

DIN EN ISO/IEC 29134

ICS 35.030

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

Information technology –
Security techniques –
Guidelines for privacy impact assessment (ISO/IEC 29134:2017);
German version EN ISO/IEC 29134:2020

Technologies de l'information –
Techniques de sécurité –
Lignes directrices pour l'évaluation d'impacts sur la vie privée (ISO/IEC 29134:2017);
Version allemande EN ISO/IEC 29134:2020

Gesamtumfang 61 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO 29134:2017 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als EN ISO/IEC 29134:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Normungsgremium ist der Arbeitskreis NA 043-01-27-05 AK „Identitätsmanagement und Datenschutz-Technologien“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Für die in diesem Dokument zitierten internationalen Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO/IEC 27000:2016	siehe	DIN EN ISO/IEC 27000:2017-10
ISO/IEC 27001:2013	siehe	DIN EN ISO/IEC 27001:2017-06
ISO/IEC 27002	siehe	DIN EN ISO/IEC 27002
ISO 9000:2015	siehe	DIN EN ISO 9000:2015-11
ISO 21500	siehe	DIN ISO 21500
ISO 31000	siehe	DIN ISO 31000

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 27000:2017-10, *Informationstechnik — Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Überblick und Terminologie (ISO/IEC 27000:2016); Deutsche Fassung EN ISO/IEC 27000:2017*

DIN EN ISO/IEC 27001:2017-06, *Informationstechnik — Sicherheitsverfahren — Informationssicherheits-managementsysteme — Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27001:2017*

DIN EN ISO/IEC 27002, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheits-maßnahmen*

DIN EN ISO 9000:2015-11, *Qualitätsmanagementsysteme — Grundlagen und Begriffe (ISO 9000:2015); Deutsche und Englische Fassung EN ISO 9000:2015*

DIN ISO 21500, *Leitlinien Projektmanagement*

DIN ISO 31000, *Risikomanagement — Leitlinien*

Deutsche Fassung

Informationstechnik —
Sicherheitsverfahren —
Leitlinien für die Datenschutz-Folgenabschätzung
(ISO/IEC 29134:2017);

Information technology —
Security techniques —
Guidelines for privacy impact assessment
(ISO/IEC 29134:2017)

Technologies de l'information —
Techniques de sécurité —
Lignes directrices pour l'évaluation
d'impacts sur la vie privée
(ISO/IEC 29134:2017)

Diese Europäische Norm wurde vom CEN am 2. März 2020 angenommen.

Die CEN- und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Management-Zentrum des CEN-CENELEC oder bei jedem CEN- und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN- und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute und elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

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 Datenschutzerfordernungen	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 Datenschutzerfordernungen	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
Anhang A (informativ) Abstufungskriterien für den Auswirkungsgrad und die Eintrittswahrscheinlichkeit		46
A.1	Allgemeines	46
A.2	Einschätzung des Auswirkungsgrades	46
A.3	Einschätzung der Eintrittswahrscheinlichkeit	47
Anhang B (informativ) Generische Bedrohungen		48
Anhang C (informativ) Hinweise zum Verständnis verwendeter Benennungen		53
C.1	Anwendungsbereich der DSFA	53
C.2	Projekt	53
C.3	Prozess	54
C.4	Bedeutung	54
C.5	Überwachung und Überprüfung	55
Anhang D (informativ) Illustrierte Beispiele zur Unterstützung des DSFA-Prozesses		56
D.1	Arbeitsablaufdiagramm für die Verarbeitung personenbezogener Daten	56
D.2	Beispiel einer Datenschutzrisiko-Karte	56
Literaturhinweise		58

Europäisches Vorwort

Der Text von ISO/IEC 29134:2017 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als EN ISO/IEC 29134:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis September 2020, und etwaige entgegenstehende nationale Normen müssen bis September 2020 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 29134:2017 wurde von CEN als EN ISO/IEC 29134:2020 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames Technisches Komitee, ISO/IEC JTC 1 (JTC, en: Joint Technical Committee), eingerichtet.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Eine Erläuterung zum freiwilligen Charakter von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO) hinsichtlich technischer Handelshemmnisse (TBT) berücksichtigt, enthält der folgende Link: www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security techniques* erarbeitet.

Einleitung

Eine Datenschutz-Folgenabschätzung (DSFA) ist ein Instrument zur Abschätzung möglicher Auswirkungen auf die Privatsphäre, die von einem Prozess, Informationssystem, Programm, Software-Modul, Gerät oder von einem sonstigen Vorhaben ausgehen, das personenbezogene Daten (pbD) verarbeitet, und erfolgt in Rücksprache mit den Stakeholdern, um notwendige Schritte zum Umgang mit den Datenschutzrisiken zu ergreifen. Ein DSFA-Bericht kann Ausführungen über die Maßnahmen zur Risikobehandlung enthalten, z. B. Maßnahmen, die aus der Anwendung des Informationssicherheitsmanagementsystems (ISMS) in ISO/IEC 27001 hervorgehen. Eine DSFA ist mehr als ein Werkzeug: Sie ist ein Prozess, der in den frühestmöglichen Schritten eines Vorhabens begonnen wird, wenn noch die Gelegenheit besteht, das Ergebnis zu beeinflussen und damit einen eingebauten Datenschutz (en: privacy by design) sicherzustellen. Sie ist ein Prozess, der fort dauert, bis das Projekt ausgerollt ist und auch darüber hinaus.

Vorhaben variieren erheblich in Umfang und Auswirkung. Zielsetzungen unter dem Stichwort „Datenschutz“ hängen ab vom kulturellen Umfeld, gesellschaftlichen Erwartungen und der Rechtsprechung. Dieses Dokument soll eine anpassbare Anleitung bieten, die für alle Vorhaben angewendet werden kann. Da eine für alle spezifischen Umstände geltende Anleitung keine Vorschrift sein kann, sollte dieses Dokument im Hinblick auf die individuellen Umstände ausgelegt werden.

Eine verantwortliche Stelle kann für die Durchführung einer DSFA zuständig sein und kann einen Auftragsdatenverarbeiter bitten, sie hierbei zu unterstützen. Ein Auftragsdatenverarbeiter oder ein Lieferant kann jeweils auch eine eigene DSFA durchführen.

Die DSFA-Informationen eines Lieferanten sind insbesondere relevant, wenn Geräte mit Datenverbindung Teil des/der zu untersuchenden Informationssystems, Anwendung oder Prozesses sind. Für den Lieferanten solcher Geräte kann es erforderlich sein, denjenigen, die die DSFA durchführen, datenschutzrelevante Informationen zur Auslegung des Gerätes bereitzustellen. Wenn der Anbieter elektronischer Geräte in der Durchführung von DSFAs nicht geschult ist und nicht über entsprechende Ressourcen verfügt, wie z. B.

- ein kleines Einzelhandelsgeschäft oder
- ein kleines oder mittelständisches Unternehmen (KMU), das Geräte mit Datenverbindung in seinem täglichen Geschäftsablauf einsetzt,

dann kann der Gerätelieferant, um diesen zu einer minimalen DSFA zu befähigen, dazu aufgefordert werden, Datenschutzinformation in großem Umfang bereitzustellen und im Hinblick auf den zu erwartenden Kontext aus betroffener Person und KMU selbst eine DSFA für die gelieferte Einrichtung durchzuführen.

Eine DSFA wird üblicherweise von einer Organisation durchgeführt, die ihre Verantwortung ernst nimmt und mit betroffenen Personen angemessen umgeht. In einigen Rechtsprechungen kann eine DSFA erforderlich sein, um den Anforderungen von Gesetzen und Verordnungen zu entsprechen.

Dieses Dokument ist zur Verwendung vorgesehen, wenn die Datenschutzfolge für betroffene Personen die Betrachtung von Prozessen, Informationssystemen oder Programmen einschließt, bei denen:

- die Verantwortung für die Umsetzung und/oder Auslieferung des Prozesses, Informationssystems oder Programms mit anderen Organisationen geteilt wird und sichergestellt werden sollte, dass sich jede Organisation mit den identifizierten Risiken angemessen befasst;

- eine Organisation Datenschutzrisikomanagement als Teil ihrer übergreifenden Risikomanagement-Bemühungen durchführt, während sie die Umsetzung oder Verbesserung ihres ISMS (eingrichtet in Übereinstimmung mit ISO/IEC 27001 oder vergleichbarem Managementsystem) vorbereitet; oder eine Organisation Datenschutzrisikomanagement als unabhängige Funktion durchführt;
- eine Organisation (z. B. eine Regierung) ein Vorhaben unternimmt (z. B. ein Programm für eine öffentlich-private Partnerschaft), in dem die zukünftig als verantwortliche Stelle agierende Organisation noch nicht bekannt ist, mit dem Ergebnis, dass der Behandlungsplan nicht direkt umgesetzt werden kann und der Behandlungsplan stattdessen Gegenstand der/des dazugehörigen Gesetzgebung, Verordnung oder Vertrages werden sollte;
- die Organisation sich gegenüber den betroffenen Personen verantwortungsbewusst verhalten möchte.

Für notwendig erachtete Steuerungsmaßnahmen zur Behandlung der während des DSFA-Prozesses identifizierten Risiken können aus einer Reihe von Maßnahmen-Sammlungen hergeleitet werden. Dazu gehören ISO/IEC 27002 (für Sicherheitsmaßnahmen) und ISO/IEC 29151 (für Datenschutzmaßnahmen) oder vergleichbare nationale Normen. Oder sie können von der für die Durchführung der DSFA zuständigen Person unabhängig von anderen Maßnahmen-Sammlungen festgelegt werden.

1 Anwendungsbereich

Dieses Dokument bietet eine Anleitung für

- einen Prozess zur Datenschutz-Folgenabschätzung, und
- Struktur und Inhalt eines DSFA-Berichts.

Es ist anwendbar für Organisationen jedes Typs und jeder Größe, einschließlich öffentlicher Unternehmen, Unternehmen der Privatwirtschaft, Regierungsinstanzen und gemeinnütziger Organisationen.

Dieses Dokument ist relevant für diejenigen, die in die Entwicklung oder Implementierung von Projekten eingebunden sind, einschließlich der Betreiber von Datenverarbeitungssystemen und Diensten, mit denen personenbezogene Daten verarbeitet werden.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO Guide 73:2009, *Risk management — Vocabulary*

ISO/IEC 27000:2016, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 29100, ISO/IEC 27000, ISO Guide 73 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

3.1

Annahmeerklärung

formelle Managementerklärung zur Übernahme der Verantwortung für die Risikoeigentümerschaft, die Risikobehandlung und das Restrisiko

3.2

Datenschutzwert

alles, was für jedwede Beteiligte von Wert ist, die in die Verarbeitung von personenbezogenen Daten (pbD) eingebunden sind

Anmerkung 1 zum Begriff: Im Zusammenhang mit dem Datenschutz-Risikomanagementprozess handelt es sich bei einem Datenschutzwert entweder um personenbezogene Daten oder um einen unterstützenden Datenschutzwert.

3.3

Prüfperson

Person, die eine *Datenschutz-Folgenabschätzung* (3.7) leitet und durchführt

Anmerkung 1 zum Begriff: Die Prüfperson kann von einem oder mehreren internen und/oder externen Experten als Teil ihres Teams unterstützt werden.

Anmerkung 2 zum Begriff: Die Prüfperson kann ein interner oder externer Experte der Organisation sein.

3.4

Prozess

Satz zusammenhängender oder sich gegenseitig beeinflussender Tätigkeiten, der Eingaben in Ergebnisse umwandelt

[QUELLE: ISO/IEC Directives, Part 1, Consolidated ISO Supplement:2014, 3.12]

3.5

Gerät

Kombination von Hardware und Software, oder nur Software, die es einem Nutzer erlaubt, Aktionen auszuführen

3.6

Datenschutzfolge

alles, was eine Auswirkung auf die Privatsphäre einer betroffenen Person und/oder einer Gruppe betroffener Personen hat

Anmerkung 1 zum Begriff: Die Datenschutzfolge kann aus der Verarbeitung personenbezogener Daten in Übereinstimmung mit oder unter Verletzung von Datenschutzanforderungen resultieren.

3.7

Datenschutz-Folgenabschätzung

DSFA

Gesamtprozess aus Identifizieren, Analysieren, Bewerten, Beraten, Kommunizieren und Planen der Behandlung von möglichen Datenschutzfolgen unter Bezug auf die Verarbeitung personenbezogener Daten, eingebettet in den unternehmensweiten Rahmen zum Risikomanagement

Anmerkung 1 zum Begriff: Basierend auf ISO/IEC 29100:2011, 2.20.

3.8

Datenschutz-Risikokarte

Diagramm, welches den Auswirkungsgrad und die Eintrittswahrscheinlichkeit von identifizierten Datenschutzrisiken angibt

Anmerkung 1 zum Begriff: Die Karte wird üblicherweise genutzt, um zu bestimmen, in welcher Reihenfolge die Datenschutzrisiken behandelt werden sollten.

3.9

Programm

Gruppe von Projekten, die koordiniert verwaltet werden, um Vorteile zu erschließen, die bei individuellem Management nicht entstehen

[QUELLE: ISO 14300-1:2011, 3.2]

3.10

Projekt

einmaliger Prozess, der aus einem Satz von abgestimmten und gesteuerten Tätigkeiten mit Anfangs- und Endterminen besteht und durchgeführt wird, um unter Berücksichtigung von Beschränkungen hinsichtlich Zeit, Kosten und Ressourcen ein Ziel zu erreichen, das spezifische Anforderungen erfüllt

[QUELLE: ISO 9000:2015, 3.4.2]

3.11

Organisation

Person oder Personengruppe, die eigene Funktionen mit Verantwortlichkeiten, Befugnissen und Beziehungen hat, um ihre Ziele zu erreichen

Anmerkung 1 zum Begriff: Der Begriff Organisation umfasst unter anderem Einzelunternehmer, Gesellschaft, Konzern, Firma, Unternehmen, Behörde, Handelsgesellschaft, Wohltätigkeitsorganisation, Institution oder Teile oder eine Kombination der genannten, ob eingetragen oder nicht, öffentlich oder privat.

[QUELLE: ISO/IEC Directives, Part 1, Consolidated ISO Supplement:2014, 3.01]

3.12

Schweregrad

Abschätzung der Größenordnung von möglichen Auswirkungen auf die Privatsphäre einer betroffenen Person

3.13

System

Informationssystem

Anwendungen, Dienste, informationstechnische Werte oder andere Information bearbeitende Komponenten

[QUELLE: ISO/IEC 27000:2016, 2.39]

3.14

Stakeholder

Person oder Organisation, die eine Entscheidung oder Tätigkeit beeinflussen kann, die davon beeinflusst sein kann oder die sich davon beeinflusst fühlen kann

Anmerkung 1 zum Begriff: Das schließt betroffene Personen, die Geschäftsführung, Regulierungsbehörden und Kunden ein.

Anmerkung 2 zum Begriff: Die Rücksprache mit den Stakeholdern ist ein unerlässlicher Bestandteil der DSFA.

[QUELLE: ISO/IEC Directives, Part 1, Consolidated ISO Supplement:2014, 3.02, modifiziert — Die Vorzugsbenennung „interessierte Partei“ wurde gestrichen.]

3.15

Technologie

Hardware-, Software- und Firmware-Systeme und -Systemelemente, einschließlich u. a. Informationstechnologie, eingebettete Systeme oder andere elektromechanische oder auf Prozessoren basierende Systeme

[QUELLE: ISO/IEC 16509:1999, 3.3]

4 Abkürzungen

API	Programmierschnittstelle (en: application programming interface)
BYOD	Bring-your-own-Device
IKT	Informations- und Kommunikationstechnik
ISMS	Informationssicherheitsmanagementsystem
pbD	personenbezogene Daten
KMU	kleine und mittlere Unternehmen

5 Grundlagen der DSFA

5.1 Vorteile der Durchführung einer DSFA

Dieses Dokument enthält Leitlinien, die auf eine Reihe von Situationen angepasst werden können, in denen personenbezogene Daten verarbeitet werden. Unabhängig davon kann eine DSFA grundsätzlich durchgeführt werden, um

- Datenschutzfolgen, Datenschutzrisiken sowie Zuständigkeiten zu identifizieren,
- Ausgangsinformationen für eingebauten Datenschutz (manchmal auch Privacy by Design genannt) zu liefern,
- Datenschutzrisiken eines neuen Informationssystems zu überprüfen und deren Folgen und Eintrittswahrscheinlichkeit zu beurteilen,
- eine Grundlage zur Bereitstellung von Datenschutzinformationen für betroffene Personen über jede empfohlene Gegenmaßnahme, die die betroffene Person ergreifen sollte, zu bieten,
- späteres Aktualisieren oder Nachrüsten mit zusätzlichen Funktionalitäten zu unterstützen, die wahrscheinlich Folgen für die personenbezogenen Daten haben, die verwendet werden,
- Datenschutzrisiken mit Stakeholdern zu teilen und abzumildern, oder Belege für die Einhaltung zu bieten.

ANMERKUNG Eine DSFA wird manchmal durch andere Benennungen bezeichnet, z. B. „Datenschutzprüfung“ oder „Folgeschätzungen in Bezug auf den Datenschutz“. Diese besonderen Formen einer DSFA können mit spezifischen Auswirkungen auf den Prozess und den Bericht einhergehen.

Eine DSFA wird oft als Frühwarnsystem beschrieben. Sie bietet einen Weg, um mögliche Datenschutzrisiken aufzudecken, die aus der Verarbeitung personenbezogener Daten entstehen, und informiert so die Organisation, wo diese Vorkehrungen treffen sollte und zugeschnittene Schutzvorrichtungen einrichten sollte, bevor und nicht erst nachdem die Organisation große Investitionen tätigen muss. Die Kosten einer Anpassung des Projektes in der Planungsphase stellen üblicherweise einen Bruchteil von denen dar, die später entstehen würden. Wenn die Datenschutzfolge nicht annehmbar ist, muss das Projekt möglicherweise sogar ganz eingestellt werden. Daher hilft eine DSFA, Datenschutzfragen früh zu erkennen und/oder die Kosten für Managementzeit, Rechtsausgaben und mögliche Bedenken seitens der Presse oder Öffentlichkeit durch frühzeitige Berücksichtigung von Datenschutzfragen zu reduzieren. Sie kann Organisationen auch helfen, kostspielige oder peinliche Datenschutzfehler zu vermeiden.

Obwohl eine DSFA mehr als ein einfacher Compliance-Test sein sollte, trägt sie dennoch dazu bei, die Übereinstimmung einer Organisation mit relevanten Anforderungen an Privatsphäre und Datenschutz bei nachträglichen Beschwerden, Datenschutz-Audits oder Compliance-Untersuchungen darzulegen. Falls ein Datenschutzrisiko oder eine Datenschutzverletzung eintritt, kann der DSFA-Bericht als Beleg dafür dienen, dass die Organisation beim Versuch der Abwendung des Eintretens angemessen gehandelt hat. Das kann helfen, Haftung, negative Presse und Reputationsverluste zu verringern oder abzuwenden.

Eine angemessene DSFA zeigt gegenüber den Kunden der Organisation und/oder den Bürgern auf, dass deren Privatsphäre respektiert und auf ihre Bedenken eingegangen wird. Kunden oder Bürger vertrauen eher einer Organisation, die eine DSFA durchführt als einer, die das nicht tut.

Eine DSFA steigert die Entscheidungsqualität und gibt Aufschluss über interne Kommunikationslücken oder versteckte Annahmen zu Datenschutzfragen des Projektes. Eine DSFA ist ein Werkzeug zur Durchführung einer systematischen Analyse von Datenschutzfragen aus einem Projekt zur Information der Entscheidungsträger. Eine DSFA kann eine glaubwürdige Informationsquelle darstellen.

Eine DSFA ermöglicht es einer Organisation, vorab die Datenschutz-Fallstricke bei einem Prozess, Informationssystem oder Programm kennenzulernen, statt von Auditoren oder Wettbewerbern darauf hingewiesen zu werden. Eine DSFA unterstützt bei der Vorwegnahme und Beantwortung gesellschaftlicher Datenschutzbedenken.

Eine DSFA kann einer Organisation helfen, gesellschaftliches Vertrauen und Zuversicht zu schaffen, dass bei der Entwicklung eines Prozesses, Informationssystems oder Programms der Datenschutz von Beginn an eingebaut wurde.

Vertrauen gründet auf Transparenz, und eine DSFA ist ein festgelegter Prozess, der offene Kommunikation, gemeinsames Verständnis und Transparenz fördert. Eine Organisation, die eine DSFA durchführt, weist gegenüber ihren Mitarbeitern und Vertragspartnern nach, dass sie den Datenschutz ernst nimmt und von ihnen erwartet, es ebenso zu tun. Eine DSFA ist eine Möglichkeit, um Mitarbeiter über den Datenschutz zu informieren und sie für Datenschutzprobleme, die die Organisation beschädigen können, zu sensibilisieren. Sie ist ein Weg, die Werte der Organisation zu bekräftigen. Eine DSFA kann als Hinweis auf die Erfüllung von Sorgfaltspflichten verwendet werden und kann die Anzahl der Kundenaudits reduzieren.

5.2 Zielsetzungen von DSFA-Berichten

Zielsetzung des DSFA-Berichts ist es, die Untersuchungsergebnisse den Stakeholdern mitzuteilen. Aus der DSFA ergeben sich Erwartungen für mehrere Stakeholder.

Nachfolgend angegeben sind Beispiele für typische Stakeholder und deren Erwartungen.

- betroffene Person — Eine DSFA ist ein Instrument, um es den durch pbD referenzierten Personen zu ermöglichen, Sicherheit darüber zu erlangen, dass ihre Privatsphäre geschützt wird.
- Management — Verschiedene Gesichtspunkte finden wie folgt Anwendung:
 - die DSFA als Instrument, um Datenschutzrisiken zu verwalten, ein Bewusstsein zu schaffen und Verantwortlichkeit zu etablieren; Transparenz zur Verarbeitung personenbezogener Daten in der Organisation und mögliche Risiken und Folgen davon; Eingaben für die Geschäfts- oder Produktstrategie;
 - die Aufstellung der DSFA in der frühesten Projektphase stellt sicher, dass die Datenschutzanforderungen in den funktionalen und nicht funktionalen Anforderungen eingeschlossen sowie erreichbar, machbar und durch Änderungs- und Risikomanagement nachvollziehbar sind und darin resultieren können, dass das Projekt nicht anläuft oder aufgelöst wird. Der Aufwand, um personenbezogene Daten des Projektes zu klassifizieren und zu verwalten, sollte als separater Ausgabeposten und Betrag im Projekt- oder Programmbudget bereitgestellt werden, das für alle Stakeholder akzeptabel ist;

- die DSFA als Gelegenheit, Datenschutzanforderungen besser zu verstehen und Aktivitäten anhand dieser Anforderungen zu beurteilen; Ausgangsgröße für die Entwicklung und Bereitstellung von Produkten und Diensten; überprüft und angepasst mittels des Änderungsmanagementprozesses nach Bereitstellung;
- die DSFA als Instrument, um die Datenschutzrisiken auf Funktions-, Projekt- und Einheiten-Ebene zu verstehen; Konsolidierung von Risiken; Ausgangsgröße für die Aufstellung von Datenschutzrichtlinien und Durchsetzungsmechanismen; Ausgangsgrößen für die Anpassung von Datenschutzprozessen;
- Regulierungsbehörde — Die DSFA ist ein Instrument, das zum Nachweis der Einhaltung geltender rechtlicher Anforderungen beiträgt. Sie kann belegen, dass eine Organisation die erforderliche Sorgfalt ergriffen hat, falls es z. B. zu einer Datenschutzverletzung, Regelabweichung oder Beschwerde kommt;
- Kunde — Die DSFA ist ein Mittel, um zu beurteilen, wie die verantwortliche Stelle oder der Auftragsdatenverarbeiter mit personenbezogenen Daten umgeht und kann belegen, dass den vertraglichen Verpflichtungen nachgekommen wird.

Der DSFA-Bericht sollte zwei Grundfunktionen erfüllen. Die erste (Bestandsliste) informiert die spezifischen Stakeholder laufend über die identifizierte(n) betroffenen Stellen, betroffene Umgebung und Datenschutzrisiken über den Lebenszyklus der betroffenen Stellen, ob inhärent oder abgemildert. Die zweite Liste (Aktionspunkte) ist ein Mechanismus zur Nachverfolgung der Aktionen/Aufgaben, die die identifizierten Datenschutzrisiken verbessern und/oder beheben. Die Sensibilität einer Verteilung und Freigabe der Berichtsinformationen muss eindeutig bewertet und klassifiziert werden (privat, vertraulich, öffentlich usw.).

5.3 Verantwortlichkeit für die DSFA-Durchführung

Eine DSFA von Prozessen oder Informationssystemen sollte von einer aus einer Anzahl verschiedener Organisationseinheiten durchgeführt werden, darf aber auch für einen Prozess, ein Informationssystem oder ein Programm durch Verbraucherorganisationen oder Nichtregierungsorganisationen ausgeführt werden.

Typischerweise sollte die Zuständigkeit (en: responsibility) dafür, dass eine DSFA durchgeführt wird, in erster Linie bei der Person liegen, die für den Schutz von pbD zuständig ist, anderenfalls bei dem Projektmanager, der die neue Technologie, den Dienst oder das Vorhaben entwickelt, welches Folgen für den Datenschutz haben kann.

Die Verantwortlichkeit (en: accountability) dafür, dass die DSFA durchgeführt wird und für die Qualität des Ergebnisses (DSFA-Verantwortlichkeit) sollte bei der Geschäftsführung der verantwortlichen Stelle liegen. Die Person, der die Zuständigkeit für die Durchführung der DSFA zugewiesen wurde, darf diese selbst durchführen, andere interne bzw. externe Stakeholder zur Hilfe heranziehen oder einen unabhängigen Dritten mit dieser Arbeit beauftragen. Jeder dieser Ansätze hat Vor- und Nachteile.

Wenn die DSFA direkt von der Organisation durchgeführt wurde, können Verbraucherverbände oder staatliche Stellen anfordern, dass die Angemessenheit der DSFA durch einen unabhängigen Auditor bestätigt wird.

Die Organisation sollte sicherstellen, dass für die Behandlung der Datenschutzrisiken, einschließlich der Umsetzung und Aufrechterhaltung des Datenschutzrisiken-Managementprozesses, und für die Angemessenheit und Wirksamkeit aller Steuerungsmaßnahmen Verantwortlichkeiten bestehen und Berechtigungen vorhanden sind. Dies kann unterstützt werden durch

- Festlegen, wer für die Entwicklung, Umsetzung und Aufrechterhaltung des Rahmens zur Verwaltung der Datenschutzrisiken verantwortlich ist, sowie

- Festlegen von Risikoeigentümern zum Umsetzen der Behandlung von Datenschutzrisiken, zum Aufrechterhalten der Steuerungsmaßnahmen für den Datenschutz und zur Berichterstattung relevanter Informationen zu den Datenschutzrisiken.

5.4 Abstufung einer DSFA

Die Abstufung der DSFA hängt ab davon, wie erheblich die vermuteten Auswirkungen sind. Wenn z. B. angenommen wird, dass die Auswirkungen nur Mitarbeiter der Organisation betreffen (z. B. wenn diese die Verbesserung der Zutrittskontrolle durch den Einsatz von biometrischen Merkmalen, wie z. B. eines Daumenabdrucks jedes Mitarbeiters, anstrebt), kann sich die DSFA nur auf die Einbindung von Arbeitnehmervertretern beschränken und mit verhältnismäßig geringer Abstufung erfolgen. Wenn aber eine Regierungsstelle ein neues Identitätsmanagementsystem für alle Bürger einführen will, muss sie eine weit umfangreichere DSFA durchführen, bei der vielfältige externe Stakeholder einbezogen werden.

Organisationen sollten eine Selbsteinschätzung zur erforderlichen Abstufung der DSFA bereitstellen, die den geltenden Gesetzen und Vorschriften entspricht. Menge und Detailierungsgrad der personenbezogenen Daten je Person, der Grad der Sensibilität dieser Daten, die Anzahl der betroffenen Personen und die Anzahl der zugriffsberechtigten Personen auf die verarbeiteten personenbezogenen Daten sind die kritischen Faktoren, um die Abstufung zu bestimmen.

Für KMU, gemeinnützige Organisationen oder Regierungsorganisationen kann die Ermittlung der angemessenen Abstufung für die DSFA gemeinsam, aber nicht verbindlich, von der mit der Durchführung der DSFA beauftragten Person (siehe 5.3), der KMU-Unternehmensleitung und/oder unter Beratung durch externe Experten vorgenommen werden.

6 Prozess-Anleitung für die Durchführung einer DSFA

6.1 Allgemeines

Der Anwendungsbereich der DSFA, die spezifischen Angaben dessen, was sie abdeckt und wie sie durchgeführt wird, müssen/muss angepasst werden an die Größe der Organisation, die örtliche Rechtsprechung und das genaue Programm, das Informationssystem oder den Prozess, das/der Gegenstand der DSFA ist. In Abschnitt 6

- ist die „Zielsetzung“ etwas, das erreicht werden sollte,
- gibt die „Eingabe“ Leitlinien dafür vor, welche Informationen möglicherweise benötigt werden, um die „Zielsetzung“ zu erreichen,
- ist das „erwartete Ergebnis“ das empfohlene Ziel der „Aktionen“,
- sind „Aktionen“ oder deren Äquivalente Leitlinien für Tätigkeiten, deren Ausführung erforderlich sein kann, um die „Zielsetzung“ zu erreichen und das empfohlene „erwartete Ergebnis“ herbeizuführen, sowie
- bietet die „Anleitung zur Umsetzung“ weitere Einzelheiten dessen, was bei der Durchführung der „Aktionen“ möglicherweise beachtet werden muss.

Die „Aktionen“ in diesem Abschnitt, oder Äquivalente, angepasst an den gewünschten Anwendungsbereich und die Abstufung der DSFA, dürfen eigenständig von einer Organisation umgesetzt werden. Sie sind dazu vorgesehen, eine vernünftige Grundlage für die Planung, Umsetzung und Nachverfolgung einer DSFA für vielfältige Einsatzbereiche zu bilden.

Es kann sein, dass die eine DSFA durchführende Organisation die nachstehende Prozessanleitung direkt an ihren spezifischen Anwendungsbereich und ihre Abstufung anpassen möchte oder als mögliche Alternative ein geeignetes risikobasierendes Managementsystem wie z.B. ISO/IEC 27001 auswählt und darin angemessen angepasste Elemente der nachfolgenden Anleitungen integriert, einschließlich der Anwendung des DSFA-Berichts (siehe Abschnitt 7), um die Datenschutzrisiken zu behandeln, die der Bericht offengelegt hat.

Der Ausdruck „eine DSFA durchführen“ wird in diesem Dokument verwendet, um sowohl eine anfängliche DSFA zu beschreiben, bei der die notwendigen Schritte und Aktionen ausgewählt werden, um der betreffenden DSFA-Anforderung zu entsprechen, als auch für eine Aktualisierung einer bestehenden DSFA, bei der nur diejenigen Schritte und Aktionen durchgeführt werden, die für die Aktualisierung erforderlich sind.

Anhang C enthält eine weitere Anleitung zum Verständnis der in diesem Dokument verwendeten Begriffe.

Um KMU beim DSFA-Prozess zu unterstützen, sollten Industrieverbände oder KMU-Vereinigungen motiviert werden, Verhaltensregeln mit wertvollen Leitlinien zu entwerfen, und KMU sollten ermutigt werden, dabei mitzuwirken. Vernünftige Verhaltensregeln müssten die in diesem Dokument vermittelten Werte berücksichtigen und könnten von den Datenschutzbehörden unterstützt werden.

6.2 Feststellen, ob eine DSFA erforderlich ist (Schwellenwertanalyse)

Zielsetzung: Feststellen, ob eine neue oder aktualisierte DSFA erforderlich ist.

Eingabe: Informationen über das Programm, Informationssystem oder den Prozess, der untersucht werden soll.

Erwartetes Ergebnis: Ergebnis der Schwellenwertanalyse und Mandat zur Vorbereitung einer neuen oder aktualisierten DSFA, falls erforderlich, und Aufgaben- und Anwendungsbereich der beschlossenen DSFA.

Aktionen:

Das Management der Organisation sollte entscheiden, ob eine neue oder aktualisierte DSFA erforderlich ist.

Wenn eine neue oder aktualisierte DSFA benötigt wird, sollte das Management der Organisation gemeinsam mit der vorgesehenen Prüfperson den Aufgabenbereich definieren und die Grenzen und den Geltungsbereich der DSFA ermitteln, um ihren Anwendungsbereich festzulegen. Die Organisation sollte ebenfalls über die Abstufung der DSFA, über den Prozess, der für die Durchführung der DSFA verwendet werden soll und über die Zielgruppen entscheiden, damit also über Art und Inhalt der zu erstellenden DSFA-Berichte, und diese Entscheidung dokumentieren.

Das Ergebnis dieses Prozesses in Form des Ergebnisses der Schwellenwertanalyse sowie des Anwendungsbereichs und des Aufgabenbereiches der DSFA sollten im DSFA-Bericht dokumentiert werden (siehe 7.2).

Anleitung zur Umsetzung:

Eine Organisation sollte eine neue oder aktualisierte DSFA durchführen, wenn sie Datenschutzfolgen erwartet aus

- einer neuen oder zukünftigen Technologie, einem Dienst oder anderen Vorhaben, worin personenbezogene Daten verarbeitet werden oder verarbeitet werden sollen,
- einer Entscheidung, dass sensible personenbezogene Daten (siehe ISO/IEC 29100:2011, 2.26) verarbeitet werden sollen,

- Änderungen an geltenden datenschutzbezogenen Gesetzen und Verordnungen, internen Richtlinien und Normen, dem Betrieb von Informationssystemen, Zwecken und Mitteln der Datenverarbeitung, neuen oder veränderten Datenflüssen usw., sowie
- Geschäftsexpansion oder Übernahmen.

Eine Organisation kann eine Richtlinie zu den Schwellenwerten, die eine neue oder aktualisierte DSFA auslösen, erlassen und die anfänglich anzuwendenden technischen und organisatorischen Maßnahmen festlegen. Solch eine Richtlinie sollte allen anwendbaren Aspekten der vorstehenden Liste Rechnung tragen und Grenzen festlegen, innerhalb derer die Verarbeitung von personenbezogene Daten entwickelt und betrieben werden darf, ohne eine neue PIA erforderlich zu machen.

6.3 Vorbereitung der DSFA

6.3.1 Team für DSFA zusammenstellen und Anweisungen erteilen

Zielsetzung: Bestimmung des Anwendungsbereichs für die DSFA und der erforderlichen Expertise und Formulierung des Aufgabenbereiches für die Durchführung der DSFA.

Eingabe: Auftrag, eine DSFA vorzubereiten (siehe 6.2).

Erwartetes Ergebnis: Zuständige Person benannt, Risikokriterien.

Aktionen:

Eine Person, die für die Durchführung der DSFA zuständig sein wird (die Prüfperson), sollte von der Organisation bestimmt und benannt werden. Die Organisation sollte außerdem die verantwortliche Person für die Freigabe des DSFA-Berichts benennen.

Die Prüfperson sollte die Risikokriterien definieren und sicherstellen, dass die Unternehmensleitung den Risikokriterien, deren Anwendung für die Bewertung der Risikobedeutung vorgesehen ist, zustimmt. Diese Kriterien dürfen auf den in Anhang A genannten basieren oder von der Organisation getrennt davon definiert werden, gemeinsam mit den Kriterien zur Einschätzung des Auswirkungsgrades und des Risikos mit ihren entsprechenden Abstufungen. Die Prüfperson sollte auch die Kriterien für die Annahme des Risikos identifizieren und sicherstellen, dass die Unternehmensleitung diesen Kriterien zustimmt.

Das Ergebnis dieses Prozesses in Form der Risikokriterien (siehe 7.3.2) und die Ressourcen (siehe 7.3.3) sollten im DSFA-Bericht dokumentiert werden.

Anleitung zur Umsetzung:

Die Kriterien sollten die Werte, Zielsetzungen und Ressourcen der Organisation widerspiegeln. Bei der Definition der Risikokriterien sollte die Prüfperson die folgenden Faktoren berücksichtigen:

- gesetzliche und regulatorische Faktoren, die sich auf den Schutz der Privatsphäre der natürlichen Person und den Schutz ihrer personenbezogenen Daten auswirken;
- externe Faktoren, wie z. B. Branchenrichtlinien, Berufsstandards, Firmengrundsätze und Vereinbarungen mit Kunden;
- Faktoren, die durch eine spezifische Anwendung vorbestimmt oder in einem spezifischen Anwendungskontext begründet sind;
- andere Faktoren, die den Entwurf von Informationssystemen und die damit verbundenen Datenschutzanforderungen betreffen können.

Das Management der Organisation sollte getrennt sowohl die Datenschutzrisiken aus dem Blickwinkel einer betroffenen Person als auch die Datenschutzrisiken aus dem Blickwinkel der Organisation untersuchen.

Diese Kriterien sollten später für die Beurteilung der Datenschutzrisiken und deren Behandlung verwendet werden. Die für die Durchführung der DSFA zuständige Person sollte den Aufgabenbereich und den Anwendungsbereich der DSFA vorschlagen.

Um die Regeln zur Bewertung der Bedeutung von Datenschutzrisiken zu definieren, sollte die Prüfperson die folgenden Fragen stellen:

- Welche Kriterien werden zur Abschätzung des Auswirkungsgrades für die betroffene Person und für die Organisation verwendet? (Zum Beispiel der Grad der Identifikation, Sensibilität der Daten im Falle einer Datenschutzverletzung, Anzahl der betroffenen Personen und Auswirkungsgrad auf die Organisation.)
- Welche Kriterien werden zur Abschätzung der Eintrittswahrscheinlichkeit verwendet? (Zum Beispiel die Schwachstellen der unterstützenden Datenschutzwerte und die Fähigkeiten der Risikoquellen, diese Schwachstellen auszunutzen.)
- Welche Abstufung(en) wird/werden bei der Bestimmung des Auswirkungsgrades genutzt?
- Welche Abstufung(en) wird/werden bei der Bestimmung der Eintrittswahrscheinlichkeit genutzt?
- Welche Bedeutung hat jede Kombination (Grad der Auswirkung und Eintrittswahrscheinlichkeit), die zur Bewertung der Risiken verwendet wird? Welche Kriterien gelten insbesondere für die Risikoakzeptanz?
- Welches ist die anzuwendende Strategie, um jedes einzelne Risiko zu behandeln? Welches ist insbesondere die Strategie für die Risiken, die akzeptiert werden können?
- Wie wird die Strategie durch die Vorteile der Verarbeitung personenbezogener Daten beeinflusst?

ANMERKUNG 1 Diese Kriterien stehen im Einklang mit den anderen Risikokriterien, die in der Organisation verwendet werden.

ANMERKUNG 2 Bei jeder Anwendung der Kriterien werden Chancen zu ihrer Verbesserung geprüft.

Die Definition der Risikokriterien sollte auf Folgendem beruhen:

- dem Schaden für Anwender des Produktes, Dienstes oder Systems. Der Schaden darf physische und finanzielle Schäden, Rufschädigung, Bloßstellung und das Eindringen in das Familienleben einschließen. Darüber hinaus sollte die Organisation verschiedene Arten der Privatsphäre berücksichtigen, wenn sie die Auswirkungen von Datenschutzrisiken für personenbezogene Daten auf die betroffene Person betrachtet, wie z. B. das Recht auf körperliche Unversehrtheit, die Unverletzlichkeit des privaten Raumes und die Privatsphäre des persönlichen Handelns, der Kommunikation, der Daten und Bilder, des Denkens und Fühlens sowie der Versammlungen;
- den gesetzlichen und regulatorischen Anforderungen und vertraglichen Verpflichtungen;
- den Erwartungen und Wahrnehmungen der Stakeholder und den negativen Folgen für Firmenwert und Reputation;
- der betrieblichen Bedeutung der Verfügbarkeit, Vertraulichkeit und Integrität der personenbezogenen Daten;
- dem strategischen Wert des Informationsprozesses;