

DIN EN 17740

ICS 03.100.30; 35.030

Einsprüche bis 2021-12-01

Entwurf**Anforderungen an Berufsprofile im Zusammenhang mit der Verarbeitung und dem Schutz personenbezogener Daten;
Deutsche und Englische Fassung prEN 17740:2021**

Requirements for professional profiles related to personal data processing and protection;
German and English version prEN 17740:2021

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2021-10-01 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 108 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (prEN 17740:2021) wurde vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ 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 17024 siehe DIN EN ISO/IEC 17024

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 17024, *Konformitätsbewertung — Allgemeine Anforderungen an Stellen, die Personen zertifizieren*

<i>Titel de:</i>	Anforderungen an Berufsprofile im Zusammenhang mit der Verarbeitung und dem Schutz personenbezogener Daten
<i>Titel en:</i>	Requirements for professional profiles related to personal data processing and protection
<i>Titel fr:</i>	

Inhalt

	Seite
Europäisches Vorwort	3
Einleitung	4
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Aufgaben des Berufsprofils und konkrete Tätigkeiten	8
5 Wissen, Fertigkeiten und Kompetenzen im Zusammenhang mit der beruflichen Tätigkeit.....	10
6 Elemente für die Bewertung und Validierung von Lernergebnissen	36
Anhang A (informativ) Index von Fertigkeiten und Wissen	38
Anhang B (normativ) Anforderungen für den Zugang zu Berufsprofilen.....	52
Literaturhinweise.....	54

Europäisches Vorwort

Dieses Dokument (prEN 17740:2021) 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

Die Definition für Anforderungen an Berufsprofile auf dem Gebiet der Verarbeitung und des Schutzes personenbezogener Daten ist notwendig, um Grundlagenwissen, -fertigkeiten und -kompetenzen festzulegen, die diese Profile unterscheiden.

Die Norm gilt für die Berufsprofile im identifizierten Bereich, unabhängig von den Arbeitsverfahren und der Art des Beschäftigungsverhältnisses. Die Aufgaben und Tätigkeiten im Zusammenhang mit dem Beruf werden auf der Grundlage aller Funktionen beschrieben, die von auf dem Gebiet der Verarbeitung und des Schutzes personenbezogener Daten beschäftigten Fachkräften in verschiedenen Arbeitsbereichen tatsächlich ausgeführt werden. Diese Funktionen sind vielfältig und betreffen technische, administrative, kulturelle, wissenschaftliche und rechtliche Aspekte.

Diese Norm wendet den europäischen Referenzrahmen für die Definition von Kompetenzen und zugehörigen Fertigkeiten an: EN 16234-1. Für damit verbundene IKT-orientierte Profile, wie z. B. den Systemadministrator, wird auf CEN CWA 16458-1 verwiesen.

Die in dieser Norm definierten Profile erheben keinen Anspruch auf Vollständigkeit und sind unabhängig vom Arbeitseinsatz der in der Branche tätigen Personen anwendbar.

Diese Norm richtet sich in erster Linie an Fachkräfte, die Orientierungshilfe für ihre berufliche Entwicklung suchen, an Unternehmen, die ihre interne Datenschutzorganisation und die damit verbundenen Einstellungsanforderungen festlegen, sowie an Stellen, die Personalschulungen, Akkreditierungs- und Zertifizierungsdienste anbieten.

Methodischer Ansatz

Bei der Entwicklung dieser Norm wurden zunächst die in der Empfehlung 2008/C 111/01 (Europäischer Qualifikationsrahmen – EQR) und der Empfehlung 2009/C 155/02 (Europäisches Leistungspunktesystem für die Berufsbildung – ECVET) dargelegten Grundsätze und Angaben berücksichtigt.

Unter methodischen Gesichtspunkten wurde insbesondere festgestellt, dass:

- die übernommenen Grundbegriffe (Abschnitt 3) sich größtenteils aus dem EQR, dem ECVET und der einschlägigen, in der Europäischen Gemeinschaft gebräuchlichen Terminologie ableiten;
- die spezifischen Begriffe des Themas „Schutz personenbezogener Daten“ mit denen der Verordnung (EU) 2016/679 übereinstimmen;
- für die Beschreibung der Anforderungen an Wissen, Fertigkeiten und Kompetenz eines bestimmten Berufsprofils es notwendig ist, von einer vorläufigen Identifizierung der Aufgaben und spezifischen Tätigkeiten des Berufsprofils auszugehen (Abschnitt 4);
- die Anforderungen des spezifischen Berufsprofils in Bezug auf Wissen, Fertigkeiten und Kompetenz definiert sind (Abschnitt 5) und die erwarteten persönlichen Fähigkeiten, soweit zutreffend, ebenfalls festgelegt wurden. Außerdem werden die Niveaus angegeben, die mit der spezifischen beruflichen Tätigkeit verbunden sind, wobei die e-CF-Niveaus verwendet werden, die direkt auf die Niveaus des Europäischen Qualifikationsrahmens (EQR) abgestimmt sind;

- die nützlichen Elemente in Bezug auf die anzuwendenden Beurteilungsverfahren werden definiert (Abschnitt 7). Diese Elemente wurden unter Berücksichtigung dessen entwickelt, was bereits im Rahmen der freiwilligen technischen Normung konsolidiert wurde, auch unter Verweisung auf das normative Korpus zur Konformitätsbewertung (Reihe EN ISO/IEC 17000);
- in Anhang A (normativ) sind die Fertigkeiten und das Wissen aufgeführt, die für die Erarbeitung der Profile anwendbar sind;
- in Anhang B (normativ) werden die Anforderungen für den Zugang zu Berufsprofilen definiert.

Darüber hinaus wurden, soweit zutreffend, auch die Leitlinien des CEN-Guides 14 befolgt.

1 Anwendungsbereich

Dieses Dokument definiert die Anforderungen an die berufliche Tätigkeit von Personen, die im Bereich der Verarbeitung und des Schutzes personenbezogener Daten tätig sind, d. h. an den intellektuellen Beruf, der auf verschiedenen Komplexitätsniveaus und in verschiedenen organisatorischen Kontexten, sowohl im öffentlichen als auch im privaten Bereich, ausgeübt wird.

Diese Anforderungen werden ausgehend von den identifizierten spezifischen Aufgaben und Tätigkeiten in Form von Wissen, Fertigkeiten und Kompetenzen in Übereinstimmung mit dem Europäischen Qualifikationsrahmen (EQR) spezifiziert und so ausgedrückt, dass sie die Evaluierungs- und Validierungsprozesse von Lernergebnissen erleichtern und so weit wie möglich zur Harmonisierung beitragen.

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).

EN 16234-1, *e-Kompetenz-Rahmen (e-CF) — Ein gemeinsamer europäischer Rahmen für IKT-Fach- und Führungskräfte in allen Branchen — Teil 1: Rahmenwerk*

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

EN ISO/IEC 29100, *Informationstechnik — Sicherheitstechniken — Rahmenwerk für Datenschutz*

ISO/IEC 17024, *Conformity assessment — General requirements for bodies operating certification of persons*

CWA 16458-3, *European ICT Professional Role Profiles — Part 3: Methodology*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach EN 16234-1, EN ISO/IEC 27000, EN ISO/IEC 29100 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 <https://www.iso.org/obp>

3.1 formales Lernen

Lernprozess, der sich aus beabsichtigten und strukturierten Schulungsaktivitäten ergibt, die von Einrichtungen/Institutionen der Aus- und Weiterbildung, die von einer zuständigen Behörde anerkannt sind, durchgeführt werden

Anmerkung 1 zum Begriff: Formales Lernen kann die Ausstellung von Zertifikaten mit Rechtsgültigkeit beinhalten.

3.2

informelles Lernen

Lernprozesse, die sich aus Berufserfahrungen, aus dem Familienleben und auch aus der Freizeit ableiten lassen

Anmerkung 1 zum Begriff: Informelles Lernen ist keine bewusst strukturierte Aktivität, und manchmal ist das Lernen nicht beabsichtigt.

3.3

nicht-formales Lernen

Lernprozess, der sich aus beabsichtigten und strukturierten Schulungsaktivitäten ergibt, die in einem anderen als dem formalen Bereich durchgeführt werden

Anmerkung 1 zum Begriff: Bei einer derartigen Schulung wird kein rechtsgültiges Zertifikat ausgestellt.

3.4

Audit

systematisches, unabhängiges und dokumentiertes Verfahren zur Erlangung von Auditnachweisen (Aufzeichnungen, Tatbestände oder andere relevante und überprüfbare Informationen) und deren objektive Bewertung, um festzustellen, inwieweit die Auditkriterien (Richtlinien, Verfahren oder Anforderungen, die als Verweisung dienen) erfüllt wurden

3.5

Validierung der Lernergebnisse

Verfahren, mit dem bestätigt wird, dass bestimmte beurteilte Lernergebnisse, die von einem Lernenden erzielt wurden, den für eine bestimmte Qualifikation oder einen Teil davon erforderlichen Ergebnissen entsprechen

Anmerkung 1 zum Begriff: Die Zertifizierung nach ISO/IEC 17024 ist ein Evaluierungs- und Validierungsprozess.

Anmerkung 2 zum Begriff: Die Anerkennung von Lernergebnissen nach festgelegten Regeln durch die Fachbereiche oder andere zuständige Organisationen ist ebenfalls ein Prozess der Evaluierung und Validierung.

3.6

Datenschutz-Folgenabschätzung (DSFA)

Gesamtprozess aus Identifizierung, Analyse, Bewertung, Beratung, Kommunikation und Planung der Verarbeitung von möglichen Datenschutzfolgen bei der Verarbeitung personenbezogener Daten, eingebunden in den Gesamtrahmen des Unternehmens für das Risikomanagement

[QUELLE: ISO/IEC 29134]

3.7

Datenschutzvereinbarung

PLA, en: Privacy Level Agreement

Schutzniveau für personenbezogene Daten, das von einem Anbieter bei der Erbringung von Dienstleistungen für seine Kunden garantiert wird, konzeptionell ähnlich wie ein SLA

3.8

Qualifikation

formelles Ergebnis eines Beurteilungs- und Validierungsprozesses, das erzielt wird, wenn eine zuständige und unparteiische Organisation erklärt, dass die Lernergebnisse einer Person mit den technischen Normen übereinstimmen

Anmerkung 1 zum Begriff: Definition basierend auf dem EQR, Anhang I, Definition a).

3.9

Ergebnisse des Lernens

Beschreibung dessen, was eine Person am Ende eines Lernprozesses weiß, versteht und in der Lage ist zu tun

Anmerkung 1 zum Begriff: Die Ergebnisse werden in Form von Wissen, Fertigkeiten und Kompetenzen beschrieben.

Anmerkung 2 zum Begriff: Lernergebnisse können aus formalem, nicht-formalem oder informellem Lernen hervorgehen.

3.10

Dienstleistungsvereinbarung

SLA, en: Service Level Agreement

Dokument, in dem die Ziele für die technische Unterstützung oder die Unternehmensleistung festgelegt sind, einschließlich der Leistungsmaßstäbe und der Folgen bei Nichterfüllung, die der Anbieter einer Dienstleistung seinen Kunden bieten kann

[QUELLE: ISO/IEC 27039]

3.11

Evaluierung der Lernergebnisse

Verfahren und Prozesse, die verwendet werden, um zu bestimmen, inwieweit eine Person ein bestimmtes Wissen, eine bestimmte Fertigkeit oder Kompetenz tatsächlich erworben hat

4 Aufgaben des Berufsprofils und konkrete Tätigkeiten

4.1 Allgemeines

Die Fachkraft, die im Bereich der Verarbeitung und des Schutzes personenbezogener Daten tätig ist, übt eine breite Palette von Tätigkeiten aus, die häufig übergreifend zu anderen Geschäftsprozessen sind, sowohl in Bezug auf den Lebenszyklus der Verarbeitung - von der Planung bis zur Einstellung - als auch in Bezug auf die untersuchten technologischen, organisatorischen, rechtlichen oder sonstigen Themen.

Die Fachkraft, die im Bereich der Verarbeitung und des Schutzes personenbezogener Daten tätig ist, trägt somit zum Management oder zur Verifizierung einer mehr oder weniger umfangreichen Reihe von Prozessen und Informationssystemen bei, die mit der Verarbeitung personenbezogener Daten im Auftrag natürlicher oder juristischer Personen, wie z. B. Einrichtungen, Institutionen, Verbänden, öffentlichen oder privaten Unternehmen, verbunden sind. Juristische Personen unterschiedlicher Größe dürfen beschließen, entweder verwandte Berufsprofile zu einem einzigen zusammenzufassen (z. B. Datenschutzmanager und Datenschutzspezialist oder ein Datenschutzauditor mit einem anderen Auditor) oder mehrere Instanzen desselben Profils in verschiedenen Zuständigkeitsbereichen, z. B. in geografischen oder organisatorischen Bereichen, zu haben. In jedem Fall sollte die Trennung zwischen kontrollbezogenen Profilen wie Wirtschaftsprüfer und Datenschutzbeauftragter und den anderen Profilen beibehalten werden.

Zum Zeitpunkt der Veröffentlichung dieser Norm sind die Aufrechterhaltung, die Aktualisierung und die Entwicklung der für die berufliche Tätigkeit erforderlichen Fertigkeiten der Personen, die in der Verarbeitung und im Schutz personenbezogener Daten tätig sind, nicht Gegenstand eines hiermit festgelegten detaillierten Ausbildungsweges. Die Fachkraft ist jedoch verpflichtet, sich im Einklang mit den Bestimmungen von Absatz 6.4 und Anhang B eigenständig oder unter Anleitung beruflich fortzubilden.

ANMERKUNG Wenn Fachkräfte bereits frühere Ausbildungen absolviert haben, die nicht mit den Vorgaben dieser Norm übereinstimmen, wird die Zertifizierungsstelle höchstwahrscheinlich einen analytischen Vergleich zwischen dem vom Zertifizierungskandidaten bereits absolvierten Weg und dem in dieser Norm dargestellten Weg durchführen müssen, wobei die entsprechenden Verantwortlichkeiten übernommen werden.

4.2 Einführung in die Berufsprofile

Zum besseren Verständnis der wichtigsten Berufsprofile, auf die in Abschnitt 6 dieser Norm Bezug genommen wird, werden im Folgenden eine Reihe von Überlegungen aufgeführt, die einleitenden Charakter haben und der Beschreibung vorausgehen.

Datenschutzbeauftragter

Es handelt sich um ein Profil, das dem in der Verordnung (EU) 2016/679 beschriebenen Berufsprofil, Art. 39, entspricht. Es ist möglich, dem Profil verschiedene Aufgaben und weitere Aufgaben zuzuweisen, die in anderen Profilen der Führungsebene enthalten sind, sofern kein Interessenkonflikt vorliegt.

Datenschutzmanager

Es handelt sich um ein Profil, das Fachkräften mit einem sehr hohen Niveau an Wissen, Fertigkeiten und Kompetenzen in einem bestimmten organisatorischen Umfeld (sowohl in einem funktionalen Bereich der Organisation als auch in einer bestimmten Branche) entspricht, um die Übernahme geeigneter organisatorischer Maßnahmen bei der Verarbeitung personenbezogener Daten sicherzustellen.

Datenschutzspezialist

Es handelt sich um ein Profil für Fachkräfte, die in der Lage sind, den Datenschutzbeauftragten und/oder den Datenschutzmanager bei der Entwicklung geeigneter technischer und organisatorischer Maßnahmen für die Verarbeitung personenbezogener Daten zu unterstützen.

Datenschutzingenieur

Es handelt sich um ein Profil für Fachkräfte, die Systeme zur Verarbeitung personenbezogener Daten entwickeln und aufbauen und die über Fachwissen zu den damit verbundenen Datenschutzfragen verfügen und dafür verantwortlich sind. Sie können mit anderen Software- und Systemingenieuren und verwandten technischen Disziplinen zusammenarbeiten, aber auch mit anderen datenschutzorientierten Profilen in einem Unternehmen, die diese Systeme entwickeln und betreiben.

Datenschutzauditor

Es handelt sich um ein Profil, das unabhängigen Fachkräften mit Wissen und Fertigkeiten in der IT-/Technologiebranche und in juristischen/organisatorischen Tätigkeiten entspricht, die in der Lage sind, die Verarbeitung und den Schutz personenbezogener Daten durchzuführen, die jedoch für die Durchführung von Auditaufträgen auf Datenschutzexperten in beiden Bereichen zurückgreifen können.

4.3 Aufgaben und Tätigkeiten der Fachkraft bei der Verarbeitung und dem Schutz personenbezogener Daten

Das Profil der Fachkraft, die im Bereich der Verarbeitung und des Schutzes personenbezogener Daten tätig ist, umfasst eine Reihe grundlegender Aufgaben, die, ohne Anspruch auf Vollständigkeit, im folgenden Abschnitt 5 beschrieben werden (siehe Punkt „Hauptaufgaben“).

Als Fachkraft für die Verarbeitung und den Schutz personenbezogener Daten wird eine Person bezeichnet, deren Profil den oben genannten Aufgaben entspricht und die die „erwarteten Ergebnisse“ erzielt bzw. darauf vorbereitet ist.

5 Wissen, Fertigkeiten und Kompetenzen im Zusammenhang mit der beruflichen Tätigkeit

5.1 Allgemeines

Jedes Berufsprofil in diesem Kapitel ist strukturiert mit einer kurzen zusammenfassenden Beschreibung, der verfolgten Mission, den Ergebnissen, für die sie verantwortlich, zuständig oder mitwirkend sind, den spezifischen, ausgeführten Hauptaufgaben, den nach EN 16234-1 und CWA 16458-3 definierten Kompetenzen, die im Abschnitt „e-CF-Kompetenzen“ mit den zugehörigen Fertigkeiten und dem Wissen identifiziert werden, und den KPIs, die ihre Leistung messen.

5.2 Berufsprofil des Datenschutzbeauftragten

Kurzbeschreibung

Berät Verantwortliche oder Auftragsverarbeiter bei der Anwendung der Verordnung (EU) 2016/679.

Mission

Berät für die Verarbeitung Verantwortliche oder Auftragsverarbeiter in Bezug auf die Risiken von Datenverarbeitungstätigkeiten, um die Einhaltung der EU-Verordnung 2016/679 und anderer lokaler Datenschutzbestimmungen sicherzustellen.

Ergebnisse¹

Rechenschaftspflichtig

- Regelmäßige risikobasierte Berichte über die Einhaltung der Gesetze zum Schutz personenbezogener Daten.
- Unterlagen zur Unterstützung des an die Datenschutzbehörden gerichteten Antrags auf Konsultation entsprechend der Entwicklung der Datenschutz-Folgenabschätzung nach Verordnung 2016/679.
- Ersuchen um Konsultation der Datenschutzbehörden zu spezifischen Anwendungsfragen.
- Dokumentation zur Unterstützung der Schnittstelle mit den Datenschutzbehörden (Auskunftersuchen, Beurteilungsverfahren oder Testen usw.).
- Dokumentation (einschließlich Formulare) zur Unterstützung der Schnittstelle mit den interessierten Parteien.
- Indikatoren für den Schutz personenbezogener Daten.
- Beratung bei Anfragen zum Datenschutzrecht und dessen Anwendung.
- Verantwortlich
- Stellungnahmen zu Datenschutz-Folgenabschätzungen nach Verordnung 2016/679.

¹ Es ist zu beachten, dass alle hier beschriebenen Berufsprofile nicht mit rechtlichen, sondern nur mit operativen Verantwortlichkeiten verbunden sind.

Beitragender

- Zuweisung von Verantwortlichkeiten bei der Verarbeitung und dem Schutz personenbezogener Daten.
- Budget für den Schutz personenbezogener Daten.
- Richtlinien für den Schutz personenbezogener Daten.
- Hinweise zum Datenschutz.
- Anforderungen an die Verarbeitung und den Schutz personenbezogener Daten.
- Betriebsverfahren für die Verarbeitung und den Schutz personenbezogener Daten.
- Ausarbeitung einer Datenschutz-Folgenabschätzung.
- Bewertung des Risikos im Zusammenhang mit der Informationssicherheit.
- Risikomanagementplan für die Informationssicherheit.
- Verhaltensregeln.
- Antworten an die betroffene Person bei der Ausübung ihrer Rechte.
- Auditprogramm für den Schutz und die Verarbeitung personenbezogener Daten.
- Weiterbildungsprogramm, berufliche Entwicklung und Bewusstsein.
- Meldung von Vorfällen, die zu einer Verletzung personenbezogener Daten führen (an die Datenschutzbehörden).

Hauptaufgaben

- Information und Beratung des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters sowie der an der Verarbeitung personenbezogener Daten beteiligten Mitarbeiter über die Verpflichtungen, die sich aus dieser Verordnung sowie aus anderen Datenschutzvorschriften der Union oder der Mitgliedstaaten ergeben;
- Überwachung der Einhaltung der Verordnung, anderer Datenschutzvorschriften der Union oder der Mitgliedstaaten und der Richtlinien des Verantwortlichen oder des für die Datenverarbeitung Verantwortlichen zum Schutz personenbezogener Daten, einschließlich der Zuweisung von Verantwortlichkeiten, des Bewusstseins und der Schulung des an der Verarbeitung beteiligten Personals und der damit verbundenen Kontrolltätigkeiten;
- Bereitstellung einer Stellungnahme zur Datenschutz-Folgenabschätzung auf Anfrage und Überwachung von deren Durchführung;
- Zusammenarbeit mit der Aufsichtsbehörde;
- Funktion als Kontaktstelle für die Aufsichtsbehörde in Fragen der Verarbeitung.

Die folgende Tabelle 1 zeigt die zugewiesenen Kompetenzen und die erforderlichen Niveaus nach dem in EN 16234-1 vorgesehenen e-CF.

Tabelle 1 — Zugewiesene Kompetenzen und erforderliche Niveaus nach dem in EN 16234-1 vorgesehenen e-CF

<i>e-CF-Kompetenz</i>	<i>Niveau</i>
D.8. Vertragsmanagement	3
D.9. Personalentwicklung	3
E.3. Risikomanagement	4
E.4. Management von Geschäftsbeziehungen	4
E.8. Informationssicherheitsmanagement	3

Fertigkeiten

- Analyse der Verarbeitung personenbezogener Daten und Bewertung ihrer Übereinstimmung mit den geltenden rechtlichen Anforderungen
- Überprüfung der Anwendung von Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- Überprüfung der angemessenen Anwendung der Datenschutzgrundsätze
- Identifizierung von Rollen, Verantwortlichkeiten und Rechtsgrundlagen für die Verarbeitung personenbezogener Daten
- Mitwirkung an der Strategie für die Verarbeitung und den Schutz personenbezogener Daten
- Beitrag zur Bereitstellung korrekter Informationen für die betroffenen Personen
- Management der Anwendung von Verhaltensregeln und Zertifizierungen, die für die Verarbeitung und den Schutz von personenbezogenen Daten gelten
- Kommunikationsfähigkeit
- Analytische Fertigkeiten
- Selbstmanagement und Stressbewältigung
- Fähigkeit zur Selbstentfaltung
- Kontrollfähigkeit
- Überzeugungsfähigkeit
- Fähigkeit zur Konfliktbewältigung
- Initiative
- Berechtigung zur Verhandlung
- Organisatorische Fertigkeiten
- Perspektivisches Denken
- Planung und Terminierung
- Konstruktive Einstellung bei der Lösung von Problemen

- Hartnäckigkeit
- S1 – Thematisieren des CPD-Bedarfs des Personals, um die Anforderungen der Organisation zu erfüllen
- S5 – Analysieren der unternehmenskritischen Vermögenswerte und Identifizieren von Schwachstellen und Anfälligkeiten für Eindringversuche oder Angriffe
- S19 – Vorkalkulieren der erforderlichen Änderungen der Informationssicherheitsstrategie der Organisation und Formulierung neuer Pläne
- S21 – Anwenden von Minderungs- und Notfallmaßnahmen
- S23 – Anwenden von relevanten Standards, bewährten Verfahrensweisen und gesetzlichen Anforderungen für die Informationssicherheit
- S40 – Betreuen (Coachen)
- S45 – Verfassen, Dokumentieren und Katalogisieren von wesentlichen Prozessen und Verfahren
- S52 – Kommunizieren und Bewerten der Risikoanalysenergebnisse und entsprechenden Risikomanagementprozesse der Organisation
- S55 – Kommunizieren guter und schlechter Nachrichten zur Vermeidung von Überraschungen
- S66 – Erstellen eines Risikomanagementplans zur Ausarbeitung des Vorbeugemaßnahmenplans
- S91 – Sicherstellen, dass die Rechte des geistigen Eigentums und der Datenschutz eingehalten werden
- S111 – Erkennen von Kompetenzlücken und fehlenden Fertigkeiten (Qualifikationslücken)
- S140 – Aushandeln von Vertragsklauseln und -bedingungen
- S153 – Erstellen von Vorlagen für gemeinsame Veröffentlichungen
- S156 – Gestalten und Dokumentieren der Prozesse zur Risikoanalyse und zum Risikomanagement
- S167 – Zusammentragen von internen und externen Wissens- und Informationsanfragen
- S171 – Bereitstellen von Informationen
- S172 – Thematisieren der beruflichen Entwicklungsanforderungen an das Personal zur Einhaltung der Anforderungen der Organisation
- S176 – Überwachen und Umsetzen der wirksamen Anwendung von Unternehmensstandards für Veröffentlichungen
- S187 – Entwickeln eines Risikomanagementplans zum Identifizieren der erforderlichen Vorbeugemaßnahmen

Wissen

- Die Grundsätze des Datenschutzes einschließlich des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- Die in den geltenden Gesetzen und Verordnungen verankerten Rechte der interessierten Parteien
- Verantwortlichkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten
- Lokale und europäische Gesetze über die Verarbeitung und den Schutz personenbezogener Daten

- Rechtliche Entwicklungen im Zusammenhang mit lokalen und europäischen Gerichtsentscheidungen.
- Gesetzgebung über die Übermittlung personenbezogener Daten ins Ausland und die Weitergabe personenbezogener Daten außerhalb der EU/des EWR
- Methoden der Datenschutz-Folgenabschätzung
- Mögliche Bedrohungen für den Schutz personenbezogener Daten
- Technische ISO/IEC-Normen für das Management personenbezogener Daten
- Die Verhaltensregeln und Zertifizierungen, die für die Verarbeitung und den Schutz personenbezogener Daten gelten
- Kommunikationstechniken und -instrumente (Beziehungen zu Institutionen, Behörden, Strafverfolgungsbehörden, lokalen Behörden und der Presse)
- Kryptographische Techniken
- Anonymisierungstechniken
- Pseudonymisierungstechniken
- Überwachungs- und Berichterstattungssysteme und -techniken
- Werkzeuge für die Erstellung, Aufbereitung und Verteilung von professionellen Dokumenten
- K49 – Kompetenzentwicklungsmethoden
- K60 – Organisationsprozesse einschließlich Entscheidungsfindung, Budget- und Leitungsstruktur
- K67 – die kritischen Risiken für das Informationssicherheitsmanagement
- K71 – die typische Leistungskennzahl (KPI, en: Key Performance Indicator)
- K83 – Potential und Möglichkeiten relevanter Standards und bewährter Verfahrensweisen
- K85 – Rendite (en: return on investment) im Vergleich zur Risikovermeidung
- K98 – Einfluss von gesetzlichen Anforderungen auf die Informationssicherheit
- K108 – Computerkriminaltechnik
- K115 – Sicherheitsmanagementpolitik der Organisation und ihre Auswirkung auf die Zusammenarbeit mit Kunden, Lieferanten und Subunternehmern
- K122 – Informationsstrategie der Organisation
- K130 – bewährte Verfahrensweisen (Methoden) und Standards für die Risikoanalyse
- K132 – bewährte Verfahrensweisen und Standards des Informationssicherheitsmanagements
- K139 – Methoden zur Analyse von Kompetenz- und Fertigungsanforderungen
- K149 – gesetzliche Vorgaben, die für IKT-Verträge gelten
- K152 – aufkommende Technologien (z. B. verteilte Systeme, Virtualisierungsmodelle, Datensätze, mobile Systeme)
- K158 – mögliche Sicherheitsbedrohungen

- K161 – Herausforderungen im Zusammenhang mit der Größe der Datensätze (z. B. Big Data)
- K162 – Herausforderungen im Zusammenhang mit unstrukturierten Daten (z. B. Datenanalyse)
- K180 – Cyber-Angriffstechniken und Gegenmaßnahmen zur Vermeidung von Angriffen

Anwendungsbereich der KPI

- Anwendung der EU-Verordnung 2016/679

5.3 Berufsprofil des Datenschutzmanagers

Kurzbeschreibung

Ist verantwortlich² für die Verarbeitung personenbezogener Daten und koordiniert diese.

Mission

Koordiniert alle an der Verarbeitung personenbezogener Daten beteiligten Personen, um die Einhaltung der geltenden Gesetze sowie die Erreichung und Aufrechterhaltung eines angemessenen Schutzniveaus auf der Grundlage der spezifischen Verarbeitung personenbezogener Daten sicherzustellen.

Ergebnisse³

Rechenschaftspflichtig

- Betriebsverfahren für die Verarbeitung und den Schutz personenbezogener Daten.
- Berichte über den Gesamtstatus des Schutzes personenbezogener Daten (d. h. Überprüfung).
- Indikatoren für den Schutz personenbezogener Daten.

Verantwortlich

- Budget für den Schutz personenbezogener Daten.
- Zuweisung von Verantwortlichkeiten bei der Verarbeitung und dem Schutz personenbezogener Daten.
- Datenschutz-Folgenabschätzung.
- Richtlinien für den Schutz personenbezogener Daten.
- Anforderungen an die Verarbeitung und den Schutz personenbezogener Daten.
- Technische und organisatorische Maßnahmen zur Sicherstellung des Datenschutzes durch Voreinstellungen.
- Vorbeugende Konsultationen.
- Meldung von Vorfällen, die zu einer Verletzung personenbezogener Daten führen (an die betroffenen Personen).

² Die Definition unterscheidet sich von der Definition des „Auftragsverarbeiters“, die in der Datenschutz-Grundverordnung (EU 2016/679) verwendet wird.

³ Es ist zu beachten, dass alle hier beschriebenen Berufsprofile nicht mit rechtlichen, sondern nur mit operativen Verantwortlichkeiten verbunden sind.

- Hinweise zum Datenschutz.
- Antworten an die betroffene Person bei der Ausübung ihrer Rechte.
- Verzeichnisse von Verarbeitungstätigkeiten.
- Weiterbildungs-, Aktualisierungsprogramm und Programm zur Bewusstseinsförderung.

Beitragender

- Bewertung des Risikos im Zusammenhang mit der Informationssicherheit⁴
- Risikoverarbeitungsplan in Bezug auf die Informationssicherheit.
- Verhaltensregeln.
- Auditprogramm für den Schutz und die Verarbeitung personenbezogener Daten.

Hauptaufgaben

- Unterstützung des für die Verarbeitung Verantwortlichen bei der Weiterverfolgung der Anträge auf Ausübung der Rechte der betroffenen Personen.
- Unterstützung des für die Verarbeitung Verantwortlichen bei der Löschung oder Rückgabe der personenbezogenen Daten nach Abschluss der Verarbeitung.
- Den für die Verarbeitung Verantwortlichen über den Stand der Verarbeitung und des Schutzes personenbezogener Daten auf dem Laufenden zu halten.
- Management des Budgets für den Schutz von personenbezogenen Daten.
- Kontinuierliche Überwachung des Gesamtniveaus des Schutzes personenbezogener Daten.
- Organisation und Zuweisung von Verantwortlichkeiten im Zusammenhang mit der Verarbeitung und dem Schutz personenbezogener Daten.
- Genehmigung der Richtlinien und Verfahren für die Verarbeitung und den Schutz von personenbezogenen Daten.
- Unterstützung des für die Verarbeitung Verantwortlichen beim Genehmigungsverfahren für die Maßnahmen, die für das Risikomanagement im Zusammenhang mit dem Schutz personenbezogener Daten zu ergreifen sind.
- Teilnahme an Risikobeurteilungen im Bereich der Informationssicherheit.
- Sicherstellung der Einhaltung der Anforderungen an die Verarbeitung und den Schutz personenbezogener Daten auch bei Projektstätigkeiten.
- Gegebenenfalls Mitteilung von Verletzungen personenbezogener Daten an die betroffenen Personen.
- Management von Aufzeichnungen über Verarbeitungstätigkeiten.
- Definition und Bewertung von SLAs und PLAs, die von Dritten, die an der Verarbeitung personenbezogener Daten beteiligt sind, garantiert werden müssen.

⁴ Solche Bewertungen sollen von Fachkräften für Informationssicherheit durchgeführt werden.

- Integration von Tätigkeiten für die Übereinstimmung mit der Verarbeitung personenbezogener Daten nach Möglichkeit mit Tätigkeiten im Zusammenhang mit anderen Arten der Übereinstimmung.
- Management von datenschutzrelevanten Verträgen (insbesondere Vereinbarungen mit dem für die Verarbeitung Verantwortlichen und Verarbeitungsverträge).

Die folgende Tabelle 2 zeigt die zugewiesenen Kompetenzen und die erforderlichen Niveaus nach dem in EN 16234-1 vorgesehenen e-CF.

Tabelle 2 — Zugewiesene Kompetenzen und erforderliche Niveaus nach dem in EN 16234-1 vorgesehenen e-CF

<i>e-CF-Kompetenz</i>	<i>Niveau</i>
A.4. Produkt- oder Serviceplanung	3
A.5. Architekturspezifikation	4
D.8. Vertragsmanagement	3
E.3. Risikomanagement	4
E.8. Informationssicherheitsmanagement	3

Fertigkeiten

- Mitwirkung an der Strategie für die Verarbeitung und den Schutz personenbezogener Daten
- Management der angewandten Verhaltensregeln und der geltenden Zertifizierungen für die Verarbeitung und den Schutz von personenbezogenen Daten
- Identifizierung von Rollen, Verantwortlichkeiten und Rechtsgrundlagen für die Verarbeitung personenbezogener Daten
- Beitrag zur Bereitstellung korrekter Informationen für die betroffenen Personen
- Kommunikationsfähigkeit
- Analytische Fertigkeiten
- Selbstmanagement und Stressbewältigung
- Fähigkeit zur Selbstentfaltung
- Kontrollfähigkeit
- Überzeugungsfähigkeit
- Kapazitäten für die Koordinierung und das Management von Mitarbeitern
- Fertigkeiten zur Entscheidungsfindung
- Flexibilität
- Fähigkeit zur Konfliktbewältigung
- Fähigkeit der Konzernleitung
- Initiative
- Berechtigung zur Verhandlung

- Organisatorische Fertigkeiten
- Ergebnisorientierung
- Perspektivisches Denken
- Planung und Terminierung
- Konstruktive Einstellung bei der Lösung von Problemen
- Hartnäckigkeit
- S1 – Thematisieren des CPD-Bedarfs des Personals, um die Anforderungen der Organisation zu erfüllen
- S5 – Analysieren der unternehmenskritischen Vermögenswerte und Identifizieren von Schwachstellen und Anfälligkeiten für Eindringversuche oder Angriffe
- S6 – Analysieren zukünftiger Entwicklungen in Geschäftsprozessen und technischen Anwendungen
- S14 – Analysieren der Durchführbarkeit in Bezug auf Kosten und Nutzen
- S21 – Anwenden von Minderungs- und Notfallmaßnahmen
- S23 – Anwenden von relevanten Standards, bewährten Verfahrensweisen und gesetzlichen Anforderungen für die Informationssicherheit
- S40 – Betreuen (Coachen)
- S42 – Zusammentragen, Formalisieren und Validieren funktioneller und nicht-funktioneller Anforderungen
- S46 – Verstehen des Einflusses neuer Technologien auf das Geschäft (z. B. Open Data oder Big Data, Virtualisierungsmöglichkeiten und -strategien)
- S45 – Verfassen, Dokumentieren und Katalogisieren von wesentlichen Prozessen und Verfahren
- S47 – Verstehen der Geschäftsziele/wirtschaftlichen Triebfaktoren, die die Architekturkomponente beeinflussen (Daten, Anwendung, Sicherheit, Entwicklung usw.)
- S48 – Verstehen der gesetzlichen und regulatorischen Vorgaben, um sie in Geschäftsanforderungen einzubeziehen
- S49 – Verstehen der Unternehmensarchitektur
- S51 – eindeutige Kommunikation mit Endanwendern und Bereitstellen von Anleitungen, wie mit Problemen umzugehen ist
- S52 – Kommunizieren und Bewerten der Risikoanalysenergebnisse und entsprechenden Risikomanagementprozesse der Organisation
- S53 – Kommunizieren des Werts, der Risiken und Möglichkeiten, die sich aus der IS-Strategie ableiten
- S55 – Kommunizieren guter und schlechter Nachrichten zur Vermeidung von Überraschungen
- S60 – Beitragen zur Entwicklung der Geschäfts- und Datenstrategie
- S61 – Beitragen zur Entwicklung der IKT-Strategie und -Richtlinien, einschließlich IKT-Sicherheit und -Qualität
- S66 – Erstellen eines Risikomanagementplans zur Ausarbeitung des Vorbeugemaßnahmenplänen

- S71 – Festlegen und Einführen von geeigneten KPI
- S91 – Sicherstellen, dass die Rechte des geistigen Eigentums und der Datenschutz eingehalten werden
- S140 – Aushandeln von Vertragsklauseln und -bedingungen
- S153 – Erstellen von Vorlagen für gemeinsame Veröffentlichungen
- S156 – Gestalten und Dokumentieren der Prozesse zur Risikoanalyse und zum Risikomanagement
- S165 – Vorschlagen wirksamer Notfallmaßnahmen
- S167 – Zusammentragen von internen und externen Wissens- und Informationsanfragen
- S171 – Bereitstellen von Informationen
- S176 – Überwachen und Umsetzen der wirksamen Anwendung von Unternehmensstandards für Veröffentlichungen
- S178 – Auswählen geeigneter IKT-Lösungen auf Grundlage von Nutzen, Risiken und Gesamteinfluss
- S181 – Erstellen des Wiederherstellungsplans
- S182 – Einrichten der systematischen und regelmäßigen Kommunikation zwischen Kunden, Nutzern und Akteuren
- S186 – Entwicklung von Designmustern und -modellen, um Systemanalytiker bei der Gestaltung konsistenter Anwendungen zu unterstützen
- S187 – Entwickeln eines Risikomanagementplans zum Identifizieren der erforderlichen Vorbeugemaßnahmen
- S198 – Bewerten der Eignung von verschiedenen Anwendungsentwicklungsverfahren für das aktuelle Szenario

Wissen

- Die Grundsätze des Datenschutzes einschließlich des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- Die in den geltenden Gesetzen und Verordnungen verankerten Rechte der interessierten Parteien
- Computernetzwerke
- Telekommunikationsnetze
- Verantwortlichkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten
- Lokale und europäische Gesetze über die Verarbeitung und den Schutz personenbezogener Daten
- Rechtliche Entwicklungen im Zusammenhang mit lokalen und europäischen Gerichtsentscheidungen.
- Rechtliche Bestimmungen über die Verarbeitung und den Schutz personenbezogener Daten im Bereich der elektronischen Kommunikation
- Gesetzgebung über die Übermittlung personenbezogener Daten ins Ausland und die Weitergabe personenbezogener Daten außerhalb der EU/des EWR
- Methoden der Datenschutz-Folgenabschätzung und DSFA

- Mögliche Bedrohungen für den Schutz personenbezogener Daten
- Werkzeuge und Verfahren zur Planung, Terminierung und Unternehmenssteuerung
- Kommunikationstechniken und -instrumente (Beziehungen zu Institutionen, Behörden, Strafverfolgungsbehörden, lokalen Behörden und der Presse)
- Überwachungs- und Berichterstattungssysteme und -techniken
- Die Verhaltensregeln und Zertifizierungen, die für die Verarbeitung und den Schutz personenbezogener Daten gelten
- K10 – DBMS, Datenlager , DSS usw.
- K11 – Architektur-Rahmenwerke
- K12 – Architektur-Rahmenwerke, Methodologien und Werkzeuge für Systemdesign
- K23 – IKT-Sicherheitsstandards
- K26 – Werkzeuge für die Erstellung, Aufbereitung und Verteilung von professionellen Dokumenten
- K27 – IKT-Geräte und -Werkzeuge für die Speicherung und den Abruf von Daten
- K28 – Werkzeuge für die Erstellung von Multimedia-Präsentationen
- K35 – Kosten, Nutzen und Risiken einer Systemarchitektur
- K36 – verschiedene technische Dokumente, die für den Entwurf, die Entwicklung und die Verbreitung von Produkten, Anwendungen und Services erforderlich sind
- K38 – die verschiedenen Servicemodelle (SaaS, PaaS, IaaS), Serviceniveaus und vertraglichen Umsetzungen (z. B. Cloud Computing)
- K49 – Kompetenzentwicklungsmethoden
- K51 – Software-Entwicklungsmethoden und ihre Begründung (z. B. Prototypenentwicklung, agile Methoden, Nachkonstruktion usw.)
- K56 – Designprinzipien für Benutzeroberflächen
- K60 – Organisationsprozesse einschließlich Entscheidungsfindung, Budget- und Leitungsstruktur
- K67 – die kritischen Risiken für das Informationssicherheitsmanagement
- K71 – typische Leistungskennzahl (KPI, en: Key Performance Indicator)
- K83 – Potential und Möglichkeiten relevanter Standards und bewährter Verfahrensweisen
- K85 – Rendite im Vergleich zur Risikovermeidung
- K97 – die Auswirkungen von geschäftlichen Veränderungen auf rechtliche Fragen
- K98 – Einfluss von gesetzlichen Anforderungen auf die Informationssicherheit
- K102 – IKT-Infrastruktur und Geschäftsorganisation
- K108 – Computerkriminaltechnik

- K115 – Sicherheitsmanagementpolitik der Organisation und ihre Auswirkung auf die Zusammenarbeit mit Kunden, Lieferanten und Subunternehmern
- K122 – Informationsstrategie der Organisation
- K127 – bestehende Anwendungen und zugehörige Architektur
- K128 – relevante IKT-Nutzeranwendungen
- K130 – bewährte Verfahrensweisen (Methoden) und Standards für die Risikoanalyse
- K132 – bewährte Verfahrensweisen und Standards des Informationssicherheitsmanagements
- K139 – Methoden zur Analyse von Kompetenz- und Fertigungsanforderungen
- K149 – gesetzliche Vorgaben, die für IKT-Verträge gelten
- K152 – aufkommende Technologien (z. B. verteilte Systeme, Virtualisierungsmodelle, Datensätze, mobile Systeme)
- K158 – mögliche Sicherheitsbedrohungen
- K161 – Herausforderungen im Zusammenhang mit der Größe der Datensätze (z. B. Big Data)
- K162 – Herausforderungen im Zusammenhang mit unstrukturierten Daten (z. B. Datenanalyse)
- K172 – digitale Strategien
- K180 – Cyber-Angriffstechniken und Gegenmaßnahmen zur Vermeidung von Angriffen
- K186 – Sicherheitserkennungstechniken, einschließlich mobiler und digitaler Techniken
- K200 – Internet-, Cloud- und Mobiltechnologien sowie Anforderungen an die Umgebung
- K201 – Trends und Auswirkungen von internen oder externen IKT-Entwicklungen für typische Organisationen
- K209 – Systemarchitekturanforderungen: Leistung, Wartbarkeit, Erweiterbarkeit, Skalierbarkeit, Verfügbarkeit, Sicherheit und Zugänglichkeit

Anwendungsbereich der KPI

- Richtlinien und Verfahren für die Verarbeitung und den Schutz von personenbezogenen Daten

5.4 Berufsprofil des Datenschutzspezialisten

Kurzbeschreibung

Sorgt für die korrekte Implementierung zur Verarbeitung personenbezogener Daten. Ist der Betriebsexperte für den Schutz personenbezogener Daten.

Mission

Führt betriebliche Tätigkeiten aus, die im Laufe des Lebenszyklus der Verarbeitung personenbezogener Daten nach und nach erforderlich werden, indem er mit einer Führungskraft (wie z. B. dem zuständigen Datenschutzmanager) zusammenarbeitet.

Ergebnisse

Rechenschaftspflichtig

- Technische Gutachten zum Schutz und zur Verarbeitung personenbezogener Daten.
- Gutachten für den Schutz und die Verarbeitung personenbezogener Daten.

Verantwortlich

- Hinweis zum Datenschutz.
- Antworten, die sich aus der Ausübung von Zugangsrechten ergeben.
- Betriebsverfahren für die Verarbeitung und den Schutz personenbezogener Daten.

Beitragender

- Meldung von Vorfällen, die zu einer Verletzung personenbezogener Daten führen.
- Datenschutz-Folgenabschätzung.
- Indikatoren für den Schutz personenbezogener Daten.
- Bewertung des Risikos im Zusammenhang mit der Informationssicherheit.
- Risikomanagementplan für die Informationssicherheit.
- Vorbeugende Absprachen.
- Anforderungen an die Verarbeitung und den Schutz personenbezogener Daten.
- Technische und organisatorische Maßnahmen zur Sicherstellung des Datenschutzes durch Voreinstellungen.
- Weiterbildungsprogramm, berufliche Entwicklung und Bewusstseinsförderung.

Hauptaufgaben

- Entwicklung von Folgenabschätzungen für den Schutz personenbezogener Daten.
- Bereitstellung von fachlicher Unterstützung zu bestimmten Themen.
- Vorschlag für Maßnahmen zur Bewältigung der relativen Risiken bei der Verarbeitung und dem Schutz personenbezogener Daten.
- Ausarbeitung und Aktualisierung von Richtlinien und Verfahren für die Verarbeitung und den Schutz personenbezogener Daten.
- Implementierung von Verfahren zum Schutz personenbezogener Daten.
- Implementierung technischer Lösungen für den Schutz personenbezogener Daten.
- Dokumentation der Prozesse im Zusammenhang mit der Verarbeitung und dem Schutz personenbezogener Daten, um den Nachweis für die Einhaltung der Vorschriften bei der durchgeführten Verarbeitung zu erbringen.
- Dokumentation des Managements von technischen Lösungen für die Verarbeitung und den Schutz personenbezogener Daten.

- Dokumentation der Verletzung personenbezogener Daten.

Die folgende Tabelle 3 zeigt die zugewiesenen Kompetenzen und die erforderlichen Niveaus nach dem in EN 16234-1 vorgesehenen e-CF.

Tabelle 3 — Zugewiesene Kompetenzen und erforderliche Niveaus nach dem in EN 16234-1 vorgesehenen e-CF

<i>e-CF-Kompetenz</i>	<i>Niveau</i>
A.5. Architekturspezifikation	3
C.1. Anwenderbetreuung	2
C.2. Veränderungsunterstützung	3
E.3. Risikomanagement	2
E.8. Informationssicherheitsmanagement	2

Fertigkeiten

- Anwendung der Grundsätze des Datenschutzes einschließlich des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen auf Informationssysteme
- Anwendung der Grundsätze des Datenschutzes, einschließlich des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, auf die Verarbeitung personenbezogener Daten
- Abwicklung von Anfragen betroffener Personen, die ihre Rechte ausüben
- Entwicklung von Transferverfahren, die angemessenen Sicherheitsvorkehrungen und/oder verbindlichen Unternehmensregeln gegenüber Drittländern oder internationalen Organisationen unterliegen
- Fähigkeit zur Gruppenarbeit
- Analytische Fertigkeiten
- Flexibilität
- Organisatorische Fertigkeiten
- Planung und Terminierung
- Neigung zur Prüfung neuer Entwicklungen
- S1 – Thematisieren des CPD-Bedarfs des Personals, um die Anforderungen der Organisation zu erfüllen
- S5 – Analysieren der unternehmenskritischen Vermögenswerte und Identifizieren von Schwachstellen und Anfälligkeiten für Eindringversuche oder Angriffe
- S13 – Analysieren des Einflusses von funktionalen/technischen Änderungen auf Anwender
- S19 – Vorkalkulieren der erforderlichen Änderungen der Informationssicherheitsstrategie der Organisation und Formulierung neuer Pläne
- S20 – Antizipieren aller erforderlichen Maßnahmen, die zum Abschwächen der Auswirkungen von Änderungen erforderlich sind (Weiterbildung, Dokumentation, neue Prozesse usw.)

- S21 – Anwenden von Minderungs- und Notfallmaßnahmen
- S28 – Anwenden von Data-Mining-Verfahren
- S37 – Verstehen, wie Webtechnologien zu Marketingzwecken eingesetzt werden können
- S40 – Betreuen (Coachen)
- S42 – Zusammentragen, Formalisieren und Validieren funktioneller und nicht-funktioneller Anforderungen
- S45 – Verfassen, Dokumentieren und Katalogisieren von wesentlichen Prozessen und Verfahren
- S47 – Verstehen der Geschäftsziele/wirtschaftlichen Triebfaktoren, die die Architekturkomponente beeinflussen (Daten, Anwendung, Sicherheit, Entwicklung usw.)
- S51 – eindeutige Kommunikation mit Endanwendern und Bereitstellen von Anleitungen, wie mit Problemen umzugehen ist
- S57 – gemeinsame Nutzung funktionaler und technischer Spezifikationen mit den für die Pflege und die Weiterentwicklung von IKT-Lösungen verantwortlichen IKT-Teams
- S89 – Sicherstellen, dass Kontrollen und Funktionalitäten in die Gestaltung integriert werden
- S91 – Sicherstellen, dass die Rechte des geistigen Eigentums und der Datenschutz eingehalten werden
- S153 – Erstellen von Vorlagen für gemeinsame Veröffentlichungen
- S167 – Zusammentragen von internen und externen Wissens- und Informationsanfragen
- S168 – Erfassung, Speicherung und Analyse komplexer, großer, unstrukturierter und in unterschiedlichen Formaten vorliegender Datensätze
- S171 – Bereitstellen von Informationen
- S176 – Überwachen und Umsetzen der wirksamen Anwendung von Unternehmensstandards für Veröffentlichungen
- S182 – Einrichten der systematischen und regelmäßigen Kommunikation zwischen Kunden, Nutzern und Akteuren
- S186 – Entwickeln von Designmustern und -modellen, um Systemanalytiker bei der Gestaltung konsistenter Anwendungen zu unterstützen
- S191 – Nutzen und Interpretieren von Webanalysen
- S198 – Bewerten der Eignung von verschiedenen Anwendungsentwicklungsverfahren für das aktuelle Szenario

Wissen

- Die Grundsätze des Datenschutzes einschließlich des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- Die in den geltenden Gesetzen und Verordnungen verankerten Rechte der interessierten Parteien
- Computernetzwerke
- Telekommunikationsnetze

- Verantwortlichkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten
- Lokale und europäische Gesetze über die Verarbeitung und den Schutz personenbezogener Daten unter besonderer Berücksichtigung der Bestimmungen des primären und sekundären Ranges (Verordnungen, Bestimmungen, Genehmigungen, Richtlinien und sektorale Normen, andere), die sich auf bestimmte Tätigkeitsbereiche beziehen
- Rechtliche Bestimmungen über die Verarbeitung und den Schutz personenbezogener Daten im Bereich der elektronischen Kommunikation
- Gesetzliche Bestimmungen über die Verarbeitung und den Schutz personenbezogener Daten zum Zwecke der Videoüberwachung
- Rechtliche Bestimmungen über die Verarbeitung und den Schutz personenbezogener Daten zum Zwecke des Marketings und der Profilerstellung
- Rechtliche Bestimmungen über die Verarbeitung und den Schutz personenbezogener Daten zum Zwecke der Kontrolle der Arbeitnehmer
- Gesetzgebung über die Übermittlung personenbezogener Daten ins Ausland und die Weitergabe personenbezogener Daten außerhalb der EU/des EWR
- Regeln und Vorschriften für die Handhabung biometrischer Daten
- Videoüberwachungssysteme
- Methoden der Datenschutz-Folgenabschätzung und DSFA
- Mögliche Bedrohungen für den Schutz personenbezogener Daten, insbesondere im Hinblick auf den jeweiligen Tätigkeitsbereich
- Kryptographische Techniken
- Die Techniken der Anonymisierung und De-Anonymisierung
- Pseudonymisierungstechniken
- IoT-Technologien (Internet der Dinge) (en: Internet of Things, IoT)
- RFID-Technologien
- Technologien zur Geolokalisierung
- Technologien zur Identifizierung
- Technologien zur biometrischen Identifizierung
- Verfolgungstechnologien für Vorgänge
- Die Verhaltensregeln und Zertifizierungen, die für die Verarbeitung und den Schutz personenbezogener Daten gelten
- K10 – DBMS, Datenlager, DSS usw.
- K12 – Architektur-Rahmenwerke, Methodologien und Systemdesign-Werkzeuge
- K26 – Werkzeuge für die Erstellung, Aufbereitung und Verteilung von professionellen Dokumenten
- K27 – IKT-Geräte und -Werkzeuge für die Speicherung und den Abruf von Daten

- K28 – Werkzeuge für die Erstellung von Multimedia-Präsentationen
- K35 – Kosten, Nutzen und Risiken einer Systemarchitektur
- K36 – verschiedene technische Dokumente, die für den Entwurf, die Entwicklung und die Verbreitung von Produkten, Anwendungen und Services erforderlich sind
- K49 – Kompetenzentwicklungsmethoden
- K50 – Verfahren zur Analyse von Informationen und Geschäftsprozessen
- K51 – Software-Entwicklungsmethoden und ihre Begründung (z. B. Prototypenentwicklung, agile Methoden, Nachkonstruktion usw.)
- K56 – Designprinzipien für Benutzeroberflächen
- K81 – mobiles Marketing (z. B. Bezahlen per Klick (PPC, en: Pay Per Click))
- K87 – Marketing für soziale Medien
- K93 – die vorhandene technische Architektur der IKT-Anwendung
- K94 – E-Mail-Marketing
- K108 – Computerkriminaltechnik
- K127 – bestehende Anwendungen und zugehörige Architekturen
- K132 – bewährte Verfahrensweisen und Standards des Informationssicherheitsmanagements
- K152 – aufkommende Technologien (z. B. verteilte Systeme, Virtualisierungsmodelle, Datensätze, mobile Systeme)
- K161 – Herausforderungen im Zusammenhang mit der Größe der Datensätze (z. B. Big Data)
- K162 – Herausforderungen im Zusammenhang mit unstrukturierten Daten (z. B. Datenanalyse)
- K170 – funktionale Spezifikationen des Informationssystems
- K173 – Organisation von Datenbankstrukturen und -inhalt
- K180 – Cyber-Angriffstechniken und Gegenmaßnahmen zur Vermeidung von Angriffen
- K186 – Sicherheitserkennungstechniken, einschließlich mobiler und digitaler Techniken
- K200 – Internet-, Cloud- und Mobiltechnologien
- K209 – Systemarchitekturanforderungen: Leistung, Wartbarkeit, Erweiterbarkeit, Skalierbarkeit, Verfügbarkeit, Sicherheit und Zugänglichkeit

Anwendungsbereich der KPI

- Verarbeitung und Schutz personenbezogener Daten

5.5 Berufsprofil des Datenschutzingenieurs

Kurzbeschreibung

Ist verantwortlich für die Aspekte des Schutzes personenbezogener Daten bei der Konzeption, Entwicklung und Verbesserung von Systemen, die personenbezogene Daten verarbeiten und von anderen Personen oder Organisationen genutzt werden sollen.

Mission

Konzeption, Entwicklung und ggf. Unterstützung bei der Implementierung, dem Betrieb und der Wartung von Systemen zur Verarbeitung personenbezogener Daten in Übereinstimmung mit den Grundsätzen und Bestimmungen des Datenschutzes durch technische und organisatorische Maßnahmen.

Ergebnisse⁵

Rechenschaftspflichtig

- Datenschutzdokumentation des Systems

Verantwortlich

- Anforderungen an die Verarbeitung und den Schutz personenbezogener Daten.
- Betriebsverfahren für die Verarbeitung und den Schutz personenbezogener Daten.
- Datenschutz-Folgenabschätzung.
- Technische und organisatorische Maßnahmen zur Sicherstellung des Datenschutzes durch datenschutzfreundliche Voreinstellungen und Technikgestaltung.

Beitragender

- Bewertung des Risikos im Zusammenhang mit der Informationssicherheit⁶
- Risikoverarbeitungsplan in Bezug auf die Informationssicherheit.
- Richtlinien für den Schutz personenbezogener Daten.
- Indikatoren für den Schutz personenbezogener Daten.

Hauptaufgaben

- Entwicklung von Datenschutz-Folgenabschätzungen im Zusammenhang mit Systemen zur Verarbeitung personenbezogener Daten.
- Entwicklung, Implementierung und Dokumentation technischer und organisatorischer Maßnahmen zum Management der Risiken, die sich aus den Tätigkeiten der Datenschutz-Folgenabschätzung und der Sicherheitsbeurteilung ergeben.
- Sicherstellung der Einhaltung der Datenschutzgrundsätze in den Systemen.

⁵ Es ist zu beachten, dass alle hier beschriebenen Berufsprofile nicht mit rechtlichen, sondern nur mit operativen Verantwortlichkeiten verbunden sind.

⁶ Solche Bewertungen müssen von Fachkräften für Informationssicherheit durchgeführt werden.

- Entwicklung, Implementierung und Dokumentation technischer und organisatorischer Maßnahmen zum Management der Risiken, die sich aus den Tätigkeiten der Datenschutz-Folgenabschätzung und der Sicherheitsbeurteilung ergeben.
- Implementierung von Prozessen, Verfahren und technischen Lösungen im Zusammenhang mit dem Schutz personenbezogener Daten in Systemen.

Die folgende Tabelle 4 zeigt die zugewiesenen Kompetenzen und die erforderlichen Niveaus nach dem in EN 16234-1 vorgesehenen e-CF.

Tabelle 4 — Zugewiesene Kompetenzen und erforderliche Niveaus nach dem in EN 16234-1 vorgesehenen e-CF

<i>e-CF-Kompetenz</i>	<i>Niveau</i>
A.4. Produkt- oder Serviceplanung	3
A.5. Architekturspezifikation	4
A.6. Anwendungsspezifikation	3
E.3. Risikomanagement	4
E.8. Informationssicherheitsmanagement	3

Fertigkeiten

- Anwendung der Grundsätze des Datenschutzes einschließlich des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen auf Informationssysteme
- Anwendung der Grundsätze des Datenschutzes, einschließlich des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, auf die Verarbeitung personenbezogener Daten
- Organisatorische Fertigkeiten
- Planung und Terminierung
- Neigung zur Prüfung neuer Entwicklungen
- Konstruktive Einstellung bei der Lösung von Problemen
- Hartnäckigkeit
- Ergebnisorientierung
- S2 – Zuweisen geeigneter Ressourcen zu Wartungstätigkeiten unter Kosten- und Risikoabschätzung
- S5 – Analysieren der unternehmenskritischen Vermögenswerte und Identifizieren von Schwachstellen und Anfälligkeiten für Eindringversuche oder Angriffe
- S6 – Analysieren zukünftiger Entwicklungen in Geschäftsprozessen und technischen Anwendungen
- S9 – Analysieren der Kundenanforderungen
- S10 – Analysieren von Symptomen, um verbreitete Arten von Anwenderfehlern oder technischem Versagen zu identifizieren
- S13 – Analysieren des Einflusses von funktionalen/technischen Änderungen auf Anwender

- S22 – Anwenden geeigneter Entwicklungs- und/oder Prozessmodelle für eine wirksame und effiziente Entwicklung
- S31 – Anwenden relevanter Standards und bewährter Verfahrensweisen zur Aufrechterhaltung der Informationsqualität
- S41 – Mitwirken bei der Änderung des Codes von Drittanbietern; Unterstützen und Warten modifizierter Software
- S42 – Zusammentragen, Formalisieren und Validieren funktioneller und nicht-funktioneller Anforderungen
- S45 – Verfassen, Dokumentieren und Katalogisieren von wesentlichen Prozessen und Verfahren
- S47 – Verstehen der Geschäftsziele/wirtschaftlichen Triebfaktoren, die die Architekturkomponente beeinflussen (Daten, Anwendung, Sicherheit, Entwicklung usw.)
- S57 – gemeinsame Nutzung funktionaler und technischer Spezifikationen mit den für die Pflege und die Weiterentwicklung von IKT-Lösungen verantwortlichen IKT-Teams
- S68 – Erstellen und Verwalten eines Testplans
- S85 – Durchführen von Tests und Bewerten von Testergebnissen im Vergleich zu Produktspezifikationen
- S89 – Sicherstellen, dass Kontrollen und Funktionalitäten in die Gestaltung integriert werden
- S91 – Sicherstellen, dass die Rechte des geistigen Eigentums und der Datenschutz eingehalten werden
- S98 – Steuern und Bewerten des Testprozesses
- S100 – Steuern des Lebenszyklus für das Produkt-/Service-Entwicklungsmanagement (einschließlich der Verwaltung von formalen Änderungsanfragen)
- S107 – Identifizieren und Analysieren von langfristigen Anwender-/Kundenbedürfnissen
- S118 – Identifizieren aller möglichen Zielgruppen für das Produkt oder den Service
- S125 – Identifizieren und Thematisieren entscheidender Elemente, die den Wert eines Produkts oder einer Lösung ausmachen
- S129 – Auslegen von Produkt-/Servicespezifikationen
- S157 – Konzipieren und Entwickeln von Hardwarearchitektur, Nutzerschnittstellen, Komponenten von Unternehmenssoftware und eingebetteten Software-Komponenten
- S161 – Entwickeln von Funktionsspezifikationen ausgehend von festgelegten Anforderungen
- S182 – Einrichten der systematischen und regelmäßigen Kommunikation zwischen Kunden, Nutzern und Akteuren
- S186 – Entwickeln von Designmustern und -modellen, um Systemanalytiker bei der Gestaltung konsistenter Anwendungen zu unterstützen
- S198 – Bewerten der Eignung von verschiedenen Anwendungsentwicklungsverfahren für das aktuelle Szenario
- S200 – Verifizieren, dass Fähigkeiten und Effizienz von integrierten Systemen den Spezifikationen entsprechen

- S202 – Erstellung eines Konzeptnachweises (Machbarkeitsnachweises)

Wissen

- Die Grundsätze des Datenschutzes einschließlich des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- Die in den geltenden Gesetzen und Verordnungen verankerten Rechte der interessierten Parteien
- Computernetzwerke
- Telekommunikationsnetze
- Verantwortlichkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten
- Lokale und europäische Gesetze über die Verarbeitung und den Schutz personenbezogener Daten unter besonderer Berücksichtigung der Bestimmungen des primären und sekundären Ranges (Verordnungen, Bestimmungen, Genehmigungen, Richtlinien und sektorale Normen, andere), die sich auf bestimmte Tätigkeitsbereiche beziehen
- Rechtliche Bestimmungen über die Verarbeitung und den Schutz personenbezogener Daten im Bereich der elektronischen Kommunikation
- Gesetzgebung über die Übermittlung personenbezogener Daten ins Ausland und die Weitergabe personenbezogener Daten außerhalb der EU/des EWR
- Regeln und Vorschriften für die Handhabung biometrischer Daten
- Methoden der Datenschutz-Folgenabschätzung und DSFA
- Mögliche Bedrohungen für den Schutz personenbezogener Daten, insbesondere im Hinblick auf den jeweiligen Tätigkeitsbereich
- Überwachungs- und Berichterstattungssysteme und -techniken
- Kryptographische Techniken
- Die Techniken der Anonymisierung und De-Anonymisierung
- Pseudonymisierungstechniken
- IoT-Technologien (Internet der Dinge) (en: Internet of Things, IoT)
- RFID-Technologien
- Technologien zur Geolokalisierung
- Technologien zur Identifizierung
- Technologien zur biometrischen Identifizierung
- Verfolgungstechnologien für Vorgänge
- Die Verhaltensregeln und Zertifizierungen, die für die Verarbeitung und den Schutz personenbezogener Daten gelten
- K10 – DBMS, Datenlager, DSS usw.
- K12 – Architektur-Rahmenwerke, Methodologien und Systemdesign-Werkzeuge

- K26 – Werkzeuge für die Erstellung, Aufbereitung und Verteilung von professionellen Dokumenten
- K27 – IKT-Geräte und -Werkzeuge für die Speicherung und den Abruf von Daten
- K30 – relevante Entwicklungen in der IKT (z. B. Virtualisierung, Open Data usw.) und deren potentielle Auswirkung auf Prozesse
- K32 – alte, bestehende und neue Hardware-Komponenten/Software-Programme/-Module
- K35 – Kosten, Nutzen und Risiken einer Systemarchitektur
- K36 – verschiedene technische Dokumente, die für den Entwurf, die Entwicklung und die Verbreitung von Produkten, Anwendungen und Services erforderlich sind
- K37 – die verschiedenen Servicemodelle (SaaS, PaaS, IaaS) und praktischen Umsetzungen (d. h. Cloud Computing)
- K39 – die verschiedenen Arten von Tests (Funktions-, Integrations-, Leistungs-, Gebrauchstauglichkeits-, Stresstest usw.)
- K51 – Software-Entwicklungsmethoden und ihre Begründung (z. B. Prototypenentwicklung, agile Methoden, Nachkonstruktion usw.)
- K56 – Designprinzipien für Benutzeroberflächen
- K57 – IPR-Prinzipien und -Regeln
- K59 – Anwendungen und Dienste
- K63 – geeignete Software-Programme/-Module
- K69 – Betriebssysteme und Software-Plattformen
- K72 – Entwicklungswerkzeuge (z. B. Entwicklungsumgebung, Management, Quellcode-Zugriffs- bzw. Änderungskontrollen)
- K76 – Lebenszyklus eines Prüfprozesses
- K93 – die vorhandene technische Architektur der IKT-Anwendung
- K103 – Integrierte Entwicklungsumgebung (en: Integrated development environment, IDE)
- K116 – funktionales und technisches Design
- K118 – Prototypenentwicklung
- K127 – bestehende Anwendungen und zugehörige Architekturen
- K132 – bewährte Verfahrensweisen und Standards des Informationssicherheitsmanagements
- K152 – aufkommende Technologien (z. B. verteilte Systeme, Virtualisierungsmodelle, Datensätze, mobile Systeme)
- K160 – Fragen zu den Rechten an geistigem Eigentum (IPR)
- K161 – Herausforderungen im Zusammenhang mit der Größe der Datensätze (z. B. Big Data)
- K162 – Herausforderungen im Zusammenhang mit unstrukturierten Daten (z. B. Datenanalyse)
- K170 – funktionale Spezifikationen des Informationssystems