DIN EN ISO/IEC 29134

DIN

ICS 35.030

Einsprüche bis 2020-02-06

Entwurf

Informationstechnik – Sicherheitsverfahren – Datenschutz-Folgenabschätzung – Leitfaden (ISO/IEC 29134:2017); Deutsche und Englische Fassung prEN ISO/IEC 29134:2019

Information technology –
Security techniques –
Guidelines for privacy impact assessment (ISO/IEC 29134:2017);
German and English version prEN ISO/IEC 29134:2019

Technologies de l'information –
Techniques de sécurité –
Lignes directrices pour l'évaluation d'impacts sur la vie privée (ISO/IEC 29134:2017);
Version allemande et anglaise prEN ISO/IEC 29134:2019

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-12-06 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin, Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 111 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29134:2020-01

Nationales Vorwort

Dieses Dokument (prEN ISO/IEC 29134:2019) wurde vom Technischen Komitee ISO/IEC/JTC 1 „Information technology“ in Zusammenarbeit mit dem Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Gremium 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 9000:2015	siehe	DIN EN ISO 9000:2015-11
ISO 21500	siehe	DIN ISO 21500
ISO 31000	siehe	DIN ISO 31000
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

Nationaler Anhang NA
(informativ)

Literaturhinweise

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

DIN EN ISO/IEC 27000:2017-10, *Informationstechnik — Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Überblick und Terminologie (ISO/IEC 27000:2018); Deutsche und Englische Fassung prEN ISO/IEC 27000:2019*

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 ISO 21500, *Leitlinien Projektmanagement*

DIN ISO 31000, *Risikomanagement — Leitlinien*

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29134:2020-01

– Entwurf –

CEN/TC 1

Datum: 2019-11

prEN ISO/IEC 29134:2019

CEN/TC 1

Sekretariat: ANSI

Informationstechnik — Sicherheitsverfahren — Datenschutz-Folgenabschätzung - Leitfaden (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)

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

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: CEN-Umfrage
Dokument-Sprache: D

STD Version 2.9p

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29134:2020-01

Inhalt

Seite

Europäisches Vorwort **4**

Vorwort **5**

Einleitung **6**

1 Anwendungsbereich **8**

2 Normative Verweisungen **8**

3 Begriffe **8**

4 Abkürzungen **10**

5 Grundlagen der DSFA **11**
5.1 Nutzen aus 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 werden soll **19**
6.3.4 Einbindung von Anspruchsgruppen **21**
6.4 Durchführung der DSFA **23**
6.4.1 Informationsflüsse personenbezogener Daten identifizieren **23**
6.4.2 Auswirkungen des Anwendungsfalles analysieren **24**
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 Ausführen des Behandlungsplans 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 Untersuchter Prozess **41**
7.3.2 Risikokriterien **43**
7.3.3 Ressourcen und beteiligte Personen **43**
7.3.4 Konsultation mit Anspruchsgruppen **43**
7.4 Datenschutzanforderungen **43**
7.5 Risikobeurteilung **43**
7.5.1 Risikoquellen **43**

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29134:2020-01

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 Behandlung der Risiken 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 Wahrscheinlichkeit 47

Anhang B (informativ) Generische Bedrohungen 48

Anhang C (informativ) Hilfestellung für die Einordnung verwendeter Begriffe 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 Datenschutz-Risikokarte 56

Literaturhinweise 58

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29134:2020-01

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 prEN ISO/IEC 29134:2019 durch das Technische Komitee CEN/TC 1 „ISO/IEC Gemeinschaftskomitee für Informationstechnik“ übernommen, dessen Sekretariat von ANSI gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 29134:2017 wurde von CEN als prEN ISO/IEC 29134:2019 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29134:2020-01

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.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

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

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29134:2020-01

Einleitung

Eine Datenschutz-Folgenabschätzung (DSFA) ist ein Instrument zur Abschätzung möglicher Auswirkungen auf die Privatsphäre, die von einem (Geschäfts-)prozess, Informationssystem, Programm, Software-Modul, Gerät oder von einem sonstigen Vorhaben ausgehen, die personenbezogene Daten (pbD) verarbeiten, und erfolgt in Rücksprache mit den Anspruchsgruppen, 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 Informationssicherheits-managementsystems (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 (Privacy by design) sicherzustellen. Sie ist ein Prozess, der fortdauert 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 für alle Vorhaben bieten. 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 könnte zur Durchführung einer DSFA verpflichtet sein und könnte einen Auftragsdatenverarbeiter, der für ihn tätig ist, bitten, ihn hierbei zu unterstützen. Es wäre aber auch möglich, dass ein Auftragsdatenverarbeiter oder ein Lieferant eine DSFA auf eigenen Wunsch durchführen möchten.

Die DSFA-Information eines Lieferanten ist insbesondere relevant wenn Geräte mit Datenverbindung Teil eines untersuchten Informationssystems, einer Anwendung oder eines Prozesse sind. Für den Lieferanten solcher Geräte kann es unter Umständen erforderlich sein, Denjenigen, die die DSFA durchführen, datenschutzrelevante Informationen zum Geräteaufbau bereitzustellen. Wenn der Anbieter elektronischer Geräte in der Durchführung von DSFAs ungeschult ist und nicht über entsprechende Ressourcen verfügt, z. B.:

— kleine Einzelhandelsgeschäfte, oder

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

dann kann der Gerätehersteller dazu aufgefordert werden, seine Datenschutzinformation zu erweitern und selbst eine DSFA im Hinblick auf den zu erwartenden Kontext aus Beteiligten und KMU für die hergestellte Einrichtung anbieten, um das entsprechende Unternehmen zu einer minimalen DSFA zu befähigen.

Eine DSFA wird üblicherweise von Organisationen durchgeführt, die ihre Verantwortung ernst nehmen und mit Betroffenen angemessen umgehen. In einigen Zuständigkeitsbereichen kann eine DSFA erforderlich sein um den Anforderungen von Gesetzen und Verordnungen zu entsprechen.

Dieses Dokument ist zur Verwendung vorgesehen wenn die Datenschutzauswirkung auf Betroffene die Betrachtung von Prozessen, Informationssystemen oder Programmen einschließt, wobei:

— die Verantwortung für die Umsetzung und/oder Auslieferung des Prozesses, Informationssystems oder Programms mit anderen Organisationen geteilt wird und sichergestellt werden sollte, dass jede Organisation die identifizierten Risiken angemessen adressiert,

— eine Organisation Datenschutzrisikomanagement als Teil ihrer übergreifenden Risikomanagement-Bemühungen durchführt, um die Umsetzung oder Verbesserung ihres ISMS (festgelegt nach

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29134:2020-01

ISO/IEC 27001 oder vergleichbarem Managementsystem) vorzubereiten; oder eine Organisation Datenschutzrisikomanagement als unabhängige Funktion durchführt,

— eine Organisation (z. B. die Regierung) ein Vorhaben unternimmt (z. B. ein öffentliches oder privates Partnerschaftsprogramm), in dem die zukünftig für die Verarbeitung verantwortliche Organisation noch nicht bekannt ist, mit dem Ergebnis dass der Behandlungsplan nicht direkt umgesetzt werden kann, und der Behandlungsplan stattdessen Gegenstand der dazugehörigen Gesetzgebung, Verordnung oder des Vertrages werden sollte,

— die Organisation sich gegenüber den Betroffenen verantwortungsbewusst verhalten möchte.

Für notwendig erachtete Steuerungsmaßnahmen zur Behandlung der während des DSFA-Prozesses ermittelten Risiken, dürfen 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 dürfen von der für die Durchführung des DSFA verantwortlichen Person unabhängig von beliebigen anderen Maßnahmen-Sammlungen festgelegt werden.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29134:2020-01

1 Anwendungsbereich

Dieses Dokument bietet Leitlinien für

— einen Prozess zur Datenschutz-Folgenabschätzung, und

— Struktur und Inhalt für einen DSFA-Bericht.

Es ist anwendbar für Organisationen jeden Typs und jeder Größe, einschließlich öffentlicher Unternehmen, Unternehmen der Privatwirtschaft, Regierungsinstanzen und gemeinnützige (Non-Profit) Organisationen.

Dieses Dokument ist relevant für diejenigen, die bei der Entwicklung oder Implementierung von Projekten eingebunden sind, einschließlich derer, die die Systeme und Dienste betreiben, 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 eingebunden sind

Anmerkung 1 zum Begriff: Im Zusammenhang mit dem Datenschutz-Risikomanagementprozess ist ein Datenschutzwert entweder die personenbezogenen Daten selbst oder ein unterstützender Datenschutzwert.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29134:2020-01

3.3
Prüfperson
Person, die eine *Datenschutz-Folgenabschätzung* (3.7) leitet und durchführt

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

Anmerkung 2 zum Begriff: Die Prüfperson darf 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 Nutzern erlaubt Aktionen auszuführen

3.6
Datenschutzfolge
alles was eine Auswirkung auf die Privatsphäre eines und oder einer Gruppe von Betroffenen hat

Anmerkung 1 zum Begriff: Die Datenschutzfolge könnte aus der Verarbeitung personenbezogener Daten in Übereinstimmung und in 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 das unternehmensweite 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 Datenschutzrisiken identifiziert

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

3.9
Programm
Gruppe von Projekten, die zur Erschließung von Vorteilen koordiniert verwaltet werden, die bei individuellem Management nicht entstehen

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

3.10
Projekt
einmaliger Prozess, bestehend aus einer Sammlung koordinierter und gesteuerter Aktivitäten mit Anfangs- und Enddatum, zur Erreichung eines Ziels durch Erfüllung spezifischer Anforderungen, einschließlich Beschränkungen von Zeit, Kosten und Ressourcen

[QUELLE: ISO 9000:2015, 3.4.2]

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29134:2020-01

3.11
Organisation
Person oder Gruppe von Personen, die über ihre eigenen Funktionen einschließlich Verantwortlichkeiten, Befugnissen und Beziehungen verfügt, um ihre Zielsetzungen 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 Folgen für die Privatsphäre eines Betroffenen

3.13
System
Informationssystem
Anwendungen, Dienste, informationstechnologische Datenschutzwerte oder andere Komponenten zur Verarbeitung von Informationen

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

3.14
Anspruchsgruppe
Person oder Organisation, welche eine Entscheidung oder Aktivität beeinflussen kann oder durch eine Entscheidung oder Aktivität betroffen ist oder sich dadurch betroffen fühlt

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

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

[QUELLE: *ISO/IEC Directives, Part 1, Consolidated ISO Supplement*:2014, 3.02 — angepasst — Die Vorzugsbenennung „interessierte Partei“ wurde nicht mit übernommen.]

3.15
Technologie
Hardware-, Software-, und Firmware-Systeme und Systemelemente, einschließlich u. a. Informationstechnologie, eingebettete Systeme, oder alle anderen elektromechanischen 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

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29134:2020-01

5 Grundlagen der DSFA

5.1 Nutzen aus 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 ausgeführt werden, um

— Auswirkungen auf den Datenschutz, Datenschutzrisiken sowie Verantwortlichkeiten zu identifizieren,

— Ausgangsinformationen für eingebauten Datenschutz (manchmal auch Privacy by design genannt) liefern,

— Datenschutzrisiken eines neuen Informationssystems zu überprüfen und seine Folgen und Eintrittswahrscheinlichkeit zu ermitteln,

— eine Grundlage zur Bereitstellung von Datenschutzinformationen für Betroffene über jede empfohlene Gegenmaßnahme, die der Betroffene 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 Anspruchsgruppen zu teilen und abzumildern, oder Belege für die Einhaltung zu bieten.

ANMERKUNG Eine DSFA wird manchmal mit anderen Begriffen bezeichnet, z. B. „Datenschutzprüfung“ oder „Datenschutz-Folgenabschätzung“. Diese besonderen Formen einer DSFA könnten mit spezifischen Auswirkungen für den Prozess und Bericht einhergehen.

Eine DSFA wurde oft als Frühwarnsystem beschrieben. Sie bietet einen Weg um mögliche Datenschutzrisiken aufzudecken, die aus der Verarbeitung personenbezogener Daten entstehen und informieren dabei die Organisation, wo sie 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 Datenschutzfolgen nicht annehmbar sind, muss das Projekt möglicherweise sogar ganz eingestellt werden. Daher hilft eine DSFA dabei, Datenschutzfragen früh zu erkennen und/oder die Kosten für Managementzeitbindung, Rechtsausgaben und mögliche Bedenken seitens der Presse oder Öffentlichkeit durch frühzeitige Behandlung der Datenschutzfragen zu reduzieren. Sie kann Organisationen unter Umständen auch helfen, kostspielige oder peinliche Datenschutzfehler zu vermeiden.

Obwohl die 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 ihres Auftretens angemessen gehandelt hat. Das kann helfen, Haftung, negative Presse und Reputationsverluste zu verringern oder abzuwenden.

Eine angemessene DSFA zeigt den Kunden der Organisation und/oder den Bürgern, 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 des Projektes und gibt interne Kommunikationslücken oder versteckte Annahmen zu Datenschutzfragen preis. 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.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29134:2020-01

Eine DSFA ermöglicht es einer Organisation, vorab die Datenschutz-Fallstricke eines Prozesses, Informationssystems oder Programms kennenzulernen, statt von Auditoren oder Wettbewerbern darauf hingewiesen werden zu müssen. Eine DSFA unterstützt bei der Vorwegnahme und Beantwortung gesellschaftlicher Datenschutzbedenken.

Eine DSFA kann Organisationen helfen gesellschaftliches Vertrauen und Zuversicht zu schaffen, dass Datenschutz von Beginn an bei einem Prozess, Informationssystem oder Programm eingebaut wurde.

Vertrauen bildet sich auf Transparenz, und eine DSFA ist ein festgelegter Prozess der offene Kommunikation, gemeinsames Verständnis und Transparenz fördert. Eine Organisation, die eine DSFA durchführt, zeigt ihren Mitarbeitern und Vertragspartnern, dass sie den Datenschutz ernst nimmt und von ihnen erwartet, es ebenso zu tun. Eine DSFA ist eine Möglichkeit, Mitarbeiter über den Datenschutz zu informieren und sie für Datenschutzprobleme, die die Organisation beschädigen könnten, zu sensibilisieren. Sie ist ein Weg, die Werte der Organisation zu bekräftigen. Eine DSFA kann als Indikator für die Sorgfaltspflicht verwendet werden und kann unter Umständen die Anzahl der Kundenaudits reduzieren.

5.2 Zielsetzungen von DSFA-Berichten

Das Ziel des DSFA-Berichts ist es, die Untersuchungsergebnisse den Anspruchsgruppen mitzuteilen. Aus der DSFA ergeben sich Erwartungen für mehrere Anspruchsgruppen.

Nachfolgend angegeben sind typische Anspruchsgruppen und ihre Erwartungen.

— Betroffene — Eine DSFA ist ein Instrument, um es den Personen (Subjekten) der personenbezogenen Daten 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 Verantwortung 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 , erreichbar, machbar und durch Änderungs- und Risikomanagement nachvollziehbar sind und unter Umständen darin resultieren können, das 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, und für alle Anspruchsgruppen;

  — die DSFA als Gelegenheit, Datenschutzanforderungen besser zu verstehen und Aktivitäten gegen diese Anforderungen abzugleichen; als Ausgangsgröße für die Entwicklung und Bereitstellung von Produkten und Diensten; überprüft und angepasst mittels des Änderungsmanagementprozesses nach Auslieferung;

  — die DSFA als Instrument, die Datenschutzrisiken auf Funktions-, Projekt- und Einheiten-Ebene zu verstehen; Konsolidierung von Risiken; Ausgangsgröße für die Aufstellung von Datenschutzgrundsätzen und Umsetzungsmechanismen; Ausgangsgrößen für die Anpassung von Datenschutzprozessen;

— Regulierungsbehörde — Die DSFA ist ein Instrument, das zum Nachweis über die Einhaltung anzuwendender 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;

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29134:2020-01

— Kunde — Die DSFA ist ein Mittel um herauszufinden, wie der für die Verarbeitung Verantwortliche oder die verantwortliche Stelle 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 Anspruchsgruppen laufend über die betroffenen Stellen, betroffene Umwelt- und Datenschutzrisiken über den Lebenszyklus der betroffenen Stellen, ob inhärent oder abgemildert. Die zweite Liste (Aktionspunkte) ist ein Mechanismus zur Nachverfolgung der Aktionen und 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 der vielen verschiedenen Organisationseinheiten durchgeführt werden, darf aber auch für einen Prozess, Informationssystem oder Programm durch Kundenorganisationen oder Nichtregierungsorganisationen ausgeführt werden.

Typischerweise sollte die Zuständigkeit dafür, dass eine DSFA durchgeführt wird, in erster Linie bei der Person liegen, die für den Datenschutz zuständig ist, anderenfalls bei dem Projektmanager, der die neue Technologie, den Dienst oder das Vorhaben entwickelt, welches unter Umständen Auswirkungen auf die Privatsphäre haben könnte.

Die Verantwortlichkeit dafür, dass die DSFA durchgeführt wird und für die Qualität des Ergebnisses (DSFA-Verantwortung) 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 Anspruchsgruppen 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, dürfen Verbraucherschutzvereinigungen 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 Unterhaltung des Datenschutzrisiken-Managementprozesses, und für die Angemessenheit und Wirksamkeit aller Steuerungsmaßnahmen die entsprechende Verantwortung übernommen wird und Fähigkeiten vorhanden sind. Dies kann unterstützt werden durch

— Festlegen, wer für die Entwicklung, Umsetzung und Unterhaltung des Rahmens zur Verwaltung der Datenschutzrisiken verantwortlich ist, sowie durch

— Festlegen von Risikoeigentümern zum Einrichten der Datenschutzmaßnahmen, Unterhalten der Steuerungsmaßnahmen für den Datenschutz und zur Berichterstattung relevanter Informationen zu den Datenschutzrisiken.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29134:2020-01

5.4 Abstufung einer DSFA

Die Abstufung der DSFA hängt ab davon, wie signifikant die vermuteten Auswirkungen sind. Wenn man z. B. annimmt, dass die Auswirkungen nur Mitarbeiter der Organisation betreffen (z. B. Verbesserung der Zutrittskontrolle durch den Einsatz von biometrischen Merkmalen, wie z. B. der Fingerabdruck der Mitarbeiter), könnte sich die DSFA nur auf die Einbindung von Arbeitnehmervertretern beschränken und mit verhältnismäßig geringer Abstufung erfolgen. Wenn aber die Regierungsstelle ein neues Identitätsmanagementsystem für alle Bürger einführen will, wird eine weit umfangreichere DSFA durchgeführt werden müssen, bei der externe Anspruchsgruppen weitreichend einbezogen werden.

Für die erforderliche Abstufung der DSFA sollten Organisationen eine Selbsteinschätzung treffen, die den geltenden Gesetzen und Vorschriften entspricht. Menge und Detailierungsgrad der personenbezogenen Daten pro Person, der Grad der Sensibilität dieser Daten, die Anzahl der Betroffenen und die Anzahl der zugriffsberechtigten Personen auf die verarbeiteten personenbezogene Daten sind die kritischen Faktoren, um die Abstufung zu bestimmen.

Für KMU, gemeinnützige oder Regierungsorganisationen kann die Ermittlung der angemessenen Abstufung für eine DSFA gemeinsam, aber nicht verbindlich, von der mit der Durchführung der DSFA beauftragten Person (siehe 5.3), der KMU-Unternehmensleitung und/oder, wo angemessen, durch den Ratschlag externer Experten erreicht 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 angepasst werden an die Größe der Organisation, das anwendbare Recht und das genaue Programm, Informationssystem oder den Prozess, der Gegenstand der DSFA ist. Im Abschnitt 6

— ist die „Zielsetzung" etwas, das erreicht werden sollte,

— gibt die „Eingabe" Leitlinien dafür vor, welche Informationen benötigt werden, um die „Zielsetzung" zu erreichen,

— ist das „erwartete Ergebnis" das empfohlene Ziel der „Aktionen",

— sind „Aktionen" Leitlinien für Tätigkeiten, deren Ausführung unter Umständen erforderlich sein kann, um die „Zielsetzung" zu erreichen und das „erwartete Ergebnis" herbeizuführen, sowie

— bietet die „Umsetzung der Anleitung" genauere Einzelheiten, die bei der Durchführung der „Aktionen" möglicherweise beachtet werden müssen.

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

Es könnte sein, dass die eine DSFA durchführende Organisation die nachstehende Prozessrichtlinie 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 hierin die nachfolgenden Anleitungen in angemessener Weise integriert und adaptiert, einschließlich der Anwendung des DSFA-Berichts (siehe Abschnitt 7), um die Datenschutzrisiken zu behandeln, die der Bericht offengelegt hat.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29134:2020-01

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 den besonderen DSFA-Anforderungen 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 KMUs beim DSFA-Prozess zu unterstützen sollten Industrieverbände motiviert werden, Verhaltensregeln mit wertvollen Anleitungen zu entwerfen und KMUs sollten zur Mitwirkung dabei ermutigt werden. Vernünftige Verhaltensregeln müssten die in diesem Dokument vermittelten Werte berücksichtigen und könnten von den Datenschutzbehörden aufgegriffen werden.

6.2 Feststellen, ob eine DSFA erforderlich ist (Schwellenwertanalyse)

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

Eingabe: Information 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 festlegen, Grenzen bestimmen und die Anwendbarkeit der DSFA für ihren Anwendungsbereich ermitteln. Die Organisation sollte ebenfalls Entscheidungen über die Abstufung der DSFA, den Prozess, der für die Durchführung der DSFA verwendet werden soll und zu den Zielgruppen, und damit der Art und den Inhalt des zu erstellenden DSFA-Berichts treffen und diese Entscheidung dokumentieren.

Das Ergebnis dieses Prozesses in Form des Schwellenwertanalyse-Ergebnisses 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 anderem Vorhaben, die personenbezogene Daten verarbeitet oder verarbeiten wird,

— einer Entscheidung, dass sensible personenbezogene Daten (siehe ISO/IEC 29100:2011, 2.26) verarbeitet werden sollen,

— Änderungen an datenschutzbezogenen Gesetzen und Verordnungen, internen Grundsätzen und Normen, dem Betrieb von Informationssystemen, Zweck und Intention der Datenverarbeitung, neuen oder veränderten Datenflüssen usw., sowie

— Geschäftsexpansion oder -Erwerbungen.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29134:2020-01

Eine Organisation könnte es für sinnvoll erachten, einen Grundsatz zu den Grenzwerten zu erlassen, welche anfänglichen technischen und organisatorischen Kenngrößen anzuwenden sind, um eine neue oder aktualisierte DSFA auszulösen. Solch ein Grundsatz 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

Ziel: Bestimmung des Aufgabenbereichs für die DSFA und der erforderlichen Expertise und Formulierung des Aufgabenbereiches für die Durchführung der DSFA.

Eingabe: Mandat eine DSFA vorzubereiten (siehe 6.2).

Erwartetes Ergebnis: Verantwortliche Person benannt, Risikokriterien.

Aktionen:

Eine Person (Prüfperson), die für die Durchführung der DSFA verantwortlich sein wird, sollte von der Organisation bestimmt und benannt werden. Die Organisation sollte außerdem die verantwortliche Person benennen, die den DSFA-Bericht abnehmen darf.

Die Prüfperson sollte die Risikokriterien definieren und sicherstellen dass die Unternehmensleitung der Anwendung dieser Risikokriterien für die Bewertung der Risikobedeutung 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 und die Ressourcen (siehe 7.3.3) sollten im DSFA-Bericht dokumentiert werden (siehe 7.3.2).

Anleitung zur Umsetzung:

Die Kriterien sollten die Werte, Zielsetzung 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 die Datenschutzrisiken getrennt sowohl aus dem Blickwinkel einer/s Betroffenen als auch aus dem Blickwinkel der Organisation untersuchen.

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

AVA Documents Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29134:2020-01

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

— Wie lauten die Kriterien, die für die Bestimmung des Auswirkungsgrades für den Betroffenen und für die Organisation verwendet werden? (Zum Beispiel der Grad der Identifikation, Sensibilität der Daten im Falle einer Datenschutzverletzung, Anzahl der Betroffenen und Auswirkungsgrad auf die Organisation.)

— Welche Kriterien werden zur Bestimmung der Eintrittswahrscheinlichkeit verwendet? (Zum Beispiel die Anfälligkeiten der unterstützenden Datenschutzwerte und die Möglichkeiten der Risikoquellen, diese Anfälligkeiten auszunutzen.)

— Welche Abstufungen werden bei der Bestimmung des Auswirkungsgrades genutzt?

— Welche Abstufungen werden bei der Bestimmung der Eintrittswahrscheinlichkeit genutzt?

— Welche Bedeutung hat jede Kombination (Grad der Auswirkung und Eintrittswahrscheinlichkeit) zur Bewertung der Risiken? Welche Kriterien gelten insbesondere für die Risikoakzeptanz?

— Welches ist die anzuwendende Strategie, um jedes einzelne Risiko zu behandeln? Wie sieht insbesondere die Strategie für die zu akzeptierenden Risiken aus?

— Wie wird die Strategie von den Vorteilen der Verarbeitung personenbezogener Daten beeinflusst?

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

ANMERKUNG 2 Bei jeder Verwendung der Kriterien müssen Verbesserungsmöglichkeiten geprüft werden.

Die Bestimmung der Risikokriterien sollte auf Folgendem beruhen:

— Schaden für den Anwender des Produktes, Dienstes oder Systems. Der Schaden kann 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 Auswirkung der Datenschutzrisiken ihrer Daten auf das Individuum betrachtet, wie z. B. das Recht auf körperliche Unversehrtheit, die Unverletzlichkeit des privaten Raumes, die Privatsphäre des persönlichen Handelns, der Kommunikation, der personenbezogenen Information in jeder Form, die Privatsphäre des Denkens und Fühlens und die Versammlungsfreiheit;

— den gesetzlichen und regulatorischen Anforderungen und vertraglichen Verpflichtungen;

— der Erwartungen und Wahrnehmungen der Anspruchsgruppen und negative Konsequenzen für Firmenwert und Reputation;

— der betrieblichen Bedeutung der Verfügbarkeit, Vertraulichkeit und Sicherheit der personenbezogenen Daten;

— dem strategischen Wert des Informationsprozesses;

— dem gegenwärtigen Wert und den zukünftigen Möglichkeiten, die der Informationsprozess ermöglicht, auch als „strategischer Wert“ bekannt.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29134:2020-01

Mit dem Aufgabenbereich der DSFA sollte festgelegt werden, ob öffentliche Konsultationen abgehalten werden sollen, an wen der Bericht der DSFA verteilt werden soll, das benannte Budget und der Zeitplan für die DSFA und ob der DSFA-Bericht oder eine Zusammenfassung veröffentlicht wird. Die Mindestanforderungen an eine DSFA sollten von den verbindlichen Gesetzen oder Verordnungen abhängen oder davon, wie bedeutsam die Datenschutzrisiken von der Organisation eingeschätzt werden.

Die Prüfperson sollte die DSFA durchführen und, falls erforderlich, Unterstützung von einem Team erhalten, das zum Beispiel Vertreter der ITK-Abteilung, der relevanten Geschäftseinheiten und der Rechtsabteilung umfasst.

Eine DSFA durchzuführen erfordert eine starke und beständige Verpflichtung des Managements der Organisation. Das Management sollte sicherstellen, dass dem DSFA-Team die erforderlichen Ressourcen zugewiesen werden.

6.3.2 Plan für die DSFA vorbereiten und die notwendigen Ressourcen zur Durchführung bestimmen

Ziel: Aufstellen eines Plans für die DSFA und Zuweisen von Personalressourcen und Budget zum Durchführen der geplanten DSFA.

Eingabe: Aufgaben- und Anwendungsbereich für die DSFA.

Erwartetes Ergebnis: Plan für die durchzuführende DSFA, den Geschäftsfall und die zugewiesenen Ressourcen.

Aktionen:

Auswahl und Planung der Schritte der DSFA und Auswahl der durchzuführenden Tätigkeiten als Aufgaben mit erforderlicher Zeit und Ressourcen.

Schätzung der Kosten und des Aufwands, Prüfung der Verfügbarkeit der Team-Mitglieder und Entscheidung über die Zuweisung von Budget und Ressourcen.

Das Ergebnis dieses Prozesses in Form der zugewiesenen Ressourcen sollte im DSFA-Bericht (siehe 7.3.3) dokumentiert werden.

Anleitung zur Umsetzung:

Der Plan sollte dem Anwendungsbereich der durchzuführenden Abschätzung Rechnung tragen und falls nötig Iterationen zulassen. Das sollte Iterationen des DSFA-Berichts einschließen. Es ist insbesondere dann sinnvoll, wenn die Abschätzung in großem Umfang Ressourcen einbezieht, aber mag für kleinere, weniger komplexe Vorhaben verzichtbar sein. Der Plan sollte auch Situationen vorsehen, bei denen das abzuschätzende Vorhaben unterbrochen wird.

Der Plan sollte darlegen, was getan werden muss, um die DSFA abzuschließen, wer aus dem DSFA-Team welche Aufgaben hat sowie den Zeitplan der DSFA umfassen und insbesondere wie die Konsultation, sofern es eine geben soll, durchzuführen ist. Er sollte spezifizieren, warum es in diesem konkreten Fall wichtig ist, Anspruchsgruppen zu befragen, wer befragt werden soll und wie sie befragt werden (z. B. über öffentliche Meinungsumfragen, Workshops, Fokusgruppen, öffentliche Anhörungen, Online-Befragungen usw.).

Sobald die Prüfperson den DSFA-Plan aufgestellt hat, sollte er oder sie die Kosten für die Durchführung schätzen und bei der Unternehmensleitung der Organisation das erforderliche Budget und die erforderlichen Personalressourcen anfordern. Der Plan könnte eine Anhebung des ursprünglich von der Unternehmensleitung genehmigten Budgets erforderlich machen oder die für die Durchführung der DSFA verantwortliche Person muss den DSFA-Plan auf Basis des verfügbaren Budgets eventuell überarbeiten.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29134:2020-01

Die Organisation sollte eine praktikable Handlungsweise entwickeln, um der DSFA angemessene Ressourcen zuzuweisen.

Folgendes sollte berücksichtigt werden:

— Menschen, Fertigkeiten, Erfahrungen und Kompetenzen;

— die Zeit, die für jede Aufgabe benötigt wird;

— die Ressourcen, die für jeden Schritt der DSFA benötigt werden.

6.3.3 Beschreiben, was untersucht werden soll

Ziel: Beschreibung des zu beurteilenden Programms, Prozesses oder Informationssystems.

Eingabe: Systemanforderungsinformationen, Systementwurfsinformationen, Informationen zu betrieblichen Plänen und Abläufen, externe und interne Faktoren.

Erwartetes Ergebnis: Beschreibung des zu untersuchenden Geschäftsprozesses und Informationssystems.

Aktionen:

Erstellen einer angemessenen Beschreibung des zu untersuchenden Programms, Prozesses oder Informationssystems.

Das Ergebnis dieses Prozesses in Form der Systemanforderungsinformationen, Systementwurfsinformationen und Informationen zu betrieblichen Plänen und Abläufen sollte im DSFA-Bericht (siehe 7.3.1) dokumentiert werden.

Anleitung zur Umsetzung:

Durch die Festlegung des Kontextes bestimmt die Organisation die relevanten internen und externen Faktoren, die beim Umgang mit den Datenschutzrisiken zu beachten sind, und legt den Anwendungsbereich und die Datenschutz-Risikokriterien für den weiteren Ablauf fest.

Die Beschreibung des zu untersuchenden Programms, Prozesses oder Informationssystems sollte unter den drei Überschriften von 7.3.1.2 (Systemanforderungsinformationen), 7.3.1.3 (Systementwurfsinformationen) und 7.3.1.4 (Informationen zu betrieblichen Plänen und Abläufen) angeordnet sein.

Um einen klaren Blick auf den zu berücksichtigenden Anwendungsbereich zu erhalten, sollte die Prüfperson zumindest zu den folgenden, nicht erschöpfenden Fragen Antworten suchen:

— Welches sind die personenbezogenen Daten, die verarbeitet werden?

— Was ist der Zweck der Verarbeitung?

— Welches sind die hauptsächlichen Vorteile, die die Verarbeitung der personenbezogenen Daten den Betroffenen oder der Gesellschaft insgesamt bietet?

— Wer sind die Empfänger der personenbezogenen Daten und wie werden sie diese Daten behandeln?

— Welche(r) Geschäftsprozess(e) wird/werden mit dieser Verarbeitung personenbezogener Daten ausgeführt?

— Wer sind die Betroffenen dieser Verarbeitung personenbezogener Daten?

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29134:2020-01

— Wie sollen die Datenschutzprozesse umgesetzt werden (Benachrichtigung, Einwilligung, Widerspruch, Zugang, Korrektur, Löschung usw.)?

— Wie sollen Betroffene benachrichtigt und ihre Einwilligung eingeholt werden? Wird der Ablauf an seinem Kontext ausgerichtet?

— Welches sind die unterstützenden Datenschutzwerte innerhalb des Anwendungsbereiches (auf die sich die personenbezogenen Daten stützen)?

Für alle personenbezogenen Daten sollte die Organisation die unterstützenden Datenschutzwerte (auf die sich die personenbezogenen Daten stützen) identifizieren, die in Zukunft verwendet werden oder jetzt verwendet werden. Sie sollte den Standort dieser unterstützenden Datenschutzwerte identifizieren. Zum Beispiel:

— Endbenutzer-Hardware und -Software (z. B. eine von der Organisation bereitgestellte Anwendung oder ein vom Benutzer mitgebrachtes Smartphone);

— Art der Hardware (Computer, Router, elektronische Speichermedien usw.);

— Art der Software (Betriebssysteme, Nachrichtensysteme, Datenbanken, Geschäftsanwendungen usw.);

— Art der Datenkommunikationsnetze (Kabel, drahtlos, Lichtwellenleiter usw.);

— Art der unterstützenden Datenschutzwerte in Papierform (Ausdrucke, Fotokopien usw.);

— Art der papiergestützten Übermittlungswege (Post, Arbeitsablauf usw.).

Zum Informationssystem und den identifizierten unterstützenden Datenschutzwerten sollte die Prüfperson die üblicherweise genutzten betrieblichen Pläne und Abläufe mit deren unterliegenden Konzepten heranziehen. Zum Beispiel:

— wie erfolgt das Identitäts- und Nutzermanagement;

— ob der Betrieb vor Ort oder extern erfolgt;

— der Einsatz von Unterauftragnehmern und der Umfang ihres Zugangs zu den Standorten und zu den personenbezogenen Daten;

— die Verwendung von Metadaten, Aufzeichnungen, Datensicherung und Wiederherstellung;

— die Vorhaltung und Löschung von Daten und die Entsorgung von Medien;

— die Außerbetriebnahme von Systemen.

Die Beschreibung kann in dreifacher Weise verwendet werden. Sie hilft der Prüfperson — der Person, die die DSFA durchführt — notwendige Bezugsinformationen bereitzustellen, sie kann in den DSFA-Bericht aufgenommen werden und sie kann als Hintergrundpapier bei der Konsultation der Anspruchsgruppen verwendet werden. Die Projektbeschreibung sollte einige Information zum Umfeld bieten (z. B. warum das Projekt durchgeführt wird, was der Zielmarkt ist, wie sich die beschriebene Technologie, der Dienst, das System oder ein anderes Vorhaben auf die Privatsphäre auswirken könnte, welche personenbezogenen Daten verarbeitet und welche Plattformen dafür verwendet werden sollen). In der Projektbeschreibung sollte angegeben werden, wer für das Projekt verantwortlich ist. Darin sollte auf wichtige Meilensteine hingewiesen werden und insbesondere auf den Zeitpunkt anstehender Entscheidungen, die sich auf das Projektvorhaben auswirken könnten.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29134:2020-01

6.3.4 Einbindung von Anspruchsgruppen

6.3.4.1 Identifizieren der Anspruchsgruppen

Ziel: Identifizieren der Einzelpersonen, die personenbezogene Daten verarbeiten könnten oder von der Verarbeitung ihrer personenbezogenen Daten betroffen sein könnten.

Eingabe: Beschreibung des zu untersuchenden Geschäftsprozesses und Informationssystems, Anwendungsbereich der DSFA.

Erwartetes Ergebnis: Betroffene.

Aktionen:

Die Organisation sollte alle Anspruchsgruppen identifizieren (einschließlich der Betroffenen), die personenbezogene Daten verarbeiten könnten oder von der Verarbeitung ihrer personenbezogenen Daten betroffen sein könnten.

Das Ergebnis dieses Prozesses in Form einer Liste der Anspruchsgruppen sollte im DSFA-Bericht verwendet werden (siehe 7.3.4).

Anleitung zur Umsetzung:

Beispiele für Anspruchsgruppen können sein:

— Mitarbeiter, z. B. aus der Personalabteilung, Rechtsabteilung, Informationssicherheit, Finanzabteilung, Aufgabenträger im Geschäftsbetrieb, der Kommunikation und interne Auditoren (insbesondere in einem regulierten Umfeld);

— betroffene Personen;

— Arbeitnehmer- und Verbrauchervertretungen;

— Unterauftragnehmer;

— Geschäftspartner;

— Anwendungs- und Datenbankadministratoren;

— Computer- oder Netzwerkadministratoren;

— Anwendungsbetreiber;

— Endgeräte- und Netzwerkbetreiber;

— Wartungspersonal;

— Menschen aus anderen Organisationen, die angemessene Interessen an der DSFA geltend machen können.

Um den DSFA-Ablauf transparent zu machen und die Ziele der DSFA zur Benennung der Datenschutzrisiken zu erreichen, sollte die für die Durchführung der DSFA verantwortliche Person die internen und externen Anspruchsgruppen detailliert identifizieren, die ein Interesse an dem zu untersuchenden Prozess haben könnten oder vom Schutz ihrer personenbezogenen Daten im Rahmen dieses Prozesses betroffen sind.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29134:2020-01

Anspruchsgruppen könnten alle Einzelpersonen oder Parteien sein, einschließlich Endbenutzern, die Zugriff auf personenbezogenen Daten haben oder sich verschaffen könnten.

Die für die Durchführung der DSFA verantwortliche Person sollte diese verschiedenen Kategorien identifizieren und dann spezifische Einzelpersonen aus diesen Kategorien ermitteln, die vorzugsweise so repräsentativ wie möglich sind.

Für die Bestimmung der geeigneten angemessenen Anspruchsgruppen sind der Anwendungsbereich und Umfang der DSFA von Bedeutung. Wo ein großes Regierungsprojekt durchgeführt wird, sind viele Anspruchsgruppen zu erwarten. In diesem Fall würden gesellschaftliche Interessengruppen, wie z. B. Verbraucherverbände, ausfindig gemacht werden müssen, ebenso wie Anspruchsgruppen, die personenbezogene Daten verarbeiten und Anspruchsgruppen, die Betroffene sind. Im Gegensatz dazu erfordern kleinere Geschäftsvorgänge unter Umständen keine so breit angelegte Liste der Anspruchsgruppen.

6.3.4.2 Erstellen eines Konsultationsplans

Ziel: Der Konsultation und Kommunikation mit den Anspruchsgruppen Struktur geben.

Eingabe: Identifizierte Privatsphäre-Anspruchsgruppen, Plan für die durchzuführende DSFA.

Erwartetes Ergebnis: Konsultations- und Kommunikationsplan.

Aktionen:

Die Prüfperson sollte frühzeitig einen Plan für die Kommunikation und Konsultation mit internen als auch externen Anspruchsgruppen entwickeln.

Das Ergebnis dieses Prozesses in Form des Konsultations- und Kommunikationsplans sollte im DSFA-Bericht verwendet werden (siehe 7.3.4).

Anleitung zur Umsetzung:

In diesem Plan sollten die Fragen in Bezug auf die Auswirkungen für die verschiedenen Privatsphäre-Anspruchsgruppen angesprochen werden, deren Konsequenzen (sofern bekannt), und die Maßnahmen, die ergriffen wurden, um ihnen zu begegnen. Der Plan sollte auch den Umfang und Zeitplan für die Konsultation enthalten.

Der Plan sollte zwei Aspekte abdecken:

— die Arbeit mit den relevanten Anspruchsgruppen beim Identifizieren und Bewerten von Datenschutzrisiken;

— die Konsultation mit den Anspruchsgruppen zum Entwurf des DSFA-Berichts, um zu prüfen ob deren Belange angemessen abgedeckt werden.

Der Kreis und die Anzahl der zu konsultierenden Anspruchsgruppen sollte eine Funktion der Datenschutzrisiken und der Annahmen zur Wahrscheinlichkeit und Auswirkung dieser Risiken und der Anzahl der möglicherweise betroffenen Bürger darstellen.

Wenn sich zum Beispiel die Risiken wahrscheinlich nur auf Mitarbeiter einer einzelnen Organisation auswirken, könnte die Konsultation auf die Mitarbeiter und/oder ihrer Vertreter begrenzt bleiben. Wenn allerdings erwartet wird, dass die Risiken jeden im Land betreffen werden, sollte die Organisation sich weitreichend mit externen Anspruchsgruppen beraten. Wenn in der Organisation anfangs davon ausgegangen wird, dass nur eine geringe Zahl von Menschen betroffen sein könnte, später aber zu der Erkenntnis gelangt wird, dass die Zahl der Betroffenen wahrscheinlich viel höher und die Risiken größer

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29134:2020-01

sind, sollte in der Organisation der Konsultationsplan entsprechend abgeändert und Anstrengungen ergriffen werden, um eine entsprechend größere Zahl von relevanten Anspruchsgruppen einzubinden.

6.3.4.3 Konsultation mit den Anspruchsgruppen

Ziel: Durchführen der Konsultation mit Anspruchsgruppen, sofern angemessen und machbar.

Eingabe: Identifizierte Privatsphäre-Anspruchsgruppen, Kommunikationsplan.

Erwartetes Ergebnis: Rückmeldung der Anspruchsgruppen.

Aktionen:

Die Organisation sollte versuchen, die Sichtweise von anderen Anspruchsgruppen zu verstehen.

Das Ergebnis dieses Prozesses in Form der Rückmeldung der Anspruchsgruppen sollte im DSFA-Bericht verwendet werden (siehe 7.3.4).

Anleitung zur Umsetzung:

Die Rückmeldung von den Anspruchsgruppen könnte Aspekte aufzeigen, die Empfindungen von Risiken darstellen, jedoch keine tatsächlichen Risiken sind. Diese sollten nicht verworfen, sondern im Rahmen des Anspruchsgruppen-Managements behandelt werden, um die Kommunikationsaktivitäten zu unterstützen.

Die möglicherweise erhebliche Auswirkung einer Konsultation mit Anspruchsgruppen für viele getrennte, aber sehr ähnliche Projekte dürfen minimiert werden, wenn die Konsultationsergebnisse wiederverwendet werden können. Wenn viele Projekte mit ähnlichen Datenschutzfragen erwartet werden, sollte die Wiederverwendung von Konsultationsergebnissen in die Vorbereitung der Konsultation eingehen. Konsultationen sollten nicht zu breit angelegt werden, aber ein gutes Urteilsvermögen darf eine solche Wiederverwendung erlauben. Die Konsultation auf Basis der inkrementellen Verbesserungen für neue Fragen in neuen Projekten könnte auch zur Vermeidung unzulässiger Auswirkungen beitragen.

Die Abstimmung mit Anspruchsgruppen kann für einzelne Marktsegmente auf Grundlage einer branchenspezifischen Anleitung durchgeführt werden. Organisationen, die das gleiche Marktsegment bedienen, dürfen branchenspezifische Anleitungen als Grundlage für die Beurteilung und Behandlung von Datenschutz- und Sicherheitsrisiken verwenden. Solche Anleitungen sollten die Grundsätze dieses Dokuments beachten und Risiken und Steuerungsmaßnahmen auf Basis der gemeinsamen Geschäftsprozesse und Dienste des konkreten Marktsegments spezifizieren.

Für KMU könnte die Einbindung von Anspruchsgruppen mit unverhältnismäßigem Zeitaufwand und Ausgaben verbunden sein. Für sie könnte das Konzept der branchenspezifischen Anleitungen die Vollständigkeit und Qualität der DSFA verbessern, wenn sie auf verfügbare Anleitungen verweisen können.

6.4 Durchführung der DSFA

6.4.1 Informationsflüsse personenbezogener Daten identifizieren

Ziel: Identifizieren der Informationsflüsse der personenbezogenen Daten im Rahmen der Abschätzung.

Eingabe: Beschreibung des zu untersuchenden Prozesses und Informationssystems.

Erwartetes Ergebnis: Zusammenfassung der Erkenntnisse zum Informationsfluss personenbezogener Daten im Prozess.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29134:2020-01

Aktionen:

Die für die Durchführung der DSFA verantwortliche Person sollte sich mit anderen in der Organisation und vielleicht auch außerhalb der Organisation beraten, um den Datenfluss der personenbezogenen Daten zu beschreiben und insbesondere:

— wie die personenbezogenen Daten erhoben werden und die dazugehörige Quelle;

— wer in der Organisation wirtschaftlich verantwortlich und wer für die Verarbeitung der personenbezogenen Daten durchführend verantwortlich ist;

— für welchen Zweck die personenbezogenen Daten verarbeitet werden;

— wie die personenbezogenen Daten verarbeitet werden sollen;

— die Anleitung zur Aufbewahrung und Entsorgung der personenbezogenen Daten;

— wie die personenbezogenen Daten behandelt und geändert werden sollen;

— wie die verantwortliche Stelle und Anwendungsentwickler die personenbezogenen Daten schützen werden;

— identifizieren jeder Übermittlung von personenbezogenen Daten in Rechtsräume, wo ein niedrigeres Schutzniveau für die personenbezogenen Daten angewendet wird;

— wenn erforderlich, die relevanten Aufsichtsstellen über jede neue Verarbeitung personenbezogener Daten benachrichtigen und die erforderlichen Genehmigungen einholen.

Das Ergebnis dieses Prozesses in Form des Informationsflusses personenbezogener Daten sollte im DSFA-Bericht dokumentiert werden (siehe 7.3.1).

Anleitung zur Umsetzung:

Die Verwendung (oder Übermittlung) von personenbezogenen Daten könnte unter Umständen den genehmigten Datenaustausch von personenbezogenen Daten mit anderen Beteiligten einschließen. D.1 zeigt ein Beispiel, wie der Informationsfluss von personenbezogenen Daten in einem Arbeitsablaufdiagramm der Verarbeitung personenbezogener Daten visualisiert werden kann.

Als Eingangsinformation für die DSFA sollte die Organisation den Informationsfluss so detailliert wie möglich beschreiben, um bei der Identifikation von Datenschutzrisiken zu helfen. Die Prüfperson sollte die Auswirkungen nicht nur auf den Datenschutz beziehen, sondern auch auf die Rechtseinhaltung (Compliance) anderer Verordnungen mit Datenschutzbezug, z. B. Telekommunikationsgesetze. Der gesamte Lebenszyklus der personenbezogenen Daten sollte berücksichtigt werden.

Dieser Schritt könnte direkt nach 6.3.3 und gleichzeitig mit den Schritten aus 6.3.4 durchgeführt werden.

6.4.2 Auswirkungen des Anwendungsfalles analysieren

Ziel: Das mögliche Nutzerverhalten erkennen.

Eingabe: Die Art möglicher Betroffener und Anwendungsfälle, insbesondere ihr Gebrauch digitaler Geräte, um hiermit einhergehende Datenschutzrisiken aufzuzeigen.

Erwartetes Ergebnis: Zusammenfassung der Erkenntnisse über die Anwendungsfälle der Anwender im Geschäftsprozess.

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29134:2020-01

Aktionen:

Aufzeigen und Beschreiben der Datenschutzfolgen im DSFA-Bericht. Reduzieren der Datenschutzrisiken durch Nutzerverhalten, auf der Grundlage der DSFA-Zusammenfassung von Informationen bezüglich der Risiken und Gegenmaßnahmen der Anwender.

Anleitung zur Umsetzung:

Beispiele von möglichem Nutzerverhalten, das unbeabsichtigte Konsequenzen nach sich ziehen könnte, sind die folgenden:

— laienhafte Änderungen an den Sicherheitseinstellungen des Betriebssystems von Verarbeitungsgeräten;

— Neigung, mobile Geräte und intelligente Speichermedien zu verlieren;

— Neigung, Geräte falsch zu bedienen oder Geräte und Anwendungseinstellungen auf eine Weise falsch zu verstehen, die die Datenschutzrisiken steigern kann;

— Anfälligkeit von Märkten für unerlaubte Aktivitäten, bei denen technologische Funktionsmerkmale eingesetzt werden, um Anwender/Verbraucher zur Aufgabe von Datenschutz und Sicherheit zu verleiten. Beispiele hierfür sind E-Mails mit eingebetteter Schadsoftware oder Links zu betrügerischen Websites in E-Mails, um persönliche Schlüsselinformationen oder Sicherheitsinformationen zu entlocken, gefälschte optische Kodierungen auf physischen Anzeigemedien, mit denen die optische Code-Erkennungssoftware des Smartphones eines Verbrauchers auf falsche Websites leitet.

Bei jedem BYOD-Anwendungsfall sollte zwischen geschäftlicher Nutzung und privater Nutzung unterschieden werden.

6.4.3 Bestimmen der relevanten Datenschutzanforderungen

ANMERKUNG Der Begriff Datenschutzanforderungen ist in ISO/IEC 29100:2011, 4.5 beschrieben.

Ziel: Bestimmen der relevanten Datenschutzanforderungen zum Zweck des zu untersuchenden Programms, Informationssystems oder Prozesses.

Eingabe: Beschreibung des zu untersuchenden Geschäftsprozesses und Informationssystems, Zusammenfassung der Erkenntnisse zum Informationsfluss personenbezogener Daten und über die Anwendungsfälle der Anwender im Geschäftsprozess.

Erwartetes Ergebnis: Liste der Datenschutzanforderungen (siehe 7.4).

Aktionen:

Die für die Durchführung der DSFA verantwortliche Person oder ihre Rechtsexperten sollten sicherstellen, dass der Geschäftsprozess im Anwendungsbereich alle gesetzlichen regulatorischen und geschäftlichen Faktoren und vertraglichen Anforderungen in Bezug auf Privatsphäre und/oder Datenschutz einhält.

Das Ergebnis dieses Prozesses in Form der Liste der Datenschutzanforderungen sollte im DSFA-Bericht verwendet werden (siehe 7.4).

Anleitung zur Umsetzung:

Bei der Ausführung ihres Rahmens zur Behandlung von Datenschutzrisiken sollte die Organisation

— relevante Gesetze, Verordnungen und Verträge identifizieren, die für den DSFA-Prozess anwendbar sind,

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29134:2020-01

— relevante Sammlungen von Steuerungsmaßnahmen zur Informationssicherheit identifizieren (z. B. Normen zur Informationssicherheit),

— die dazugehörigen Datenschutzanforderungen identifizieren,

— die schon geplanten oder bereits bestehenden Steuerungsmaßnahmen beschreiben, von denen erwartet wird, dass sie die Datenschutzanforderungen erfüllen,

— relevante Informationen nutzen, die aus früheren Projekten verfügbar sind.

Die Grundsätze aus ISO/IEC 29100 können in detailliertere Anforderungen unterteilt und um weitere Anforderungen ergänzt werden.

Die Compliance-Anforderungen können Folgendes einschließen:

— Sicherstellung, dass die Betroffenen ordnungsgemäß über den Zweck für die Verarbeitung der personenbezogenen Daten nach dem Grundsatz von Einwilligung und Wahlfreiheit informiert wurden;

— Sicherstellung, dass die Betroffenen die Möglichkeit des Zugangs und der Überprüfung ihrer personenbezogenen Daten nach dem Grundsatz der individuellen Mitwirkung und des Zugangs haben.

6.4.4 Beurteilen der Datenschutzrisiken

6.4.4.1 Aufzeigen der Datenschutzrisiken

Ziel: Identifizieren der Risiken für relevante Anspruchsgruppen, die aus dem zu untersuchenden Programm, Informationssystem oder Prozess entstehen.

Eingabe: Beschreibung des zu untersuchenden Programms, Informationssystems oder Prozesses.

Erwartetes Ergebnis: Die identifizierten Datenschutzrisiken.

Aktionen:

Organisationen sollten die zu bewertenden Risiken identifizieren.

Das Ergebnis der identifizierten Risiken sollte im DSFA-Bericht dokumentiert werden (siehe 7.5.1).

Anleitung zur Umsetzung:

Die Organisation sollte Werkzeuge und Techniken zur Identifizierung von Datenschutzrisiken anwenden, die für ihre Ziele und Fähigkeiten und den zu begegnenden Risiken geeignet sind. Die jeweiligen gesetzlichen Datenschutzgrundsätze des Landes, in dem die Lösung eingesetzt werden soll, sollten verwendet werden, um die Identifikation von Risiken für eine Datenschutzverletzung zu stützen.

Datenschutzrisiken schließen ein, sind aber nicht begrenzt auf:

— nicht autorisierter Zugriff auf personenbezogene Daten (Verlust der Vertraulichkeit);

— nicht autorisierte Veränderung von personenbezogenen Daten (Verlust der Integrität);

— Verlust, Diebstahl oder nicht autorisierte Entfernung personenbezogener Daten (Verlust der Verfügbarkeit).

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29134:2020-01

Es ist möglich, andere Aspekte zu berücksichtigen, z. B. die folgenden:

— ausufernde Erhebung personenbezogener Daten (Verlust der betrieblichen Steuerungsfähigkeit);

— nicht autorisierte oder unangemessene Verknüpfung von personenbezogenen Daten;

— unzureichende Information über den Zweck der Verarbeitung personenbezogener Daten (Mangel an Transparenz);

— Nichtbeachtung von Betroffenenrechten (z. B. Verlust des Rechtes auf Zugang);

— Verarbeitung personenbezogener Daten ohne das Wissen oder die Einwilligung des Betroffenen (es sei denn, eine solche Verarbeitung ist in den einschlägigen Rechtsvorschriften oder Verordnungen vorgesehen);

— Teilen oder Wiederverwenden von personenbezogenen Daten mit dritten Parteien ohne die Einwilligung des Betroffenen;

— unnötig verlängerte Aufbewahrung personenbezogener Daten.

ANMERKUNG Diese Möglichkeiten von nicht oder schlechter Umsetzung der Grundrechte könnten nur geprüft und verbessert werden. Tatsächlich stellt die Nichtumsetzung dieser Grundrechte keine Option dar.

Relevante und aktuelle Informationen sind beim Identifizieren der Datenschutzrisiken wichtig. Die Prüfperson sollte Personen mit entsprechenden Kenntnissen beim Identifizieren der Datenschutzrisiken einbeziehen. Nach der Identifizierung, was passieren könnte, ist es erforderlich, mögliche Szenarien zu betrachten, die Konsequenzen aufzeigen können. Alle Szenarien sollten berücksichtigt werden.

Szenarien einschließlich falscher oder missbräuchlicher Nutzung sowie technische oder umweltbezogene Störungen, sollten ebenfalls als mögliche Bedrohungen berücksichtigt werden.

Wo immer es gerechtfertigt ist, sollte sich die für die Durchführung der DSFA verantwortliche Person beim Identifizieren der Datenschutzrisiken die Mühe machen, die Unterstützung der Anspruchsgruppen einzuholen.

6.4.4.2 Analyse der Datenschutzrisiken

Ziel: Analysieren der möglichen Konsequenzen und Bedrohungen aus den identifizierten Datenschutzrisiken und Einschätzen des jeweiligen Grades der Auswirkung und der Eintrittswahrscheinlichkeit.

Eingabe: Die identifizierten Datenschutzrisiken.

Erwartetes Ergebnis: Die analysierten Datenschutzrisiken (d. h. ihre Beschreibung und Einschätzung zum Grad der Auswirkung und Eintrittswahrscheinlichkeit).

Aktionen:

Organisationen sollten die Auswirkung der Datenschutzrisiken bestimmen.

Das Ergebnis der Analyse der Datenschutzrisiken sollte im DSFA-Bericht dokumentiert werden (siehe 7.5.2 und 7.5.3).

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29134:2020-01

Anleitung zur Umsetzung:

Die Risikoanalyse basiert auf einer detaillierten Analyse eines Programms, Informationssystems oder Prozesses, oder einer Änderung an diesen. Die Risikoanalyse umfasst die Identifizierung der personenbezogenen Daten und der zugrunde liegenden Datenschutzwerte, die einem Risiko ausgesetzt sein können, die Anfälligkeiten, die mit diesen Datenschutzwerten verbunden sind, die Bedrohungen, die diese Anfälligkeiten ausnutzen könnten, die Wahrscheinlichkeit und die Auswirkungen dieses Ereignisses , sowie jede bestehende Steuerungsmaßnahme, die das Risiko beeinflussen könnte. Alle Feststellungen, die während der Risikoanalyse getroffen werden, sollten angemessen dokumentiert werden. Risikoquellen, sowohl innerhalb als auch außerhalb der Organisation sollten einbezogen werden, wenn sie Auswirkungen auf den Betroffenen haben. Die Organisation sollte eine Liste der Datenschutzrisiken erzeugen, die so umfassend wie möglich ist.

Die Analyse der Datenschutzrisiken umfasst Betrachtungen zu den Ursachen und Risikoquellen von Datenschutzrisiken, ihre positiven wie negativen Konsequenzen und die Wahrscheinlichkeit, dass diese Konsequenzen eintreten können. Die Prüfperson sollte Faktoren identifizieren, die sich auf die Konsequenzen und Wahrscheinlichkeit auswirken. Ein Ereignis kann mehrere Konsequenzen haben und sich auf mehrere Ziele auswirken. Die Prüfperson sollte bestehende Steuerungsmaßnahmen und deren Wirksamkeit berücksichtigen.

Wenn die Untersuchung eines Datenschutzrisikos eine hohe oder sehr hohe Folgewirkung und/oder ein wahrscheinliches oder sehr wahrscheinliches Eintreten ergibt, sollte die Organisation eine Aufteilung des Risikos in seine Einzelbestandteile vornehmen. Diese Aufteilung ermöglicht es der Organisation zu identifizieren, welches der Einzelbestandteile zu der hohen Folgewirkung oder Eintrittswahrscheinlichkeit beiträgt und dieses dann getrennt zu analysieren. Dies sollte dazu beitragen, geeignetere Steuerungsmaßnahmen zu finden.

Bei der Einschätzung der Eintrittswahrscheinlichkeit der Bedrohungen (siehe ISO/IEC 27000:2016, 2.83), sollte die Organisation die Leistungsfähigkeit der Risikoquellen, die Anfälligkeit der unterstützenden Datenschutzwerte und die vorhandenen oder geplanten Steuerungsmaßnahmen berücksichtigen. Anhang A darf verwendet werden.

Für jedes dieser Risiken (siehe 6.4.4.1), werden identifiziert:

— die wahrscheinlichsten Risikoquellen (siehe ISO Guide 73:2009, 3.5.1.2);

— die wahrscheinlichsten Bedrohungen;

— die schwerwiegendsten Auswirkungen auf die Privatsphäre der Betroffenen;

— ein Risikoeigentümer (siehe ISO Guide 73:2009, 3.5.1.5);

— die vorhandenen Steuerungsmaßnahmen und die Risiken, zu deren Behandlung sie beitragen.

Dann sollte der Grad der Auswirkungen eingeschätzt werden, basierend auf den möglichen Konsequenzen und den Abstufungen, die für die Risikokriterien festgelegt wurden.

Anhang B enthält eine Liste generischer Bedrohungen, die helfen kann, damit relevante Bedrohungen nicht übersehen werden.

Die Art und Weise, wie Konsequenzen und Wahrscheinlichkeiten ausgedrückt werden, und wie sie zur Bestimmung eines Risikograds kombiniert werden, hängt von der Art des Datenschutzrisikos und vom Risikograd ab, dem die involvierten Betroffenen und die Organisation ausgesetzt sind. Im Falle einer Datenschutzverletzung sollte die Organisation die verfügbaren Informationen und das Ergebnis der Analyse der Datenschutzrisiken nutzen. Diese sollten alle konsistent zu den Risikokriterien sein.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29134:2020-01

Die Prüfperson sollte den Vertrauensbereich bei der Bestimmung der Datenschutzrisiken und deren Sensibilität für die Voraussetzungen in der Analyse berücksichtigen und dies bei Bedarf an Entscheidungsträger und andere Anspruchsgruppen mitteilen. Die Prüfperson sollte Faktoren wie abweichende Meinungen unter den Experten und Einschränkungen bei der Modellierung angeben und gegebenenfalls hervorheben. Die Prüfperson sollte die in 6.3.4.1 ermittelten Anspruchsgruppen per Interview oder im Rahmen eines Workshops als Teil der Untersuchung der Datenschutzrisiken konsultieren.

ANMERKUNG Der Vertrauensbereich ist in ISO 772 definiert als der Prozentsatz von Fällen, bei dem eine Reihe gleichartiger Tests den wahren Mittelwert ergibt.

Eine Analyse der Datenschutzrisiken kann abhängig vom Datenschutzrisiko, dem Zweck der Analyse und den Informationen, Daten und Ressourcen, die der Analyse zur Verfügung stehen, mit verschiedenen Detailgraden durchgeführt werden. Die Untersuchung kann qualitativ, halbqualitativ oder quantitativ oder als Kombination von diesen sein, je nach den Umständen.

Üblicherweise wird oft erst eine qualitative Untersuchung durchgeführt, um allgemeine Angaben zum Risikograd zu erlangen und die Hauptrisiken aufzuzeigen. Wenn möglich und angebracht, sollte außerdem eine spezifischere und quantitative Untersuchung der Risiken vorgenommen werden.

Eine Risikoabschätzung besteht darin, den potentiellen Folgen (Auswirkungsgrad) und den Bedrohungen (Wahrscheinlichkeit) eines Risikos Werte zuzuordnen.

Die Organisation sollte Werkzeuge und Techniken zur Datenschutzrisikoabschätzung verwenden, die für ihre Ziele und Fähigkeiten und für die zu begegnenden Risiken geeignet sind.

Die Prüfperson sollte bei der Schätzung der Datenschutzrisiken Personen mit entsprechenden Kenntnissen einbeziehen.

Wenn mehrere DSFAs unter Einbeziehung gemeinsamer Programm-, Informationssystem- oder Prozess-Elemente durchgeführt werden, ist eine Koordination zwischen den DSFA-Teams erforderlich, um sicherzustellen, dass die Risiken auf konsistente Weise ermittelt und abgeschätzt werden und dass die späteren Aktionspläne ebenfalls konsistent sind.

6.4.4.3 Bewerten der Datenschutzrisiken

Ziel: Priorisieren der identifizierten Datenschutzrisiken.

Eingabe: Die identifizierten Datenschutzrisiken, Analyse der Datenschutzrisiken.

Erwartetes Ergebnis: Datenschutzrisiko-Karte.

Aktionen:

Eine Bewertung des Datenschutzrisikos sollte erstellt werden.

Das Ergebnis in Form der Datenschutzrisiko-Karte sollte im DSFA-Bericht dokumentiert werden (siehe 7.5.4).

Anleitung zur Umsetzung:

Bei der Erstellung einer Risikobewertung sollte die relative Priorisierung der Datenschutzrisiken berücksichtigt werden, die auf dem Schweregrad der Datenschutzfolgen für die Betroffenen sowie der Gesamtauswirkung auf die Organisation, basiert.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29134:2020-01

Die Behandlung identifizierter Risiken kann unter Umständen mehr Ressourcen erfordern als der Organisation zur Verfügung stehen. Die Priorisierung der identifizierten Risiken hilft der Organisation, die Zuweisung von Ressourcen für ihre Behandlung zu priorisieren.

Soweit machbar und angemessen sollten Risikoentscheidungen alle relevanten Faktoren einbeziehen, einschließlich die Risikotoleranz der Anspruchsgruppen, u. a. Betroffene. Die Entscheidungen sollten in Übereinstimmung mit Gesetzen, Verordnungen und anderen Anforderungen getroffen werden.

Unter bestimmten Umständen kann die Bewertung der Datenschutzrisiken zu der Entscheidung führen, weitere Untersuchungen durchzuführen.

Anhand der Bewertung des Auswirkungsgrades und der Wahrscheinlichkeit der bewerteten Risiken sollte eine Datenschutzrisiko-Karte erstellt werden können.

Es sollten Prioritäten festgelegt werden, die sich nach der Anordnung der Risiken auf der Karte (in der Reihenfolge ihrer Priorität) und nach den Risikokriterien richten.

D.2 enthält ein illustriertes Beispiel einer Datenschutzrisiko-Karte.

6.4.5 Vorbereitung zum Behandeln der Datenschutzrisiken

6.4.5.1 Wählen der Behandlungsoptionen für Datenschutzrisiken

Ziel: Entscheidung über die Behandlungsoption für jedes bewertete Datenschutzrisiko.

Eingabe: Datenschutzrisiko-Karte.

Erwartetes Ergebnis: Liste der am besten geeigneten Behandlungsoptionen für jedes bewertete Datenschutzrisiko.

Aktionen:

Die Behandlungsoptionen für das Datenschutzrisiko sollten identifiziert und die am besten geeignete Option ausgewählt werden.

Das Ergebnis in Form der Behandlungsoptionsliste für jedes bewertete Datenschutzrisiko sollte in 6.4.5.2 wiederverwendet werden.

Anleitung zur Umsetzung:

Die Risikobehandlung kann je nach Anwendungsbereich der Untersuchung, dem Risikomanagement-Kontext oder der Industriebranche die Durchführung eines Anwendungs- oder Prozessumbaus einschließen, ist aber nicht darauf beschränkt.

Bei der Auswahl der am besten geeigneten Behandlungsoption für das Datenschutzrisiko müssen die Kosten und der Aufwand betrachtet werden, die bei der Umsetzung der Organisationspflichten zum Schutz der Privatsphäre jeder Anspruchsgruppe, deren Privatsphäre durch die Organisation belastet werden könnte (z. B. deren personenbezogene Daten von der Organisation verwaltet oder verarbeitet werden), berücksichtigt werden.

Bei den Entscheidungen der Organisation sollten auch Risiken beachtet werden, die Risikobehandlungsaktionen rechtfertigen, die aus ökonomischen Gründen nicht zu rechtfertigen sind, z. B. erhebliche (hohe negative Auswirkung), aber seltene (geringe Wahrscheinlichkeit) Risiken.

Die Bewertung der Datenschutzrisiken kann auch zu der Entscheidung führen, das Datenschutzrisiko nicht anders zu behandeln als durch die Pflege bestehender Steuerungsmaßnahmen für den Datenschutz. Diese

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29134:2020-01

Entscheidung wird von der Risikobereitschaft der Organisation oder deren Einstellung gegenüber Risiken und den eingeführten Datenschutz-Risikokriterien beeinflusst.

Wann immer es angemessen erscheint, sollten die Organisation und/oder die Prüfperson die Unterstützung der Anspruchsgruppen bei der Auswahl der Behandlungsoptionen für das Datenschutzrisiko einholen.

Eine Reihe von Behandlungsoptionen kann sowohl im Einzelfall als auch in Kombination berücksichtigt und angewendet werden. Die Organisation kann von der Einführung kombinierter Behandlungsoptionen profitieren.

Bei der Auswahl der Behandlungsoptionen für das Datenschutzrisiko sollte die Organisation die Werte und Erwartungen der Anspruchsgruppen und die am besten geeigneten Wege für die Kommunikation berücksichtigen. Wenn Behandlungsoptionen für das Datenschutzrisiko Auswirkungen auf Risiken an anderer Stelle der Organisation haben können, sollten diese Bereiche in die Entscheidung einbezogen werden. Obwohl sie in gleicher Weise wirksam sind, mögen manche Risikobehandlungen für Anspruchsgruppen akzeptabler sein als andere.

Da die Ressourcen zur Behandlung von Datenschutzrisiken begrenzt sein können, sollte der Behandlungsplan zu den Datenschutzrisiken die Abfolge der Prioritäten klar ermitteln, in der die einzelnen Datenschutzrisiko-Behandlungen umgesetzt werden.

Auch die Datenschutzrisiko-Behandlung selbst kann Datenschutzrisiken herbeiführen, die untersucht, behandelt, überwacht und überprüft werden müssen. Ein erhebliches Datenschutzrisiko kann im Ausfall oder der Wirkungslosigkeit von Risikobehandlungsmaßnahmen liegen. Diese sekundären Datenschutzrisiken sollten in denselben Behandlungsplan zu den Datenschutzrisiken eingearbeitet werden wie das ursprüngliche Datenschutzrisiko und nicht als ein neues Datenschutzrisiko behandelt werden. Die Verbindung zwischen den beiden Datenschutzrisiken sollte erkennbar sein.

Entscheidungsträger und andere geeignete Anspruchsgruppen sollten sich der Art und des Umfangs des nach der Behandlung der Datenschutzrisiken verbleibenden Restrisikos bewusst sein. Das verbleibende Datenschutzrisiko sollte aufgezeichnet werden und Gegenstand einer Überwachung, Überprüfung und, falls angemessen, einer weiteren Behandlung werden.

Die Überwachung muss ein integraler Teil des Datenschutz-Risikomanagementplans sein, um den internen Anspruchsgruppen die Sicherheit zu geben, dass die Maßnahmen effektiv bleiben.

Für die Behandlung von Datenschutzrisiken sind vier Optionen verfügbar: Risikominderung, Risiko-behandlung, Risikovermeidung und Risikoübertragung.

a) Risikominderung:

Eine Risikominderung kann durch Auswählen geeigneter Steuerungsmaßnahmen erreicht werden. Wenn nach der Auswahl der Steuerungsmaßnahmen immer noch ein Restrisiko besteht, sollte die Organisation festlegen, ob das Restrisiko nicht annehmbar ist und diesem durch die Auswahl zusätzlicher Steuerungsmaßnahmen begegnet werden sollte, oder ob es akzeptabel für die Organisation und die Anspruchsgruppen ist.

Es mag Fälle geben, bei denen Risikominderungsmaßnahmen die Vorteile beeinträchtigen, die Anspruchsgruppen unter Umständen aus der in Frage stehenden Informationsverarbeitung ableiten. In solchen Situationen sollte die Prüfperson eine Risiko-/Nutzen-Analyse durchführen, um festzustellen, ob die Risiken die Vorteile überwiegen oder umgekehrt. Bei Ersterem sollte die Organisation die Risikomaßnahmen umsetzen. Bei Letzterem sollte die Organisation sich dafür entscheiden, die Risiken innerhalb der Compliance-Anforderungen zu akzeptieren.

Steuerungsmaßnahmen zur Risikominderung können sich in ihrer Art unterscheiden. Sie können enthalten:

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29134:2020-01

— Änderungen an der Art der verarbeiteten personenbezogenen Daten;

— Änderungen an der Organisationsstruktur, den Anleitungen und/oder Abläufen;

— Änderungen an den Qualifikationen der Mitarbeiter (z. B. Unbedenklichkeitsbescheinigungen, Schulungen, Bescheinigungen usw.).

Veränderungen an den unterstützenden Datenschutzwerten oder an Anwendungen können von dreierlei Art sein: vorbeugende Maßnahmen, erkennende Maßnahmen oder behebende Maßnahmen.

b) Risikobehandlung:

Wenn der Risikograd den (tolerierten) Risikokriterien entspricht, besteht keine Notwendigkeit zur Einführung zusätzlicher Steuerungsmaßnahmen und das Risiko kann beibehalten werden.

c) Risikovermeidung:

Wenn die identifizierten Risiken als zu hoch eingestuft werden, sollte die Organisation entscheiden das Risiko vollständig zu vermeiden, indem sie ein geplantes oder bestehendes Vorhaben oder Vorhabenpaket zurückzieht oder die Bedingungen verändert, unter denen das Vorhaben betrieben wird.

d) Risikoübertragung:

Die Risikoübertragung geht mit der Entscheidung einher, bestimmte Risiken mit externen Parteien zu teilen. Die Übertragung kann durch eine Versicherung erfolgen, die die Folgen trägt, oder durch Unterbeauftragung eines Partners, dessen Aufgabe es sein wird, das Informationssystem zu überwachen und sofortige Maßnahmen zu ergreifen, um einen Angriff zu stoppen, bevor dieser einen definierten Schaden verursacht.

Die Übertragung erheblicher oder maximaler Risiken an Betroffene, wie z. B. Betrug, der aus dem Verlust von personenbezogenen Daten resultiert, ist keine gute Praxis. Die Risikostreuung sollte zwischen Unternehmen und anderen Organisationen erfolgen, und erhebliche Risiken sollten nicht an den Betroffenen weitergegeben werden.

Die Übertragung von Risiko kann neue Risiken erzeugen oder bestehende, erkannte Risiken verändern. Daher könnte eine zusätzliche Risikobehandlung unter Umständen notwendig werden.

Es könnte möglich sein, die Verantwortung für das Risikomanagement zu übertragen, aber normalerweise ist es nicht möglich, die Haftung für eine Auswirkung zu übertragen. Die Anspruchsgruppen werden in der Regel negative Auswirkungen als Fehler der Organisation ansehen.

Wenn eine Organisation in ihrer Datenschutzerklärung eine spezielle Datenschutzregel definiert und die Annahmeerklärung festgelegt hat, sollte die Organisation berücksichtigen, dass nur die Vermeidung eine akzeptable Option wäre, um das Risiko zu behandeln, das bei diesem Kriterium die höchste Auswirkung verursacht.

ANMERKUNG Die Datenschutzrichtlinie ist grundsätzlich als eine Zusammenstellung von Regeln zu verstehen, die angibt, welche bestimmten personenbezogenen Daten von einer Organisation erhoben werden dürfen, wie sie verwendet werden und ob sie innerhalb der Organisation verbleiben oder mit anderen Organisationen geteilt oder an sie verkauft werden.

Eine Datenschutzrichtlinie enthält die allgemeine Absicht und Richtung, Regeln und Verpflichtungen, so wie sie von der verantwortlichen Stelle für die Verarbeitung personenbezogener Daten in einem bestimmten Rahmen formal formuliert wurden.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29134:2020-01