

Informationstechnik - Sicherheitsverfahren - Datenschutz-  
Folgenabschätzung - Leitfaden (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)

Dieser Europäische Norm-Entwurf wird den CEN-Mitgliedern zur Umfrage vorgelegt. Er wurde vom Technischen Komitee CEN/CLC/JTC 13 erstellt.

Wenn aus diesem Norm-Entwurf eine Europäische Norm wird, sind die CEN und CENELEC-Mitglieder gehalten, die CEN und 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.

Dieser Europäische Norm-Entwurf wurde von CEN und CENELEC in drei offiziellen Fassungen (Deutsch, Englisch, Französisch) erstellt. Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem CEN-CENELEC-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.

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

**Warnvermerk :** Dieses Schriftstück hat noch nicht den Status einer Europäischen Norm. Es wird zur Prüfung und Stellungnahme vorgelegt. Es kann sich noch ohne Ankündigung ändern und darf nicht als Europäischen Norm in Bezug genommen werden.



CEN-CENELEC Management Centre:  
Rue de la Science 23, B-1040 Brussels

# 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 Datenschutzerfordernngen .....	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 Handlungsplans 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 Untersucher Prozess .....	41
7.3.2 Risikokriterien .....	43
7.3.3 Ressourcen und beteiligte Personen .....	43
7.3.4 Konsultation mit Anspruchsgruppen .....	43
7.4 Datenschutzerfordernngen .....	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 Behandlung der Risiken .....	44
7.7	Schlussfolgerungen und Entscheidungen .....	44
7.8	Öffentliche Zusammenfassung der DSFA .....	44
<b>Anhang A (informativ) Abstufungskriterien für den Auswirkungsgrad und die</b>		
	<b>Eintrittswahrscheinlichkeit .....</b>	<b>46</b>
A.1	Allgemeines .....	46
A.2	Einschätzung des Auswirkungsgrades .....	46
A.3	Einschätzung der Wahrscheinlichkeit .....	47
<b>Anhang B (informativ) Generische Bedrohungen .....</b>		<b>48</b>
<b>Anhang C (informativ) Hilfestellung für die Einordnung verwendeter Begriffe .....</b>		<b>53</b>
C.1	Anwendungsbereich der DSFA .....	53
C.2	Projekt .....	53
C.3	Prozess .....	54
C.4	Bedeutung .....	54
C.5	Überwachung und Überprüfung .....	55
<b>Anhang D (informativ) Illustrierte Beispiele zur Unterstützung des DSFA-Prozesses .....</b>		<b>56</b>
D.1	Arbeitsablaufdiagramm für die Verarbeitung personenbezogener Daten .....	56
D.2	Beispiel einer Datenschutz-Risikokarte .....	56
<b>Literaturhinweise .....</b>		<b>58</b>

## 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.

## 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](http://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](http://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](http://www.iso.org/iso/foreword.html).

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

## 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 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 (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 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 Prozesses 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

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.