

DIN EN 17529

ICS 35.030

**Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen;
Deutsche Fassung EN 17529:2022**

Data protection and privacy by design and by default;
German version EN 17529:2022

Protection des données et de la vie privée dès la conception et par défaut;
Version allemande EN 17529:2022

Gesamtumfang 66 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (EN 17529:2022) wurde von WG 5 „Datensicherheit, Datenschutz und Identitätsmanagement“ des Technischen Komitees 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).

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

Deutsche Fassung

Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Data protection and privacy by design and by default

Protection des données et de la vie privée dès la
conception et par défaut

Diese Europäische Norm wurde vom CEN am 20. Dezember 2020 angenommen.

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

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

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



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

Inhalt

	Seite
Europäisches Vorwort	5
Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe und Abkürzungen	7
4 Allgemeines	8
4.1 Grundlagen für den Datenschutz und den Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen	8
4.2 Struktur für die Zerlegung von Produkten und Diensten in anwendbare Kategorien	10
4.2.1 Einleitung	10
4.2.2 Produktperspektiven	10
4.2.3 Dienstelemente	11
4.3 Eigenerklärung und Zielerreichungsgrade	12
5 Datenschutzbewusste Entwicklung von Produkten und Diensten	14
5.1 Führung und Marktkenntnis	14
5.2 Vorbereitung	14
5.3 Gestaltung	15
5.3.1 Bestimmung der Anforderungen für DSTV	15
5.3.2 Entwicklung	16
5.3.3 Produktion und Dienstleistung	16
5.3.4 Freigabe von Produkten und Diensten	16
5.4 Leistungsbewertung	17
5.5 Verbesserung	17
6 Anforderungen an die Datenschutzzfähigkeit bei der Gestaltung von Produkten und Diensten	17
6.1 Zugang	17
6.1.1 Zugang zu Daten	17
6.1.2 Kopie der Daten	18
6.2 Verantwortlichkeit	18
6.3 Genauigkeit	19
6.4 Entpersonalisierung von Daten	20
6.5 Datenminimierung	21
6.6 Datenübertragbarkeit	22
6.7 Vertraulichkeit	23
6.8 Löschung	25
6.9 Einwilligung und Kinder	26
6.9.1 Bestimmung des Benutzeralters	26
6.9.2 Konfigurierbare Altersgrenze für Kinder	27
6.10 Informationssicherheit	27
6.10.1 Unbefugte oder unrechtmäßige Verarbeitung	27
6.10.2 Datenverlust	30
6.10.3 Ziele des Informationsschutzes	31
6.10.4 Wiederherstellung	32
6.11 Rechtmäßigkeit	32
6.11.1 Datenoffenlegung	32

6.11.2	Einwilligung.....	33
6.12	Widerspruch gegen die Verarbeitung.....	33
6.13	Automatisierte Entscheidungsfindung.....	34
6.14	Einschränkung der Verarbeitung.....	34
6.15	Speicherbegrenzung.....	35
6.16	Transparenz.....	37
6.16.1	Informationen.....	37
6.16.2	Verzeichnis von Verarbeitungstätigkeiten.....	39
7	Anforderungen an die Eigenerklärung datenschutzbewusster Gestaltung.....	40
7.1	Prozessanforderungen.....	40
7.1.1	Vorbereitung basierend auf den Anforderungen der Produktperspektive und des Dienstelements.....	40
7.1.2	Zusätzliche Überlegungen im Zusammenhang mit DSFA.....	40
7.1.3	Bestimmung des Zielerreichungsgrads.....	41
7.2	Aussage zur Eigenerklärung.....	42
Anhang A (informativ) Zuordnung der Anwendbarkeit zwischen den Anforderungen und Perspektiven oder Elementen von Abschnitt 6.....		43
A.1	Allgemeines.....	43
Anhang B (informativ) Ansatz für a Spezifikation.....		55
B.1	Allgemeines.....	55
B.2	Datenschutz.....	55
B.3	Privatsphäre.....	55
B.4	Datenschutz und Privatsphäre durch Technikgestaltung.....	56
B.5	Datenschutz und Privatsphäre durch datenschutzfreundliche Voreinstellungen.....	56
Anhang C (informativ) Leitfaden in Bezug auf EN ISO 9001.....		57
C.1	Allgemeines.....	57
C.2	Kontext der Organisation.....	57
C.2.1	Verstehen der Organisation und ihres Kontextes.....	57
C.2.2	Verstehen der Erfordernisse und Erwartungen der interessierten Parteien.....	57
C.2.3	Festlegen des Anwendungsbereichs des Qualitätsmanagementsystems.....	57
C.2.4	Qualitätsmanagementsystem und seine Prozesse.....	57
C.3	Führung.....	57
C.3.1	Führung und Verpflichtung.....	57
C.3.2	Politik.....	57
C.3.3	Organisatorische Rollen, Verantwortlichkeiten und Befugnisse.....	58
C.4	Planung.....	58
C.4.1	Maßnahmen zum Umgang mit Risiken und Chancen.....	58
C.4.2	Qualitätsziele und Planung zu deren Erreichung.....	58
C.4.3	Planung von Änderungen.....	58
C.5	Unterstützung.....	58
C.5.1	Ressourcen.....	58
C.5.2	Kompetenz.....	58
C.5.3	Bewusstsein.....	58
C.5.4	Kommunikation.....	58
C.5.5	Dokumentierte Informationen.....	58
C.6	Betrieb.....	59
C.6.1	Betriebliche Planung und Steuerung.....	59
C.6.2	Anforderungen an Produkte und Dienste.....	59
C.6.3	Gestaltung und Entwicklung von Produkten und Diensten.....	59
C.6.4	Steuerung von extern bereitgestellten Prozessen, Produkten und Diensten.....	59
C.6.5	Produktion und Dienstleistung.....	59
C.6.6	Freigabe von Produkten und Diensten.....	60
C.6.7	Steuerung fehlerhafter Ausgaben.....	60

C.7 Leistungsbewertung 60

C.7.1 Überwachung, Messung, Analyse und Bewertung..... 60

C.7.2 Internes Audit 60

C.7.3 Managementbewertung 60

C.8 Verbesserung 61

C.8.1 Allgemeines 61

C.8.2 Nichtkonformität und Korrekturmaßnahmen 61

C.8.3 Fortlaufende Verbesserung 61

Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den
Anforderungen der abzudeckenden Verordnung EU 2016/679 an den Datenschutz durch
Technikgestaltung und datenschutzfreundliche Voreinstellungen 62

Literaturhinweise..... 64

Europäisches Vorwort

Dieses Dokument (EN 17529:2022) wurde von WG 5 „Datensicherheit, Datenschutz und Identitätsmanagement“ des Technischen Komitees CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis November 2022, und etwaige entgegenstehende nationale Normen müssen bis November 2022 zurückgezogen werden.

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

Dieses Dokument wurde im Rahmen des Arbeitsprogramms von CEN/CLC/JTC 13 erarbeitet, und zwar nicht nur als erstes Ergebnis des Normungsauftrags M/530, der von der Europäischen Kommission an CEN und CENELEC erteilt wurde, sondern auch mit dem Ziel, generisch genug zu sein, damit es auf eine Vielzahl anderer Bereiche außer der Sicherheitsindustrie, die im Fokus des Normungsauftrags stand, anwendbar ist.

Zum Zusammenhang mit EU-Verordnungen siehe informativen Anhang ZA, der Bestandteil dieses Dokuments ist.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

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

Einleitung

0.1 Allgemeines

Dieses Dokument stellt den Entwicklern von Komponenten und Teilsystemen einen frühzeitig formalisierten Prozess zur Identifizierung von Datenschutzzielsetzungen und -anforderungen sowie die notwendige Anleitung für die damit verbundene Abschätzung bereit. Darüber hinaus bietet es Unterstützung für das Verständnis der kaskadierten Haftung und Verpflichtung von Herstellern und Dienstbringern (Verweisung auf DSGVO, insbesondere auf Artikel 25 sowie auf die für staatliche Anwendungen geltenden Regeln).

Die Datenschutz-Grundverordnung beauftragt in Art. 25 die für die Datenverarbeitung Verantwortlichen und implizit die Hersteller mit der Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.

Ziel dieses Dokuments ist es, den Herstellern und/oder Dienstbringern Anforderungen an die Hand zu geben, damit sie Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (DSTV) frühzeitig in der Entwicklung ihrer Produkte und Dienste umsetzen, d. h. vor (oder unabhängig von) einer bestimmten Anwendungsintegration, um sicherzustellen, dass sie im Hinblick auf die zu erwartenden Märkte möglichst datenschutzfähig sind.

Das Qualitätsmanagementsystem nach EN ISO 9001 bietet einen Prozessrahmen, durch den Produkte und Dienstleistungen den Datenschutz und den Schutz der Privatsphäre durch Technikgestaltung berücksichtigen können. Anhang C zeigt, wie EN ISO 9001 für die Anwendung in diesem Bereich interpretiert und gegebenenfalls erweitert werden kann. Aus der Datenschutz-Grundverordnung wurden Maßnahmenziele und Anforderungen abgeleitet, die der Komponentenhersteller bzw. der Anbieter von Software-Teilsystemen oder Subdiensten möglicherweise ansprechen möchte. Diese Abschnitte sind auf den B2B-Markt anwendbar, da Hersteller, die diese Teilkomponenten in größeren Systemen zusammensetzen, die Grenzen und Fähigkeiten jeder Komponente als Teil ihres Systemdesigns verstehen müssen. Schließlich wird ein Mechanismus zur Eigenerklärung festgelegt, der von Komponentenherstellern und Dienstbringern im Rahmen ihrer Attestierung von Fähigkeiten, Schutzmaßnahmen und Einschränkungen dieser Komponente oder dieses Dienstes gegenüber Systemintegratoren verwendet werden kann.

Für einige Zwecke der Verarbeitung und für einige Kategorien personenbezogener Daten muss eine Datenschutz-Folgenabschätzung (DSFA) nach EN ISO/IEC 29134 durchgeführt werden, und zusätzlich zu den in diesem Dokument aufgeführten Anforderungen muss auch der aus der DSFA resultierende Behandlungsplan erfüllt werden.

Dieses Dokument ist für die Verwendung durch Hersteller, Lieferanten, Hard- und Softwareentwickler bestimmt, die Produkte und Dienste für Systemintegratoren bereitstellen, die ihrerseits beabsichtigen, Produkte und Dienste für die Verwendung durch für die Datenverarbeitung Verantwortliche und Auftragsverarbeiter anzubieten. Es ermöglicht Systemintegratoren, die Angebote von Teilsystem- und Komponentenlieferanten und -herstellern auszuwählen und richtig zu nutzen, wenn sie Systeme entwickeln, die möglicherweise Datenschutzanforderungen haben.

0.2 Kompatibilität mit Managementsystemnormen

Dieses Dokument wendet das von CEN/CENELEC und ISO entwickelte Rahmenwerk an, um die Angleichung zwischen ihren Managementsystemnormen zu verbessern. Dieses Dokument selbst stellt jedoch keine Managementsystemnorm dar.

Dieses Dokument unterstützt eine Organisation dabei, ihre Entwicklungsüberlegungen zum Datenschutz an die Anforderungen von Managementsystemnormen anzugleichen oder sie entsprechend zu integrieren.

1 Anwendungsbereich

Dieses Dokument legt Anforderungen an Hersteller und/oder Dienstleister fest, Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (DSTV) frühzeitig in der Entwicklung ihrer Produkte und Dienste umzusetzen, d. h. vor (oder unabhängig von) einer bestimmten Anwendungsintegration, um sicherzustellen, dass sie so datenschutzfähig wie möglich sind. Dieses Dokument ist anwendbar für alle Wirtschaftszweige, einschließlich der Sicherheitsindustrie.

2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

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

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

3.1.1

Datenschutz durch Technikgestaltung

technische und organisatorische Maßnahmen zur Umsetzung der Datenschutzgrundsätze

Anmerkung 1 zum Begriff: Die Maßnahmen müssen in wirksamer Weise implementiert und die erforderlichen Schutzvorkehrungen in der Verarbeitung getroffen werden.

3.1.2

Datenschutz durch datenschutzfreundliche Voreinstellungen

technische und organisatorische Maßnahmen, um sicherzustellen, dass nur solche personenbezogenen Daten, die für jeden spezifischen Zweck der Verarbeitung notwendig sind, verarbeitet werden

Anmerkung 1 zum Begriff: Solche Maßnahmen sollten mindestens die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, die Speicherfrist und ihre Zugänglichkeit umfassen.

3.1.3

Datenschutz-Folgenabschätzung

DSFA

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

Anmerkung 1 zum Begriff: Basierend auf ISO/IEC 29134:2017, 3.7.

3.1.4

datenschutzbewusst

Attribut eines Produkts oder Dienstes für die Verarbeitung personenbezogener Daten, was bedeutet, dass die Datenschutzanforderungen bei der Technikgestaltung und Vorkonfiguration berücksichtigt wurden und datenschutzwidrige funktionale Anforderungen nur insoweit gestellt wurden, wie dies für den beabsichtigten Zweck des Produkts oder Dienstes unerlässlich ist

3.1.5

besondere Kategorien personenbezogener Daten

Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

[QUELLE: DSGVO Artikel 9, Abschnitt 1]

3.2 Abkürzungen

DSTV	Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
DSFA	Datenschutz-Folgenabschätzung
DSGVO	EU-Datenschutz-Grundverordnung 679/2016
GSMA	Global System for Mobile Communications Association
ISACA	Information Systems Audit and Control Association
ZEG	Zielerreichungsgrad

4 Allgemeines

4.1 Grundlagen für den Datenschutz und den Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Neben den weit gefassten Erwartungen an den Schutz personenbezogener Daten bei Datenverarbeitungsverfahren beziehen sich Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen auf die Fähigkeit der vorgesehenen technischen Systeme und Komponenten, diesen Schutz unterstützen zu können. Es wird auf den Erwägungsgrund 78, Satz 4 zur Verabschiedung der DSGVO verwiesen. Dennoch sind die Hersteller nach DSGVO nicht dazu verpflichtet. Es sind daher andere Instrumente erforderlich, um sie in einem Prozess zu begleiten, durch den ihre Produkte oder Dienste so ausgelegt werden, dass sie den Datenschutz und den Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen für die Höchstzahl von Anwendungsfällen entsprechend dem erwarteten Markt erfüllen. Eine zugrunde liegende Reihe von Anforderungen, die mit dem Qualitätsprozess des Unternehmens konsistent sind, wird im Folgenden detailliert beschrieben. Erwartete Vorteile sind für die Endbenutzer (Kunden/Verantwortliche für die Datenverarbeitung) die einfache Umsetzung ihrer Datenschutzpflichten und für den Hersteller ein Wettbewerbsvorteil.

Die DSGVO enthält viele gesetzliche Bestimmungen, die durch den für die Datenverarbeitung Verantwortlichen und die Auftragsverarbeiter zu beachten sind; solche Bestimmungen hängen weitgehend von den unterschiedlichen funktionalen und betrieblichen Bedingungen ab, unter denen das Produkt oder der Dienst voraussichtlich verwendet wird. In diesem Zusammenhang und um die Anbieter von Produkten und Diensten bei ihrer Abschätzung zu unterstützen, wurden die Verpflichtungen der für die Datenverarbeitung Verantwortlichen generisch daraufhin analysiert, ob sie explizit oder implizit die Notwendigkeit von funktionalen Fähigkeiten zur Unterstützung der Verpflichtungen der für die Datenverarbeitung Verantwortlichen enthalten.

Die folgenden Grundsätze werden für den Datenschutz und den Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen erwartet:

- 1) DSTV sollte proaktiv und präventiv, nicht reaktiv und korrektiv sein.
- 2) Voreinstellungen und -konfiguration sollten sicher und datenschutzbewusst sein.
- 3) Datenschutz und Schutz der Privatsphäre sollten in die Gestaltung einbezogen werden.
- 4) DSTV strebt nach voller Funktionalität im Einklang mit legitimen Interessen und Zielen, ohne Kompromisse.
- 5) DSTV sollte den gesamten Datenlebenszyklus betreffen.
- 6) DSTV sollte sichtbar und transparent sein und einer unabhängigen Verifizierung unterliegen.
- 7) Die Interessen des Einzelnen sollten im Vordergrund stehen, indem starke Vorgaben und eine angemessene Benachrichtigung angeboten werden, und die Benutzer sollten durch benutzerfreundliche Optionen im Mittelpunkt stehen, auch wenn solche Bestimmungen als weniger datenschutzfreundlich erscheinen.
- 8) DSTV-Maßnahmen sollten wirksam sein.
- 9) Die Maßnahmen für DSTV sollten so ausgelegt werden, dass sie robust sind und nach Maßgabe des erhöhten Risikos einer Verletzung der Datenschutzgrundsätze aufgestockt werden können.
- 10) Die Maßnahmen für DSTV sollten regelmäßig bewertet werden.

Wenn Datenschutz durch Technikgestaltung so weit wie möglich verstanden werden soll, darf nicht nur der Zeitpunkt der Lieferung und Bereitstellung berücksichtigt werden. Der gesamte Lebenszyklus sowohl der personenbezogenen Daten als auch des Produkts und/oder des Dienstes muss ebenfalls berücksichtigt werden.

Besonderes Augenmerk sollte auf Instandhaltungsmaßnahmen sowie auf die allgemeinen Bedingungen gelegt werden, unter denen eine Wiederverwendung von Produkten stattfinden könnte. Darüber hinaus umfasst der Dienst den Vorgang der Verarbeitung als Auftragsverarbeiter im Auftrag der für die Datenverarbeitung Verantwortlichen. Einige Anforderungen dieses Dokuments werden die Aufmerksamkeit auf diese Szenarien lenken.

Wenn der Dienstbringer als für die Datenverarbeitung Verantwortlicher angesehen werden muss, sollten zusätzliche organisatorische und technische Maßnahmen ergriffen und durch ein geeignetes Managementsystem, z. B. EN ISO/IEC 27701, geregelt werden. Diese organisatorischen und technischen Maßnahmen liegen außerhalb des Anwendungsbereichs dieses Dokuments.

Dieses Dokument bietet in 4.2 eine Struktur für die Aufteilung integrierter Produkte und Dienste in Schichten, die verwendet werden dürfen, um sie in Bausteine zu modulieren, die die gleiche Reihe von Anforderungen erfüllen müssen. Für die Beschreibung der Systemarchitektur darf jeder sinnvolle Ansatz gewählt werden, sofern er eine Zuordnung der Datenschutzanliegen auf der Architektur ermöglicht. Bei der Gestaltung einer Hauptkomponente aus Teilsystemen und Diensten ist es unter Umständen notwendig, dass für die übergreifende Systemarchitekturzerlegung die Beschreibungen der enthaltenen Komponenten genutzt werden. Solche Ansätze dürfen auf opake oder transparente Modelle für die Komponentenelemente zurückgreifen. In 4.3 wird das Konformitätsschema für eine Eigenerklärung angegeben.

In Abschnitt 5 werden die Anforderungen für einen exemplarischen Prozess der datenschutzbewussten Entwicklung von Produkten und Diensten angegeben.

In Abschnitt 6 gibt es grundlegende Anforderungen an die Gestaltung der bereitgestellten Produkte und Dienste. Die Anwendung wird für die jeweiligen in 4.2 festgelegten Produktperspektiven und Dienstelemente festgelegt, und die Maßnahmenziele nehmen Bezug auf die DSGVO.

Abschnitt 7 enthält einen Leitfaden für den Prozess der Eigenerklärung und die Anforderungen zur Bestimmung des Zielerreichungsgrads.

In Anhang A, Anhang B und Anhang C werden detaillierte Informationen über die Zuordnung der grundlegenden Anforderungen an Produktperspektiven oder Dienstelemente, über die Definition von Datenschutz durch Technikgestaltung und über eine Anleitung zur Anwendung von EN ISO 9001 als Managementsystem bei der Entwicklung gegeben. Zusätzlich enthält der Anhang ZA die Konformitätserklärung für den EU-Normungsauftrag M/530.

4.2 Struktur für die Zerlegung von Produkten und Diensten in anwendbare Kategorien

4.2.1 Einleitung

Da es nicht praktikabel erscheint, Anforderungen direkt für Produkte und Dienste zu erstellen, die sich in der Zusammensetzung von Untermodulen, Architektur und Bündelung stark unterscheiden können, wird in den nächsten beiden Abschnitten eine Reihe von Modulkategorien festgelegt. Jedes komplexe Produkt oder jeder Dienst im Sinne dieses Dokuments kann in Komponententeile oder Schichten zerlegt werden. Diese können zur Darstellung von Produkten und Diensten verwendet werden. Die strukturelle Zerlegung ist zur besseren Beschreibbarkeit in produkt- und dienstbezogene Aspekte unterteilt.

4.2.2 Produktperspektiven

Die Modulkategorien, aus denen ein Produkt bestehen kann, sind wie folgt festgelegt:

- 1) **Komponentenperspektive** — hauptsächlich physikalische Untermodule wie Mikroprozessoren und Mikrocontroller, DRAM-Module, Schnittstellen-Controller, Medienlaufwerke, physikalische Speichermedien, Sensoren, Stellteile oder Stromversorgung. Diese Perspektive kann Konnektivitätstreiber und kleine Programme wie z. B. zur Aufrüstung oder dynamischen Verbindung enthalten.
- 2) **Geräteperspektive** — Hauptplatine mit Einbaurahmen, Abschirmung, Display, Tastaturen und Gehäuse. Die Geräteperspektive integriert Komponenten aus der Komponentenperspektive und fügt Programme für BIOS und Boot-Fähigkeiten hinzu.
- 3) **Betriebssystemperspektive** — Softwareperspektive mit Programmen, die sich für die Konfiguration des Geräts, die grundlegende Interaktion mit dem Benutzer, wie Tastatureingabe und -ausgabe über Bildschirm oder Drucker, die Unterstützung der Benutzerauthentifizierung, die Verwaltung des Geräts selbst und seine Interkonnektivität mit Netzwerken und mit Werkzeugen, die lokale Maßnahmen auf dem Gerät unterstützen, eignen.
- 4) **Kommunikationsperspektive** — Konnektivitätskomponenten, die physikalische Verbindungen (drahtgebunden oder drahtlos) zum Zweck der Informationsübertragung emulieren. Diese Perspektive ähnelt der Komponentenperspektive, unterscheidet sich jedoch hinsichtlich spezifischer Belange, die mit dem Aspekt des von ihr aufgebauten Netzwerks zusammenhängen.
- 5) **Speicherperspektive** — logische Perspektive für das Management von Speicherorten auf angeschlossenen physischen Speichermedien über die Komponentenperspektive. Dazu gehören lokal oder per Fernzugriff angeschlossene Medien, Raid- oder Cluster-Architekturen, NAS- oder SAN-Konzepte sowie Fileserver und Cloud-Storage.

- 6) Benutzungsschnittstellenperspektive — logische Perspektive für das Management der Benutzer-interaktion mit einem Gerät oder Dienst, die sich nicht auf der Betriebssystemperspektive befindet. Zu dieser Perspektive gehören auch Portale und bis zu einem gewissen Grad Content-Management-Systeme.
- 7) Integrierte-Systeme-Perspektive — diese Perspektive gilt, wenn ein Produkt eine Integration von mehr als einem Gerät ist. Sie erfordert ein Kommunikationsmodell zwischen den Geräten mit spezifizierten Protokollen und Übertragungsmanagement. Von integrierten Systemen wird erwartet, dass sie die Fähigkeiten und Voreinstellungen für eine angemessene Netzwerksicherheit nachweisen.
- 8) Anwendungsperspektive — Softwareperspektive, die die erwartete Funktionalität eines Geräts oder eines integrierten Systems bereitstellt.
- 9) Geschäftsprozessperspektive — logische Perspektive über der Anwendungsperspektive, die den Informationsaustausch zwischen vielen Geräten, integrierten Systemen oder sogar Organisationen verwaltet.
- 10) Systemmanagementperspektive — logische Perspektive für das Management der Betriebs- und Informationssicherheit in Bezug auf die Geräte, integrierten Systeme, Anwendungen, Speicher und/oder Kommunikationsflüsse.

4.2.3 Dienstelemente

Die Modulkategorien, aus denen ein Dienst bestehen kann, sind wie folgt festgelegt:

- 1) Dienstmanagmentelement — menschlich basierter Dienst zur Konfiguration, Betriebssteuerung und Reaktion auf einen Zwischenfall.
- 2) Selbstbedienungselement — Anwendungsdienst, der dem Kunden oder Benutzer Werkzeuge zur Konfiguration anderer Produkt- oder Dienstelemente zur Verfügung stellt.
- 3) Integrationsdienstelement — kundenspezifischer Dienst zur Herstellung der Interoperabilität von Teilsystemen, der üblicherweise innerhalb eines dedizierten Projekts unter einem vom Kunden festgelegten Managementrahmen organisiert wird.
- 4) Übertragungsdienstelement — Dienst, der Übertragungsleitungen über organisatorische Grenzen miteinander verbindet.
- 5) Aktualisierungsdienstelement — Programmcode-Updates, diese können z. B. proaktiv durch Menschen, reaktiv durch ein automatisiertes System bereitgestellt oder zum Herunterladen veröffentlicht werden.
- 6) Cloud-Dienstelement — Dienstbereitstellung von Betriebseinrichtungen auf Infrastruktur-, Plattform- oder Anwendungsebene.
- 7) Inhaltsdienstelement — Dienst, der zusätzliche Daten (z. B.: Nachrichten, Bewertungszahlen, Adressen) zur Verfügung stellt, manchmal mit der Möglichkeit, erhobene personenbezogene Daten anzureichern.
- 8) Element ausgegliederter Geschäftsprozesse — funktionale Datenverarbeitung entweder kundenspezifisch oder als normalisiertes Angebot an ähnliche Kunden.
- 9) Ausgabedienstelement — Dienste, die Kundendaten zum Zweck der Produktion von Ausgabemedien (z. B.: Fotokalender oder Marketing-E-Mails) empfangen.
- 10) Wartungsdienstelement — Dienst, der auf Anforderung von Anwendern und/oder Kunden reagiert, um Produkte und Dienste über die gesamte Lebensdauer nutzbar zu halten, einschließlich Abhol- oder Bringdienste und Gerätetausch.

- 11) Sicherheitsdienstelement — Dienste, die Systeme, Verkehr und Protokolleinträge auswerten, um Schwachstellen und Sicherheitsverletzungen zu erkennen, zu verhindern oder darauf zu reagieren.
- 12) Medienwiederherstellungsdienstelement — Dienst auf kundeneigenen physischen Speichermedien zum Zweck der Wiederherstellung der darin enthaltenen Informationen.
- 13) Medienvernichtungsdienstelement — physische Vernichtung von Speichermedien auf eine Art und Weise, die eine Wiederherstellung von Daten unmöglich macht, üblicherweise am Ende des Lebenszyklus.
- 14) Systemwiedervermarktungsdienstelement — Dienst an Produkten durch Reinigung, Rekonstruktion und Neulizenzierung, um dem Produkt ein zweites Leben bei einem anderen Kunden zu ermöglichen.

4.3 Eigenerklärung und Zielerreichungsgrade

Obwohl die Berücksichtigung des Datenschutzes und des Schutzes der Privatsphäre durch Technikgestaltung im Rahmen des Qualitätsmanagementsystems einer Organisation als Voraussetzung für die Bereitstellung von DSTV angesehen werden könnte, würde es nicht ausreichen, die entsprechenden Prozesse einzuhalten, um datenschutzbewusste Produkte und Dienste zu entwickeln. Es ist auch unabdingbar, dass das Produkt oder der Dienst den spezifischen Anforderungen entspricht, die für jede der Perspektiven des Produkts bzw. für jedes der Elemente des Dienstes gelten, um die Grundsätze des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen zu erfüllen.

In der Praxis wäre es manchmal begründbar, einen Kompromiss zwischen den Marktbedürfnissen oder den von Kunden geäußerten Anforderungen sowie den Grundsätzen und Anforderungen zu finden. Dies wird das Schutzniveau für die betroffene Person senken, aber nicht zu einem Produkt oder einem Dienst führen, das bzw. der nicht datenschutzbewusst ist. Als weiteres Beispiel könnte eine Organisation planen, ein Produkt oder einen Dienst für die Verarbeitung spezieller Datenkategorien unter rechtmäßigen Umständen bereitzustellen, und sie wendet zusätzliche Maßnahmen oder Funktionen an, die aus einer Datenschutz-Folgenabschätzung abgerufen wurden. Ein lediglich datenschutzbewusster Zustand wird nicht das erhöhte Maß an Schutz widerspiegeln, das erforderlich ist und durch zusätzliche Anstrengungen nachgewiesen wird.

Lieferanten von Teilkomponenten und Erbringern von Diensten für Systemintegratoren möchten möglicherweise bestimmte Datenschutzerfordernisse erfüllen, während sie andere ignorieren. So könnte zum Beispiel eine Datenspeicherkomponente Garantien hinsichtlich der Vollständigkeit und Rechtzeitigkeit der Löschung bieten, aber nur für verschlüsselte Daten ohne geräteseitige Entschlüsselung vorgesehen sein. In diesem Fall könnte es sein, dass dieses Gerät keine Korrektur von personenbezogenen Daten ermöglicht, da es Bitblöcke enthalten würde – ein übergeordneter datenschutzbewusster Dienst müsste den gespeicherten Inhalt ersetzen. Der Mechanismus der Eigenerklärung ermöglicht es einem Komponentenhersteller, diejenigen Facetten des Datenschutzes zu identifizieren, die die Marktausrichtung seines Produkts bestimmen.

Um das Potential für eine unvollständige Berücksichtigung von Datenschutzbelangen, die Praxis der Kompromisse und die Notwendigkeit der Angemessenheit unter besonderen Verarbeitungsbedingungen widerzuspiegeln, wurden in der nachstehenden Tabelle 1 sechs Zielerreichungsgrade festgelegt.

Tabelle 1 — Definitionen von Zielerreichungsgraden

Zielerreichung	Untergeordnete Zielerreichung	Zielerreichungsgrad	Voraussetzungen
Die Anforderungen werden vollständig erfüllt. Es wurden keine Kompromisse eingegangen. Spezielle Kategorien personenbezogener Daten sind zur Verarbeitung vorgesehen, und es wurden dementsprechend zusätzliche Gestaltungsanliegen berücksichtigt.	Spezielle Kategorien für den Schutz personenbezogener Daten und den Schutz der Privatsphäre werden durch Technikgestaltung und datenschutzfreundliche Voreinstellungen berücksichtigt.	A	Eine Datenschutz-Folgenabschätzung wurde durchgeführt und entsprechende Gestaltungsanliegen wurden berücksichtigt.
Die Anforderungen werden vollständig erfüllt. Es wurden keine Kompromisse eingegangen. Der Zweck passt zum Schutzniveau.	Datenschutz und Schutz der Privatsphäre werden durch Technikgestaltung und datenschutzfreundliche Voreinstellungen berücksichtigt.	B	Die Anforderungen werden vollständig erfüllt. Es wurden keine Kompromisse eingegangen. Die vorrangige Berücksichtigung der Interessen der betroffenen Person wird bestätigt.
Bei der Anwendung der Anforderungen wurden Kompromisse eingegangen.	Die Technikgestaltung ist datenschutzbewusst.	C	Die Anforderungserfüllungsrate beträgt $95 \% \leq x < 100 \%$.
	Die Technikgestaltung ist größtenteils datenschutzbewusst.	D	Die Anforderungserfüllungsrate beträgt $80 \% \leq x < 95 \%$.
	Überlegungen zu einer datenschutzbewussten Technikgestaltung wurden im Allgemeinen angestellt.	E	Die Anforderungserfüllungsrate beträgt $50 \% \leq x < 80 \%$.
Die Anwendung der Anforderungen ist unzureichend.		Z	Die Anforderungserfüllungsrate ist niedriger als 50 %.

Die Zielerreichung muss durch Konformität mit den ausgewählten Anforderungen an die Datenschutzfähigkeit in Abschnitt 6 und deren Zuordnung auf einem Architekturmodell der Komponente, des Dienstes oder des Teilsystems nachgewiesen werden. Ein Ansatz dazu wird in diesem Dokument am Beispiel von Produktperspektiven und/oder Dienstelementen gezeigt. Eine gleichwertige Zuordnung von Datenschutzanforderungen zu Architekturkomponenten könnte verwendet werden, um ein gleichwertiges System für Teilsysteme zu entwickeln, die aus mehreren Teilen zusammengesetzt sind, oder aus Komponenten der Basisebene, für die ein nicht schichtweiser Ansatz (z. B. serviceorientierte Architektur) bevorzugt wird. Im Falle einer bestimmten Verarbeitung, die wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen führt, muss eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden, deren Ergebnis ebenfalls in die Technikgestaltung einbezogen werden muss. Diese DSFA muss durchgeführt und aufgezeichnet werden. Ein Beispiel für eine DSFA wird durch EN ISO/IEC 29134 bereitgestellt.

Komponentenlieferanten und Dienstbringer für Teilsysteme dürfen ihr Produkt oder ihren Dienst durch eine Eigenerklärung zusammen mit der Zielerreichung als datenschutzbewusst kennzeichnen, um potentielle Systemintegratoren zu informieren, sofern sie die Konformität mit den Anforderungen entsprechend Abschnitt 7 nachweisen können.

Wird Systemintegratoren eine Komponente, ein Teilsystem oder ein Dienst mit einer Eigenerklärung für den Zielerreichungsgrad C, D, E oder Z angeboten, sollte es eine Begleitdokumentation geben, die dem Systemintegrator hilft zu verstehen, welche Datenschutzmaßnahmen von dieser Komponente angeboten werden und welche nicht.

Dieses Dokument konzentriert sich auf B2B-Aktivitäten und unterstützt die Entwickler von Komponenten und Teilsystemen bei der Behandlung spezifischer Datenschutzprobleme. Produkte und Dienste, die den Grad A oder B erreichen, sollten alle in Abschnitt 6 dargelegten Anforderungen erfüllen. Diese Anforderungen stellen jedoch nicht die gesamte Datenschutzgrundlinie dar, die in der DSGVO in allen Einzelheiten verankert ist. Es sollte daher nicht davon ausgegangen werden, dass eine Eigenerklärung des Grades A oder B einer vollständigen Erfüllung der Anforderungen der DSGVO entspricht. Es wären weitere Analysen auf der Grundlage des tatsächlichen Produkts erforderlich, bevor eine solche Einschätzung begründet werden könnte.

5 Datenschutzbewusste Entwicklung von Produkten und Diensten

5.1 Führung und Marktkennntnis

5.1.1 Die Organisation muss ein Verständnis dafür schaffen und aufrechterhalten, dass Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen für die Entwicklung und Bereitstellung aller ihrer Produkte und Dienste, die möglicherweise Auswirkungen auf die Privatsphäre haben, unabdingbar ist.

ANMERKUNG Dies bedeutet, dass der Datenschutz und der Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen in der Verpflichtung der Unternehmensleitung zum Ausdruck kommt, die sich in schriftlichen Richtlinien ausdrückt, und dass die jeweiligen Verantwortlichkeiten und die Rechenschaftspflicht den entsprechenden organisatorischen Rollen zugewiesen werden.

5.1.2 Um eine angemessene Übereinstimmung zwischen der Vielfalt der durch den Zielmarkt implizierten Anwendungsfälle und deren Auswirkungen auf die Aktivierung der DSGVO-Bestimmungen sicherzustellen, muss die Organisation das für den nachstehenden Prozess verantwortliche Personal auswählen, schulen und umfassend über die DSGVO informieren, sodass es eine umfassende Übersicht über alle Nutzungsbedingungen in Bezug auf die verschiedenen Segmente hat, die von den Marketingplänen abgedeckt werden.

ANMERKUNG Diese umfassende funktionale Perspektive gilt für den gesamten in diesem Abschnitt 5 beschriebenen Prozess, wobei zu berücksichtigen ist, dass die Datenschutzanalyse in Bezug auf die spezifische Beschaffung eines Produkts oder Systems außerhalb des Anwendungsbereichs dieses Dokuments liegt.

5.2 Vorbereitung

5.2.1 Die Organisation muss bestimmen, ob das bereitzustellende Produkt und/oder der zu erbringende Dienst eine aktive Rolle bei der Verarbeitung personenbezogener Daten vorsieht.

ANMERKUNG Eine aktive Rolle ist in Betracht zu ziehen, wenn die personenbezogenen Daten auf Produkten oder Diensten verarbeitet werden, bei denen der Kunde und/oder Benutzer nicht die volle und alleinige Kontrolle über die Erhebung, Speicherung, gemeinsame Nutzung und Löschung dieser personenbezogenen Daten hat.

5.2.2 Um die Auswirkungen von Produkten und Diensten auf die Privatsphäre einer betroffenen Person zu behandeln, muss die Organisation eine geeignete Methodik und die Struktur des Folgenabschätzungsberichts festlegen.

ANMERKUNG EN ISO/IEC 29134 enthält Anleitungen für die Datenschutz-Folgenabschätzung

5.2.3 Die Organisation muss den Entwicklungsabteilungen Zugang zu ausreichenden personellen Ressourcen mit der entsprechenden Kompetenz in rechtlichem und technischem Fachwissen auf dem Gebiet des Datenschutzes gewähren.

ANMERKUNG Wenn ein Datenschutzbeauftragter für die Organisation ernannt wird, wird erwartet, dass dieser in den Gestaltungsprozess einbezogen wird. Es ist sicherzustellen, dass keine Interessenkonflikte entstehen. Eine andere Option könnte darin bestehen, eine spezielle Rolle als Datenschutzingenieur in der Entwicklungsabteilung zu haben.

5.2.4 Die Organisation muss ihren bestehenden Entwicklungsprozess auf die Eignung zur Erfüllung der Anforderungen dieses Dokuments bewerten und falls erforderlich ändern.

5.3 Gestaltung

5.3.1 Bestimmung der Anforderungen für DSTV

5.3.1.1 Grundlegende Anforderungen an die Gestaltung

5.3.1.1.1 Die für die Produkt- und/oder Dienstgestaltung verantwortliche Person muss das beabsichtigte Marktangebot logisch in die Perspektiven und Elemente zerlegen, aus denen es sich zusammensetzt.

ANMERKUNG Die Perspektiven und Elemente sind in 4.2 festgelegt.

5.3.1.1.2 Für jede Perspektive und jedes Element, die als Teil des beabsichtigten Marktangebots identifiziert wurden, müssen alle für diese Perspektive bzw. dieses Element geltenden grundlegenden Anforderungen aus Abschnitt 6 ermittelt werden.

ANMERKUNG Anhang A, Tabelle A.1 und Tabelle A.2 enthalten Zuordnungstabellen für die anwendbaren grundlegenden Anforderungen an eine bestimmte Produktperspektive oder ein bestimmtes Dienstelement.

5.3.1.2 Erweiterte Gestaltungsanforderungen bei der Verarbeitung personenbezogener Daten

5.3.1.2.1 Für den Fall, dass die Organisation bestätigt hat, eine aktive Rolle bei der Verarbeitung personenbezogener Daten für das beabsichtigte Marktangebot zu übernehmen, muss die für die Produkt- und/oder Dienstgestaltung verantwortliche Person die Umsetzung geeigneter technischer und organisatorischer Maßnahmen in Betracht ziehen.

ANMERKUNG 1 EN ISO/IEC 27701 enthält entsprechende Anforderungen und Leitlinien.

ANMERKUNG 2 Wenn es einen Datenschutzbeauftragten der Organisation gibt, muss dieser informiert und konsultiert werden, um die geeigneten Maßnahmen zur Durchführung der Verarbeitung zu bestimmen.

ANMERKUNG 3 Es wird auf DSGVO Artikel 32 verwiesen.

5.3.1.3 Folgenbedingte Gestaltungsanforderungen

5.3.1.3.1 Die für die Produkt- und/oder Dienstgestaltung verantwortliche Person muss bestimmen, ob die erhobenen, verarbeiteten und/oder übermittelten Daten so genannte „besondere Kategorien personenbezogener Daten“ im Sinne von Artikel 9 DSGVO oder personenbezogene Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten enthalten oder eine Datenverarbeitung mit hohem Risiko beinhalten.

ANMERKUNG Es wird auf DSGVO Artikel 9 und Artikel 10 verwiesen.

5.3.1.3.2 Falls bestätigt wird, dass es sich um Daten mit hohem Risiko oder besondere Kategorien von personenbezogenen Daten handelt, muss die für die Produkt- und/oder Dienstgestaltung verantwortliche Person eine Datenschutz-Folgenabschätzung (DSFA) in Übereinstimmung mit den Bestimmungen in 5.2.2 durchführen.

ANMERKUNG Es wird auf DSGVO Artikel 35 verwiesen. Es könnte weitere Fälle geben, in denen ebenfalls eine DSFA durchgeführt werden muss.

5.3.1.3.3 Kommt die DSFA zu dem Schluss, dass zusätzliche Anforderungen an die Gestaltung und die Voreinstellung des Produkts und/oder des Dienstes gestellt werden müssen, muss die für die Gestaltung des Produkts und/oder des Dienstes verantwortliche Person sicherstellen, dass diese Anforderungen bei der Entwicklung ebenfalls berücksichtigt werden.

5.3.1.4 Spezielle Geschäftsbereiche oder verbraucherbezogene Gestaltungsanforderungen

5.3.1.4.1 Wenn ein Produkt und/oder ein Dienst für bestimmte Kategorien von betroffenen Personen bereitgestellt werden sollen, muss die für die Produkt- und/oder Dienstgestaltung verantwortliche Person bestimmen, ob besondere Erwartungen an die datenschutzbewusste Gestaltung und die Vorkonfiguration bestehen.

5.3.1.4.2 Jede dieser Erwartungen muss entweder durch eine bestehende oder eine neue Anforderung an die Gestaltung und die Voreinstellung des Produkts und/oder des Dienstes abgedeckt werden. Die für die Gestaltung des Produkts und/oder des Dienstes verantwortliche Person muss sicherstellen, dass diese Anforderungen bei der Entwicklung ebenfalls berücksichtigt werden.

ANMERKUNG In einen bestimmten Geschäftsbereich, einem bestimmten Anwendungsfall oder einer bestimmten Umgebung könnten die Kunden- und/oder Verbrauchererwartungen für eine datenschutzbewusste Technikgestaltung und datenschutzfreundliche Voreinstellungen weitaus detaillierter sein als die rechtlichen Erwartungen aus der DSGVO.

5.3.2 Entwicklung

5.3.2.1 Die für die Entwicklung des Produkts und/oder des Dienstes verantwortliche Person muss sicherstellen, dass alle in 5.3.1 genannten Gestaltungsanforderungen in der Entwicklungsphase des Produkts oder des Dienstes berücksichtigt werden.

5.3.2.2 Die für die Entwicklung des Produkts und/oder des Dienstes verantwortliche Person muss sicherstellen, dass die größten Anstrengungen unternommen werden, um angemessene Funktionen, Maßnahmen und Kontrollen in dem jeweiligen Produkt und/oder dem Dienst zu implementieren, um die in 5.3.2.1 genannten Anforderungen zu erfüllen.

5.3.2.3 Die für die Entwicklung des Produkts und/oder des Dienstes verantwortliche Person muss die Festlegung ausreichend datenschutzfreundlicher Voreinstellungen für jede konfigurierbare Funktion überwachen, die mit dem in Entwicklung befindlichen Produkt und/oder Dienst geliefert wird.

ANMERKUNG Als Leitgrundsatz ist u. a. die Datenminimierung zu berücksichtigen.

5.3.2.4 Die für die Entwicklung des Produkts und/oder des Dienstes verantwortliche Person muss sicherstellen, dass die Voreinstellungen des Produkts und/oder des Dienstes mit den in 5.3.2.3 festgelegten Einstellungen übereinstimmen.

5.3.3 Produktion und Dienstleistung

5.3.3.1 Die Organisation muss geeignete Prüfungen durchführen und entsprechende Nachweise dokumentieren, um die Umsetzung der Funktionen, Maßnahmen und Kontrollen aus 5.3.2.2 und der Vorkonfiguration aus 5.3.2.4 zu bestätigen.

5.3.3.2 Für das Produkt und/oder den Dienst muss die Organisation den Zielerreichungsgrad bestimmen.

ANMERKUNG 7.1.3 enthält die Anforderungen für die Bestimmung des Zielerreichungsgrads.

5.3.4 Freigabe von Produkten und Diensten

Die Organisation muss dem Kunden Informationen in einfacher Sprache als Teil der Produktdokumentation über alle datenschutzbezogenen Funktionen und Einstellungen des freigegebenen Produkts und/oder Dienstes zur Verfügung stellen.

5.4 Leistungsbewertung

Wenn die Organisation einen Jahresbericht über die soziale Verantwortung der Unternehmen vorlegt, muss dieser Bericht auch den Prozentsatz der Produkte und Dienste nach ihrem jeweiligen Zielerreichungsgrad enthalten. Nach dem ersten Jahr der Berichterstattung muss auch die Abweichung gegenüber dem vorangegangenen Bericht oder einem anderen geeigneten Bezugsjahr angegeben werden.

5.5 Verbesserung

5.5.1 Die Organisation muss alle datenschutzbezogenen Rückmeldungen von Kunden, Anwendern und anderen Anspruchsgruppen zu einem freigegebenen Produkt oder Dienst beachten.

5.5.2 In regelmäßigen Abständen, spätestens mit Beginn der Gestaltung für die nächste größere Freigabe, müssen die in 5.5.1 erhaltenen Rückmeldungen ausgewertet und spezifische Erwartungen für die neue Freigabe vorgeschlagen werden.

5.5.3 Jede Anforderung, die im Rahmen des aktuellen Entwicklungszyklus nicht erfüllt werden konnte, muss aufgezeichnet werden und darf zu einer Anforderung für das nachfolgende Entwicklungsrelease des Produkts und/oder des Dienstes werden.

6 Anforderungen an die Datenschutzfähigkeit bei der Gestaltung von Produkten und Diensten

6.1 Zugang

6.1.1 Zugang zu Daten

6.1.1.1 Maßnahmenziel:

Bereitstellung von Fähigkeiten für die betroffene Person, auf ihre Daten zuzugreifen.

ANMERKUNG Es wird auf DSGVO Artikel 15, Absatz 1, verwiesen.

6.1.1.2 Das Rechte-und-Rollen-Modell des Produkts und/oder Dienstes muss einer betroffenen Person die Möglichkeit geben, auf ihre Daten (einschließlich der Daten über sie) zuzugreifen.

Diese Anforderung gilt für die folgenden Produktperspektiven:

- Benutzungsschnittstellenperspektive;
- Anwendungsperspektive und
- Geschäftsprozessperspektive.

Diese Anforderung gilt für die folgenden Dienstelemente:

- Selbstbedienungselement;
- Inhaltsdienstelement und
- Element ausgegliederter Geschäftsprozesse.

ANMERKUNG Folgerichtig sind damit auch die benötigten Zugriffsrechte z. B. für Verzeichnisse oder Datentabellen eingeschlossen.

6.1.2 Kopie der Daten

6.1.2.1 Maßnahmenziel:

Bereitstellung von Fähigkeiten zur Bereitstellung einer Kopie der personenbezogenen Daten in einer häufig verwendeten elektronischen Form.

ANMERKUNG Es wird auf DSGVO Artikel 15, Absatz 3 verwiesen.

6.1.2.2 Das Produkt und/oder der Dienst müssen eine Exportfähigkeit für Datensätze in einem für Personen lesbaren Format bieten.

Diese Anforderung gilt für die folgenden Produktperspektiven:

- Betriebssystemperspektive;
- Speicherperspektive;
- Benutzungsschnittstellenperspektive;
- Anwendungsperspektive und
- Geschäftsprozessperspektive.

Diese Anforderung gilt für die folgenden Dienstelemente:

- Selbstbedienungselement;
- Cloud-Dienstelement;
- Inhaltsdienstelement und
- Element ausgegliederter Geschäftsprozesse.

ANMERKUNG Dies könnte auch durch die Bereitstellung von Transformationswerkzeugen für ein von Personen nicht lesbares Format oder im Falle von Audio- oder Videodaten durch die Bereitstellung in einem gängigen Format für die Wiedergabe erreicht werden.

6.2 Verantwortlichkeit

6.2.1 Maßnahmenziel:

Alle relevanten Nachweise aufgezeichnet anzubieten, die der Verantwortliche zum Nachweis einer Compliance benötigen könnte.

ANMERKUNG Es wird auf DSGVO Artikel 5, Absatz 2, verwiesen.

6.2.2 Die Produkt- und/oder Dienstdokumentation muss angemessene Informationen über die Erfüllung der Anforderungen aus dem gesamten Abschnitt 6 enthalten und darüber, durch welche Funktion, Einstellung oder Maßnahmen dies erreicht wird.

Diese Anforderung gilt für jede Produktperspektive und jedes Dienstelement.