

DIN EN 17799

ICS 03.120.20; 03.160

Einsprüche bis 2022-01-26

Entwurf**Anforderungen an den Datenschutz bei Verarbeitungsvorgängen;
Deutsche und Englische Fassung prEN 17799:2021**

Personal data protection requirements for processing operations;
German and English version prEN 17799:2021

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2021-11-26 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 oder Am DIN-Platz, Burggrafenstr. 6, 10787 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 58 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (prEN 17799:2021) wurde vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitskreis NA 043-04-27-05 AK „Identitätsmanagement und Datenschutz-Technologien“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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

ISO/IEC 27000	siehe	DIN EN ISO/IEC 27000
ISO/IEC 27701	siehe	DIN EN ISO/IEC 27701
ISO/IEC 29134	siehe	DIN EN ISO/IEC 29134
ISO/IEC 29151	siehe	DIN EN ISO/IEC 29151*

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

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 27000, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Überblick und Terminologie*

DIN EN ISO/IEC 27701, *Sicherheitstechniken — Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz — Anforderungen und Leitlinien*

DIN EN ISO/IEC 29134, *Informationstechnik — Sicherheitsverfahren — Leitlinien für die Datenschutz-Folgenabschätzung*

DIN EN ISO/IEC 29151, *Informationstechnik — Sicherheitsverfahren — Leitfaden für den Schutz personenbezogener Daten*

* Zurzeit Entwurf.

Titel de: Anforderungen an den Datenschutz bei Verarbeitungsvorgängen

Titel en: Personal data protection requirements for processing operations

Titel fr:

Inhalt

	Seite
Europäisches Vorwort.....	4
Einleitung	5
1 Anwendungsbereich.....	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Übersicht.....	8
5 Planung.....	8
5.1 Allgemeines.....	8
5.2 Verstehen der Bedürfnisse und Erwartungen der interessierten Parteien.....	9
5.3 Umfang der Tätigkeiten zur Verarbeitung personenbezogener Daten	9
5.3.1 Allgemeines.....	9
5.3.2 Aufzeichnungen über Datenverarbeitungstätigkeiten	9
5.3.3 Ermittlung der Rechtsgrundlage.....	10
5.3.4 Minimierung der Datenmenge.....	11
5.3.5 Speicherung von Daten.....	11
5.4 Politik zum Schutz personenbezogener Daten.....	11
5.5 Rollen und Verantwortlichkeiten	12
5.5.1 Allgemeines.....	12
5.5.2 Interne Rollen.....	13
5.5.3 Externe Rollen	14
5.6 Risikomanagement.....	14
5.6.1 Allgemeines.....	14
5.6.2 Datenschutz-Risikobeurteilung und Auswirkungsanalyse	15
5.6.3 Bewertung der Auswirkungen auf den Datenschutz	16
5.6.4 Umgang mit Risiken und Risikobehandlungsplan	16
5.7 Schutz personenbezogener Daten durch Technik und durch datenschutzfreundliche Voreinstellungen	17
6 Operative Tätigkeiten.....	17
6.1 Allgemeines.....	17
6.2 Datenschutzerklärung und Einwilligung.....	18
6.2.1 Datenschutzerklärung.....	18
6.2.2 Einwilligung	18
6.3 Aktualisierung von Rollen.....	18
6.4 Schutz personenbezogener Daten	19
6.4.1 Löschung von Daten	19
6.4.2 Umsetzung und Anwendung von Sicherheitsmaßnahmen.....	19
6.4.3 Umgang mit Verletzungen des Schutzes personenbezogener Daten.....	20
6.5 Anträge der betroffenen Personen zur Durchsetzung ihrer Rechte.....	21
6.5.1 Allgemeines.....	21
6.5.2 Zugang zu Daten	21
6.5.3 Berichtigung.....	22
6.5.4 Löschung	22
6.5.5 Einschränkung der Verarbeitung	22
6.5.6 Datenübertragbarkeit	23
6.5.7 Widerspruch	23

6.5.8	Automatisierte Entscheidungen, einschließlich Profiling	23
6.5.9	Beschwerden und Einsprüche	23
6.6	Schulung und Sensibilisierung	23
7	Kontrolle	24
7.1	Allgemeines	24
7.2	Interne Audits	24
7.3	Regelmäßiger Bericht	25
7.4	Nichtkonformitäten und Korrekturmaßnahmen	25
Anhang A (informativ) Zuordnung der Anforderungen an Verantwortliche und Auftragsverarbeiter		27
Literaturhinweise		29

Europäisches Vorwort

Dieses Dokument (prEN 17799:2021) wurde vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Einleitung

Der Schutz personenbezogener Daten ist europaweit durch Rechtsakte geregelt, von denen der wichtigste die Verordnung (EU) 2016/679 (im Folgenden „Verordnung“) ist. Darin wird der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten geregelt, aber nicht in einen Zusammenhang mit einer Reihe von Folge- oder verwandten Tätigkeiten gestellt, und es wird speziell auf Mechanismen zur Zertifizierung des Schutzes personenbezogener Daten verwiesen, um die Einhaltung der Verordnung nachzuweisen.

ISO/IEC 27701 durchläuft derzeit das Verfahren zur Übernahme als EN, und CEN/CLC JTC 13 führt einen neuen Arbeitsschritt zur „Verbesserung von ISO/IEC 27701 für den EU-Kontext“ durch. Diese Bemühungen werden auch eine solide Grundlage für die Konformität mit der Datenschutz-Grundverordnung (DSGVO) und die Angleichung der europäischen Datenschutzlandschaft an globale Normen bilden. Diese Normen haben jedoch einen grundlegend anderen Schwerpunkt, da sie auf ein Managementsystem und nicht wie das vorliegende Dokument auf Dienstleistungen und Prozesse ausgerichtet sind.

1 Anwendungsbereich

Dieses Dokument legt die grundlegenden Anforderungen für den Nachweis fest, dass die Verarbeitungstätigkeiten dem europäischen normativen Bezugsrahmen für den Schutz personenbezogener Daten in Übereinstimmung mit EN ISO/IEC 17065 entsprechen. Es gilt jedoch nicht für Produkte oder Managementsysteme, die für die Verarbeitung personenbezogener Daten vorgesehen sind.

Dieses Dokument gilt für alle Organisationen, die – als für die Datenverarbeitung Verantwortliche („Verantwortlicher“) und/oder Auftragsverarbeiter – personenbezogene Daten verarbeiten, und sein Ziel ist es, eine Reihe von Anforderungen bereitzustellen, die es diesen Organisationen ermöglichen, sich wirksam an den europäischen normativen Bezugsrahmen für den Schutz personenbezogener Daten anzupassen.

Eine Organisation kann beschließen, dass die Norm nur auf eine bestimmte Untergruppe ihrer Verarbeitungstätigkeiten anwendbar ist, wenn eine solche Entscheidung nicht die Nichteinhaltung des normativen europäischen Bezugsrahmens für den Schutz personenbezogener Daten beinhaltet.

Dieses Dokument enthält auch Angaben für die Bewertung der Konformität mit den vorgenannten Anforderungen.

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

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 27000 und die folgenden Begriffe.

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

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

3.1

Aufsichtsbehörde

von einem Mitgliedstaat gemäß Artikel 51 eingerichtete unabhängige staatliche Stelle

[QUELLE: Verordnung (EU) 2016/679]

3.2

betroffene Aufsichtsbehörde

Aufsichtsbehörde, die von der Verarbeitung personenbezogener Daten betroffen ist, weil a) der Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist, b) diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann oder c) eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde

[QUELLE: Verordnung (EU) 2016/679]

3.3

Einwilligung

Einwilligung der betroffenen Person

jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist

[QUELLE: Verordnung (EU) 2016/679]

3.4

personenbezogene Daten

alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann

[QUELLE: Verordnung (EU) 2016/679]

3.5

Profiling

jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen

[QUELLE: Verordnung (EU) 2016/679]

3.6

Auftragsverarbeiter

natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet

[QUELLE: Verordnung (EU) 2016/679]

3.7

Verarbeitung

jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung

[QUELLE: Verordnung (EU) 2016/679]

3.8

Verantwortlicher

natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden

[QUELLE: Verordnung (EU) 2016/679]

3.9

Dritter

natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten

[QUELLE: Verordnung (EU) 2016/679]

3.10

Auswirkung

Datenschutzauswirkung

alles, was sich auf den Schutz einer betroffenen Person und/oder einer Gruppe von betroffenen Personen auswirkt

[QUELLE: ISO/IEC 27557]

3.11

Folge

Ergebnis eines Ereignisses, das die Ziele der Organisation beeinflusst

[QUELLE: ISO/IEC 27557]

4 Übersicht

In diesem Dokument werden die grundlegenden Anforderungen an die Verarbeitung personenbezogener Daten festgelegt, damit eine Organisation, sei es ein Verantwortlicher oder ein Auftragsverarbeiter, in der Lage ist, die Einhaltung des europäischen und des anwendbaren nationalen normativen Bezugsrahmens für den Schutz personenbezogener Daten zu erreichen. Die Trennung zwischen den Tätigkeiten des Verantwortlichen und des Auftragsverarbeiters beruht auf den Anforderungen des oben genannten normativen Bezugsrahmens, doch könnten den Auftragsverarbeitern von den entsprechenden Verantwortlichen weitere Tätigkeiten übertragen werden, wodurch die Anwendbarkeit der in diesem Dokument dargelegten zusätzlichen Anforderungen auf sie übertragen wird.

Das vorliegende Dokument wird durch Anhang A ergänzt, der die Angaben zur Bewertung der Konformität mit den Anforderungen des Dokuments enthält.

5 Planung

5.1 Allgemeines

In diesem Abschnitt sind die Tätigkeiten festgelegt, die ein Verantwortlicher oder ein Auftragsverarbeiter durchführen muss, um den Schutz personenbezogener Daten im Rahmen der Verarbeitungstätigkeiten systematisch und organisiert durchzuführen. Die Tätigkeiten müssen in regelmäßigen Abständen oder nach relevanten Änderungen durchgeführt werden, wie z. B. Änderungen der Gesetzgebung oder der Unternehmensorganisation und die IT oder ihre Merkmale betreffende strukturelle Änderungen.

5.2 Verstehen der Bedürfnisse und Erwartungen der interessierten Parteien

Der Verantwortliche oder der Auftragsverarbeiter muss Folgendes bestimmen:

- a) alle interessierten Parteien, die an der Verarbeitung personenbezogener Daten beteiligt sind, einschließlich der betroffenen Personen, der Auftragsverarbeiter und der Verantwortlichen; und
 - b) die Anforderungen dieser interessierten Parteien in Bezug auf die Verarbeitung personenbezogener Daten;
- die verpflichtenden Anforderungen des normativen Bezugsrahmens nationaler Gesetze und der vertraglichen Verpflichtungen.

5.3 Umfang der Tätigkeiten zur Verarbeitung personenbezogener Daten

5.3.1 Allgemeines

Der Verantwortliche muss die Grenzen und die Anwendbarkeit der Verarbeitung personenbezogener Daten festlegen und Folgendes dokumentieren: Aufzeichnungen über die Datenverarbeitungstätigkeiten, ihre Rechtsgrundlage, die Standorte, die Organisationsstruktur (einschließlich aller unter 5.1 genannten interessierten Parteien), die Informationssysteme und die wichtigsten verwendeten Hilfsmittel.

5.3.2 Aufzeichnungen über Datenverarbeitungstätigkeiten

Der Verantwortliche oder der Auftragsverarbeiter muss die personenbezogenen Daten und ihre Weitergabe im Zusammenhang mit jeder Verarbeitung identifizieren und sie in den Aufzeichnungen über die Verarbeitung personenbezogener Daten auf dem neuesten Stand halten. Insbesondere muss der Verantwortliche oder der Auftragsverarbeiter aktuelle Aufzeichnungen über die Datenverarbeitungstätigkeiten erstellen und führen, aus denen Folgendes hervorgeht:

- 1) der für die Verarbeitung Verantwortliche;
- 2) die Prozesse, bei denen personenbezogene Daten verwendet werden;
- 3) die Quellen der verarbeiteten personenbezogenen Daten;
- 4) die verarbeiteten personenbezogenen Daten und die entsprechenden Kategorien;
- 5) der Zweck der Verwendung der personenbezogenen Daten;
- 6) die Empfänger personenbezogener Daten, einschließlich Dritter;
- 7) die Rolle (Verantwortlicher, Auftragsverarbeiter oder für die Verarbeitung Mitverantwortlicher der Organisation);
- 8) die Informationssysteme, die an der Archivierung personenbezogener Daten beteiligt sind;
- 9) jede Weitergabe von personenbezogenen Daten an Dritte, internationale Organisationen oder Drittländer;
- 10) die Dauer der Speicherung personenbezogener Daten oder die Kriterien für die Festlegung dieser Dauer, und die am Ende der Dauer getroffenen Maßnahmen;
- 11) die Standorte, an denen eine Verarbeitung stattfindet.

ANMERKUNG Dies steht im Einklang mit Artikel 30 der Verordnung.

5.3.3 Ermittlung der Rechtsgrundlage

Der Verantwortliche muss die Rechtsgrundlage für die Verarbeitung personenbezogener Daten feststellen und sie den betroffenen Personen mitteilen. Der Verantwortliche muss die Rechtsgrundlage dokumentieren.

ANMERKUNG Die in Artikel 6 der Verordnung enthaltenen Rechtsgrundlagen lauten wie folgt:

- die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
- die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Werden besondere Kategorien personenbezogener Daten verarbeitet, so muss der Verantwortliche die Rechtsgrundlage für die Verarbeitung personenbezogener Daten ermitteln, festlegen, mitteilen und dokumentieren, wobei eine der folgenden Rechtsgrundlagen zu wählen ist:

- die ausdrückliche Einwilligung der betroffenen Person für bestimmte Zwecke;
- die Verarbeitung ist zur Erfüllung einer arbeitsrechtlichen Verpflichtung erforderlich;
- die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person erforderlich;
- die Verarbeitung ist auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten erforderlich;
- es handelt sich um Informationen, die von den betroffenen Personen offensichtlich öffentlich gemacht wurden;
- die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich;
- die Verarbeitung ist aus Gründen eines erheblichen öffentlichen Interesses erforderlich;
- die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin bzw. für die Erbringung von Dienstleistungen im Gesundheits- oder Sozialbereich erforderlich;
- die Verarbeitung ist aus Gründen der öffentlichen Gesundheit oder zur Wahrung des Berufsgeheimnisses erforderlich;
- die Verarbeitung ist für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erforderlich.

ANMERKUNG Wie in Artikel 9 der Verordnung festgelegt.

5.3.4 Minimierung der Datenmenge

Der Verantwortliche muss bei jeder Verarbeitung stets sicherstellen, dass:

- a) die Organisation die geringste Menge an personenbezogenen Daten verarbeitet, die zur Erfüllung ihrer rechtmäßigen Zwecke erforderlich ist;
- b) sonstige nicht relevante personenbezogene Daten nicht erhoben werden, es sei denn, die Bereitstellung solcher Informationen ist optional und diese werden nur mit Einwilligung der betroffenen Person verarbeitet;
- c) alle Verarbeitungstätigkeiten und die entsprechenden Zwecke entsprechend der Datenschutzerklärung durchgeführt werden;
- d) neue Systeme und Prozesse, die die Verarbeitung personenbezogener Daten einschließen, überprüft werden, um sicherzustellen, dass die verarbeiteten Informationen relevant und nicht unnötig sind.

5.3.5 Speicherung von Daten

Die Speicherfristen für personenbezogene Daten oder, falls deren Festlegung nicht möglich ist, die Kriterien für die Festlegung dieser Fristen, müssen:

- a) von dem Verantwortlichen unter Berücksichtigung der tatsächlichen Notwendigkeit der Verarbeitungszwecke und der in den normativen Anforderungen und in den Zwecken der Verarbeitung angegebenen Fristen festgelegt werden; und
- b) in der relevanten Datenschutzerklärung angegeben sein.

Der Verantwortliche muss eine Dokumentation über die Gründe führen, die zur Festlegung dieser Fristen geführt haben.

5.4 Politik zum Schutz personenbezogener Daten

Die oberste Leitung des Verantwortlichen oder des Auftragsverarbeiters muss eine Politik zum Schutz personenbezogener Daten festlegen, die:

- a) mit den Zielen der Organisation vereinbar ist;
- b) einen Bezugsrahmen für die Festlegung von Zielen für den Schutz personenbezogener Daten liefert;
- c) eine Verpflichtung zur Erfüllung der geltenden Anforderungen an den Schutz personenbezogener Daten im Einklang mit dem vorliegenden Dokument und dem normativen Bezugsrahmen für den Schutz personenbezogener Daten enthält;
- d) eine Verpflichtung enthält, den Schutz personenbezogener Daten kontinuierlich zu verbessern;
- e) für die Unternehmensorganisation und ihren geografischen Standort, die Architektur und Verbindung der Netzwerke und IT-Systeme sowie die bestehenden Politiken für den Datenaustausch geeignet ist.

Die Politik zum Schutz personenbezogener Daten muss:

- dokumentiert werden;
- innerhalb der Organisation kommuniziert werden;

- allen interessierten externen und internen Parteien, die an der Verarbeitung personenbezogener Daten beteiligt sind, zur Verfügung gestellt werden; und
- regelmäßig überprüft und erforderlichenfalls aktualisiert werden.

Die Politik für den Schutz personenbezogener Daten muss jede Verarbeitung personenbezogener Daten von betroffenen Personen einschließen, die unter EU-Recht fallen.

5.5 Rollen und Verantwortlichkeiten

5.5.1 Allgemeines

Die oberste Leitung des Verantwortlichen oder des Auftragsverarbeiters muss sicherstellen, dass die Zuständigkeiten und Befugnisse der relevanten Rollen zugewiesen und kommuniziert werden.

Die oberste Leitung des Verantwortlichen oder des Auftragsverarbeiters muss die Zuständigkeiten und Befugnisse zuweisen, um:

- a) sicherzustellen, dass die Tätigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten im Einklang mit dem vorliegenden Dokument und dem normativen Bezugsrahmen stehen; und
- b) der obersten Leitung über die Ergebnisse dieser Tätigkeiten Bericht zu erstatten.
- c) Zuständigkeiten müssen angemessen zugewiesen werden für:
 - d) die Überwachung der Übereinstimmung der Politik zum Schutz personenbezogener Daten mit dem normativen Bezugsrahmen;
 - e) die Umsetzung der Ziele für den Schutz personenbezogener Daten, einschließlich derjenigen, die in der Praxis hinsichtlich der Verarbeitung personenbezogener Daten aufgeführt oder in für die Organisation geltenden Verhaltensregeln festgelegt sind;
 - f) das Management des Schulungsprogramms und Sensibilisierung;
 - g) die Zuweisung von Berechtigungen für die Verarbeitung personenbezogener Daten;
 - h) die Festlegung und Freigabe der folgenden dokumentierten Verfahren für die Verarbeitung personenbezogener Daten:
 - 1) Erhebung und Verarbeitung personenbezogener Daten;
 - 2) Management und Kommunikation aller Informationen hinsichtlich des Schutzes personenbezogener Daten;
 - 3) Verarbeitung von Anträgen von betroffenen Personen;
 - 4) Beschwerdemanagement;
 - 5) Umgang mit Verletzungen des Schutzes personenbezogener Daten;
 - 6) Management von Lieferanten und externen Beauftragten;
 - 7) Kontrollen und jegliche Weitergabe personenbezogener Daten an Dritte oder internationale Organisationen;

- 8) Überwachung der Aktualisierung von normativen Vorgaben und rechtlichen Entwicklungen im Bereich des Schutzes personenbezogener Daten.

5.5.2 Interne Rollen

5.5.2.1 Datenschutzmanager

Mindestens ein Mitglied des Managements des Verantwortlichen oder des Auftragsverarbeiters muss als verantwortliche Person für Fragen des Datenschutzes bei Tätigkeiten zur Verarbeitung personenbezogener Daten innerhalb einer Organisation benannt werden, um die Einhaltung der Datenschutzanforderungen und bewährter Verfahren sicherzustellen.

In prEN 17740 sind die für das Profil geltenden Kompetenzanforderungen und seine Hauptmerkmale festgelegt.

5.5.2.2 Datenschutzbeauftragter

Ist ein Verantwortlicher oder ein Auftragsverarbeiter gemäß Artikel 37 der Verordnung verpflichtet, einen Datenschutzbeauftragten zu benennen, oder beschließt er, dies aufgrund besonderer betrieblicher Erfordernisse zu tun, so muss er eine Person, die für die Wahrnehmung dieser Aufgaben hinreichend qualifiziert ist, benennen und dieser Person diese Rolle zuweisen.

ANMERKUNG Die Zuweisung dieser Rolle zu dieser Person wird in Artikel 38 der Verordnung beschrieben.

Die Kontaktdaten des Datenschutzbeauftragten müssen der zuständigen Aufsichtsbehörde mitgeteilt und in der Datenschutzerklärung angegeben werden (siehe 6.2.1).

Der Datenschutzbeauftragte oder, falls ein solcher nicht vorhanden ist, eine entsprechend qualifizierte Person, muss zumindest die Durchführung der Aufgaben sicherstellen.

ANMERKUNG Die Aufgaben werden in Artikel 39 der Verordnung beschrieben.

In prEN 17740 sind die für das Profil geltenden Kompetenzanforderungen und seine Hauptmerkmale festgelegt.

5.5.2.3 Zur Verarbeitung personenbezogener Daten befugte Personen

Personen, die befugt sind, personenbezogene Daten innerhalb der Organisation eines Verantwortlichen oder eines Auftragsverarbeiters zu verarbeiten, müssen über ihre Rolle bei der Verarbeitung dieser personenbezogenen Daten und über die entsprechenden Verfahren, die sie einhalten müssen, informiert und dafür sensibilisiert werden. Sie müssen sich auch der Konsequenzen bewusst sein, die sich ergeben, wenn sie diese Verfahren nicht anwenden.

5.5.3 Externe Rollen

5.5.3.1 Auftragsverarbeiter

Externe interessierte Parteien im Sinne von 5.1 a), einschließlich Lieferanten oder Partner, die im Auftrag des Verantwortlichen oder eines anderen Auftragsverarbeiters Daten verarbeiten, ohne jedoch die Zwecke und Mittel der Verarbeitung personenbezogener Daten festzulegen, müssen:

- a) nachweisen, dass sie in der Lage sind, die Umsetzung von technischen und organisatorischen Maßnahmen, die dem Schutz personenbezogener Daten angemessen sind (siehe folgender Absatz), und die Einhaltung des normativen Bezugsrahmens für den Schutz personenbezogener Daten sicherzustellen;
- b) über einen Vertrag oder ein anderes Rechtsinstrument mit der Organisation verfügen, der bzw. das mindestens die folgenden Klauseln enthält:
 - 1) Vorgabe, dass die Verarbeitung personenbezogener Daten nur auf dokumentierte Weisung des Verantwortlichen erfolgen darf;
 - 2) Sicherstellung, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Wahrung des Datengeheimnisses verpflichtet sind;
 - 3) Verbot, weitere Auftragsverarbeiter ohne schriftliche Genehmigung des Verantwortlichen zu beauftragen;
 - 4) Vorgabe, die gleichen Datenschutzverpflichtungen, die in dem Vertrag oder anderen Rechtsinstrument festgelegt sind, auf ihre Auftragsverarbeiter anzuwenden;
 - 5) Vorgabe, den Verantwortlichen bei der Einhaltung der Verpflichtungen in Bezug auf die Meldung von Datenschutzverletzungen, Kommunikation und Datenschutz-Folgenabschätzung zu unterstützen, einschließlich etwaiger vorheriger Konsultationen;
 - 6) Vorgabe, nach Beendigung des Vertrags oder des Rechtsinstruments alle personenbezogenen Daten zu löschen oder an den Verantwortlichen zurückzugeben;
 - 7) Vorgabe, dem Verantwortlichen alle Informationen zur Verfügung zu stellen, die erforderlich sind, um die Einhaltung ihrer Pflichten nachzuweisen, sowie Überprüfungen und Inspektionen durch den Verantwortlichen zu ermöglichen und dazu beizutragen.

ANMERKUNG Die Klauseln sind in Artikel 28 der Verordnung aufgeführt.

5.6 Risikomanagement

5.6.1 Allgemeines

Der Verantwortliche oder der Auftragsverarbeiter muss unter Berücksichtigung der in 5.1 genannten Faktoren in regelmäßigen Abständen die Risiken und Chancen ermitteln, denen er begegnen muss, um unerwünschte Auswirkungen der Verarbeitung personenbezogener Daten zu verhindern oder zu verringern.

5.6.2 Datenschutz-Risikobeurteilung und Auswirkungsanalyse

Der Verantwortliche oder der Auftragsverarbeiter muss eine Risikobeurteilung und eine Auswirkungsanalyse hinsichtlich des Datenschutzes bei der Verarbeitung personenbezogener Daten erstellen, die, ausgehend von den in den Aufzeichnungen über die Datenverarbeitungstätigkeiten gesammelten Informationen und der Rechtsgrundlage für die Verarbeitung, Folgendes ermöglichen:

- a) Ermittlung der Risiken für die Rechte und Freiheiten der betroffenen Personen und, im Falle einer Verletzung des Schutzes personenbezogener Daten, auch für die Organisation;
- b) Bewertung der technischen und organisatorischen Maßnahmen zur Sicherstellung eines angemessenen Sicherheitsniveaus gegen Risiken;
- c) Bereitstellung der erforderlichen Garantien für die Erfüllung der Anforderungen des vorliegenden Teils des Dokuments und des normativen Bezugsrahmens für den Schutz personenbezogener Daten.

Diese Prozesse müssen:

- d) Folgendes festlegen und anwenden:
 - 1) Kriterien für die Akzeptanz der Risiken hinsichtlich des Schutzes personenbezogener Daten;
 - 2) Kriterien für die Durchführung von Risikobeurteilungen hinsichtlich des Schutzes personenbezogener Daten;
- e) sicherstellen, dass wiederholte Risikobeurteilungen hinsichtlich des Schutzes personenbezogener Daten zu widerspruchsfreien, gültigen und vergleichbaren Ergebnissen führen;
- f) Risiken hinsichtlich des Schutzes personenbezogener Daten ermitteln, die zusammenhängen mit:
 - 1) der Nichteinhaltung von Gesetzen, technischen Standards und normativen Bezugsrahmen zum Schutz personenbezogener Daten;
 - 2) Auswirkungen auf die Rechte und Freiheiten der betroffenen Personen;
 - 3) physischen, materiellen oder immateriellen Schäden; und
 - 4) Auswirkungen auf die Organisation (einschließlich, aber nicht beschränkt auf Rufschädigung, Sanktionen, wirtschaftliche Verluste usw.);
- g) die Verantwortlichen für risikobezogene Entscheidungen ermitteln;
- h) Risiken hinsichtlich des Schutzes personenbezogener Daten analysieren durch:
 - 1) eine Bewertung der Wahrscheinlichkeit des Eintretens der ermittelten Risiken;
 - 2) eine Bewertung der möglichen Folgen und Auswirkungen, die sich ergeben würden, wenn die ermittelten Risiken eintreten würden;
 - 3) eine Bestimmung des Risikolevels;
- i) Risiken hinsichtlich des Schutzes personenbezogener Daten bewerten durch:
 - 4) Vergleich der Ergebnisse der Risikobeurteilungen mit Risikoakzeptanzkriterien; und
 - 5) Festlegen der Prioritäten der analysierten Risiken für den Umgang mit Risiken.

Der Prozess der Risikobeurteilung hinsichtlich des Schutzes personenbezogener Daten muss umgesetzt werden:

- j) mit der vom Management für die gesamte Verarbeitung personenbezogener Daten festgelegten und freigegebenen Häufigkeit;
- k) wenn wesentliche Änderungen an den Modalitäten oder Instrumenten zur Durchführung von Tätigkeiten im Rahmen der IT-Datenverarbeitung vorgenommen werden.

Der Verantwortliche und die Auftragsverarbeiter müssen regelmäßig relevante Informationen über die Risiken bei Verarbeitungstätigkeiten austauschen. Der Verantwortliche oder der Auftragsverarbeiter muss dokumentierte Verfahren für die Datenschutz-Risikobeurteilung anwenden und Aufzeichnungen über die durchgeführten Tätigkeiten und deren Ergebnisse aufbewahren.

5.6.3 Bewertung der Auswirkungen auf den Datenschutz

Bei Verarbeitungstätigkeiten, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellen (einschließlich der in Artikel 35 Absatz 3 der Verordnung genannten Risiken), muss der Verantwortliche in den Fällen, in denen die unter Buchstabe f) oben genannten Auswirkungen eintreten, und unter der Annahme, dass keine Maßnahmen zur Risikominderung ergriffen werden,

- a) die vorherige Zustimmung durch die Aufsichtsbehörde beantragen;

ANMERKUNG Dies wird in Artikel 36 der Verordnung beschrieben.

- b) eine Dokumentation über die Kriterien und Prozesse für die Interaktion mit der zuständigen Aufsichtsbehörde führen.

Der Verantwortliche muss dokumentierte Verfahren für die Bewertung der Auswirkungen auf den Schutz personenbezogener Daten anwenden und Aufzeichnungen über die durchgeführten Tätigkeiten und die entsprechenden Ergebnisse aufbewahren.

ANMERKUNG Weitere Hinweise zu einer Methodologie für die Durchführung von Auswirkungsanalysen hinsichtlich des Schutzes personenbezogener Daten sind in ISO/IEC 29134 zu finden.

5.6.4 Umgang mit Risiken und Risikobehandlungsplan

Der Verantwortliche oder der Auftragsverarbeiter muss ein Verfahren zum Umgang mit Risiken hinsichtlich des Schutzes personenbezogener Daten festlegen und anwenden zur:

- a) Auswahl geeigneter Strategien für den Umgang mit Risiken hinsichtlich des Schutzes personenbezogener Daten unter Berücksichtigung der Ergebnisse der Risikobeurteilung;
- b) Festlegung der Maßnahmen, die für den Umgang mit Risiken im Hinblick auf die gewählten Strategien erforderlich sind, einschließlich der Umsetzung neuer Maßnahmen oder der Änderung bestehender Maßnahmen;
- c) Ermittlung geplanter technischer und organisatorischer Maßnahmen zur Sicherstellung eines dem Risiko angemessenen Sicherheitsniveaus.

ANMERKUNG Organisationen können zur Ermittlung der erforderlichen Maßnahmen und zum Nachweis, dass die Verarbeitung in Übereinstimmung mit diesem Dokument erfolgt, Verhaltensregeln anwenden, die von den zuständigen Regulierungs- und Aufsichtsbehörden oder anderen Normen wie ISO/IEC 29151 oder ISO/IEC 27701 vorgeschrieben werden.

- d) Ausarbeitung eines Risikobehandlungsplans für den Schutz personenbezogener Daten;