generische Bedrohungen .....</b>		
<b>48</b>		
<b>Anhang C (informativ) Hinweise zum Verständnis verwendeter Benennungen .....</b>		
<b>53</b>		
C.1	Anwendungsbereich der DSFA.....	53
C.2	Projekt .....	53
C.3	Prozess.....	54
C.4	Bedeutung.....	54
C.5	Überwachung und Überprüfung.....	55
<b>Anhang D (informativ) Illustrierte Beispiele zur Unterstützung des DSFA-Prozesses .....</b>		
<b>56</b>		
D.1	Arbeitsablaufdiagramm für die Verarbeitung personenbezogener Daten.....	56
D.2	Beispiel einer Datenschutzrisiko-Karte .....	56
<b>Literaturhinweise .....</b>		
<b>58</b>		