



Datenschutz- Reifegradmodell

Reifegradmodell zur Abbildung von technisch-organisatorischen Maßnahmen bei der Auftragsverarbeitung

Herausgeber

Bitkom e. V.
Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner

Isabelle Stroot | Referentin Datenschutz
T 030 27576-228 | i.stroot@bitkom.org

Paul Breitbarth, LL.M. | Wissenschaftlicher Mitarbeiter
T 030 27576-259 | p.breitbarth@bitkom.org

verantwortliches Gremium

AK Datenschutz | AG Reifegradmodell TOMs

Lead Autoren

Anastasia Meletiadou, Head of Privacy Management / DPO, Vodafone |
Andreas Link, Senior Expert, Deutsche Telekom |
Donald Ortmann, CEO, Don Luigi It-Service |
Frank Ingenrieth, Stellvertretender Geschäftsführer, SRIW |
Heiko Gossen, Geschäftsführer, migosens |
Michael Ochs, Geschäftsfeldmanager Software & Platform Business, Fraunhofer IESE |
Stephan Rehfeld, Geschäftsführer, scope & focus Service-Gesellschaft mbH

Layout

Lea Joisten | Bitkom

Titelbild

© jan antonin kolar – unsplash.com

Copyright

Bitkom 2024

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom.

1	Einleitung	8
2	Zielsetzung des Reifegradmodells	10
3	Struktur des Reifegradmodells und Verhältnis zu anderen Standards	12
	Themengebiete des Reifegradmodells und deren inhaltliche Struktur	14
	Reifegrade im Datenschutz	16
	Themengebiete, Fähigkeitsgrade und Reifegrade	17
	Fähigkeitsgrade (Stufen) der Themengebiete	18
	Bindung von Reifegraden und Fähigkeitsgraden	20
	Datenschutz-Reifegrad 1 – DSR1 (Initial)	20
	Datenschutz-Reifegrad 2 – DSR2	20
	Höhere Datenschutz-Reifegrade	22
4	Begriffe	24
5	Datenschutzleitlinie	26
	Vorgaben der Leitung für den Datenschutz	27
	Datenschutzleitlinie und Überprüfung	27
6	Organisation des Datenschutzes	29
	Datenschutzmanagementsystem	30
	Datenschutz-Risikoanalyse nach Art. 32 DS-GVO	31
	Datenschutzprozesse	33
	Datenschutzrechtliche Zulässigkeitsprüfung	33
	Gewährleistung der Betroffenenrechte	34
	Meldung von Datenschutzvorfällen	36
	Datenschutzprozesse	38
	Verzeichnis der Verarbeitungstätigkeiten (VVT)	38
	Datenschutzfolgenabschätzung	38
	Berichte an Leitung	39

7

Personalsicherheit

40

Vor der Beschäftigung

41

Sicherheitsüberprüfung

41

Beschäftigungs- und Vertragsbedingungen

42

Während der Beschäftigung

43

Verantwortlichkeiten der Leitung

43

Datenschutzbewusstsein, -ausbildung und -schulung

44

Maßregelungsprozess

45

Beendigung und Änderung der Beschäftigung

46

Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung

46

8

Verwaltung der Werte

48

Verantwortlichkeit für Werte

49

Führung eines Verarbeitungsverzeichnisses

49

Inventarisierung von Werten

51

Informationsklassifizierung

52

Klassifizierung personenbezogener Daten

52

Handhabung von Datenträgern

53

Handhabung und Transport von Datenträgern

53

Löschung und Entsorgung von Datenträgern

54

9

Zugangssteuerung

55

Geschäftsanforderungen an die Zugangssteuerung

56

Allgemein

56

Leitlinie zur Zugangskontrolle

57

Verfahren und Verwaltung von Rechten und Zugängen

59

An- und Abmeldeverfahren und Zugangsbereitstellung

59

Umgang mit privilegierten Konten

61

Benutzerverantwortlichkeiten

63

Regelung zum Umgang mit vertraulichen Anmeldeinformationen

63

Zugangssteuerung für Systeme und Anwendungen

65

Zugriffsbeschränkungen von Nutzenden beim Zugriff von Applikationen und Informationen

65

10	Kryptographie	67
	Regelungen bezüglich kryptographischer Maßnahmen	68
	Schlüsselverwaltung	70
11	Physische und umgebungsbezogene Sicherheit	72
	Sicherheitsbereiche	73
	Physische Sicherheitsperimeter	73
	Schutz vor externen und umweltbedingten Bedrohungen	75
	Geräte und Betriebsmittel	76
	Platzierung und Schutz von Geräten und Betriebsmitteln	76
	Richtlinien für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren	77
12	Betriebsicherheit	79
	Betriebsabläufe und Verantwortlichkeiten	80
	Änderungssteuerung	80
	Trennung von Entwicklungs-, Test- und Betriebsumgebungen	81
	Schutz vor Schadsoftware	81
	Patchmanagement	82
	Datensicherung	84
	Sicherung von Information	84
	Protokollierung und Überwachung	86
	Protokollierung der Datenverarbeitung bei Personenbezug	86
	Handhabung von technischen Schwachstellen	87
	Einschränkungen von Softwareinstallation	88
13	Kommunikationssicherheit	89
	Netzwerkkontrollen	90
	Sicherheit von Netzwerkdiensten	92
	Segmentierung von Netzwerken	93
	Schutz von personenbezogenen Daten bei der Datenübermittlung	94
	Vertraulichkeitsvereinbarungen und die Verpflichtung auf das Datengeheimnis	96
	Informationssicherheit bei der Übermittlung von personenbezogenen Daten	98

14	Anschaffung, Entwicklung und Instandhaltung von Systemen	100
	Sicherheitsanforderungen an Informationssysteme	101
	Anschaffung von Systemen	101
	Weiterentwicklung von Systemen	103
	Entwicklung und Wartung von Software für die Verarbeitung personenbezogener Daten: Konzeption und Abnahme	105
	Entwicklung und Wartung von Software für die Verarbeitung personenbezogener Daten: Technische Umsetzung (Architektur, Code) und Tests bis zur Ebene Systemtests	107
	Instandhaltung und Wartung von Systemen	111
15	Lieferantenbeziehungen	112
	Technische und organisatorische Maßnahmen bei der Auftragsverarbeitung (Organisation als Auftraggeber)	113
16	Handhabung von Datenschutzvorfällen	115
	Mitwirkung des Informationssicherheitsbeauftragten	116
	Einrichtung einer Problem-Management-Organisation	117
	Datenschutzvorfall-Management-Prozess	118
17	Datenschutzaspekte beim Business Continuity Management	120
	Planung zur Aufrechterhaltung des Datenschutzes	121
	Umsetzung der Aufrechterhaltung des Datenschutzes	122
	Überprüfen und Bewerten der Aufrechterhaltung des Datenschutzes	123
	Maßnahmen zur Erhöhung der Verfügbarkeit	124
18	Compliance	125
	Einhaltung gesetzlicher und vertraglicher Anforderungen	126
	Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen	127
	Geistige Eigentumsrechte	128
	Schutz vor Aufzeichnungen	128

Überprüfungen der Compliance-Anforderungen	130
Unabhängige Überprüfung der Compliance-Anforderungen	130
Optimierung von Datenschutz- und Sicherheitsrichtlinien und -standards	131
Technische Überprüfung der Compliance-Anforderungen	131

Abbildung

Modellstruktur des Datenschutz-Reifegradmodells	17
---	----

Tabellen

Tabelle 1

Schablone für die Stufen (Fähigkeitsgrade) der Themengebiete des Datenschutz-Reifegradmodells und inhaltliche Definitionen	19
--	----

Tabelle 2

Themengebiete des DSR2 (<Name>) im Datenschutz-Reifegradmodell	21
--	----

Tabelle 3

Zuordnung von Themengebieten und Fähigkeitsgraden (Stufen) zu Reifegraden (DSR).	23
--	----

1 Einleitung

Mit der Anwendung der Europäischen Datenschutzgrundverordnung (DS-GVO) ab Mai 2018 ergaben sich auch für die Auftragsdatenverarbeitung Änderungen. Mit Einführung der DS-GVO entfällt der Anhang zu § 9 Satz 1 BDSG und das Ordnungsschema der technisch-organisatorischen Maßnahmen zur Darstellung des Datenschutz-Niveaus. Bereits vorgeschlagene Ordnungsschemata konnten sich in der bisherigen Diskussion nicht durchsetzen. Dennoch wird ein einheitliches Ordnungsschema benötigt, um Abstimmungen und Prüfungen von technischen und organisatorischen Maßnahmen zwischen verschiedenen Parteien zu strukturieren.

Das vorliegende Dokument soll einen ersten Ansatz für ein solches einheitliches Ordnungsschema bieten. Es soll Unternehmen, die sich in der Rolle eines Auftragsverarbeiters für personenbezogene Daten befinden, einen Leitfaden mit Best Practices für die Identifikation und Umsetzung relevanter technisch-organisatorischer Maßnahmen hinsichtlich Privacy by Design und Sicherheit der Verarbeitung an die Hand geben. Überdies soll es als Diskussionsgrundlage innerhalb des Bitkom und mit anderen Verbänden sowie Behörden und Ministerien dienen. Ziel des Dokuments ist ferner die Unterstützung der Anwenderinnen und Anwender bei der Abbildung des Datenschutzniveaus bei der Verarbeitung personenbezogener Daten im Rahmen einer Auftragsverarbeitung nach der Datenschutz-Grundverordnung (DS-GVO).

Die DS-GVO definiert neben bekannten und erweiterten Anforderungen an die Verarbeitung personenbezogener Daten auch eine Reihe neuer Anforderungen. Diese betreffen technische und organisatorische Aspekte sowie Maßnahmen des Datenschutzes, der Informationssicherheit und der IT-Sicherheit.

Aktueller Stand der Entwicklung sowie die Möglichkeit zur Rückmeldung und Kritik

Das Reifegradmodell wurde zunächst als Beta-Version veröffentlicht, um im Rahmen eines iterativen Prozesses das Konzept als solches einer breiteren Öffentlichkeit zugänglich zu machen und somit Gegenstand eines umfassenden und diversen Feedbacks zu machen.

Das Feedback wurde nunmehr ausgewertet und eingearbeitet. Diese Version stellt in der vorliegenden veröffentlichten Version nun die erste Version dar. Die Autorinnen und Autoren sind auch zukünftig für Rückmeldungen und Verbesserungsvorschläge offen, insbesondere wenn praktische Erfahrungen in der Anwendung vorliegen.

Feedback kann jederzeit unter isabelle.stroot@bitkom.org kommuniziert werden.

2 Zielsetzung des Reifegradmodells

Das vorliegende Dokument beschreibt ein Reifegradmodell für technische und organisatorische Maßnahmen, das primär kleine und mittelständische Unternehmen, die als Auftragsverarbeiter im Sinne der DS-GVO arbeiten oder arbeiten möchten, bei der schnellen und pragmatischen Erreichung von messbaren Niveaus für Datenschutz unterstützen soll.

Ziel des Reifegradmodells ist es, Organisationen, insbesondere Auftragsverarbeitern im Sinne der DS-GVO, eine praktische Unterstützung bei

- der systematischen Bewertung ihrer Fähigkeiten und des Reifegrads der Organisation in den Bereichen Datenschutz und Sicherheit der Datenverarbeitung (Baseline),
- der zielgerichteten Weiterentwicklung der Fähigkeiten und des Reifegrads der Organisation, angepasst auf das Tätigkeitsprofil des Auftragsverarbeiters (Improvement), und
- dem Vergleich der eigenen Fähigkeiten und des eigenen Reifegrads mit dem anderer Organisationen zu geben (Benchmark).

In der Praxis können mithilfe des Reifegradmodells z. B.

- Anforderungen an Auftragsverarbeiter, durch deren Auftraggeber einfach benannt, unmissverständlich und einheitlich formuliert,
- Selbstbewertungen der Auftragsverarbeiter durchgeführt,
- die Auswahl eines Auftragsverarbeiters unterstützt,
- interne Optimierung in Auftragsverarbeiter-Organisationen geplant und entlang der Inhalte des Reifegradmodells zielführend durchgeführt,
- externe Bewertungen des Datenschutz-Reifegrads von Auftragsverarbeitern durchgeführt, oder
- auf Basis externer Bewertungen und Selbstbewertungen Vergleiche und Fortschritte bei der Erhöhung des Reifegrades zwischen Unternehmen ermöglicht werden.

3 Struktur des Reifegradmodells und Verhältnis zu anderen Standards

Die Themen Datenschutz, Informationssicherheit und IT-Sicherheit strahlen in nahezu alle Bereiche, Prozesse und Assets einer Organisation (Aufbau und Ablauf), die sich mit der Verarbeitung von personenbezogenen Daten befasst, aus. Viele Aspekte zum Aufbau und Abläufen sind jedoch zum Teil auch schon durch bestehende Standards, Modelle und Regularien betroffen. Dies gilt hauptsächlich für die reine Betrachtung von Themen wie Informationssicherheit und insbesondere IT-Sicherheit.

Eine Vielzahl von Querbeziehungen zu bereits existierenden Standards, Modellen und Regularien sind dabei zu berücksichtigen. Dazu gehören unter anderem Modelle für Software-Entwicklungsprozesse wie SPICE, CMMI für Development oder CMMI für Acquisition, für IT-Betriebsprozesse wie z. B. CMMI für Services und ITIL oder für Informationssicherheit und Datenschutz wie ISO 27001 und ISO 27701.

Das Reifegradmodell wurde so konzipiert, dass es die Themen Datenschutz und Sicherheit der Datenverarbeitung in ihren vielfältigen Ausprägungen in einer Organisation möglichst umfassend abbildet. Es kann dabei als Ergänzung zu bereits etablierten Modellen und Standards dienen oder auch als eigenständiges Instrument eingesetzt werden, falls in einer Organisation noch kein Modell oder Standard etabliert ist. Das Modell ist als Unterstützung aus datenschutzrechtlicher Perspektive zu Standards wie ISO 27001 und ISO 27701 zu sehen, die ein entsprechendes Managementsystem beschreiben und mit ihren Anhängen einzelne, abstrakte Maßnahmen beschreiben. Der Standard ISO 27002 beschreibt zwar die Umsetzung von Maßnahmen detaillierter, ohne jedoch eine abgestufte Umsetzung oder gar eine entsprechende Gewichtung einzelner Aspekte zu berücksichtigen. Das Reifegradmodell kann daher gut ergänzend zur Umsetzung dieser oder ähnlicher Standards unterstützend eingesetzt werden. Ebenso kann es eigenständig intern, sowie in der Zusammenarbeit bei der Auftragsverarbeitung eingesetzt werden. Im letzteren Fall kann das gemeinsame Verständnis der Anforderungen an die technischen und organisatorischen Maßnahmen erheblich vereinfacht werden.

Das Reifegradmodell ist in Reifegrade und Themengebiete unterteilt. Je ein Reifegrad fasst dabei mehrere Themengebiete zusammen.

3.1 Themengebiete des Reifegradmodells und deren inhaltliche Struktur

Das Datenschutz-Reifegradmodell ist in eine Reihe von Themenbereichen gegliedert, die jeweils bestimmte Datenschutzzwecke und die damit verbundenen Schutzziele wie Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität verfolgen und unterstützen. Die Themengebiete tragen so zu den durch die DS-GVO adressierten Bereiche Datenschutz, Informationssicherheit und IT-Sicherheit bei. Jedes Themengebiet leistet somit einen definierten Beitrag zu den Fähigkeiten und dem Reifegrad einer Organisation im Bereich des Datenschutzes. Es ist langfristig angedacht, dass ein Themengebiet grundsätzlich drei möglichen Ausprägungen (Typen) folgen kann:

- **Dokumente**, die für Datenschutz, Informationssicherheit und IT-Sicherheit hinsichtlich Auftragsverarbeitung relevant sind, z. B. Richtlinien im Unternehmen
- **Prozesse**, die für Datenschutz, Informationssicherheit und IT-Sicherheit hinsichtlich Auftragsverarbeitung relevant sind, z. B. Geschäftsprozesse, Softwareentwicklungsprozesse, IT-Betriebsprozesse, Prozesse zum Umgang mit Datenträgern und Unterlagen, Management physischer Zugangskontrollen
- **Physische Objekte**, die für Datenschutz, Informationssicherheit und IT-Sicherheit hinsichtlich Auftragsverarbeitung relevant sind, z. B. physische Zugangskontrollen, Hardware im Bereich Security, Checklisten, Templates oder Formulare

Die **Themengebiete** im **Datenschutz-Reifegradmodell** sind eine **Analogie zu den Prozessgebieten bzw. Prozessen**, wie sie aus Standards wie dem CMMI bzw. SPICE bereits bekannt sind. Da Themengebiete – wie oben beschrieben – jedoch nicht nur Prozesse sein können, sondern auch Dokumente und allgemeine physische Objekte in einer Organisation, wurde bewusst vom Begriff Prozessgebiet Abstand genommen. Dies hat auch den Hintergrund, dass aus pragmatischer Sicht nicht für jeden Fall auch zwingend ein Prozess im Reifegradmodell vorhanden sein muss, beispielsweise ein Dokument zur Informationssicherheitsrichtlinie.

Die **Struktur der Themengebiete** ist so angelegt, dass bei Nachweis der Umsetzung einer festgelegten **Menge von Aspekten** jeweils eine weitere **Stufe im Fähigkeitsgrad** des jeweiligen Themengebiets erreicht wird. Die einzelnen **Aspekte** können dabei **technischer (T)** und **organisatorischer (O)** Art sein. Es ist langfristig vorgesehen, dies für die jeweiligen Aspekte auch auszuweisen; hierdurch ergeben sich dauerhaft erweiterte Möglichkeiten automatisierter Auswertungen.

Die Stufen der Themengebiete sind dabei aufeinander aufbauend angelegt und werden mit Buchstaben, beginnend bei A, bezeichnet. Eine Stufe wird immer dann erreicht, wenn alle Aspekte der zugehörigen Stufe umgesetzt sind, d. h. die Stufenzuordnung erfolgt immer mit dem letzten umgesetzten Aspekt einer Stufe. Dies ist ebenfalls eine grundsätzliche Analogie zu den aus Modellen wie CMMI bzw. SPICE bekannten Fähigkeitsgraden, die dort in Stufen (Capability Levels) 1 bis 3 beziehungsweise 1 bis 5 strukturiert sind. Auch hier liegt der Grund für die alternative Aspekt- und Stufengestaltung in den möglichen verschiedenartigen Ausprägungen der Themengebiete im Datenschutz-Reifegradmodell in Form eines Dokuments, Prozesses oder physischen Objekts. Eine Verwendung der bekannten Stufen aus CMMI bzw. SPICE würde zu erheblichen Missverständnissen führen.

Insbesondere um auch kleineren Unternehmen die Anwendung zu erleichtern und den Aufwand und Mehrwert eventuell kleiner Schritte leichter nutzbar zu machen, definiert dieses Reifegradmodell Aspekte im Vergleich zu anderen Standards teils relativ feingliedrig. Dies ermöglicht es, neben den Hauptstufen auch Zwischenstufen, und damit auch Reifegradentwicklungspotenziale abzubilden.

3.2 Reifegrade im Datenschutz

Ebenfalls analog zum CMMI werden im Datenschutz-Reifegradmodell Reifegrade auf Organisationsebene definiert.

Hierbei soll das Reifegradmodell neben einem Basislevel auch weitere, vordefinierte Reifegrade abbilden. Diese können sich sowohl aus sektoralen Anforderungen ableiten, als auch anderen regulatorischen Ansätzen folgen.

Ein Reifegrad bindet grundsätzlich eine dem Reifegrad zugeordnete Menge von Themengebieten, die eine hohe Relevanz für den Reifegrad besitzen, zusammen. Die so einem Reifegrad zugeordneten Themengebiete müssen dann einen definierten Mindestfähigkeitsgrad erfüllen. Ist diese Bedingung für alle dem Reifegrad zugeordneten Themengebiete in einer Organisation erfüllt, so ist der Reifegrad auf Organisationsebene erreicht. Beispielsweise könnten zwölf Themengebiete dem Datenschutzreifegrad 2 (DSR2) zugeordnet sein. Eine Organisation befindet sich genau dann auf DSR2, wenn für diese zwölf Themengebiete je mindestens der Fähigkeitsgrad B nachgewiesen wird. Für einen nächsthöheren Reifegrad, beispielsweise DSR3, werden der bereits in DSR2 bestehenden Menge von Themengebieten zusätzliche Themengebiete hinzugefügt. Genau dann, wenn diese zusätzlichen Themengebiete, sowie die auf DSR2 bereits bestehenden relevanten Themengebiete jeweils alle den Fähigkeitsgrad C erreicht haben, hat die Organisation DSR3 erreicht. Dieses Schema lässt sich auf weitere Reifegrade, z. B. DSR4, DSR5 fortsetzen. So entsteht eine strukturierte Sicht auf den Datenschutz-Reifegrad einer Organisation.

3.3 Themengebiete, Fähigkeitsgrade und Reifegrade

Abbildung 1 visualisiert die Struktur des Datenschutz-Reifegradmodells auf den verschiedenen Ebenen, beginnend auf der obersten Ordnungsebene eines Reifegrades, der ein oder mehrere Themenfelder einbindet. Die Themenfelder bestehen jeweils aus einer oder mehreren Stufen (Fähigkeitsgrade), zu welchen jeweils ein oder mehrere Aspekte fachlicher oder generischer Natur zugeordnet werden. Daneben besitzt jedes Themengebiet eine Typbestimmung und eine Beschreibung seines jeweiligen Zwecks.

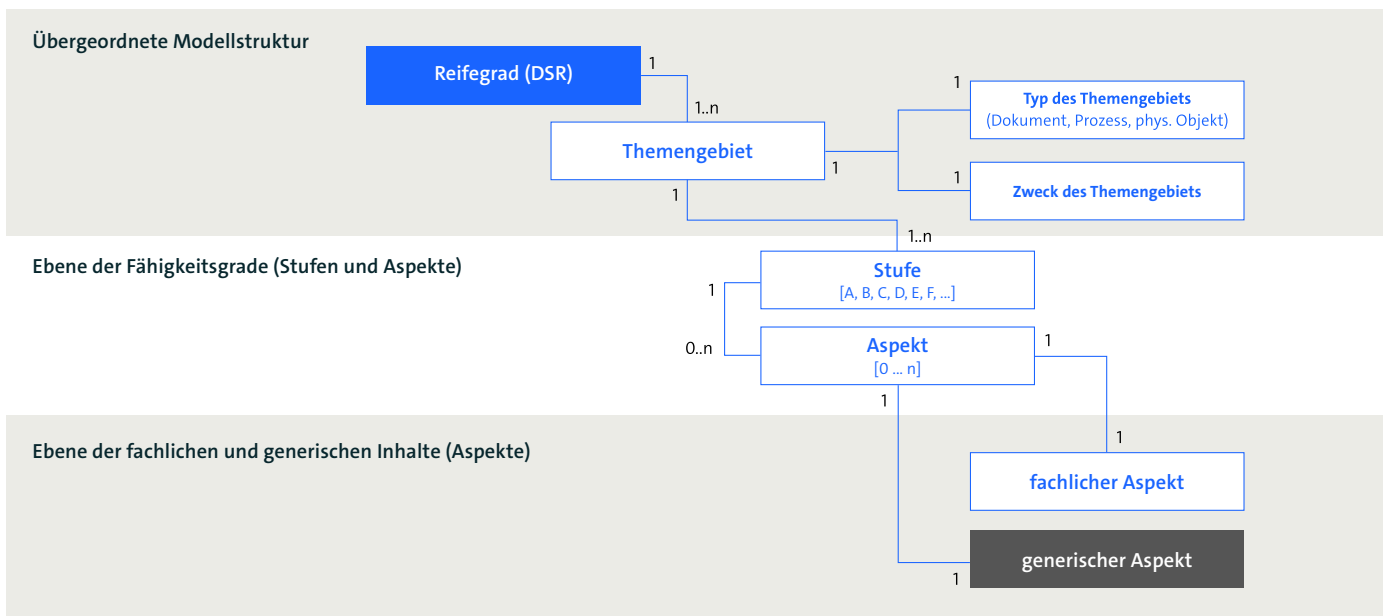


Abbildung 1: Modellstruktur des Datenschutz-Reifegradmodells

Daher wurde auf die Konzepte **Aspekt** (0, 1, 2, 3 usw.) und **Stufe** (A, B, C, D usw.) ausgewichen. Dieses strukturelle Konzept ist bereits in der Vergangenheit in stark praxisorientierten Reifegradmodellen verwendet worden. Das TPI (Test Process Improvement) Modell aus der Softwareentwicklung, welches schon in den 1990ern entwickelt wurde, nutzt insbesondere dieses Konzept zur Darstellung und Ordnung der Fähigkeitsgrade hinsichtlich der für Softwaretesting und Testprozesse relevanten Themengebiete.

3.4 Fähigkeitengrade (Stufen) der Themengebiete

Je Themengebiet können, wie bereits erwähnt, verschiedene Fähigkeitengrade als Stufen erreicht werden. Diese Stufen beginnen bei Stufe A und können bis Stufe E bzw. F, bedarfsweise auch höher reichen. Dabei sind für jede Stufe fachlich-spezifische Aspekte passend zum Themengebiet relevant und beschrieben. Genauso gehören zu den Stufen eines Themengebiets generische Aspekte, die je nach Ausprägung des Themengebiets relevant sind. In Abbildung 2 unten ist das Konzept der Aspekte in den Themengebieten mit fachlich-spezifischen Aspekten (weiß unterlegt) und generischen Aspekten (grau hinterlegt) dargestellt. Abbildung 2 stellt damit eine angedachte Schablone für die Beschreibung der Themengebiete in den späteren Kapiteln des Dokuments dar. Die Standardisierung über Themengebiete hinweg ist Ziel dieses Reifegradmodells. Zugleich bemüht sich das Reifegradmodell aber im Besonderen die tatsächlichen Begebenheiten – insbesondere in kleineren und mittelständischen Unternehmen – zu berücksichtigen. Diese mittels dieser Beta-Version eingeleitete Fachdiskussion soll, wie zuvor beschrieben, auch dazu dienen, den weiteren Prozess in dieser Beziehung an Marktanforderungen rückzukoppeln. Die Zuordnung der Relevanz der einzelnen Aspekte für die Ausprägungen »Dokument«, »Prozess« und »physisches Objekt« ist in Abbildung 2 ebenfalls enthalten.

Stufe	Inhalte für das Themengebiet je Stufe und je Control (Ein Control pro Zeile)	Prozess	Dokument	physisches Objekt
NULL	Es werden keine spezifischen Anforderungen an das Themengebiet erfüllt.	x	x	x
	Erste, einfache fachliche Inhalte, spezifisch für das Themengebiet, sind evident.	x	x	x
A	Eine Richtlinie zum Themengebiet ist in der Organisation vorhanden und verabschiedet.	x	x	x
	Weitere /weitergehende fachliche Anforderungen an das Themengebiet.	x	x	x
B	Richtlinien und Beschreibungen von Abläufen zum Themengebiet enthalten eine Zuweisung von Rechten und Pflichten (Verantwortlichkeiten). Hier können mehrere, separate Controls, je nach Bedarf in einem Themengebiet, eingeführt werden.	x		
	Eine Erfolgskontrolle zum Themengebiet findet statt.	x		
	Das Themengebiet ist als Prozess in der Organisation verankert bzw. in den Prozessen der Organisation abgebildet	x		
	Die relevanten Stakeholder in der Organisation sind in das Themengebiet eingebunden.	x	x	x

Stufe	Inhalte für das Themengebiet je Stufe und je Control (Ein Control pro Zeile)	Prozess	Dokument	physisches Objekt
	Die relevanten Stakeholder in der Organisation kennen das Themengebiet durch, z. B. Schulung, und die Informationen sind allen relevanten Rollen zugänglich.	x	x	
	Die Dokumentation des Themengebietes besteht und ist vom Management als verbindlich gekennzeichnet.	x		x
	Für das Themengebiet wird eine Ressourcenplanung durchgeführt.	x		x
	Für das Themengebiet werden Ressourcen gemäß Plan bereitgestellt.	x		x
C	Weitere fachliche Anforderungen für das Themengebiet, die besondere Aspekte der Situation des Auftragsverarbeiters berücksichtigen, z. B. im Bereich besonderer SLA-Erfordernisse, State-of-the-Art Technologieeinsatz, usw.	x	x	x
	Eine Verfolgbarkeit von Richtlinien und TOMs in die relevanten Themengebiete ist sichergestellt, z. B. durch Katalogisierung (Tabellenform)	x		x
	Die Dokumentation des Themengebiets steht unter Versions- bzw. Konfigurationsmanagement.	x	x	
	Erfolgskontrolle zum Themengebiet, z. B. regelmäßige Überprüfung der Umsetzung des Themengebiets (Einhaltung von Richtlinien) durch Stichproben, interne Überprüfungen / Audits und Aufzeichnung von Abweichungen zum Themengebiet.	x	x	
	Regelmäßige Informationen des höheren Managements über Abweichungen und Status.	x		
	Ermittlung von Ursachen zu Abweichungen in Abläufen und Problemen in Dokumenten oder Assets in regelmäßigen Abständen.	x		x
	Ursachenbehandlung und -abstellung durch gezielte Verbesserungsmaßnahmen und passende Ressourcenbereitstellung.	x	x	
D	Weitere, gegebenenfalls hochspezifische, fachliche Anforderungen an das Themengebiet.	x	x	x
	Kennzahlen zu Abläufen, z. B. Verletzungen, Schwachstellen, aber auch Erfolge werden im Rahmen eines KVP zielführend eingesetzt.	x		
	Kennzahlen zu Abläufen, z. B. Verletzungen, Schwachstellen, aber auch Erfolge werden erhoben, gespeichert und analysiert.	x		x
	Integration des gesamten Themengebiets in einen internen KVP und ein unternehmensweites Kennzahlensystem (vgl. Kapitel REF)	x		x
E	Weitere, gegebenenfalls hochspezifische, fachliche Anforderungen an das Themengebiet.	x	x	x
F, G, ...	Weitere, gegebenenfalls hochspezifische, fachliche Anforderungen an das Themengebiet, bei denen im Bedarfsfall auch eine weitere Trennung in Stufen sinnvoll ist.	x	x	x

Tabelle 1: Schablone für die Stufen (Fähigkeitsgrade) der Themengebiete des Datenschutz-Reifegradmodells und inhaltliche Definitionen.

3.5 Bindung von Reifegraden und Fähigkeitsgraden

In Abschnitt 3.4 wurde bereits der grundsätzliche Zusammenhang zwischen Fähigkeitsgraden und Reifegraden beschrieben. In diesem Abschnitt sollen in einem experimentellen Stadium die ersten beiden Reifegrade definiert werden. Die Definition dient insbesondere einer Veranschaulichung des Konzepts, stellt aber noch keine konkreten DSR dar.

3.5.1 Datenschutz-Reifegrad 1 – DSR1 (Initial)

Der initiale Datenschutz-Reifegrad DSR1 kann durch jede Organisation praktisch sofort erreicht werden. DSR1 wird genau dann erreicht, wenn eine beliebige Menge von Themengebieten in Stufe NULL oder Stufe A nachgewiesen wird.

Auf DSR1 folgen höhere Reifegrade, die auch Anforderungen an Stufen oberhalb von Stufe NULL beziehungsweise A für eine festgelegte und sinnvolle Menge von Themengebieten festlegt.

3.5.2 Datenschutz-Reifegrad 2 – DSR2

Auf DSR2 werden die in Abbildung 3 dargestellten Themengebiete beispielhaft mit der Anforderung »Stufe B« verknüpft und so als Konstellation für diesen Reifegrad der jeweiligen Organisation festgelegt. Relevant für DSR2 sind dabei die durch den blauen Bereich zu Stufe B markierten Themengebiete. Alle weiteren Themengebiete spielen für DSR2 keine relevante Rolle. Dennoch ist es möglich, und in bestimmten Konstellationen auch vorstellbar und sinnvoll, wenn einzelne der anderen Themengebiete, die nicht DSR2 zugeordnet sind, im Bedarfsfall auf Stufe B oder auch höher betrieben werden. Genauso kann es sinnvoll sein, in DSR2 auch dem DSR2 zugeordnete Themengebiete auf höheren Stufen als Stufe B zu betreiben. Auf die Festlegung eines nach außen sichtbaren Datenschutz-Reifegrad hätte dies jedoch keinen Einfluss.

DSR-Themengebiete	Stufen		
	NULL	A	B
Themengebiet 1	DSR1: Initial		DSR2: <Name>
Themengebiet 2			
Themengebiet 3			
Themengebiet 4			
Themengebiet 5			
Themengebiet 6			
Themengebiet 7			
Themengebiet 8			
Themengebiet 9			
Themengebiet 10			
Themengebiet 11			
Themengebiet 12			
Themengebiet 13			
Themengebiet 14			
Themengebiet 15			
Themengebiet 16			
Themengebiet 17			
Themengebiet 18			
Themengebiet 19			
Themengebiet 20			
Themengebiet 21			
Themengebiet 22			
Themengebiet 23			
Themengebiet 24			
Themengebiet 25			
Themengebiet 26			
Themengebiet 27			
Themengebiet 28			

Tabelle 2: Themengebiete des DSR2 (<Name>) im Datenschutz-Reifegradmodell.

3.5.3 Höhere Datenschutz-Reifegrade

Höhere Datenschutz-Reifegrade können in zukünftigen Versionen des Datenschutz-Reifegradmodells definiert und zur Verfügung gestellt werden.

Die Umsetzung des DSR2 und der Scope der in den DSR2 eingebunden Themengebiete soll zunächst in der Praxis validiert und gegebenenfalls angepasst werden. Dabei kann eine Anpassung, eine Erweiterung, oder eine Verschlankung der im Scope DSR2 eingebundenen Menge von Themengebieten bedeuten.

Die Zuordnung von Themengebieten bestimmter Stufen (Fähigkeitsgraden) zu Reifegraden (DSR) ist in Abbildung 4 unten schematisch auch über DSR2 hinaus schematisch dargestellt.

DSR-Themengebiete	Stufen								
	NULL	A	B	C	D	E	F	G	H
Themengebiet 1	DSR1: Initial		DSR2: <Name>	DSR3: <Name>	DSR4: <Name>
Themengebiet 2									
Themengebiet 3									
Themengebiet 4									
Themengebiet 5									
Themengebiet 6									
Themengebiet 7									
Themengebiet 8									
Themengebiet 9									
Themengebiet 10									
Themengebiet 11									
Themengebiet 12									
Themengebiet 13									
Themengebiet 14									
Themengebiet 15									
Themengebiet 16									
Themengebiet 17									
Themengebiet 18									
Themengebiet 19									
Themengebiet 20									
Themengebiet 21									
Themengebiet 22									
Themengebiet 23									
Themengebiet 24									
Themengebiet 25									
Themengebiet 26									
Themengebiet 27									
Themengebiet 28									

Tabelle 3: Zuordnung von Themengebieten und Fähigkeitsgraden (Stufen) zu Reifegraden (DSR).

4

Begriffe

Abkürzung	Bedeutung
DS-GVO	Datenschutz Grundverordnung
TOM	technisch-organisatorische Maßnahmen
DSFA	Datenschutzfolgenabschätzung
SWA	Schwellwertanalyse
Asset	Werte im Sinne der Informationssicherheit (Informationswerte, Hard- oder Software-Werte)
Stakeholder	die jeweiligen Personen oder relevanten Fachbereiche im Unternehmen / in der Organisation, die für die wirksame Umsetzung einer Maßnahme relevant sind oder über deren Existenz oder Art der Umsetzung informiert werden müssen. Im Falle einer Auftragsverarbeitung können dies ggf. auch bestimmte Ansprechpartnerinnen und Ansprechpartner beim Verantwortlichen / Auftraggeber sein. Dabei handelt es sich in der Regel nicht um betroffene Personen im Sinne des Art. 4 DS-GVO.

5 Datenschutzleitlinie

5.1 Vorgaben der Leitung für den Datenschutz

5.1.1 Datenschutzleitlinie und Überprüfung

Frage: Ist in der Organisation eine Datenschutzleitlinie von der Leitung verabschiedet und veröffentlicht worden und werden die definierten Datenschutzgrundsätze überprüft und die Ergebnisse der Überprüfung analysiert?

Aspekt	Stufe	Argument
0	NULL	In der Organisation existiert keine Datenschutzleitlinie oder sie ist nicht verabschiedet oder sie ist nicht veröffentlicht.
1	A	Eine Datenschutzleitlinie ist von der Organisation verabschiedet und veröffentlicht worden.
2	A	In der Datenschutzleitlinie sind mindestens die folgenden Aspekte geregelt: a) Geschäftsstrategie b) Relevante Regulierung, Gesetzgebung und Verträge c) Die aktuelle und zukünftig mögliche Bedrohungen des Datenschutzes im Allgemeinen
3	B	Die Datenschutzleitlinie sollte folgende Aussagen treffen: a) Definition des Datenschutzes in der Organisation, Ziele und leitende Prinzipien, um alle Aktivitäten mit Bezug zum Datenschutz zu leiten b) Zuordnung und Festlegung allgemeiner und spezifischer Verantwortlichkeiten im Datenschutz und im Datenschutzmanagement zu bestimmten Rollen, z. B. Datenschutzbeauftragter, Datenschutzkoordinator, Leitung, Vorgesetzter etc. c) Nennung der aktuellen und zukünftig möglichen, beziehungsweise vorhersagbaren unternehmensspezifischen Datenschutz-Risiken
4	C	Die in der Datenschutzleitlinie geforderten Maßnahmen sind in die Geschäftsprozesse der Organisation eingearbeitet.
5	C	Die Inhalte der Datenschutzleitlinie werden in der Organisation gelebt.
6	C	Die vorher beschriebenen Maßnahmen und Prozesse sind dokumentiert und die Dokumentation ist den relevanten Stakeholdern zugänglich und bekannt.
7	D	Die Datenschutzleitlinie ist ein gelenktes Dokument.
18	D	Die Umsetzung und Einhaltung der Datenschutzleitlinie wird konsequent verfolgt, z. B. durch regelmäßige interne Überprüfungen oder Audits. Auch wird regelmäßig untersucht, ob die Datenschutzleitlinie für die Organisation angemessen ist und wird den aktuellen Rahmenbedingungen angepasst.

Aspekt	Stufe	Argument
19	D	Das Management der jeweils höheren Ebene wird regelmäßig über Schwachstellen der Datenschutzleitlinie informiert und entscheidet über weitere Eskalationen.
20	D	Verletzungen und Schwachstellen der Datenschutzleitlinie werden klassifiziert, bewertet und aufgezeichnet.
21	D	Zu den Aufzeichnungen werden in regelmäßigen und geplanten Abständen Analysen durchgeführt und mögliche Ursachen ermittelt.
22	E	Identifizierte Ursachen für Verletzungen und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an der Datenschutzleitlinie selbst und den Geschäftsprozessen, inkl. Rollen und Verantwortlichkeiten, ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.
24	E	Kennzahlen zu Verletzungen und Schwachstellen werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt.
25	E	Die Verbesserung der Datenschutzleitlinie ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.

6 Organisation des Datenschutzes

Die Regelungen zum Datenschutz unterliegen regelmäßigen Änderungen. Dies erfordert eine geregelte Organisation, um die Anforderung zu erfüllen und die Änderungen lenken und steuern zu können.

6.1 Datenschutzmanagement- system

In der DIN ISO/IEC 27000:2011-07 wird als Managementsystem ein »Rahmenwerk von Leitlinien [...], Verfahren [...], Richtlinien [...] und den zugehörigen Ressourcen, um die Ziele der Institution zu erreichen« genannt. Das Datenschutzmanagement basiert auf einem PDCA-Zyklus.

Ein Managementsystem besteht aus den allgemeinen Management-Mechanismen und den fachspezifischen Prozessen. Die allgemeinen Management-Mechanismen können etwa das Anforderungsmanagement, das Risikomanagement oder auch Audits sein. Sie werden im Managementrahmenwerk beschrieben. Die fachspezifischen Prozesse sind zum Beispiel die Datenschutzprozesse.

Frage: Betreibt die Organisation ein Datenschutzmanagementsystem (DSMS)?

Aspekt	Stufe	Argument
0	Null	Es wird kein Datenschutzmanagementsystem (DSMS) betrieben und es befindet sich auch keines im Aufbau. Unabhängig von Anforderungen an die Erfüllung des Datenschutzes wurden noch keine Planungen zum Aufbau eines DSMS vorgenommen
1	A	Erforderliche Leitlinien (z. B. die Datenschutzleitlinie aus 5.1.1), Verfahren und Richtlinien zum Betrieb eines DSMS sind von der Organisation verabschiedet und veröffentlicht.
2	B	Für die erforderlichen Leitlinien, Verfahren und Richtlinien sind die Rechte und Pflichten zugewiesen worden.
3	C	Die erforderlichen Leitlinien, Verfahren und Richtlinien sind in die Geschäftsprozesse der Organisation eingearbeitet.
4	C	Für die Umsetzung der erforderlichen Leitlinien, Verfahren und Richtlinien sind notwendigen Ressourcen identifiziert und geplant worden.
5	C	Für die Umsetzung der erforderlichen Leitlinien, Verfahren und Richtlinien sind die notwendigen Ressourcen bewilligt worden und werden planmäßig freigegeben.
6	C	Die relevanten Stakeholder in der Organisation sind in das Themengebiet eingebunden.
7	C	Die erforderlichen Leitlinien, Verfahren und Richtlinien werden den betroffenen Stakeholdern zugänglich gemacht und sind bekannt, z. B. geschult.
8	C	Die erforderlichen Leitlinien, Verfahren und Richtlinien sind dokumentiert und müssen verbindlich umgesetzt werden.
9	C	Besondere Anforderungen sind identifiziert und berücksichtigt worden (z. B. Berufsrecht).

Aspekt	Stufe	Argument
10	D	Die erforderlichen Leitlinien, Verfahren und Richtlinien stehen in der Organisation unter Konfigurationsmanagement. (Konfigurationsmanagement bedeutet hier, dass alle Anforderungen an das DSMS bekannt und verifiziert sind, sowie Änderungen am DSMS erkannt und dokumentiert werden.)
11	D	Die Umsetzung und Einhaltung der erforderlichen Leitlinien, Verfahren und Richtlinien wird konsequent verfolgt, z. B. durch regelmäßige interne Überprüfungen oder Audits. Alle vorher genannten Aspekte müssen erfüllt sein.
12	D	Das Management der jeweils höheren Ebene wird regelmäßig über Verletzungen und Schwachstellen der Leitlinien, Verfahren und Richtlinien informiert und entscheidet über weitere Eskalationen.
13	D	Verletzungen und Schwachstellen der Leitlinien, Verfahren und Richtlinien werden klassifiziert, bewertet und aufgezeichnet.
14	D	Zu den Aufzeichnungen werden in regelmäßigen und geplanten Abständen Analysen durchgeführt und mögliche Ursachen ermittelt.
15	E	Identifizierte Ursachen für Verletzungen und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an den Leitlinien, Verfahren und Richtlinien selbst und den Geschäftsprozessen inkl. Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.
16	E	Kennzahlen zu Verletzungen und Schwachstellen werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt. Eine mögliche Kennzahl kann die »Summe der in diesem Jahr durchgeführten Datenschutzaudits« / »Summe der in diesem Jahr geplanten Datenschutzaudits« sein.
17	E	Die Verbesserung der Leitlinien, Verfahren und Richtlinien ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.
18	E	Ein ausgereiftes Kennzahlensystem ist identifiziert, eingeführt und wird betrieben und ausgewertet.

6.1.1 Datenschutz-Risikoanalyse nach Art. 32 DS-GVO

Frage: Betreibt die Organisation einen Prozess zur Datenschutz-Risikoanalyse nach Art. 32 DS-GVO?

Aspekt	Stufe	Argument
0	Null	In der Organisation existiert kein Prozess zur Datenschutz-Risikoanalyse nach Art. 32 DS-GVO oder er ist nicht verabschiedet oder er ist nicht veröffentlicht.
1	A	Eine Richtlinie zur Datenschutz-Risikoanalyse nach Art. 32 DS-GVO ist von der Organisation verabschiedet und veröffentlicht.

Aspekt	Stufe	Argument
2	B	Für den Prozess der Datenschutz-Risikoanalyse nach Art. 32 DS-GVO sind die Rechte und Pflichten zugewiesen worden.
3	C	Die erforderlichen Regelungen zur Datenschutz-Risikoanalyse nach Art. 32 DS-GVO sind in die Geschäftsprozesse der Organisation eingearbeitet.
4	C	Für die Umsetzung der erforderlichen Richtlinien sind die notwendigen Ressourcen identifiziert und geplant worden.
5	C	Für die Umsetzung der erforderlichen Richtlinien sind die notwendigen Ressourcen bewilligt worden und werden planmäßig freigegeben.
6	C	Die relevanten Stakeholder in der Organisation sind in das Themengebiet eingebunden.
7	C	Die erforderlichen Regelungen zur Datenschutz-Risikoanalyse nach Art. 32 DS-GVO werden den betroffenen Stakeholdern zugänglich gemacht und sind bekannt, z. B. durch Schulungen.
8	C	Die erforderlichen Richtlinien sind dokumentiert und müssen verbindlich umgesetzt werden.
9	C	Besondere Anforderungen sind identifiziert und berücksichtigt worden.
10	D	Die erforderlichen Richtlinien stehen in der Organisation unter Konfigurationsmanagement.
11	D	Die Umsetzung und Einhaltung des Prozesses der Datenschutz-Risikoanalyse nach Art. 32 DS-GVO wird konsequent verfolgt, z. B. durch regelmäßige interne Überprüfungen oder Audits.
12	D	Das Management der jeweils höheren Ebene wird regelmäßig über Verletzungen und Schwachstellen der erforderlichen Richtlinien informiert und entscheidet über weitere Eskalationen.
13	D	Verletzungen und Schwachstellen der erforderlichen Richtlinien werden klassifiziert, bewertet und aufgezeichnet.
14	D	Zu den Aufzeichnungen werden in regelmäßigen und geplanten Abständen Analysen durchgeführt und mögliche Ursachen ermittelt.
15	E	Identifizierte Ursachen für Verletzungen und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an den Richtlinien zur Datenschutz-Risikoanalyse nach Art. 32 DS-GVO selbst und den Geschäftsprozessen inkl. Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.
16	E	Kennzahlen zu Verletzungen und Schwachstellen werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt. Eine mögliche Kennzahl kann die »Summe der Verarbeitungstätigkeiten, für die eine Risikoanalyse durchgeführt werden muss« / »Summe der Verarbeitungstätigkeiten« sein.
17	E	Die Verbesserung der Richtlinien zur Datenschutz-Risikoanalyse nach Art. 32 DS-GVO ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.
18	E	Ein ausgereiftes Kennzahlensystem ist identifiziert, eingeführt und wird betrieben und ausgewertet.

6.2 Datenschutzprozesse

6.2.1 Datenschutzrechtliche Zulässigkeitsprüfung

Frage: Betreibt die Organisation einen Prozess zur Prüfung der datenschutzrechtlichen Zulässigkeit?

Aspekt	Stufe	Argument
0	Null	In der Organisation existiert kein Prozess zur datenschutzrechtlichen Zulässigkeitsprüfung oder er ist nicht verabschiedet oder er ist nicht veröffentlicht.
1	A	Eine Richtlinie zur datenschutzrechtlichen Zulässigkeitsprüfung ist von der Organisation verabschiedet und veröffentlicht. Diese umfasst insbesondere Aspekte zu <ul style="list-style-type: none"> ▪ Einhaltung der Datenschutzgrundsätze ▪ Rechtmäßigkeit der Verarbeitung ▪ Transparenz bei der Datenverarbeitung ▪ Sicherheit in der Verarbeitung (s. hierzu Abschnitt 6.1.1 und die weiteren Maßnahmen) ▪ Datenschutzkonforme Auftragsverarbeitung (s. hierzu Kapitel 15) ▪ Übermittlung an Drittstaaten ▪ Dokumentation der Verarbeitungstätigkeiten (s. hierzu Kapitel 8)
2	B	Für den Prozess der datenschutzrechtlichen Zulässigkeitsprüfung sind die Rechte und Pflichten zugewiesen worden.
3	C	Die erforderlichen Regelungen zur datenschutzrechtlichen Zulässigkeitsprüfung sind in die Geschäftsprozesse der Organisation eingearbeitet.
4	C	Für die Umsetzung der erforderlichen Richtlinien sind die notwendigen Ressourcen identifiziert und geplant worden.
5	C	Für die Umsetzung der erforderlichen Richtlinien sind die notwendigen Ressourcen bewilligt worden und werden planmäßig freigegeben.
6	C	Die relevanten Stakeholder in der Organisation sind in das Themengebiet eingebunden
7	C	Die erforderlichen Regelungen zur datenschutzrechtlichen Zulässigkeitsprüfung werden den betroffenen Stakeholdern zugänglich gemacht und sind bekannt, z. B. durch Schulungen.
8	C	Die erforderlichen Richtlinien sind dokumentiert und müssen verbindlich umgesetzt werden.
9	C	Besondere Anforderungen sind identifiziert und berücksichtigt worden.
10	D	Die erforderlichen Richtlinien stehen in der Organisation unter Konfigurationsmanagement.
11	D	Die Umsetzung und Einhaltung des Prozesses der Prüfung der datenschutzrechtlichen Zulässigkeit wird konsequent verfolgt, z. B. durch regelmäßige interne Überprüfungen oder Audits.

Aspekt	Stufe	Argument
12	D	Das Management der jeweils höheren Ebene wird regelmäßig über Verletzungen und Schwachstellen der erforderlichen Richtlinien informiert und entscheidet über weitere Eskalationen.
13	D	Verletzungen und Schwachstellen der erforderlichen Richtlinien werden klassifiziert, bewertet und aufgezeichnet.
14	D	Zu den Aufzeichnungen werden in regelmäßigen und geplanten Abständen Analysen durchgeführt und mögliche Ursachen ermittelt.
15	E	Identifizierte Ursachen für Verletzungen und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an den Richtlinien zur datenschutzrechtlichen Zulässigkeitsprüfung selbst und den Geschäftsprozessen inkl. Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.
16	E	Kennzahlen zu Verletzungen und Schwachstellen werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt. Eine mögliche Kennzahl kann sein, die »Summe der durchgeführten Zulässigkeitsprüfungen« / »Summe der durchzuführenden Zulässigkeitsprüfungen«.
17	E	Die Verbesserung der Richtlinien zur datenschutzrechtlichen Zulässigkeitsprüfung ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.
18	E	Ein ausgereiftes Kennzahlensystem ist identifiziert, eingeführt und wird betrieben und ausgewertet.

6.2.2 Gewährleistung der Betroffenenrechte

Das vorliegende Reifegradmodell ist für die Beschreibung der technischen und organisatorischen Maßnahmen im Auftragsverhältnis zwischen dem Auftragnehmer und dem Auftraggeber konzipiert worden. Dementsprechend sind zwingende Aspekte, die in einer Richtlinie zu Betroffenenrechten beschrieben werden müssen, die Schnittstellen zwischen Auftragnehmer und Auftraggeber, die Anforderungen an die Kommunikation zwischen den beiden Parteien und die Verantwortlichkeiten.

Frage: Betreibt die Organisation einen Prozess zur Gewährleistung der Betroffenenrechte?

Aspekt	Stufe	Argument
0	Null	In der Organisation existiert kein Prozess zur Gewährleistung der Betroffenenrechte oder er ist nicht verabschiedet oder er ist nicht veröffentlicht (Basisanforderung)
1	A	Eine Richtlinie zur Gewährleistung der Betroffenenrechte ist von der Organisation verabschiedet und veröffentlicht.
2	B	Für den Prozess der Gewährleistung der Betroffenenrechte sind die Rechte und Pflichten zugewiesen worden.
3	C	Die erforderlichen Regelungen zur Gewährleistung der Betroffenenrechte sind in die Geschäftsprozesse der Organisation eingearbeitet.

Aspekt	Stufe	Argument
4	C	Für die Umsetzung der erforderlichen Richtlinien sind notwendigen Ressourcen identifiziert und geplant worden.
5	C	Für die Umsetzung der erforderlichen Richtlinien sind die notwendigen Ressourcen bewilligt worden und werden planmäßig freigegeben.
6	C	Die relevanten Stakeholder in der Organisation sind in das Themengebiet eingebunden.
7	C	Die erforderlichen Regelungen zur Gewährleistung der Betroffenenrechte werden den betroffenen Stakeholdern zugänglich gemacht und sind bekannt, z. B. durch Schulung.
8	C	Die erforderlichen Richtlinien sind dokumentiert und müssen verbindlich umgesetzt werden.
9	C	Besondere Anforderungen sind identifiziert und berücksichtigt worden.
10	D	Die erforderlichen Richtlinien stehen in der Organisation unter Konfigurationsmanagement.
11	D	Die Umsetzung und Einhaltung des Prozesses der Gewährleistung der Betroffenenrechte wird konsequent verfolgt, z. B. durch regelmäßige interne Überprüfungen oder Audits.
12	D	Das Management der jeweils höheren Ebene wird regelmäßig über Verletzungen und Schwachstellen der erforderlichen Richtlinien informiert und entscheidet über weitere Eskalationen.
13	D	Verletzungen und Schwachstellen der erforderlichen Richtlinien werden klassifiziert, bewertet und aufgezeichnet.
14	D	Zu den Aufzeichnungen werden in regelmäßigen und geplanten Abständen Analysen durchgeführt und mögliche Ursachen ermittelt.
15	E	Identifizierte Ursachen für Verletzungen und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an den Richtlinien zur Gewährleistung der Betroffenenrechte selbst und den Geschäftsprozessen inkl. Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.
16	E	Kennzahlen zu Verletzungen und Schwachstellen werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt. Eine mögliche Kennzahl kann sein, die »Summe der Datenschutzbeschwerden wegen Auskünften pro Jahr« / »Anzahl aller Auskunftsanfragen pro Jahr«.
17	E	Die Verbesserung der Richtlinien zur Gewährleistung der Betroffenenrechte ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.
18	E	Ein ausgereiftes Kennzahlensystem ist identifiziert, eingeführt und wird betrieben und ausgewertet.

6.2.3 Meldung von Datenschutzvorfällen

Frage: Betreibt die Organisation einen Prozess zur Meldung von Datenschutzvorfällen?

Aspekt	Stufe	Argument
0	Null	In der Organisation existiert kein Prozess zur Meldung von Datenschutzvorfällen oder er ist nicht verabschiedet oder veröffentlicht.
1	A	<p>Eine Richtlinie zur Meldung von Datenschutzvorfällen ist von der Organisation verabschiedet und veröffentlicht. Diese umfasst insbesondere:</p> <ul style="list-style-type: none"> ▪ Kennzeichnung und leichte Identifizierbarkeit entsprechender Meldungen ▪ Zeithorizonte zur angemessenen Eskalation, besonders unter Berücksichtigung der gesetzlichen Meldepflichten ▪ Integration und Wechselwirkung mit dem Prozess der IT-Sicherheitsvorfälle ▪ Risikoanalysen ▪ allgemeine Kriterien zur Ermittlung erforderlicher Notifikationen
2	B	Für den Prozess der Meldung von Datenschutzvorfällen sind die Rechte und Pflichten zugewiesen worden.
3	C	Die erforderlichen Regelungen zur Meldung von Datenschutzvorfällen sind in die Geschäftsprozesse der Organisation eingearbeitet.
4	C	Für die Umsetzung der erforderlichen Richtlinien sind notwendigen Ressourcen identifiziert und geplant worden.
5	C	Für die Umsetzung der erforderlichen Richtlinien sind die notwendigen Ressourcen bewilligt worden und werden planmäßig freigegeben.
6	C	Die relevanten Stakeholder in der Organisation sind in das Themengebiet eingebunden.
7	C	Die erforderlichen Regelungen zur Meldung von Datenschutzvorfällen werden den betroffenen Stakeholdern zugänglich gemacht und sind bekannt, z. B. durch Schulung.
8	C	Die erforderlichen Richtlinien sind dokumentiert und müssen verbindlich umgesetzt werden.
9	C	Besondere Anforderungen sind identifiziert und berücksichtigt worden.
10	D	Die erforderlichen Richtlinien stehen in der Organisation unter Konfigurationsmanagement.
11	D	Die Umsetzung und Einhaltung des Prozesses der Meldung von Datenschutzvorfällen wird konsequent verfolgt, z. B. durch regelmäßige interne Überprüfungen oder Audits.
12	D	Das Management der jeweils höheren Ebene wird regelmäßig über Verletzungen und Schwachstellen der erforderlichen Richtlinien informiert und entscheidet über weitere Eskalationen.
13	D	Verletzungen und Schwachstellen der erforderlichen Richtlinien werden klassifiziert, bewertet und aufgezeichnet.
14	D	Zu den Aufzeichnungen werden in regelmäßigen und geplanten Abständen Analysen durchgeführt und mögliche Ursachen ermittelt.

Aspekt	Stufe	Argument
15	E	Identifizierte Ursachen für Verletzungen und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an den Richtlinien zur Meldung von Datenschutzvorfällen selbst und den Geschäftsprozessen inkl. Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.
16	E	Kennzahlen zu Verletzungen und Schwachstellen werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt. Eine Kennzahl zu Datenschutzverletzungen kann die »Anzahl der Datenschutzvorfälle pro Jahr« / »Anzahl der Mitarbeitenden, die mit personenbezogenen Daten arbeiten pro Jahr« sein.
17	E	Die Verbesserung der Richtlinien zur Meldung von Datenschutzvorfällen ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.
18	E	Ein ausgereiftes Kennzahlensystem ist identifiziert, eingeführt und wird betrieben und ausgewertet.

6.3 Datenschutzprozesse

6.3.1 Verzeichnis der Verarbeitungstätigkeiten (VVT)

Frage: Wie ausgereift ist das Verzeichnis von Verarbeitungstätigkeiten der Organisation?

Aspekt	Stufe	Argument
0	Null	Es existiert kein Verzeichnis von Verarbeitungstätigkeiten (VVT).
1	A	Das vorhandene VVT enthält die meisten der nach Art. 30 DS-GVO geforderten Angaben.
2	A	Es existiert ein VVT, in dem noch nicht alle Verarbeitungstätigkeiten vollständig erfasst wurden, jedoch mit sämtlichen in Art. 30 geforderten Angaben.
3	A	Das VVT wird sporadisch auf Aktualität geprüft.
4	B	Die Eigentümer der Verarbeitungstätigkeiten sind für deren Aktualisierung im VVT verantwortlich.
5	B	Die Aktualisierung der Verarbeitungstätigkeiten ist in einem Prozess definiert und wird in der Organisation gelebt.
6	B	Bereits im Entwicklungsstadium werden Verarbeitungstätigkeiten mit entsprechender Kennzeichnung in das VVT aufgenommen, sodass bereits vor der Einführung neuer Verarbeitungstätigkeiten und neuer Produkte die Auswirkungen auf den Datenschutz (Privacy by Design und Privacy by Default) geprüft werden können.
7	C	Die Aktualisierung der Verarbeitungstätigkeiten wird von den Eigentümern der Verarbeitungstätigkeiten dem VVT-Verantwortlichen selbstständig gemeldet.
8	C	Das VVT wird zentral in einem Datenschutzmanagementsystem verwaltet. Dies beinhaltet nicht nur die Inventarisierung neuer oder geänderter Verarbeitungstätigkeiten, sondern auch die Information über den Entfall gelöschter, oder nicht mehr anwendbarer Verarbeitungstätigkeiten.
9	D	Es gibt Kennzahlen, wie die Anzahl der dokumentierten und/oder meldepflichtigen Vorfälle auf deren Basis die Wirksamkeit der beschriebenen Verarbeitungstätigkeiten in Bezug auf die Erfüllung der Datenschutzziele gemessen wird.
10	E	Basierend auf den Ergebnissen aus Aspekt 9, werden Verbesserungen der Verarbeitungstätigkeiten erarbeitet und umgesetzt.

6.3.2 Datenschutzfolgenabschätzung

Frage: Ist die Organisation für die Notwendigkeit von Datenschutzfolgenabschätzungen sensibilisiert und werden diese anlassbezogen durchgeführt?

Aspekt	Stufe	Argument
0	Null	Datenschutzfolgenabschätzungen (DSFA) werden nicht durchgeführt.
1	A	DSFA werden sporadisch bei Bedarf durchgeführt.
2	A	Es existiert ein, für die Organisation angemessener, Prozess zur Feststellung der Notwendigkeit einer DSFA (Schwellenwertanalyse).
3	B	Es existiert ein Prozess zur Durchführung einer DSFA.
4	C	Die Prozesse zur Feststellung und Durchführung einer DSFA sind dokumentierter Bestandteil des Datenschutzmanagementsystems.
5	C	Es existiert ein definierter Prozess, nach dem DSFA regelmäßig durchzuführen und zu überprüfen sind. Darin sind insbesondere geregelt: <ul style="list-style-type: none"> ▪ Verantwortlichkeiten im Prozess ▪ Risikomethodik ▪ Kommunikations- und Berichtswege.
6	D	Es gibt Kennzahlen, wie die Anzahl der dokumentierten und/oder meldepflichtigen Vorfälle, und auf deren Basis die Wirksamkeit der DSFA in Bezug auf die Erfüllung der Datenschutzziele, gemessen wird.
7	D	Diese werden gemessen, um die Effektivität und Wirksamkeit der DSFA zu beschreiben.
8	E	Basierend aus den Ergebnissen aus Aspekt 7, werden Verbesserungen des DSFA-Prozesses erarbeitet und umgesetzt.

6.3.3 Berichte an Leitung

Frage: Wird der obersten Leitung über das Thema Datenschutz berichtet?

Aspekt	Stufe	Argument
0	Null	Es werden keine Berichte zum Thema Datenschutz erstellt.
1	A	Unregelmäßig, zumeist anlassbezogen nach konkreten Vorfällen, werden Berichte zum Datenschutz erstellt und der obersten Leitung vorgelegt.
2	B	Die oberste Leitung wird regelmäßig durch den Datenschutzbeauftragten zum Thema Datenschutz unterrichtet. Ein entsprechender, für die Organisation angemessener Prozess ist dokumentiert.
3	C	Es finden mindestens einmal jährlich Management-Reviews innerhalb des DS-Managementsystems statt. Als Teil dieser Reviews gibt die oberste Leitung Rückmeldung zu den Berichten und zum Datenschutz.
4	D	Es sind für das Thema Datenschutz Kennzahlen definiert. Diese werden gemessen und im Rahmen des Berichtswesens gemeldet, um die Effektivität und Wirksamkeit der Umsetzung zu beschreiben. Die Kennzahlen leiten sich aus den übergeordneten Unternehmenszielen ab und erlauben gleichzeitig die Ableitung von Zielen zur Verbesserung und Steigerung der Effektivität hinsichtlich des Themenkomplexes Datenschutz. Das beschriebene Verfahren zur Definition und Messung sowie zum Berichtswesen und Management-Review ist in der Organisation dokumentiert.
5	E	Es werden zusätzlich projektbezogen datenschutzrelevante Kennzahlen erhoben und berichtet.

7

Personalsicherheit

Grundsätzlich gelten die Anforderungen an die Überprüfung, Verpflichtung und Schulung sowohl für interne Beschäftigte (fest angestellte Mitarbeitende, Auszubildende, Aushilfen etc.) als auch für externe Mitarbeitende (Freiberuflerinnen und Freiberufler, Beraterinnen und Berater, Auftragnehmerinnen und Auftragnehmer etc.). Wenn in diesem Kapitel allgemein von »Beschäftigten« gesprochen wird, sind damit die internen Beschäftigten gemeint. Leiharbeiter im Rahmen der Arbeitnehmerüberlassung werden den Beschäftigten hinzugezählt. Für externe Mitarbeitende müssen, sofern diese nicht explizit aufgeführt werden, ggf. vergleichbare Regelungen existieren beziehungsweise adäquate vertragliche Regelungen existieren.

7.1 Vor der Beschäftigung

7.1.1 Sicherheitsüberprüfung

Frage: Wie wird die Zuverlässigkeit der Beschäftigten (aller Beschäftigungsformen) überprüft?

Aspekt	Stufe	Argument
0	NULL	Es findet keine Überprüfung neuer Beschäftigter, die ggf. Zugriffs- und Bearbeitungsrechte auf personenbezogene Daten erhalten werden, statt.
1	A	Neue Beschäftigte werden anhand eines amtlichen Lichtbildausweises legitimiert.
2	A	Bei neuen Beschäftigten wird der Lebenslauf auf Plausibilität und nicht erklärbare Lücken geprüft. Nicht erklärbare Lücken führen zu einer intensiveren Überprüfung der Personalie.
3	B	Die fachliche Qualifikation wird überprüft.
4	B	Abschluss-, Fortbildungs- und Arbeitszeugnisse werden im Original eingesehen und ggfs. die Echtheit überprüft.
5	B	Akademische Titel werden überprüft.
6	B	Potenzielle neue Beschäftigte werden vor Einstellung gegen EU-Sanktionslisten geprüft. Personen, die auf EU-Sanktionslisten stehen, werden nicht beschäftigt.
7	C	Alle vorgenannten Überprüfungen werden revisionssicher dokumentiert.
8	C	Es existiert ein Prozess, der sicherstellt, dass für jede zu besetzende Stelle vorab definiert ist, ob eine Hintergrundüberprüfung erforderlich ist und wenn ja, in welcher Form (z. B. schriftliche Erklärung über bestehende einschlägige Vorstrafen, laufende Ermittlungsverfahren, Bonität, polizeiliches Führungszeugnis, erweitertes pol. Führungszeugnis, Sicherheitsüberprüfung) diese erfolgt.
9	C	Neue Beschäftigte werden im zulässigen Rahmen um Angaben für die Informationseinholung bei früheren Arbeitgebern gebeten.
10	D	Der Prozess und die Durchführung der Überprüfung der Beschäftigten vor Einstellung wird regelmäßig kontrolliert.
11	E	Referenzeinholung bei früheren Arbeitgebern im rechtlich zulässigen Rahmen wird eingeholt.

7.1.2 Beschäftigungs- und Vertragsbedingungen

Frage: Wie werden Beschäftigte vertraglich zur Einhaltung der datenschutzrechtlichen Anforderungen verpflichtet? Welche internen Regelungen existieren?

Aspekt	Stufe	Argument
0	NULL	Es gibt keine schriftlichen Regelungen und Vorgaben für die Beschäftigten bzgl. Datenschutz.
1	A	Alle Beschäftigten sind vertraglich allgemein zur Einhaltung rechtlicher Vorgaben und zur Vertraulichkeit verpflichtet.
2	B	Alle Beschäftigten sind gemäß Artikel 29 DS-GVO schriftlich verpflichtet, personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen zu verarbeiten.
3	C	Es existieren verbindliche Datenschutzvorgaben (z. B. Richtlinien, Arbeitsanweisungen) im Unternehmen, die die Anforderungen an die Beschäftigten klar und eindeutig regeln und für alle Beschäftigten verbindlich gelten.
4	D	Die Verantwortung für die Einhaltung der datenschutzrechtlichen und internen Anforderungen ist klar geregelt und über die gesamte Aufbauorganisation festgelegt.

7.2 Während der Beschäftigung

7.2.1 Verantwortlichkeiten der Leitung

Frage: Verlangt die Leitung von allen Beschäftigten und Auftragnehmern, dass sie die Datenschutzanforderungen im Einklang mit den eingeführten Richtlinien und Verfahren der Organisation umsetzen?

Aspekt	Stufe	Argument
0	NULL	Es existieren keine besonderen Verantwortlichkeitsregelungen für das Management und die Führungskräfte.
1	A	Es gibt eine allgemeine Verantwortlichkeitszuordnung für das obere Management, die die Einhaltung und Umsetzung der datenschutzrechtlichen Anforderungen regelt.
2	A	Es gibt eine allgemeine Verantwortlichkeitszuordnung für alle Management- und Führungsebenen, die die Einhaltung und Umsetzung der datenschutzrechtlichen Anforderungen regelt.
3	B	<p>Es gibt klar geregelte, aufgaben- oder rollenbasierte Verantwortlichkeitszuordnungen auf allen Management- und Führungsebenen, die die Einhaltung und Umsetzung der datenschutzrechtlichen Anforderungen regeln. Insbesondere ist geregelt, wer sicherzustellen hat, dass Beschäftigte und externe Mitarbeitende</p> <ul style="list-style-type: none"> ▪ vor der Erteilung von Zugriffs- und Zugangsrechten zu personenbezogenen Daten ordnungsgemäß über ihre Aufgaben und Verantwortlichkeiten im Bereich des Datenschutzes informiert werden ▪ mit den existierenden Vorgaben vertraut gemacht werden, um die Erwartungen an die Einhaltung und Umsetzung von Datenschutzvorgaben an ihre Rolle zu klären ▪ diese regelmäßig im Umgang mit personenbezogenen Daten und den Sicherheitsvorgaben geschult und sensibilisiert werden
4	C	Das Management wird regelmäßig hinsichtlich ihrer Verantwortung für die Einhaltung und Umsetzung von Datenschutzvorgaben sensibilisiert.
5	D	Festgestellte Abweichungen aus Audits und Vorfällen werden gemäß den Verantwortlichkeitsregelungen den entsprechenden Führungskräften zugeordnet und die Behebung von Abweichungen werden konsequent eingefordert und nachgehalten.
6	E	Es wird regelmäßig überprüft und dokumentiert, dass sich alle Manager und Führungskräfte ihrer Verantwortung bewusst sind und diese wahrnehmen (z. B. im Rahmen von Feedback-Runden oder durch regelmäßige Teilnahme in internen Datenschutz-Gremien).

7.2.2 Datenschutzbewusstsein, -ausbildung und -schulung

Frage: Werden die Beschäftigten regelmäßig zu den datenschutzrechtlichen Anforderungen geschult und über Pflichten aufgeklärt?

Aspekt	Stufe	Argument
0	NULL	Es sind keine Maßnahmen umgesetzt.
1	A	Neue Beschäftigte werden bei Eintritt schriftlich informiert (z. B. Merkblätter, Aushändigung von Präsentationsunterlagen)
2	A	Neue Beschäftigte müssen innerhalb eines definierten Zeitraums nach Eintritt eine Online- / Präsenzsulung oder Unterweisung durch den Vorgesetzten absolvieren.
3	A	Der Datenschutzbeauftragte hat eine fundierte Datenschutz-Grundlagenausbildung (oder vergleichbare Berufsausbildung) abgeschlossen und bildet sich anlassbezogen fort.
4	B	Neue Beschäftigte müssen innerhalb eines definierten Zeitraums nach Eintritt oder bei wichtigen Änderungen eine Online- oder Präsenzsulung absolvieren.
5	B	Die Teilnahme an Schulungen und Unterweisungen wird dokumentiert und überprüft.
6	B	Der Datenschutzbeauftragte bildet sich regelmäßig fort (mind. regelmäßiges Studium einer Fachzeitschrift (z. B. ZD, RDV, DuD) und entweder Besuch eines Seminars p. a. oder regelmäßige Teilnahme an überbetrieblichen Erfahrungsaustauschen).
7	B	Beschäftigte müssen regelmäßig innerhalb eines definierten Zeitraums von max. zwei (2) Jahren eine Online- / Präsenzsulung oder Unterweisung durch den Vorgesetzten absolvieren.
8	B	Beschäftigte müssen regelmäßig innerhalb eines definierten Zeitraums von max. zwei (2) Jahren eine Online- / Präsenzsulung durch einen datenschutzfachlich qualifizierten Trainer absolvieren.
9	B	Schulungen schließen teilweise mit einer Erfolgskontrolle ab.
10	C	Schulungen schließen immer mit einer Erfolgskontrolle ab.
11	C	Sofern feste Ansprechpartner für Datenschutzfragen in Fachbereichen (z. B. Datenschutzkoordinatoren oder -champions) eingesetzt werden, erhalten diese eine qualifizierte Datenschutz-Grundlagenschulung.
12	C	Beschäftigte in Bereichen mit höheren Datenschutzanforderungen (z. B. mit höheren Risikobewertungen) müssen regelmäßig innerhalb eines definierten Zeitraums von max. einem (1) Jahr eine Online- / Präsenzsulung durch einen datenschutzfachlich qualifizierten Trainer absolvieren.
13	C	Es gibt weitere Sensibilisierungsmaßnahmen / Kampagnen, die sporadisch durchgeführt werden (z. B. Newsletter, Informationsstände, Live-Hacking-Demos etc.).
14	D	Es gibt weitere Sensibilisierungsmaßnahmen / Kampagnen, die regelmäßig durchgeführt werden.
15	E	Für die Planung und Umsetzung von Sensibilisierungsmaßnahmen sind Kennzahlen definiert (z. B. die Teilnahme an Awareness-Angeboten oder die Anzahl an Rückmeldungen zu bestimmten Maßnahmen), die regelmäßig ausgewertet werden und soweit erforderlich auch Korrekturmaßnahmen abgeleitet und umgesetzt werden.

7.2.3 Maßregelungsprozess

Frage: Ist ein Maßregelungsprozess eingerichtet, um Sanktionen gegen Beschäftigte und externe Mitarbeitende zu ergreifen, die einen Datenschutzverstoß begangen haben?

Aspekt	Stufe	Argument
0	NULL	Es existiert kein Maßregelungsprozess.
1	A	Es existiert ein allgemeines Verständnis im Unternehmen, dass Verletzungen der Richtlinien zum Datenschutz genauso wie andere Pflichtverletzungen eines Beschäftigten arbeitsrechtlich gemäßregelt werden können.
2	A	Es gibt einen Prozess mit klar geregelten Verantwortlichkeiten, wie Pflichtverletzungen eines Beschäftigten gemäßregelt werden.
3	B	Es gibt einen Prozess mit klar geregelten Verantwortlichkeiten, wie Pflichtverletzungen von externen Mitarbeitenden gemäßregelt werden.
4	B	Es existieren klare Regelungen im Unternehmen, dass Verletzungen der Richtlinien zum Datenschutz eines Beschäftigten arbeitsrechtlich, die eines externen Mitarbeitenden zivilrechtlich gemäßregelt werden können – genauso wie andere Pflichtverletzungen.
5	C	Der Maßregelungsprozess ist dokumentiert.
6	C	Im Rahmen der Behandlung von Datenschutzverletzungen ist festgelegt, dass der Maßregelungsprozess angewandt werden muss.
7	C	Für Beschäftigte (Arbeitnehmer als auch für externe Mitarbeitende) ist die Form der Maßregelung in Abhängigkeit der Schwere des Verstoßes verbindlich beschrieben.
8	C	Im Rahmen der Nachbereitung von Datenschutzvorfällen findet eine Überprüfung der Einhaltung des Maßregelungsprozesses statt.
9	D	Die Wirksamkeit des Maßregelungsprozesses wird regelmäßig überprüft.
10	D	Innerhalb des Maßregelungsprozesses findet eine Prüfung statt, ob die Verletzung der Datenschutzvorgaben entsprechend Kapitel 16.3 als Datenschutzvorfall gemeldet und behandelt wurden.
11	E	Im Maßregelungsprozess werden zur kontinuierlichen Verbesserung des Prozesses Kennzahlen erhoben und ausgewertet.

7.3 Beendigung und Änderung der Beschäftigung

7.3.1 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung

Frage: Sind die Verantwortlichkeiten und Pflichten im Bereich des Datenschutzes, die auch über die Beschäftigung / Beauftragung hinaus bestehen bleiben, festgelegt und dem Beschäftigten oder Auftragnehmer bekannt?

Aspekt	Stufe	Argument
0	NULL	Es existieren keine Regelungen hinsichtlich Verantwortlichkeiten und Pflichten von Beschäftigten und Auftragnehmern, die über die Beschäftigung hinaus bestehen bleiben.
1	A	Es existieren allgemeine Vertraulichkeitsregelungen mit Beschäftigten, die über die Beschäftigung hinaus bestehen bleiben.
2	A	Es existieren Vertraulichkeitsvereinbarungen mit Auftragnehmern, die über die Beauftragung hinaus bestehen bleiben.
3	A	Die Verträge mit Beschäftigten und Auftragnehmern enthalten klare Regelungen hinsichtlich der Verantwortlichkeiten und Pflichten der Beschäftigten und Auftragnehmern, die über die Beschäftigung beziehungsweise Beauftragung hinaus bestehen bleiben. Insbesondere sind Regelungen enthalten <ul style="list-style-type: none"> ▪ zur Wahrung der Vertraulichkeit (Datengeheimnis) ▪ zum Verbot der Nutzung von Daten zur Schädigung anderer Personen oder zur Verschaffung persönlicher Vorteile ▪ zum Verbot der Nutzung von evtl. noch bestehenden Zugängen oder Zugriffsrechten auf Daten und / oder Systeme des Unternehmens, von Kunden oder Partnern
4	B	Es ist vertraglich mit Dienstleistern verankert, dass deren Beschäftigte auch über die Beschäftigung hinaus die datenschutzrechtlichen Vorgaben zu wahren haben.
5	B	Es existiert ein Prozess zur Risikobewertung beim Ausscheiden von Beschäftigten (auch Externen), der das Risiko für die Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten, das von dem jeweiligen Beschäftigten ausgeht, bewertet und im Falle hoher Risiken mitigierende Maßnahmen auslöst (bspw. Freistellung, unverzüglicher Entzug von Berechtigungen etc.)
6	B	Es ist sichergestellt, dass relevante Personen (ggf. auch Kunden, Lieferanten und Partner) spätestens nach dem Ausscheiden von Beschäftigten oder Auftragnehmern darüber informiert werden, um u. a. der unrechtmäßigen oder versehentlichen Offenlegung von personenbezogenen Daten vorzubeugen.
7	C	Ausscheidende Beschäftigte und Auftragnehmer werden persönlich (z. B. im Rahmen eines Offboarding-Gesprächs) auf die weiterhin bestehenden Verantwortungen und Pflichten sowie mögliche Konsequenzen bei Verstößen explizit hingewiesen.

Aspekt	Stufe	Argument
8	D	Der Prozess zur Risikobewertung beim Ausscheiden von Beschäftigten und eingeleitete Maßnahmen werden regelmäßig auf Wirksamkeit geprüft.
9	E	Im Prozess zur Risikobewertung bei Ausscheiden von Beschäftigten werden zur kontinuierlichen Verbesserung des Prozesses Kennzahlen erhoben und ausgewertet.

8 Verwaltung der Werte

8.1 Verantwortlichkeit für Werte

8.1.1 Führung eines Verarbeitungsverzeichnisses

Frage: Wird in der Organisation für jedes Verfahren automatisierter Verarbeitung, in dem personenbezogene Daten verarbeitet werden, sichergestellt, dass die in der Europäischen Datenschutzgrundverordnung (Artikel 30 DS-GVO) geforderten Angaben in die internen Verzeichnisse der Verarbeitungstätigkeiten (VVT) aufgenommen werden und allen nutzenden Legal-Einheiten zur Verfügung stehen?

Aspekt	Stufe	Argument
0	Null	In der Organisation gibt es keine Vorgaben, ein Verarbeitungsverzeichnis für die Auftragsverarbeitung zu führen. Es ist kein Verzeichnis vorhanden.
1	A	<p>Die Geschäftsführung oder ein berechtigter Vertreter der Organisation hat Vorgaben verabschiedet und veröffentlicht, in denen das Führen eines Verarbeitungsverzeichnisses für die Auftragsverarbeitung vorgeschrieben ist.</p> <ul style="list-style-type: none"> Es existieren Vorgaben, z. B. in einer Datenschutzrichtlinie, in denen das Führen eines Verfahrenszeichnisses vorgegeben wird. Es gibt jedoch keine Vorgaben zu Form und Inhalt. <p>Es sind keine weiteren Vorgaben, z. B. die Zuordnung von Verantwortlichen, definiert.</p>
2	A	<p>Das Verarbeitungsverzeichnis wird geführt, Aktualität, Vollständigkeit und gesetzeskonformes Format sind nicht sichergestellt.</p> <ul style="list-style-type: none"> In der Organisation werden an einer oder mehreren Stellen Listen über die vorhandenen IT-Systeme und der darauf befindlichen Anwendungen geführt Die Listen sind nicht zentral geführt und enthalten nicht alle Angaben nach Artikel 30 <p>Es gibt keinen Nachweis oder eine Methode, welche die vollständige Auflistung aller eingesetzter Verfahren bei der Auftragsverarbeitung belegt oder sicherstellt.</p>
3	B	<p>Für den Inhalt des Verarbeitungsverzeichnisses gibt es verbindliche inhaltliche Vorgaben, die den Regelungen der DS-GVO entsprechen. Das Verzeichnis enthält mindestens die folgenden Angaben gemäß Artikel 30:</p> <ul style="list-style-type: none"> den Namen und die Kontaktdaten des Auftragsverarbeitenden oder der Auftragsverarbeitenden und jedes Verantwortlichen, in dessen Auftrag der Verarbeitende tätig ist, sowie gegebenenfalls der Vertretenden und eines etwaigen Datenschutzbeauftragten die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentation geeigneter Garantien <p>wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.</p>

Aspekt	Stufe	Argument
4	B	<p>Das Anlegen / Aktualisieren des Verarbeitungsverzeichnisses ist in den Prozessen vor Aufnahme der Auftragsverarbeitung vorgesehen.</p> <ul style="list-style-type: none"> Es ist durch geeignete Prozesse des Auftragsverarbeiters sichergestellt, dass ein Eintrag in ein zentrales Verzeichnis vor Aufnahme der Auftragsverarbeitung erfolgt <p>Es sind Verantwortliche benannt, die ein solches Verzeichnis führen.</p>
5	C	<p>Interne Prozesse stellen sicher, dass Verantwortliche benannt werden, die die Führung des Verzeichnisses, die Schulung und die Prozessdokumentation sicherstellen und kontrollieren.</p> <ul style="list-style-type: none"> In der Organisation ist klar geregelt, wer für das Führen eines Verarbeitungsverzeichnisses zuständig ist Der für das Verarbeitungsverzeichnis Verantwortliche ist auch für die zeitnahe Erstellung einer Kopie / Auszug für die Aufsichtsbehörden zuständig <p>Der für das Verarbeitungsverzeichnis Verantwortliche ergreift Maßnahmen, die die Verfügbarkeit des Verarbeitungsverzeichnisses sicherstellen.</p>
6	D	<p>In den Prozessen der Organisation sind zwingende Schritte (Stoppunkte, Gates, Freigaben,...) vorgesehen, die vor Aufnahme der Auftragsdatenverarbeitung sicherstellen, dass die Eintragung der Verarbeitung in ein Verzeichnis erfolgt.</p>
7	D	<p>Es finden regelmäßige Schulungen bzgl. Änderungen der gesetzlichen Anforderungen sowie in der Anwendung / Pflege der verwendeten IT / Tools zum Führen des Verarbeitungsverzeichnisses statt.</p>
8	E	<p>In der Organisation sind Maßnahmen zur Kontrolle (regelmäßige Audits) der Wirksamkeit umgesetzt:</p> <ul style="list-style-type: none"> Es finden regelmäßige Kontrollen statt, ob alle Auftragsverarbeitungen vollständig und richtig im Verzeichnis abgebildet sind Es wird kontrolliert, ob alle beendeten Auftragsverarbeitungen aus dem Verzeichnis gelöscht wurden <p>Abgeleitet aus den Kontrollergebnissen werden Korrekturmaßnahmen durchgeführt, um die zuvor definierten Datenschutzziele eines vollständigen und formal richtigen Verarbeitungsverzeichnisses sicherzustellen.</p>
9	F	<p>In der Organisation werden Maßnahmen zur Optimierung und Effizienzsteigerung genutzt, mit dem Ziel:</p> <ul style="list-style-type: none"> Die Prozessqualität zum Anlegen, Pflegen und Löschen von Einträgen zu optimieren Effizienzsteigernde Ablageformen (z. B. Überführung in eine elektronische Form, automatische Datenübernahme aus ERP-Systemen, ...) Verbesserung der Prozessabläufe
10	F	<p>Der Auftragsverarbeiter kann der Aufsichtsbehörde auf Verlangen das Verzeichnis in einem gängigen Format zur Verfügung stellen.</p> <ul style="list-style-type: none"> Die Organisation kann auf Verlangen eine Kopie oder einen Auszug aus dem Verarbeitungsverzeichnis vorlegen Der Auszug / Kopie können zeitnah erstellt werden <p>Wird das Verzeichnis elektronisch geführt, kann der Auszug / Kopie auch in einem gängigen elektronischen Dateiformat erfolgen.</p>

8.1.2 Inventarisierung von Werten

Frage: Gibt es in der Organisation Regelungen (Inventarisierung, Verantwortlichkeiten, Gebrauch, Rückgabe) zum Umgang mit Werten (Personenbezogene Daten, Hard- und Software, Zutrittsmittel)?

Aspekt	Stufe	Argument
0	Null	Die Geschäftsführung der Organisation hat keine Leitlinie oder Vorgaben verabschiedet und veröffentlicht, in der die Inventarisierung von datenschutzrelevanten Werten geregelt wird.
1	A	Es gibt in verschiedenen Bereichen der Organisation Inventarlisten. Es bestehen aber keine verbindlichen Regelungen und Vorgaben, wie speziell datenschutzrelevante Werte zu inventarisieren sind.
2	B	In der Organisation existieren Vorgaben zur Inventarisierung von Werten. Es ist geregelt, wie Werte erfasst, ausgegeben und zurückgenommen werden. Die Vorgaben sind umgesetzt und werden in der Organisation angewendet.
3	C	Es ist für jeden datenschutzrelevanten Wert oder Wertegruppe (z. B. mobile Datenträger) durch einen fest installierten Prozess sichergestellt, dass dieser erfasst, sein Gebrauch beschrieben und seine Rückgabe/Vernichtung zwingend erfolgt. Für den gesamten Prozess sind Verantwortliche benannt und die richtige Anwendung wurde durch Informationen und Schulungen bekannt gemacht.
4	C	Der Inventarisierungsprozess wird in der gesamten Organisation eingesetzt und die Umsetzung wird kontrolliert. Für besonders sensible Werte, insbesondere kritische Daten und Betriebsmittel, wurden spezielle Prozesse und Maßnahmen eingeführt. Der Prozess stellt zudem sicher, dass die Inventarlisten stets aktuell sind.
5	D	Die Prozessdurchführung wird in geeigneter Weise revisionssicher dokumentiert und ständig auf ihre Wirksamkeit kontrolliert. Es existieren Projekte und Prozesse mit eigenen Ressourcen (Personal und Budget), mit dem Ziel Prozessschwächen zu identifizieren und notwendige Anpassungen der Vorgaben umzusetzen.

8.2 Informationsklassifizierung

8.2.1 Klassifizierung personenbezogener Daten

Frage: Gibt es in der Organisation verbindliche Vorgaben für eine gesonderte Klassifizierung personenbezogener Daten, einer Kennzeichnung solcher und Vorgaben zur Handhabung (Erhebung, Verarbeitung, Weitergabe, Löschung)?

Aspekt	Stufe	Argument
0	Null	Die Geschäftsführung der Organisation hat keine verbindlichen Vorgaben zur Klassifizierung verabschiedet und veröffentlicht.
1	A	In der Organisation bestehen Vorgaben zur Klassifizierung personenbezogener Daten, indem verschiedene Schutzbedarfsklassen definiert sind und <ul style="list-style-type: none"> ▪ in den Vorgaben zur Klassifikation wird zwischen Informationsschutz und Datenschutz unterschieden wird ▪ in denen die Einordnung personenbezogener Daten in eine bestimmte Klasse vorgegeben wird
2	B	In der Organisation bestehen verbindliche Vorgaben zur Klassifizierung personenbezogener Daten, in denen verschiedene Schutzklassen definiert sind und <ul style="list-style-type: none"> ▪ in der verbindlich geregelt wird, wie eine Kennzeichnung der Daten umzusetzen ist und ▪ in der Handlungsanweisungen zum Umgang der Daten entsprechend ihrer Einstufung vorgegeben sind
3	C	Die schriftlichen Vorgaben zur Klassifizierung von Daten sind in allen Prozessen der Organisation verbindlich umgesetzt. Die Prozesse sind dokumentiert und die Einhaltung wird protokolliert. Es sind Verantwortlichkeiten/Rollen definiert, Informationen und Schulungen für die Nutzer stehen zur Verfügung.
4	D	Die Vorgaben zur Klassifizierung von Daten werden regelmäßig auf ihre Wirksamkeit hin überprüft. Die Einhaltung der Vorgaben zu Einordnung, Kennzeichnung, Speicherung und revisionssicherer Dokumentation wird regelmäßig überprüft. Es finden Kontrollen und Audits statt.
5	E	Die Prozessdurchführung wird ständig auf ihre Wirksamkeit kontrolliert. Es existieren Projekte und Prozesse mit eigenen Ressourcen (Personal und Budget) mit dem Ziel, Prozessschwächen zu identifizieren und notwendige Anpassungen der Vorgaben umzusetzen.

8.3 Handhabung von Datenträgern

8.3.1 Handhabung und Transport von Datenträgern

Frage: Gibt es in ihrer Organisation verbindliche Vorgaben für die Handhabung und den Transport von Datenträgern in Abhängigkeit der Schutzwürdigkeit (Klassifikation) der darauf gespeicherten personenbezogenen Daten?

Aspekt	Stufe	Argument
0	NULL	In der Organisation existieren keine verbindlichen Vorgaben zu Handhabung und Transport von Datenträgern oder es sind keine Vorgaben verabschiedet oder veröffentlicht.
1	A	Vorgaben zu Handhabung und Transport von Datenträgern sind von der Organisation erlassen und veröffentlicht worden.
2	A	Die Inhalte der Vorgaben zu Handhabung und Transport von Datenträgern werden in der Organisation gelebt.
3	B	In den Vorgaben zur Handhabung und Transport von Datenträgern sind mindestens die folgenden Aspekte geregelt: <ul style="list-style-type: none"> ▪ Ablage von Datenträgern abhängig von Schutzbedarf und Schutzklasse ▪ Versand von Datenträgern abhängig von Schutzbedarf und Schutzklasse ▪ Vernichtung von Datenträgern abhängig von Schutzbedarf und Schutzklasse
4	C	Die Umsetzung und Einhaltung der Richtlinie zu Handhabung und Transport von Datenträgern wird konsequent verfolgt, z. B. durch regelmäßige interne Überprüfungen oder Audits. Zugriffsrechte auf Datenträger für verschiedene Rollen sind abhängig von Schutzbedarf und Schutzklasse umgesetzt.
5	C	Eine Information der betroffenen Mitarbeitenden hat stattgefunden, z. B. Schulung, schriftliche Vorgaben.
6	D	Die Protokollierung von Handhabung / Transport von Datenträgern wird regelmäßig geprüft. Abweichungen von den Vorgaben werden dokumentiert und relevante Vorfälle werden, auf Basis vorgegebener Entscheidungskriterien, dem Management gemeldet.
7	D	Der Umfang und die Art und Weise der Protokollierungen werden in regelmäßigen und geplanten Abständen analysiert und möglicher Änderungsbedarf ermittelt.
8	E	Identifizierte Änderungsbedarfe (vgl. Aspekt 10) werden im Rahmen eines eingeführten Prozesses behandelt. Dabei können sich Änderungen an der Richtlinie zu Handhabung und Transport von Datenträgern selbst und den Geschäftsprozessen inkl. Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für den Prozess werden hinreichende Ressourcen bereitgestellt.
9	F	Kennzahlen zu Verletzungen und Schwachstellen werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt.

Aspekt	Stufe	Argument
10	F	Die Verbesserung der Richtlinie zur Handhabung und Transport von Datenträgern ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.
11	B	Der Umgang mit Datenträgern wird revisionssicher protokolliert (z. B. Versand- und Vernichtungsprotokolle)
12	C	Die Vorgaben zu Handhabung und Transport von Datenträgern sind in Form einer verbindlichen Richtlinie verabschiedet und veröffentlicht worden. Die in der Richtlinie geforderten Maßnahmen sind in die Geschäftsprozesse der Organisation eingearbeitet.

8.3.2 Löschung und Entsorgung von Datenträgern

Frage: Gibt es in der Organisation verbindliche Vorgaben für die Löschung / Entsorgung von Datenträgern in Abhängigkeit der Schutzwürdigkeit (Klassifikation) der darauf gespeicherten personenbezogenen Daten?

Aspekt	Stufe	Argument
0	Null	In der Organisation gibt es keine verbindlichen Vorgaben zu Löschung und Entsorgung von Datenträgern.
1	A	In der Organisation gibt es einheitliche und allgemeingültige Vorgaben für die Löschung und die Entsorgung von Datenträgern und es existieren Handlungsanweisungen.
2	B	Die Vorgaben zur Löschung und Entsorgung berücksichtigen den Schutzbedarf personenbezogener Daten anhand ihrer Klassifizierung bei der Auswahl der Entsorgungs- oder Löschmethode.
3	C	In der Organisation bestehen Prozesse zur Löschung und Entsorgung von Datenträgern in denen abhängig vom Schutzbedarf vorgegeben wird, wie Daten zu Löschen sind und wie Datenträger, auf den personenbezogene Daten gespeichert sind oder waren, entsorgt werden müssen. Diese Vorschriften kommen in der gesamten Organisation und bei beauftragten Entsorgungsunternehmen zur Anwendung und basieren auf anerkannten Standards.
4	D	Die Prozessdurchführung wird in geeigneter Weise revisionssicher dokumentiert.
5	E	Die Prozessdurchführung wird in geeigneter Weise ständig auf ihre Wirksamkeit hin kontrolliert.
6	F	Es existieren Projekte und Prozesse mit eigenen Ressourcen (Personal und Budget) mit dem Ziel Prozessschwächen zu identifizieren und notwendige Anpassungen der Vorgaben umzusetzen.

9 Zugangssteuerung

9.1 Geschäftsanforderungen an die Zugangssteuerung

9.1.1 Allgemein

Frage: Inwieweit sind Regelungen zum Zugang zu IT-Systemen und Applikationen in der Organisation vorhanden?

Aspekt	Stufe	Argument
0	Null	In der Organisation existiert keine Richtlinie zur Zugriffskontrolle oder sie ist nicht verabschiedet oder nicht veröffentlicht.
1	A	Eine Richtlinie zur Zugriffskontrolle ist von der Organisation verabschiedet und veröffentlicht worden.
2	A	In der Richtlinie zur Zugriffskontrolle sind die folgenden Aspekte geregelt: <ul style="list-style-type: none"> Die eingesetzten Verfahren zur Benutzerauthentifikation gelten als sicher und entsprechen dem aktuellen Stand der Technik Es wird ein Genehmigungsverfahren zur Bestimmung der Personen eingesetzt, denen der Zugang zu IT-Systemen der Organisation gewährt wird Minimalprinzip und Funktionstrennung sind in Applikationen umgesetzt.
3	B	In der Richtlinie zur Zugriffskontrolle sind auch die folgenden Aspekte geregelt: <ul style="list-style-type: none"> Die Anforderungen an die Verfahren zur Authentifizierung und Datenübermittlung richten sich nach der Sensibilität der personenbezogenen Daten (bei hohem Risiko für die Rechte und Freiheiten der betroffenen Personen kann sogar eine Zwei-Faktor-Authentifikation erforderlich sein) Der Einsatz starker Passwörter wird vorgeschrieben Regelmäßiger Passwortwechsel, spätestens nach drei Monaten In den Applikationen gibt es ebenfalls ein Rollen- und Rechtekonzept und es ist umgesetzt.
4	B	In der Richtlinie zur Zugriffskontrolle sind Rechte und Pflichten klar zugewiesen.
5	C	Die Umsetzung und Einhaltung der Richtlinie zur Zugriffskontrolle wird konsequent verfolgt, z. B. durch regelmäßige interne Überprüfungen oder Audits.
6	C	Die in der Richtlinie zur Zugriffskontrolle geforderten Aspekte sind in die Geschäftsprozesse der Organisation eingearbeitet.
7	C	Die relevanten Stakeholder in der Organisation sind in das Themengebiet eingebunden.
8	C	Die relevanten Stakeholder in der Organisation kennen das Themengebiet durch, z. B. Schulung, und die erforderlichen Informationen sind allen relevanten Rollen zugänglich.
9	C	Die vorgenannten Aspekte sind dokumentiert, z. B. integriert in Prozesse.
10	D	Die Dokumentation ist den betroffenen Stakeholdern und Rollen zugänglich und bekannt.
11	D	Die Richtlinie zur Zugriffskontrolle steht in der Organisation unter Konfigurationsmanagement.

Aspekt	Stufe	Argument
12	D	Die Umsetzung und Einhaltung der Richtlinie zur Zugriffskontrolle wird konsequent verfolgt, z. B. durch regelmäßige interne Stichproben.
13	D	Verletzungen und Schwachstellen der Richtlinie zur Zugriffskontrolle werden klassifiziert, bewertet und aufgezeichnet.
14	D	Das Management der jeweils höheren Ebene wird regelmäßig über Verletzungen und Schwachstellen der Richtlinie zur Zugriffskontrolle informiert und entscheidet über weitere Eskalationen.
15	D	Es werden in regelmäßigen und geplanten Abständen Analysen zu den Aufzeichnungen der Richtlinie zur Zugriffskontrolle durchgeführt und mögliche Ursachen ermittelt.
16	D	Identifizierte Ursachen für Verletzungen und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an der Richtlinie zur Zugriffskontrolle selbst und den Geschäftsprozessen inkl. Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.
17	E	Kennzahlen zu Verletzungen und Schwachstellen der Richtlinie zur Zugriffskontrolle werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt.
18	E	Die Verbesserung der Richtlinie zur Zugriffskontrolle ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.

9.1.2 Leitlinie zur Zugangskontrolle

Frage: Wie ist in der Organisation der Zugang zu IT-Systemen geregelt?

Aspekt	Stufe	Argument
0	Null	In der Organisation existieren keine Regelungen zur Zugangskontrolle oder sie sind nicht verabschiedet oder nicht veröffentlicht.
1	A	Regelungen zur Zugangskontrolle sind von der Organisation verabschiedet und veröffentlicht.
2	B	Folgende Inhalte zur Zugangskontrolle müssen geregelt sein: <ul style="list-style-type: none"> ▪ Identifikation der Anforderungen an die Zugangsrechte ▪ die Beantragung und Entziehung von Zugangsrechten und das Genehmigungsverfahren ▪ die regelmäßige Überprüfung von Zugangsrechten ▪ der Umgang mit Administrationszugängen ▪ zu welchen Netzwerken und -diensten Zugang gewährt wird ▪ Anforderung an die Zugangssicherung (z. B. VPN, Benutzerauthentifizierung) ▪ Netzwerküberwachung
3	B	Für die Regelungen zur Zugangskontrolle sind die Rechte und Pflichten zugewiesen worden.
4	C	Die erforderlichen Regelungen für die Zugangskontrolle sind in die Geschäftsprozesse der Organisation eingearbeitet.

Aspekt	Stufe	Argument
5	C	Für die Umsetzung der Regelungen zur Zugangskontrolle sind notwendigen Ressourcen identifiziert und geplant.
6	C	Für die Umsetzung der Regelungen zur Zugangskontrolle sind die notwendigen Ressourcen bewilligt worden und werden planmäßig freigegeben.
7	C	Die relevanten Stakeholder in der Organisation sind in das Themengebiet eingebunden.
8	C	Die erforderlichen Regelungen für die Zugangskontrolle werden den betroffenen Stakeholdern zugänglich gemacht und sind bekannt, z. B. geschult.
9	C	Die Leitlinie zur Zugangskontrolle sind dokumentiert und müssen verbindlich umgesetzt werden.
10	C	Besondere Anforderungen sind identifiziert und berücksichtigt worden (zum Beispiel spezielle vertragliche Regelungen mit Auftraggebern).
11	D	Die erforderlichen Regelungen stehen in der Organisation unter Konfigurationsmanagement.
12	D	Die Umsetzung und Einhaltung der Leitlinie zur Zugangskontrolle wird konsequent verfolgt, z. B. durch regelmäßige interne Überprüfungen oder Audits. Alle vorher genannten Aspekte müssen erfüllt sein.
13	D	Das Management der jeweils höheren Ebene und der Auftraggeber wird regelmäßig über Verletzungen und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen informiert und entscheidet über weitere Eskalationen.
14	D	Datenschutzvorfälle und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen werden klassifiziert, bewertet und aufgezeichnet.
15	D	Zu den Aufzeichnungen werden in regelmäßigen und geplanten Abständen Analysen durchgeführt und mögliche Ursachen ermittelt.
16	E	Identifizierte Ursachen für Verletzungen und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an der Leitlinie zur Zugangskontrolle selbst und den Geschäftsprozessen inkl. Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.
17	E	Kennzahlen zur Leitlinie zur Zugangskontrolle werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt.
18	E	Die Verbesserung der Leitlinie zur Zugangskontrolle ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.
19	E	Ein ausgereiftes Kennzahlensystem ist identifiziert, eingeführt und wird betrieben und ausgewertet.

9.2 Verfahren und Verwaltung von Rechten und Zugängen

9.2.1 An- und Abmeldeverfahren und Zugangsbereitstellung

Frage: Wie ist der Umgang mit Anmeldedaten und Accounts in der Organisation geregelt?

Aspekt	Stufe	Argument
0	Null	In der Organisation existieren keine Regelungen zum An- und Abmeldeverfahren und zur Zugangsbereitstellung oder sie sind nicht verabschiedet oder nicht veröffentlicht.
1	A	Regelungen zum An- und Abmeldeverfahren und zur Zugangsbereitstellung sind von der Organisation verabschiedet und veröffentlicht.
2	B	<p>Folgende Inhalte zum An- und Abmeldeverfahren und zur Zugangsbereitstellung müssen geregelt sein:</p> <ul style="list-style-type: none"> ▪ Eindeutige Benutzernamen, Gruppenzugänge nur in Ausnahmefällen, bei der Datenverarbeitung sensibler Daten muss die Nutzung der Gruppenzugänge nachvollziehbar sein ▪ Regelungen für Rechteverwaltung beim Abteilungswechsel ▪ Account-Löschung bei Ausscheiden ▪ Sperrung von Accounts von Dritten (Dienstleistern) nach Aufgabenerfüllung ▪ Keine Weitergabe von Accounts ▪ Verfahren zur Account-Einrichtung und -Löschung ▪ Sichere Zustellung von Anmeldeinformationen ▪ Alle Accounts sind dokumentiert ▪ Maßnahmen gegen Brute-Force-Angriffe wurden getroffen ▪ Alle Rechte zu den Accounts werden regelmäßig überprüft
3	B	Für die Regelungen zum An- und Abmeldeverfahren und zur Zugangsbereitstellung sind die Rechte und Pflichten zugewiesen worden. Die rechtebeantragende Person und die genehmigende Person sind nicht personenidentisch (Segregation of Duties). Bei der rechtebeantragenden Person und der genehmigenden Person gibt es jeweils keinen Interessenkonflikt.
4	C	Die erforderlichen Regelungen zum An- und Abmeldeverfahren und zur Zugangsbereitstellung sind in die Geschäftsprozesse der Organisation eingearbeitet (zum Beispiel in die Richtlinie »Joiner-Mover-Leaver«).
5	C	Für die Umsetzung der Regelungen zum An- und Abmeldeverfahren und zur Zugangsbereitstellung sind notwendigen Ressourcen identifiziert und geplant worden.
6	C	Für die Umsetzung der Regelungen zum An- und Abmeldeverfahren und zur Zugangsbereitstellung sind die notwendigen Ressourcen bewilligt worden und werden planmäßig freigegeben.
7	C	Die relevanten Stakeholder in der Organisation sind in das Themengebiet eingebunden

Aspekt	Stufe	Argument
8	C	Die erforderlichen Regelungen zum An- und Abmeldeverfahren und zur Zugangsbereitstellung werden den betroffenen Stakeholdern zugänglich gemacht und sind bekannt, z. B. geschult.
9	C	Die Regelungen zum An- und Abmeldeverfahren und zur Zugangsbereitstellung sind dokumentiert und müssen verbindlich umgesetzt werden.
10	C	Besondere Anforderungen sind identifiziert und berücksichtigt worden (z. B. spezielle vertragliche Regelungen mit Auftraggebern).
11	D	Die erforderlichen Regelungen stehen in der Organisation unter Konfigurationsmanagement.
12	D	Die Umsetzung der Regelungen zum An- und Abmeldeverfahren und zur Zugangsbereitstellung wird konsequent verfolgt, z. B. durch regelmäßige interne Überprüfungen oder Audits. Alle vorher genannten Aspekte müssen erfüllt sein.
13	D	Das Management der jeweils höheren Ebene und der Auftraggeber wird regelmäßig über Verletzungen und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen informiert und entscheidet über weitere Eskalationen.
14	D	Datenschutzvorfälle und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen werden klassifiziert, bewertet und aufgezeichnet.
15	D	Zu den Aufzeichnungen zum An- und Abmeldeverfahren und zur Zugangsbereitstellung werden in regelmäßigen und geplanten Abständen Analysen durchgeführt und mögliche Ursachen ermittelt.
16	E	Identifizierte Ursachen für Verletzungen und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an den Regelungen zum An- und Abmeldeverfahren und zur Zugangsbereitstellung selbst und den Geschäftsprozessen inkl. der Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.
17	E	Kennzahlen zu den Regelungen zum An- und Abmeldeverfahren und zur Zugangsbereitstellung werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt.
18	E	Die Verbesserung der Regelungen zum An- und Abmeldeverfahren und zur Zugangsbereitstellung ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.
19	E	Ein ausgereiftes Kennzahlensystem zum An- und Abmeldeverfahren und zur Zugangsbereitstellung ist identifiziert, eingeführt und wird betrieben und ausgewertet.

9.2.2 Umgang mit privilegierten Konten

Frage: Wie ist in der Organisation der Umgang mit privilegierten Konten (Administrationskonten) geregelt?

Aspekt	Stufe	Argument
0	Null	In der Organisation existieren keine Regelungen zum Umgang mit privilegierten Konten (Administrationskonten) oder sie sind nicht verabschiedet oder nicht veröffentlicht.
1	A	Regelungen zum Umgang mit privilegierten Konten (Administrationskonten) sind von der Organisation verabschiedet und veröffentlicht.
2	B	Folgende Inhalte zum Umgang mit privilegierten Konten (Administrationskonten) müssen geregelt sein: <ul style="list-style-type: none"> ▪ die Regelungen aus 9.2.1 sind anzuwenden ▪ Gruppenzugänge sind nicht zulässig ▪ für privilegierte Konten (Administrationskonten) gibt es eigene Genehmigungsverfahren ▪ privilegierte Konten (Administrationskonten) werden ausschließlich für Administrationsarbeit genutzt, andere Arbeiten werden über das Benutzerkonto bearbeitet.
3	B	Für die Regelungen zum Umgang mit privilegierten Konten (Administrationskonten) sind die Rechte und Pflichten zugewiesen worden.
4	C	Die erforderlichen Regelungen zum Umgang mit privilegierten Konten (Administrationskonten) sind in die Geschäftsprozesse der Organisation eingearbeitet.
5	C	Für die Umsetzung der Regelungen zum Umgang mit privilegierten Konten (Administrationskonten) sind notwendigen Ressourcen identifiziert und geplant worden.
6	C	Für die Umsetzung der Regelungen zum Umgang mit privilegierten Konten (Administrationskonten) sind die notwendigen Ressourcen bewilligt worden und werden planmäßig freigegeben.
7	C	Die relevanten Stakeholder in der Organisation sind in das Themengebiet eingebunden.
8	C	Die erforderlichen Regelungen zum Umgang mit privilegierten Konten (Administrationskonten) werden den betroffenen Stakeholdern zugänglich gemacht und sind bekannt, z. B. geschult.
9	C	Die Regelungen zum Umgang mit privilegierten Konten (Administrationskonten) sind dokumentiert und müssen verbindlich umgesetzt werden.
10	C	Besondere Anforderungen sind identifiziert und berücksichtigt worden (z. B. spezielle vertragliche Regelungen mit Auftraggebern).
11	D	Die erforderlichen Regelungen stehen in der Organisation unter Konfigurationsmanagement.
12	D	Die Umsetzung der Regelungen zum Umgang mit privilegierten Konten (Administrationskonten) wird konsequent verfolgt, z. B. durch regelmäßige interne Überprüfungen oder Audits. Alle vorher genannten Aspekte müssen erfüllt sein.
13	D	Das Management der jeweils höheren Ebene und der Auftraggeber wird regelmäßig über Verletzungen und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen informiert und entscheidet über weitere Eskalationen.
14	D	Datenschutzvorfälle und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen werden klassifiziert, bewertet und aufgezeichnet.
15	D	Zu den Aufzeichnungen werden in regelmäßigen und geplanten Abständen Analysen durchgeführt und mögliche Ursachen ermittelt.

Aspekt	Stufe	Argument
16	E	Identifizierte Ursachen für Verletzungen und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an den Regelungen zum Umgang mit privilegierten Konten (Administrationskonten) selbst und den Geschäftsprozessen inkl. Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.
17	E	Kennzahlen zu den Regelungen zum Umgang mit privilegierten Konten (Administrationskonten) werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt.
18	E	Die Verbesserung der Regelungen zum Umgang mit privilegierten Konten (Administrationskonten) ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.
19	E	Ein ausgereiftes Kennzahlensystem zum Umgang mit privilegierten Konten (Administrationskonten) ist identifiziert, eingeführt und wird betrieben und ausgewertet.

9.3 Benutzerverantwortlichkeiten

9.3.1 Regelung zum Umgang mit vertraulichen Anmeldeinformationen

Frage: Wie ist in der Organisation der Umgang mit vertraulichen Anmeldeinformationen geregelt?

Aspekt	Stufe	Argument
0	Null	In der Organisation existieren keine Regelungen zum Umgang mit vertraulichen Anmeldeinformationen oder sie sind nicht verabschiedet oder nicht veröffentlicht.
2	A	Regelungen zum Umgang mit vertraulichen Anmeldeinformationen sind von der Organisation verabschiedet und veröffentlicht.
3	B	Folgende Inhalte zum Umgang mit vertraulichen Anmeldeinformationen müssen geregelt sein: <ul style="list-style-type: none"> ▪ Vertraulichkeit der Anmeldeinformationen (keine Offenbarung gegenüber einer anderen Person) ▪ Notierung von Anmeldeinformationen nur in sicheren Speichern (z. B. verschlüsselte Passwort-Safes, Achtung bei automatisierten Anmeldeverfahren) ▪ Sofortige Änderung von Anmeldeinformationen beim Verdacht der Kompromittierung ▪ Trennung von dienstlichen und privaten Anmeldeinformationen ▪ Nutzung starker Passwörter
4	B	Für die Regelungen zum Umgang mit vertraulichen Anmeldeinformationen sind die Rechte und Pflichten zugewiesen worden.
6	C	Die erforderlichen Regelungen zum Umgang mit vertraulichen Anmeldeinformationen sind in die Geschäftsprozesse der Organisation eingearbeitet.
8	C	Für die Umsetzung der Regelungen zum Umgang mit vertraulichen Anmeldeinformationen sind notwendigen Ressourcen identifiziert und geplant.
9	C	Für die Umsetzung der Regelungen zum Umgang mit vertraulichen Anmeldeinformationen sind die notwendigen Ressourcen bewilligt worden und werden planmäßig freigegeben.
10	C	Die relevanten Stakeholder in der Organisation sind in das Themengebiet eingebunden.
11	C	Die erforderlichen Regelungen zum Umgang mit vertraulichen Anmeldeinformationen werden den betroffenen Stakeholdern zugänglich gemacht und sind bekannt, z. B. geschult.
13	C	Die Regelungen zum Umgang mit vertraulichen Anmeldeinformationen sind dokumentiert und müssen verbindlich umgesetzt werden.
16	C	Besondere Anforderungen sind identifiziert und berücksichtigt worden (zum Beispiel spezielle vertragliche Regelungen mit Auftraggebern).
18	D	Die erforderlichen Regelungen stehen in der Organisation unter Konfigurationsmanagement.

Aspekt	Stufe	Argument
19	D	Die Umsetzung der Regelungen zum Umgang mit vertraulichen Anmeldeinformationen wird konsequent verfolgt, z. B. durch regelmäßige interne Überprüfungen oder Audits. Alle vorher genannten Aspekte müssen erfüllt sein.
20	D	Das Management der jeweils höheren Ebene und der Auftraggeber wird regelmäßig über Verletzungen und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen informiert und entscheidet über weitere Eskalationen.
21	D	Datenschutzvorfälle und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen werden klassifiziert, bewertet und aufgezeichnet.
22	D	Zu den Aufzeichnungen werden in regelmäßigen und geplanten Abständen Analysen durchgeführt und mögliche Ursachen ermittelt.
24	E	Identifizierte Ursachen für Verletzungen und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an den Regelungen zum Umgang mit vertraulichen Anmeldeinformationen selbst und den Geschäftsprozessen inkl. Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.
25	E	Kennzahlen zu den Regelungen zum Umgang mit vertraulichen Anmeldeinformationen werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt.
27	E	Die Verbesserung der Regelungen zum Umgang mit vertraulichen Anmeldeinformationen ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.
28	E	Ein ausgereiftes Kennzahlensystem zum Umgang mit vertraulichen Anmeldeinformationen ist identifiziert, eingeführt und wird betrieben und ausgewertet.

9.4 Zugangssteuerung für Systeme und Anwendungen

9.4.1 Zugriffsbeschränkungen von Nutzenden beim Zugriff von Applikationen und Informationen

Frage: Wie werden die Zugriffe von Nutzenden auf Ebene der Applikationen und der Informationen eingeschränkt?

Aspekt	Stufe	Argument
0	Null	In der Organisation existieren keine Regelungen zur Zugangsbeschränkung von Nutzenden auf Informationen und Applikationen oder sie sind nicht verabschiedet oder veröffentlicht.
1	A	Regelungen zur Zugangsbeschränkung von Nutzenden auf Informationen und Applikationen sind von der Organisation verabschiedet und veröffentlicht.
2	B	Folgende Inhalte zur Zugangsbeschränkung von Nutzenden auf Informationen und Applikationen müssen geregelt sein: <ul style="list-style-type: none"> die Regelungen aus 9.2.1 sind anzuwenden, für Applikationen wurde ein Rollenkonzept erarbeitet und umgesetzt.
3	B	Für die Regelungen zur Zugangsbeschränkung von Nutzenden auf Informationen und Applikationen sind die Rechte und Pflichten zugewiesen worden.
4	C	Die erforderlichen Regelungen zur Zugangsbeschränkung von Nutzenden auf Informationen und Applikationen sind in die Geschäftsprozesse der Organisation eingearbeitet.
5	C	Für die Umsetzung der Zugangsbeschränkung von Nutzenden auf Informationen und Applikationen sind notwendigen Ressourcen identifiziert und geplant worden.
6	C	Für die Umsetzung der Zugangsbeschränkung von Nutzenden auf Informationen und Applikationen sind die notwendigen Ressourcen bewilligt worden und werden planmäßig freigegeben.
7	C	Die relevanten Stakeholder in der Organisation sind in das Themengebiet eingebunden.
8	C	Die erforderlichen Regelungen zur Zugangsbeschränkung von Nutzenden auf Informationen und Applikationen werden den betroffenen Stakeholdern zugänglich gemacht und sind bekannt, z. B. geschult.
9	C	Die Regelungen zur Zugangsbeschränkung von Nutzenden auf Informationen und Applikationen sind dokumentiert und müssen verbindlich umgesetzt werden.
10	C	Besondere Anforderungen sind identifiziert und berücksichtigt worden (zum Beispiel spezielle vertragliche Regelungen mit Auftraggebern).
11	D	Die erforderlichen Regelungen stehen in der Organisation unter Konfigurationsmanagement.

Aspekt	Stufe	Argument
12	D	Die Umsetzung der Regelungen zur Zugangsbeschränkung von Nutzenden auf Informationen und Applikationen wird konsequent verfolgt, z. B. durch regelmäßige interne Überprüfungen oder Audits. Alle vorher genannten Aspekte müssen erfüllt sein.
13	D	Das Management der jeweils höheren Ebene und der Auftraggeber wird regelmäßig über Verletzungen und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen informiert und entscheidet über weitere Eskalationen.
14	D	Datenschutzvorfälle und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen werden klassifiziert, bewertet und aufgezeichnet.
15	D	Zu den Aufzeichnungen werden in regelmäßigen und geplanten Abständen Analysen durchgeführt und mögliche Ursachen ermittelt.
16	E	Identifizierte Ursachen für Verletzungen und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an den Regelungen zur Zugangsbeschränkung von Nutzenden auf Informationen und Applikationen selbst und den Geschäftsprozessen inkl. Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.
17	E	Kennzahlen zu den Regelungen zur Zugangsbeschränkung von Nutzenden auf Informationen und Applikationen werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt.
18	E	Die Verbesserung der Regelungen zur Zugangsbeschränkung von Nutzenden auf Informationen und Applikationen ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.
19	E	Ein ausgereiftes Kennzahlensystem zur Zugangsbeschränkung von Nutzenden auf Informationen und Applikationen ist identifiziert, eingeführt und wird betrieben und ausgewertet.

10

Kryptographie

10.1 Regelungen bezüglich kryptographischer Maßnahmen

Frage: Besteht hinreichende Kenntnis zum adäquaten Einsatz kryptographischer Maßnahmen und werden derartige Maßnahmen entsprechend den gesetzlichen Anforderungen, insbesondere dem Risiko der verarbeiteten Daten, eingesetzt?

Aspekt	Stufe	Argument
0	NULL	Es sind keine kryptographischen Maßnahmen implementiert.
1	A	Es wurden grundsätzliche Erwägungen bzgl. des Einsatzes kryptographischer Maßnahmen angestellt.
2	A	Es besteht ein Konzept, welche Maßnahmen zur Anwendung kommen.
3	A	Gängige kryptographische Maßnahmen sind begrifflich bekannt.
4	A	Es kann zwischen technisch aktuellen und technisch nicht mehr zeitgemäßen, gängigen kryptographischen Maßnahmen unterschieden werden.
5	B	Ein Abgleich mit eventuell datenschutzrechtlichen Erfordernissen findet teilweise statt.
6	B	Daten zur Authentifizierung, insbesondere Kennwörter, werden nicht im Klartext gespeichert.
7	B	Bei Übermittlungen von Daten über das Internet ist eine Transportverschlüsselung implementiert.
8	C	Es besteht ein ganzheitliches Konzept zur Anwendung kryptographischer Methoden und es integriert auch die Schlüsselverwaltung.
9	C	Grundkenntnisse über kryptographische Maßnahmen, sowie die Unterschiede zwischen Hashing und Verschlüsselung, sowie innerhalb der Verschlüsselung zwischen Transport und Speicherverschlüsselung, sind vorhanden.
10	C	Der Einsatz der jeweiligen Methode orientiert sich an den gesetzlichen Erfordernissen und entspricht zum Zeitpunkt der Implementierung dem Stand der Technik.
11	C	Die Integrität des Systems wird teilweise mittels kryptographischer Verfahren sichergestellt.
12	C	Die Einhaltung des Konzepts wird teilweise durch interne Verfahren und Kontrollen sichergestellt und Abweichungen in der Regel behoben.
13	D	Der Zugriff auf die Schlüssel wird dokumentiert und die Berechtigung orientiert sich am Verzeichnisverzeichnis und dort hinterlegten Zuständigkeiten.
14	D	Konzepte und Leitlinien sind mit der zuständigen Leitungsebene abgestimmt.
15	D	Kryptographische Maßnahmen sind ganzheitlich im Datenschutzkonzept implementiert und berücksichtigen das Risiko betroffener personenbezogener Daten.

Aspekt	Stufe	Argument
16	D	Der aktuelle Stand der Technik der implementierten Maßnahmen wird nachverfolgt und dokumentiert. Etwaige, nicht mehr dem Stand der Technik entsprechende kryptographische Maßnahmen werden konsequent durch dem jeweiligen Stand der Technik entsprechende Maßnahmen ersetzt oder ergänzt.
17	D	Eine Transportverschlüsselung ist auch innerhalb des Netzwerks vollständig implementiert.
18	D	Eine Speicherverschlüsselung wurde in der Planung berücksichtigt und kann bei Bedarf aktiviert werden.
19	D	Die Integrität des Systems wird entsprechend etablierter Branchenstandards mittels kryptographischer Verfahren überwacht.
20	E	Die Einhaltung des Konzepts wird vollständig durch interne Verfahren und Kontrollen sichergestellt; Ergebnisse werden an die zuständige Leitungsebene berichtet.
21	E	Die jeweils implementierten Maßnahmen orientieren sich an den Risikoklassen der betroffenen Daten und einer detaillierten Bewertung des Schutzbedarfs.
22	F	Es ist ein Notfall-System implementiert, welches beim Zugriff unberechtigter Dritter verhindert, dass berechnigte Dritte durch Wechsel der Schlüssel ausgeschlossen werden können.
23	F	Die Verfahren und Kontrollen des Konzepts sind so ausgestaltet, dass Interessenkollisionen vermieden werden; soweit Abweichungen festgestellt werden, werden auch interne Prozesse überprüft und ggf. angepasst, sodass entsprechende Abweichungen zukünftig vermieden werden können.
24	G	Dokumentationen erfolgen revisionssicher.
25	G	Das Konzept zur Schlüsselverwaltung wird intern durchgesetzt.
26	G	Es ist eine Transportverschlüsselung auch zwischen einzelnen Prozessen implementiert.
27	G	Bei Übermittlungen über das Internet ist eine P2P-Verschlüsselung implementiert.
28	G	Es ist eine Speicherverschlüsselung aktiv.
29	G	Die Befolgung des Konzepts zum Einsatz kryptographischer Maßnahmen wird nach anerkannten Regeln sichergestellt.
30	H	Die Implementierung der Maßnahmen, deren Angemessenheit und Effektivität wird ergänzend durch externe Kontrollen sichergestellt.

10.2 Schlüsselerwaltung

Frage: Wird der Einsatz kryptographischer Maßnahmen durch eine angemessene Verwaltung der kryptographischen Schlüssel komplettiert?

Aspekt	Stufe	Argument
0	NULL	Es besteht keinerlei geordnete Schlüsselverwaltung.
1	A	Es ist bekannt, dass eine Schlüsselverwaltung für einen sicheren Einsatz kryptographischer Maßnahmen erforderlich ist; konkrete Sachzusammenhänge und Maßnahmen können aber noch nicht abgeleitet werden.
2	B	Es ist teilweise bekannt, ob verwendete Schlüssel selbst generiert und implementiert wurden, oder durch Dritte implementiert werden.
3	B	Soweit Schlüssel selbst generiert und implementiert wurden, werden diese teilweise entsprechend unterschiedlicher Ablage- und Speicherregeln abgelegt.
4	B	Schlüssel und / oder Zertifikate werden noch von mehreren Prozessen oder Personen gleichzeitig verwendet.
5	B	Schlüssel werden von Zeit zu Zeit, aber eher zufällig, ausgetauscht.
6	C	Die Ablage selbst generierter Schlüssel folgt einem flächendeckenden Ablage- und Speicherkonzept.
7	C	Der Wechsel der Schlüssel erfolgt nach einem Regelwerk – z. B. im Falle eines korrumpierten Schlüssels - jedoch keinen zeitlichen Vorgaben.
8	C	Schlüssel und / oder Zertifikate werden nicht mehr durch mehrere Prozesse oder Personen eingesetzt, insbesondere solche zur Authentifizierung und Autorisierung; in anderen Fällen wird jedenfalls dokumentiert und begründet, warum ein Schlüssel-Sharing erforderlich ist.
9	C	Der Zugriff auf die Schlüssel unterliegt besonderen Schutzmaßnahmen (Zugriffskonzept).
10	C	Die Schlüsselverwaltung inklusive aller damit verbundenen Konzepte (z. B. Ablage- und Speicherkonzept, Schlüssel-Zugriffskonzept, etc.) ist dokumentiert.
11	D	Selbst generierte Schlüssel werden ausschließlich lokal und auf eigenen Systemen generiert.
12	D	Soweit technisch möglich und mit dem Risiko der verarbeiteten Daten vereinbar, wird auf fremdgenerierte Schlüssel verzichtet.
13	D	Die Einhaltung der Schlüsselverwaltung wird regelmäßig intern überprüft.
14	D	Festgestellte Verstöße werden klassifiziert und durch angemessene Maßnahmen adressiert – z. B. Schulung des Personals, Evaluation und Modifikation.
15	E	Die Schlüsselverwaltung folgt einem Konzept, welches einen Wechsel nach klaren, branchenstandards entsprechenden zeitlichen Vorgaben vorsieht.

Aspekt	Stufe	Argument
16	F	Die Einhaltung der Schlüsselverwaltung wird regelmäßig extern überprüft und evaluiert.
17	F	Die Durchsetzung der Einhaltung der Schlüsselverwaltung wird teilweise technisch unterstützt.
18	F	Die Durchsetzung der Einhaltung der Schlüsselverwaltung wird vollständig technisch unterstützt.

11

Physische und umgebungsbezogene Sicherheit

Die physische und umgebungsbezogene Sicherheit adressiert Maßnahmen zur Absicherung von Gebäuden, Räumen und etwaigen Betriebsmitteln (Papier, USBs, Clients etc.). Es geht konkret um die Konzeption von Zutrittsberechtigungen, Definition von Maßnahmen zum Schutz von Umwelteinflüssen sowie zur Nutzung und Entsorgung von Betriebsmitteln.

11.1 Sicherheitsbereiche

11.1.1 Physische Sicherheitsperimeter

Frage: Sind physische Schutzmaßnahmen anhand eines Sicherheitszonenkonzepts definiert und werden diese überwacht?

Aspekt	Stufe	Argument
0	NULL	Keine Schutzmaßnahmen vorhanden oder Schutzmaßnahmen folgen keinem Konzept oder Schutzmaßnahmen folgen keinem (einheitlichen) Sicherheitsstandard oder es sind keine besonderen Schutzzonen definiert.
1	A	Es existieren Zutrittsberechtigungen und -beschränkungen für besonders kritische Bereiche, wie z. B. Serverräume, Technikräume, Archivräume.
2	A	In der physischen Sicherheitskonzeption werden folgende Aspekte einbezogen: <ul style="list-style-type: none"> Es existieren nach Schutzbedarf und Kritikalität (Risikobewertung) festgelegte Sicherheitszonen Es existieren dokumentierte Schutzmaßnahmen (Katalog) für die verschiedenen Sicherheitszonen Es existiert ein Konzept für Zutrittsberechtigungen und – beschränkungen Der Umgang mit betriebsfremden Personen und Besuchern einschließlich Reinigungs-, Wartungs- und sonstigem Personal (im Folgenden: Externe) ist geregelt, z. B. Einschränkungen (räumlich, zeitlich) der Zutrittsberechtigungen für Externe, Erkennbarkeit Externen, Erfordernis von Begleitung Externer durch Mitarbeitende des Unternehmens, zeitliche Befristung des generellen Zugangs
3	A	In der physischen Sicherheitskonzeption werden folgende Aspekte einbezogen und besonders gewürdigt: <ul style="list-style-type: none"> Notausgänge und Fluchtwege aus Sicherheitszonen, z. B. durch Videoüberwachung Anlieferungs- und Versandbereiche, z. B. durch Videoüberwachung und Zugangskontrolle
4	A	Die Nachvollziehbarkeit von Zutritten ist personengenau gewährleistet.
5	A	Es finden regelmäßige Überprüfungen der vergebenen Zutrittsberechtigungen statt.
6	A	Die Mitarbeitenden im Bereich physischer Sicherheitskonzeption sind für ihre Aufgaben qualifiziert und werden regelmäßig weitergebildet.
7	B	Die Mitarbeitenden, die Prozesse ausführen, die unter dem Regime der physischen Sicherheitskonzeption stehen, sind in den Prozessen geschult und werden bei Änderungen der Prozesse zeitnah nachgeschult.
8	B	Die Umsetzung und Einhaltung der physischen Sicherheitskonzeption wird konsequent verfolgt, z. B. durch regelmäßige interne Stichproben.
9	B	Die in der physischen Sicherheitskonzeption geforderten Maßnahmen sind in die Geschäftsprozesse der Organisation eingearbeitet.

Aspekt	Stufe	Argument
10	B	Die Geschäftsprozesse und deren Aktivitäten, die unter dem Regime der physischen Sicherheitskonzepte stehen, sind in einer Liste im Anhang der Dokumentation der physischen Sicherheitskonzepte katalogisiert.
11	B	Die Aspekte 1-10 sind dokumentiert, z. B. integriert in Prozesse, und die Dokumentation ist den betroffenen Stakeholdern und Rollen zugänglich und bekannt
12	B	In der physischen Sicherheitskonzeption werden folgende Aspekte einbezogen: <ul style="list-style-type: none"> ▪ Verkabelungswege sind Teil der Sicherheitszonen ▪ Überwachungsmaßnahmen, z. B. Einbruchsmeldeanlagen, Gas- oder Rauchmeldeanlagen, Videoüberwachung
13	C	Die Konzeption der physischen Sicherheitsparameter, z. B. Zutrittsberechtigungen, Sicherheitszonen, Maßnahmenkatalog, steht in der Organisation unter Konfigurationsmanagement.
14	C	Verletzungen und Schwachstellen der physischen Sicherheitskonzeption werden klassifiziert, bewertet und aufgezeichnet.
15	C	Das Management der jeweils höheren Ebene wird regelmäßig über Verletzungen und Schwachstellen der physischen Sicherheitskonzeption informiert und entscheidet über weitere Eskalationen.
16	C	Zu den Aufzeichnungen werden in regelmäßigen und geplanten Abständen Analysen durchgeführt und mögliche Ursachen ermittelt.
17	C	Identifizierte Ursachen für Verletzungen und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an der physischen Sicherheitskonzeption selbst und den Geschäftsprozessen inkl. Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.
18	D	Die in die Prozesse integrierten Vorgaben und die physische Sicherheitskonzeption werden regelmäßig durch Audits und Stichproben auf ihre Adäquatheit und Wirksamkeit überprüft. Hierzu gehören neben der Überprüfung der Prozesse und Falldokumentationen auch simulierte Angriffe, z. B. mittels Social Engineering.
19	E	In der physischen Sicherheitskonzeption werden folgende Aspekte einbezogen: <ul style="list-style-type: none"> ▪ Geschützte Arbeitsbereiche für besonders sensible Datenverarbeitung (Closed Shops) ▪ 24/7 Überwachung besonders sensibler Bereiche durch Sicherheits- oder Wachpersonal ▪ Mehrstufiges Sicherheitskonzept für physische Sicherheit, z. B. aufeinander aufbauende Schutzzonen, Mehrfaktoridentifizierung, Vereinzelung
20	E	Kennzahlen zu Verletzungen und Schwachstellen werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt. Kennzahlen können z. B. sein: <ul style="list-style-type: none"> ▪ Brüche der physischen Sicherheit (klassifiziert) pro Monat, ▪ Ausfälle von physischer Sicherheitstechnik pro Monat, ▪ Verluste von Zugangskarten / IDs pro Monat, ▪ Brüche der physischen Sicherheit (klassifiziert) / Anzahl aller Zugangsvorgänge pro Monat.
21	F	Die Verbesserung des physischen Sicherheitskonzepts ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.

11.1.2 Schutz vor externen und umweltbedingten Bedrohungen

Frage: Sind externen und umweltbedingten Bedrohungen angemessene Schutzmaßnahmen entgegengesetzt?

Aspekt	Stufe	Argument
0	Null	Es gibt keine Vorgaben oder Richtlinie zum Umgang mit umweltbedingten Bedrohungen (wie Feuer, Überflutung, Erdbeben) oder externen Bedrohungen (wie Explosion, zivile Unruhen oder Katastrophen)
1	A	Eine Risikoanalyse für externe Bedrohungen und Umwelteinflüsse wurde durchgeführt.
2	A	Business-Impact-Analyse und Risikoanalyse für externe Bedrohungen und Umwelteinflüsse wurden methodisch durchgeführt und die Ergebnisse dokumentiert.
3	B	Abhängig von den davor resultierten Ergebnissen wurden Maßnahmen für die relevanten externen Bedrohungen und Umwelteinflüsse definiert und in einer Richtlinie dokumentiert.
4	B	Die Richtlinie samt erhaltenen Maßnahmen wird umgesetzt.
5	C	Die umgesetzten Maßnahmen werden regelmäßig überprüft.
6	D	Business-Impact-Analyse und Risikoanalyse werden regelmäßig wiederholt und identifizierte Verbesserungen in die Richtlinie aufgenommen.
7	E	Kennzahlen zu Verletzungen und Schwachstellen der Richtlinie werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses eingesetzt. Kennzahlen könnten die Anzahl der umweltbedingten Bedrohungen oder externen Bedrohungen sowie der entsprechende Schadensausmaß (z. B. finanzielle Verluste oder Investitionen) sein.

11.2 Geräte und Betriebsmittel

11.2.1 Platzierung und Schutz von Geräten und Betriebsmitteln

Frage: Inwieweit sind Vorgaben und Verfahrensweisen für die Nutzung von datenverarbeitenden Betriebsmitteln, einschließlich ihrer Mitnahme und Entsorgung, vorhanden und umgesetzt?

Aspekt	Stufe	Argument
0	Null	Es gibt keine Richtlinie (Vorgaben und Verfahren) zum Umgang mit Betriebsmitteln, deren Platzierung/Positionierung und Entsorgung.
1	A	Es gibt eine dokumentierte Methode um die kritischen Betriebsmittel bzgl. der personenbezogenen Daten zu identifizieren.
2	A	Anhand der o.g. Methode wurden alle kritischen Betriebsmittel (z. B. Server, Clients, Räumen, Verkabelung etc.) identifiziert.
3	B	<p>Es existieren eine oder mehrere Richtlinien, welche die Sicherheitsanforderungen an kritischen Betriebsmittel beschreiben. Die Richtlinien sollen z. B. folgende Angaben beinhalten:</p> <ul style="list-style-type: none"> ▪ Vorgaben und Verfahren zur Positionierung/Platzierung von Betriebsmitteln (z. B. in Büroräumen, in Serverräumen, in Trassen etc.) ▪ Vorgaben und Verfahren zur Nutzung und Mitnahme von Betriebsmitteln (z. B. was außerhalb der Organisation mitgenommen werden darf, welche Maßnahmen für HomeOffice existieren etc.) ▪ Vorgaben und Verfahren Instandhaltung von Betriebsmitteln (z. B. wie ist der Umgang mit Updates, welche Wartungsverträge sind notwendig) <p>Vorgaben und Verfahren zur Wiederverwendung und Entsorgung von Betriebsmitteln (z. B. wie sollen Festplatten oder Unterlagen mit personenbezogenen Daten entsorgt werden etc.).</p>
4	C	Die Richtlinien werden in der Organisation gelebt.
5	D	Die Einhaltung der Vorgaben und Verfahren werden regelmäßig überprüft und identifizierte Verbesserungen in die Richtlinie aufgenommen.
6	E	Kennzahlen zu Verletzungen und Schwachstellen der Richtlinien werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses eingesetzt.

11.2.2 Richtlinien für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren

Frage: Gibt es eine clean desk policy, die den Umgang mit Unterlagen, mit mobilen Datenträgern und Bildschirmsperren regelt?

Aspekt	Stufe	Argument
0	Null	Es gibt keine Vorgaben zum Umgang mit Unterlagen, mit mobilen Datenträger und Bildschirmsperren (= sogenannte clean desk policy).
1	A	<p>Es gibt einzelne Vorgaben zum Umgang mit Unterlagen oder mobilen Datenträger oder Bildschirmsperren. Vorgaben könnten sein:</p> <ul style="list-style-type: none"> ▪ Unterlagen mit personenbezogenen Daten sollten in abgeschlossenen Schränken aufbewahrt werden ▪ Bildschirme sollten nach Nicht-Aktivität automatisch gesperrt werden ▪ Passwörter sollten nach Nicht-Aktivität gesperrt werden ▪ Nutzung von USBs sollten geregelt werden, z. B. nicht als Wechselmedien aktiviert <p>Kopierer ohne Authentifizierung-Maßnahmen sollten nicht für sensible Informationen genutzt werden oder in öffentlichen Räumen platziert werden.</p>
2	B	Es gibt dokumentierte Vorgaben zum Umgang mit Unterlagen, mobilen Datenträgern und Bildschirmsperren. Diese sind definiert entsprechend einer Risikoanalyse und der Kritikalität der enthaltenen Daten.
3	C	Die Richtlinien werden in der Organisation gelebt.
4	D	Die Einhaltung der Vorgaben und Verfahren werden regelmäßig überprüft und identifizierte Verbesserungen in die Richtlinie aufgenommen.
5	E	Kennzahlen zu Verletzungen und Schwachstellen der Richtlinien werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses eingesetzt.

11.2.3 Richtlinien für mobiles Arbeiten und Heimarbeitsplätze

Frage: Gibt es klare Regelungen und Schutzmaßnahmen, die das Arbeiten mit personenbezogenen Daten außerhalb der Räumlichkeiten des Unternehmens regelt?

Aspekt	Stufe	Argument
0	Null	Es gibt keine Vorgaben, die das Arbeiten mit personenbezogenen Daten außerhalb der Räumlichkeiten des Unternehmens regeln.
1	A	Es gibt einzelne Vorgaben, die das Arbeiten mit personenbezogenen Daten außerhalb der Räumlichkeiten des Unternehmens regeln.
2	A	Der Datenaustausch über öffentliche Netze findet verschlüsselt statt. Die Verschlüsselung entspricht dem aktuellen Stand der Technik.
3	A	Alle eingesetzten Datenträger für das Arbeiten Daten außerhalb der Räumlichkeiten des Unternehmens sind nach aktuellem Stand der Technik verschlüsselt.
4	A	Mobile Arbeitsgeräte (Notebook, Smartphones, Tablets etc.) sind vor unbefugten Einblick (z. B. mit Sichtschutzfolien) geschützt.

Aspekt	Stufe	Argument
5	A	Alle mobilen Arbeitsgeräte verfügen über angemessene Authentifizierungsverfahren für Nutzende und werden automatisch bei Inaktivität gesperrt.
6	A	Das Führen von dienstlichen Telefonaten / Webkonferenzen in Umgebungen mit Sprachassistenten oder in Hörweite von Unbeteiligten ist geregelt.
7	B	Mit Nutzenden, die mit personenbezogenen Daten außerhalb der Räumlichkeiten des Unternehmens arbeiten sollen, wird eine angemessene Zusatzvereinbarung über die einzuhaltenden Sicherheitsmaßnahmen geschlossen.
8	B	Mobile Arbeitsgeräte werden durch ein zentrales Management administriert. Die Installation von Anwendungen ist den Nutzenden ausschließlich aus einem geprüften Katalog oder nach individueller Prüfung möglich. Der Prüf- und Freigabeprozess ist definiert und Prüfungen sowie deren Ergebnisse werden dokumentiert.
9	B	Für mobiles Arbeiten im Ausland wurde, sofern dies gestattet ist, eine dokumentierte Risikobetrachtung durchgeführt und Regelungen zur Umsetzung angemessener Schutzmaßnahmen getroffen.
10	B	Im Verlustfall können Inhalte auf den Endgeräten durch den Nutzer oder das Unternehmen ferngelöscht werden.
11	B	USB- (und vergleichbare) Schnittstellen sind überwacht und lassen sich nur für fest definierte Speichermedien oder ausschließlich für Peripheriegeräte (Maus, Tastatur, Webcam etc.) nutzen.
12	B	Die Möglichkeit einer Begehung oder vergleichbaren Kontrolle des mobilen Arbeitsplatzes ist geregelt.
13	B	Das Booten von alternativen Speichermedien ist geschützt.
14	C	Das Arbeiten mit personenbezogenen Daten außerhalb der Räumlichkeiten des Unternehmens erfolgt möglichst papierlos oder der Umgang mit Papierdokumenten inkl. deren Aufbewahrung und Vernichtung ist angemessen geregelt.
15	C	Mobile Arbeitsgeräte werden vollständig durch ein zentrales Management administriert und es können Inhalte auf Endgeräten ferngelöscht werden, auch zu präventiven Zwecken und ohne Mitwirkung der betroffenen Benutzer.
16	C	Die Umstände der Begehung oder vergleichbaren Kontrolle sind näher geregelt, auch in Bezug auf Ankündigungsfristen und Umfang der Kontrollen.
17	D	Die näheren Regelungen zu Umständen und Umfang der technischen Kontrollen betreffen mindestens eine Protokollierung und Kontrolle der Logins, der Dauer der Anmeldung sowie eine regelmäßige Kontrolle per Video-Call.
18	D	Die Einhaltung der Vorgaben und Verfahren werden regelmäßig überprüft und identifizierte Verbesserungen in die Richtlinie aufgenommen.
19	E	Kennzahlen zu Verletzungen und Schwachstellen der Richtlinien werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses eingesetzt.

12

Betriebssicherheit

12.1 Betriebsabläufe und Verantwortlichkeiten

12.1.1 Änderungssteuerung

Frage: Werden Änderungen an Einrichtungen oder Systemen, die personenbezogene Daten verarbeiten, innerhalb der Organisation oder der Geschäftsprozesse, gesteuert?

Aspekt	Stufe	Argument
0	Null	In der Organisation gibt es für Änderungen an Systemen zur Verarbeitung personenbezogener Daten kein Vorgabe.
1	A	In der Organisation bestehen Vorgaben, wie bei Änderungen an Systemen vorzugehen ist.
2	B	Für die Planung von Änderungen gibt es Prozessvorgaben (zu beachtende Randbedingungen, Informationen, zwingend einzuhaltende Prozessschritte). Zudem werden mögliche Auswirkungen der Änderungen vorab bewertet.
3	C	Der Änderungsprozess ist für alle Systeme definiert und die Anwendung ist zwingend vorgegeben.
4	C	Die Kommunikation von geplanten oder umgesetzten Änderungen erfolgt an alle relevanten Stellen.
5	C	Es gibt ein formelles Genehmigungsverfahren für geplante Änderungen.
6	D	Es werden Verfahren bereitgestellt und auch regelmäßig getestet, um bei nicht erfolgreichen Änderungen und unvorhergesehenen Ereignissen den Vorgang abubrechen und die Änderungen rückgängig zu machen.
7	E	Die Güte der Änderungsprozesse und -verfahren wird gemessen und bewertet.
8	F	Auf Basis der Prozessdokumentation und Effizienzmessungen werden regelmäßig Maßnahmen zur Verbesserung umgesetzt.
9	C	Es erfolgt eine Feststellung und Protokollierung wesentlicher Änderungen.

12.1.2 Trennung von Entwicklungs-, Test- und Betriebsumgebungen

Frage: Gibt es in der Organisation Vorgaben, welche die gesonderte Verwendung personenbezogener Daten in Test- oder Entwicklungsumgebungen regeln oder verbieten?

Aspekt	Stufe	Argument
0	Null	In der Organisation gibt es keine Vorgaben zur Verwendung personenbezogener Daten in Entwicklungs- oder Testumgebungen.
1	A	In der Organisation bestehen Vorgaben für die Nutzung personenbezogener Daten in Test- und Entwicklungsumgebungen.
2	B	Es existieren verbindliche Vorgaben, die die Nutzung personenbezogener Daten auf Test- oder Entwicklungssystemen vermeiden und es sind noch keine Ausnahmeregelungen definiert.
3	B	Die Nutzung personenbezogener Daten in Test- und Entwicklungsumgebungen, ohne vorausgegangene Anonymisierung oder Pseudonymisierung, ist grundsätzlich untersagt.
4	C	Die Freigabe und die Nutzung personenbezogener Daten (Klardaten) in Test- und Entwicklungsumgebungen ist durch einen verbindlichen Prozess geregelt.
5	C	Es existieren verbindliche Vorgaben, wie eine Pseudonymisierung oder Anonymisierung personenbezogener Daten vor der Nutzung in solchen Systemen durchzuführen ist. Diese Vorgaben definieren auch geeignete Verfahren und Algorithmen zur Pseudonymisierung und Anonymisierung.
6	C	Bei Einsatz personenbezogener Daten (auch pseudonymisierter Daten) auf Testsystemen gibt es verbindliche Vorgaben bezüglich eingeschränkter Nutzerrechte, Personenkreis und strenger IT-Sicherheitsvorgaben.
7	C	Alle personenbezogenen Daten (auch Pseudonyme) werden nach Testende datenschutzgerecht gelöscht. Die Löschung wird protokolliert.
8	D	Ist die Nutzung anonymisierter oder spezieller Testdaten nicht möglich, gibt es verbindliche Vorgaben inklusive der Durchführung einer Datenschutzfolgeabschätzung, sowie Freigabe- und Kontrollmechanismen zur eingeschränkten Nutzung personenbezogener Daten.
9	E	Die Einhaltung der Vorgaben wird regelmäßig kontrolliert und bei Bedarf optimiert.

12.1.3 Schutz vor Schadsoftware

Frage: Gibt es in der Organisation Maßnahmen für den Schutz personenbezogener Daten vor Schadsoftware?

Aspekt	Stufe	Argument
0	Null	In der Organisation gibt es keine Vorgaben für technische oder organisatorische Maßnahmen zum Schutz vor Schadsoftware.
1	A	Es existieren in der Organisation vereinzelt Vorgaben für Nutzung und Schutz der eingesetzten Software. Vereinzelt wird Software (z. B. Virens Scanner, Contentfilter) zum Schutz der Systeme vor Schadsoftware eingesetzt.

Aspekt	Stufe	Argument
2	B	In der Organisation gibt es für alle Systeme eine verbindliche Richtlinie und Prozesse zum Schutz vor Schadsoftware. Es ist geregelt, wer für die Installation, Konfiguration und Auswahl der Software verantwortlich ist.
3	B	Prozesse und eingesetzte Produkte entsprechen dem Stand der Technik.
4	C	Es existieren Freigabeprozesse für jede Software die im Unternehmen eingesetzt werden soll. In der Organisation finden regelmäßig Kontrollen statt, ob auf Systemen Schadsoftware oder nicht freigegebene Software installiert ist.
5	C	Die Mitarbeitenden wurden über die geltenden Richtlinien informiert und werden regelmäßig in der Nutzung der IT-Systeme geschult.
6	D	In der Organisation existiert für alle relevanten Systeme eine Inventarisierung der installierten und freigegebenen Software. Die Inventarisierung wird stichprobenartig überprüft.
7	E	Die Ergebnisse der Systemüberprüfung und Protokollierung werden regelmäßig ausgewertet, kritische Prozesse oder Konfigurationen identifiziert und Verbesserungsmaßnahmen daraus abgeleitet.
8	C	In der Organisation gibt es für alle Systeme ein verbindliches Konzept zum Schutz vor Schadsoftware und Regelungen (z. B. Notfallpläne), wie nach einem Befall mit Schadsoftware vorzugehen ist.
9	C	In der Organisation gibt es Maßnahmen, welche die Verbreitung von Schadsoftware erschweren. Zu solchen Maßnahmen zählen beispielsweise die Systemhärtung, ein Schwachstellenmanagement oder die Trennung / Segmentierung von Netzen und IT-Systemen).
10	F	Die Systeme werden regelmäßig hinsichtlich nicht freigegebener Software überprüft (z. B. durch Audits, Stichproben, Security-Checks oder dem Einsatz von Prüfsoftware).

12.1.4 Patchmanagement

Frage: Gibt es in der Organisation Vorgaben, wie und von wem Systeme gepatched werden?

Aspekt	Stufe	Argument
0	Null	In der Organisation gibt es keine Regelungen, wer wann welche Anwendungen oder Systeme patched.
1	A	In der Organisation werden Betriebssystempatches installiert, wenn diese durch den Anbieter zur Verfügung gestellt werden.
2	A	In der Organisation werden Anwendungspatches installiert, wenn diese vom Hersteller zur Verfügung gestellt werden.
3	A	Für die Installation von Betriebssystem- oder Anwendungspatches sind verantwortliche benannt.
4	B	In der Organisation gibt es bereits Regelungen dafür, wer welche Patches einspielt, z. B.: <ul style="list-style-type: none"> ▪ Betriebssystemupdates von Rechnern und Laptops durch die Systemadministratoren ▪ Betriebssystemupdates von mobilen Endgeräten (Android, iOS) durch den Nutzenden

Aspekt	Stufe	Argument
5	B	In der Organisation werden Patches kategorisiert (Sicherheitspatches, Anwendungspatches) und priorisiert.
6	B	Es gibt bereits Vorgaben, wann Patches installiert werden müssen.
7	B	Patches werden vor der Installation getestet.
8	C	In der Organisation gibt es einen dokumentierten Prozess zum Patchmanagement, in dem festgelegt wird: <ul style="list-style-type: none"> ▪ wie und durch wen notwendige Patches identifiziert werden ▪ wer für den Patchprozess verantwortlich ist ▪ wer am Prozess zu beteiligen oder zu informieren ist ▪ wie Patches kategorisiert und priorisiert werden ▪ wie Patches geprüft und freigegeben werden ▪ bis wann ein Patch eingespielt werden muss ▪ wie Patches verteilt und installiert werden
9	D	In der Organisation gibt es einen eingeführten Prozess zum Patchmanagement, die Verantwortlichen und deren Vertreter sind benannt. Der Prozess wird regelmäßig überprüft (werden alle Systeme und Anwendungen erfasst). Die Regelungen sind allen Beteiligten und Mitarbeitenden bekannt.
10	E	Das Patchmanagement wird regelmäßig auf seine Wirksamkeit hin überprüft. Kriterien können dabei sein: <ul style="list-style-type: none"> ▪ Dauer bis zur Verteilung / Installation von kritischen Sicherheitspatches ▪ Auswirkungen auf den Betriebsablauf der Organisation ▪ Verfügbarkeit der Anwendungen vor, nach und während der Installation ▪ Verteilungsgrad der Patches (Vollständer RollOut?)
11	F	Das Patchmanagement wird überprüft und bewertet. Das Ergebnis dieser Bewertung wird für die kontinuierliche Verbesserung des Prozesses genutzt. In der Organisation stehen für diesen Verbesserungsprozess ausreichend Mittel bereit.

12.2 Datensicherung

12.2.1 Sicherung von Information

Frage: Wie werden personenbezogene Daten in der Organisation gesichert? Wie wurde das Risiko eines Datenverlustes behandelt?

Aspekt	Stufe	Argument
0	Null	In der Organisation gibt es keine Vorgaben, wann und wie Datensicherungen durchzuführen sind.
1	A	Für betriebsnotwendige Systeme gibt es Vorgaben / Pläne was zu sichern ist und wie die Sicherungskopien zu lagern sind.
2	A	In der Organisation werden regelmäßig Datensicherungen von betriebsnotwendigen Systemen und Datenbanken erstellt.
3	A	Es gibt in der Organisation Leit- oder Richtlinien, in der zumindest die regelmäßige Durchführung einer Datensicherung gefordert wird.
4	B	In der Organisation wurden relevante Systeme und Daten identifiziert, für die eine Datensicherung notwendig ist.
5	B	Die Umsetzung der Datensicherung wird protokolliert.
6	B	Es wurden verbindliche Regelungen für eine Datensicherung verabschiedet und in der Organisation eingeführt.
7	C	In der Organisation wird ein Datensicherungskonzept erstellt und die folgenden Aspekte werden dabei berücksichtigt: <ul style="list-style-type: none"> ▪ Personenbezogene Daten wurden unter Berücksichtigung von Verfügbarkeitsanforderungen in das Datensicherungskonzept mit einbezogen ▪ Es wurde für alle relevanten Systeme oder Daten festgelegt, welche Datensicherungsstrategie zum Einsatz kommt ▪ Es wurde festgelegt, wie und an welchen Ort Datensicherungen abgelegt werden ▪ Es wurden Verantwortliche Stellen oder Personen benannt ▪ Es wurde festgelegt, wie Datensicherungen protokolliert und gekennzeichnet werden
8	C	Das zuvor erstellte Datensicherungskonzept wird in allen Punkten umgesetzt und angewendet.
9	C	Für die Datensicherungen wird festgelegt, wie und unter welchen Bedingungen diese in das System zurückgespielt werden können. Verantwortliche werden festgelegt und der Vorgang wird protokolliert (Wiederherstellungskonzept).
10	D	Der Sicherungsprozess wird so gestaltet, dass Löschanforderungen/-vorgaben des Datenschutzes umgesetzt werden können.

Aspekt	Stufe	Argument
11	D	Die Prüfung der Wiederherstellungsfähigkeit erfolgt regelmäßig auf einem gesonderten, vom Wirksystem entkoppelten Prüfsystem. Es erfolgt nach jedem Rückspielen ein umfangreicher Funktionstest. Identifizierte Fehler werden dokumentiert, ausgewertet und abgestellt.
12	D	Es erfolgt eine Protokollierung der Prüfung.
13	E	Die Protokolle / Aufzeichnungen / Logdateien der Datensicherung / Rückversicherungen werden unter folgenden Gesichtspunkten ausgewertet: <ul style="list-style-type: none">▪ Bedarf an Zeit und Aufwand für den Prozess▪ Erfüllungsgrad der Prozessanforderungen bezüglich Sicherheit und Verfügbarkeit▪ Optimierungsmöglichkeiten▪ Einsatz alternativer Verfahren

12.3 Protokollierung und Überwachung

12.3.1 Protokollierung der Datenverarbeitung bei Personenbezug

Frage: Werden in der Organisation Datenverarbeitungen mit Personenbezug protokolliert?

Aspekt	Stufe	Argument
0	Null	In der Organisation gibt es bezüglich der Protokollierung keine Vorgaben oder Prozesse.
1	A	In der Organisation findet an verschiedenen Stellen eine Ereignisprotokollierung statt, meist werden dabei die Herstellereinstellungen zur Protokollierung genutzt.
2	A	Die Protokolle werden gespeichert und können bei Bedarf ausgewertet werden.
3	B	In der Organisation wurde verbindlich festgelegt, welche Ereignisse unter Datenschutzgesichtspunkten zu protokollieren sind, insbesondere zur Gewährleistung der Vertraulichkeit und Integrität der verarbeiteten personenbezogenen Daten. Hierzu sachdienliche Ereignisse können, einzeln oder in einer Kombination davon, beispielsweise sein: <ul style="list-style-type: none"> ▪ Zugriffe auf personenbezogene Daten (Lesen/Schreiben/Löschen) ▪ Benutzeraktivitäten (Anmelden/Abmelden) ▪ Fehlermeldungen ▪ Betriebszustände ▪ Änderungen ▪ Löschungen ▪ Schnittstellenaktivitäten
4	B	In der Organisation wurde festgelegt, welche Personen / Stellen oder Organisationseinheiten mit der Erstellung und Auswertung der Protokolle betraut sind.
5	C	In der Organisation wurde festgelegt, in welchem Umfang und in welchem Format Protokollinformationen generiert werden. Zu den Festlegungen gehören: <ul style="list-style-type: none"> ▪ Welche Information im Protokoll wie abgelegt wird ▪ Wie oft ein Ereignis protokolliert wird ▪ Welche personenbezogenen Daten im Protokoll Eingang finden ▪ Wie Protokolle überschrieben und aktualisiert werden
6	C	In der Organisation ist festgelegt, wie lange Protokolle gespeichert werden müssen und wann diese gelöscht werden müssen.
7	C	Der Zugriff auf die Protokolle ist nur durch berechtigte Personen oder Instanzen möglich.
8	D	In der Organisation wurden Schutzmaßnahmen für Protokolle definiert und umgesetzt. Es wurde festgelegt, wie Protokolle so abgelegt / gespeichert werden, sodass nachträgliche Manipulationen (Veränderungen / Löschung) verhindert werden.

Aspekt	Stufe	Argument
9	D	In der Organisation wurde geprüft, welche externen Anforderungen, etwa durch Aufsichtsbehörden, an die Protokollierung bestehen. Die Protokollierung wurde entsprechend den Anforderungen der Aufsichtsbehörden (Dauer bis zur Bereitstellung, Übergabeformat, Ansprechpartner) angepasst.
10	D	Es wurde geprüft welche speziellen Anforderungen des Datenschutzes an Protokolle bestehen (bezügl. Löschung oder Art und Umfang der Speicherung personenbezogener Protokolldaten) und wie diese in Abhängigkeit zu anderen gesetzlichen Anforderungen stehen. Die Protokollierung wurde entsprechend angepasst.
11	E	In der Organisation gibt es einen Prozess und verantwortliche Stellen, die regelmäßig die Prozesse der Protokollierung auf: <ul style="list-style-type: none"> ▪ Vollständigkeit ▪ Vertraulichkeit ▪ Verfügbarkeit und Gesetzeskonformität hin überprüfen und notwendige Änderungen umsetzen.

12.3.2 Handhabung von technischen Schwachstellen

Frage: Gibt es in der Organisation Maßnahmen, um technische Schwachstellen zu vermeiden, rechtzeitig zu identifizieren und zu beseitigen?

Aspekt	Stufe	Argument
0	Null	In der Organisation gibt es keine Prozesse oder Verantwortlichen, die Informationen über technische Schwachstellen einholen. In der Organisation existieren keine Mechanismen, Vorgaben oder Prozesse, die bei identifizierten technischen Schwachstellen Maßnahmen ergreifen um das Risiko zu behandeln.
1	A	Die Organisation hat eine aktuelle und vollständige Ausstellung der Werte (Anlagen, Systeme, Daten vertrauliche und / oder personenbezogene Daten).
2	A	Die Organisation hat eine Bewertung vorgenommen, welche Werte welchen Schutzbedarf haben und diese entsprechend kategorisiert.
3	A	Es wurden potentielle Risiken durch technische Schwachstellen für die Werte identifiziert und dokumentiert.
4	B	In der Organisation wurde festgelegt, wie Information über technische Schwachstellen regelmäßig eingeholt werden.
5	B	In der Organisation wurden Maßnahmen identifiziert, wie technische Schwachstellen behandelt werden können.
6	B	In der Organisation wurden bestimmten potentiellen technischen Schwachstellen Risiken zugeordnet.
7	C	In der Organisation wurden für alle relevanten Werte mit möglichen technischen Schwachstellen die korrespondierenden Risiken identifiziert. In Abhängigkeit von der Schwere der Risiken wurden Maßnahmen definiert.
8	C	Es wurden Methoden, Informationsquellen, Techniken und Verantwortliche festgelegt, mit dem Ziel auch zukünftig technische Schwachstellen rechtzeitig zu identifizieren und geeignete Maßnahmen abzuleiten.
9	C	Es wurden Vorgaben, Handlungsanweisungen und Zeitpläne definiert, wie bei auftretenden Schwachstellen zu verfahren ist.

Aspekt	Stufe	Argument
10	D	Für die Organisation wurde ein Gesamtprozess unter Berücksichtigung der folgende Aspekte definiert: <ul style="list-style-type: none"> ▪ Der sicherstellt, dass Informationen über technische Schwachstellen rechtzeitig vorliegen ▪ Geeignete Vorsorgemaßnahmen ableitet ▪ Verantwortliche und Mittel bereitstellt ▪ Zeit- und Umsetzungsvorgaben beinhaltet ▪ Mögliche Abhilfemaßnahmen bewertet und geeignete auswählt ▪ Die Umsetzung der Maßnahmen dokumentiert
11	D	Der zuvor definierte Prozess wird in allen Punkten vollständig umgesetzt und angewendet.
12	E	Der Prozess zur Risikominimierung wird regelmäßig überprüft, bewertet und verbessert.
13	E	In der Organisation ist ein Verbesserungsprozess etabliert, der: <ul style="list-style-type: none"> ▪ die Risikoabschätzung technischer Schwachstellen regelmäßig aktualisiert ▪ Methoden und technische Mechanismen zur Bewertung von Wirksamkeit und Leistungsfähigkeit der eingesetzten Maßnahmen bereitstellt
14	F	Die Ergebnisse der Leistungsmessungen werden der Leitung der Organisationseinheit zur Kenntnis gebracht. Falls erforderlich, werden Verbesserungen der Prozesse, Richtlinien oder technischen Systeme eingeleitet.

12.3.3 Einschränkungen von Softwareinstallation

Frage: Gibt es in der Organisation Vorgaben / Regelungen bezüglich der Installation neuer Software oder neuer Softwareversionen?

Aspekt	Stufe	Argument
0	Null	In der Organisation gibt es keine Regeln / Richtlinien oder technische Einschränkungen für die Softwareinstallation durch den Nutzenden /Anwendenden.
1	A	In der Organisation gibt es Einschränkungen, z. B. durch Steuerung über die Benutzerrechte, welche die Softwareinstallation durch den Benutzer einschränken.
2	B	Es existieren Richtlinien zur Nutzung und Installation von Software.
3	B	Die Benutzer in den Systemen der Organisation haben nicht nur beschränkte Rechte für die Softwareinstallation, sondern auch nur beschränkte Möglichkeiten, installierte Software oder Systeme zu konfigurieren.
4	B	Es gibt in der Organisation genaue Vorgaben, welche Benutzergruppe Systemkonfigurationen oder Softwareinstallationen durchführen darf.
5	C	Es ist genau geregelt welche Software auf den Systemen installiert sein darf.
6	C	Es ist geregelt ob / wann Aktualisierungen oder Patches installiert werden dürfen.
7	C	Es gibt genaue Vorgaben welcher Nutzer oder Bereich welche Software nutzt.
8	C	Die private Nutzung der Systeme ist untersagt oder geregelt.
9	D	In der Organisation gibt es einen gesteuerten Prozess zur Installation von Software (Freigabe, RollOut-Prozess, Konfiguration, Patch-Management, ...)

13

Kommunikations- sicherheit

13.1 Netzwerkkontrollen

Frage: Wie werden von der Organisation die Netzwerke verwaltet und kontrolliert?

Aspekt	Stufe	Argument
0	Null	In der Organisation existieren keine Regelungen zur Verwaltung und Kontrolle von Netzwerken oder sie sind nicht verabschiedet oder nicht veröffentlicht.
1	A	Regelungen zur Verwaltung und Kontrolle von Netzwerken sind von der Organisation verabschiedet und veröffentlicht.
2	B	Folgende Inhalte zur Verwaltung und Kontrolle von Netzwerken müssen geregelt sein: <ul style="list-style-type: none"> ▪ Einschränkung von Anbindungen an das Netzwerk ▪ Verschlüsselter Zugang bei externen Verbindungen (zum Beispiel VPN) ▪ Protokollierung von Handlungen mit Relevanz zur Netzwerksicherheit ▪ Schutz der Netzwerke vor Angreifern (zum Beispiel Firewall, IDS, IPS)
3	B	Für die Regelungen zur Verwaltung und Kontrolle von Netzwerken sind die Rechte und Pflichten zugewiesen worden.
4	C	Die erforderlichen Regelungen zur Verwaltung und Kontrolle von Netzwerken sind in die Geschäftsprozesse der Organisation eingearbeitet.
5	C	Für die Umsetzung der Regelungen zur Verwaltung und Kontrolle von Netzwerken sind notwendigen Ressourcen identifiziert und geplant worden.
6	C	Für die Umsetzung der Regelungen zur Verwaltung und Kontrolle von Netzwerken sind die notwendigen Ressourcen bewilligt worden und werden planmäßig freigegeben.
7	C	Die relevanten Stakeholder in der Organisation sind in das Themengebiet eingebunden.
8	C	Die erforderlichen Regelungen zur Verwaltung und Kontrolle von Netzwerken werden den betroffenen Stakeholdern zugänglich gemacht und sind bekannt, z. B. geschult.
9	C	Die Regelungen zur Verwaltung und Kontrolle von Netzwerken sind dokumentiert und müssen verbindlich umgesetzt werden.
10	C	Besondere Anforderungen sind identifiziert und berücksichtigt worden (zum Beispiel spezielle vertragliche Regelungen mit Auftraggebern).
11	D	Die erforderlichen Regelungen stehen in der Organisation unter Konfigurationsmanagement.
12	D	Die Umsetzung der Regelungen zur Verwaltung und Kontrolle von Netzwerken wird konsequent verfolgt, z. B. durch regelmäßige interne Überprüfungen oder Audits. Alle vorher genannten Aspekte müssen erfüllt sein.
13	D	Das Management der jeweils höheren Ebene und der Auftraggeber wird regelmäßig über Verletzungen und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen informiert und entscheidet über weitere Eskalationen.

Aspekt	Stufe	Argument
14	D	Datenschutzvorfälle und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen werden klassifiziert, bewertet und aufgezeichnet.
15	D	Zu den Aufzeichnungen werden in regelmäßigen und geplanten Abständen Analysen durchgeführt und mögliche Ursachen ermittelt.
16	E	Identifizierte Ursachen für Verletzungen und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an den Regelungen zur Verwaltung und Kontrolle von Netzwerken selbst und den Geschäftsprozessen inkl. Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.
17	E	Kennzahlen zu den Regelungen zur Verwaltung und Kontrolle von Netzwerken werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt.
18	E	Die Verbesserung der Regelungen zur Verwaltung und Kontrolle von Netzwerken ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.
19	E	Ein ausgereiftes Kennzahlensystem zu Regelungen zur Verwaltung und Kontrolle von Netzwerken ist identifiziert, eingeführt und wird betrieben und ausgewertet.

13.2 Sicherheit von Netzwerkdiensten

Frage: Wie wird von der Organisation die Sicherheit von Netzwerkdiensten sichergestellt?

Aspekt	Stufe	Argument
0	Null	In der Organisation existieren keine Regelungen zur Sicherheit von Netzwerkdiensten oder sie sind nicht verabschiedet oder nicht veröffentlicht.
2	A	Regelungen zur Sicherheit von Netzwerkdiensten sind von der Organisation verabschiedet und veröffentlicht.
3	B	Folgende Inhalte zur Sicherheit von Netzwerkdiensten müssen geregelt sein: <ul style="list-style-type: none"> ▪ Entsprechende SLAs sind identifiziert und bei externen Dienstleistungen vertraglich festgehalten ▪ Netzwerkdienste werden, wenn erforderlich, redundant betrieben ▪ Netzwerke werden überwacht
4	B	Für die Regelungen zur Sicherheit von Netzwerkdiensten sind die Rechte und Pflichten zugewiesen worden.
6	C	Die erforderlichen Regelungen zur Sicherheit von Netzwerkdiensten sind in die Geschäftsprozesse der Organisation eingearbeitet.
8	C	Für die Umsetzung der Regelungen zur Sicherheit von Netzwerkdiensten sind die notwendigen Ressourcen identifiziert und geplant worden.
9	C	Für die Umsetzung der Regelungen zur Sicherheit von Netzwerkdiensten sind die notwendigen Ressourcen bewilligt worden und werden planmäßig freigegeben.
10	C	Die relevanten Stakeholder in der Organisation sind in das Themengebiet eingebunden.
11	C	Die erforderlichen Regelungen zur Sicherheit von Netzwerkdiensten werden den betroffenen Stakeholdern zugänglich gemacht und sind bekannt, z. B. geschult.
13	C	Die Regelungen zur Sicherheit von Netzwerkdiensten sind dokumentiert und müssen verbindlich umgesetzt werden.
16	C	Besondere Anforderungen sind identifiziert und berücksichtigt worden (zum Beispiel spezielle vertragliche Regelungen mit Auftraggebern).
18	D	Die erforderlichen Regelungen stehen in der Organisation unter Konfigurationsmanagement.
19	D	Die Umsetzung der Regelungen zur Sicherheit von Netzwerkdiensten wird konsequent verfolgt, z. B. durch regelmäßige interne Überprüfungen oder Audits. Alle vorher genannten Aspekte müssen erfüllt sein.
20	D	Das Management der jeweils höheren Ebene und der Auftraggeber wird regelmäßig über Verletzungen und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen informiert und entscheidet über weitere Eskalationen.
21	D	Datenschutzvorfälle und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen werden klassifiziert, bewertet und aufgezeichnet.

Aspekt	Stufe	Argument
22	D	Zu den Aufzeichnungen werden in regelmäßigen und geplanten Abständen Analysen durchgeführt und mögliche Ursachen ermittelt.
24	E	Identifizierte Ursachen für Verletzungen und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an den Regelungen zur Sicherheit von Netzwerkdiensten selbst und den Geschäftsprozessen inkl. Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.
25	E	Kennzahlen zu den Regelungen zur Sicherheit von Netzwerkdiensten werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt.
27	E	Die Verbesserung der Regelungen zur Sicherheit von Netzwerkdiensten ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.
28	E	Ein ausgereiftes Kennzahlensystem zur Regelungen zur Sicherheit von Netzwerkdiensten ist identifiziert, eingeführt und wird betrieben und ausgewertet.

13.2.1 Segmentierung von Netzwerken

Frage: Wie wird von der Organisation die Segmentierung von Netzwerken sichergestellt?

Aspekt	Stufe	Argument
0	Null	In der Organisation existieren keine Regelungen zur Segmentierung von Netzwerken oder sie sind nicht verabschiedet oder nicht veröffentlicht.
1	A	Regelungen zur Segmentierung von Netzwerken sind von der Organisation verabschiedet und veröffentlicht.
2	B	Folgende Inhalte zur Segmentierung von Netzwerken müssen geregelt sein: <ul style="list-style-type: none"> ▪ Anforderungen an die Netzwerksegmentierung sind bestimmt ▪ Netzwerksegmentierungen sind umgesetzt
3	B	Für die Regelungen zur Segmentierung von Netzwerken sind die Rechte und Pflichten zugewiesen worden.
4	C	Die erforderlichen Regelungen zur Segmentierung von Netzwerken sind in die Geschäftsprozesse der Organisation eingearbeitet.
5	C	Für die Umsetzung der Regelungen zur Segmentierung von Netzwerken sind notwendigen Ressourcen identifiziert und geplant worden.
6	C	Für die Umsetzung der Regelungen zur Segmentierung von Netzwerken sind die notwendigen Ressourcen bewilligt worden und werden planmäßig freigegeben.
7	C	Die relevanten Stakeholder in der Organisation sind in das Themengebiet eingebunden.
8	C	Die erforderlichen Regelungen zur Segmentierung von Netzwerken werden den betroffenen Stakeholdern zugänglich gemacht und sind bekannt, z. B. geschult.
9	C	Die Regelungen zur Segmentierung von Netzwerken sind dokumentiert und müssen verbindlich umgesetzt werden.

Aspekt	Stufe	Argument
10	C	Besondere Anforderungen sind identifiziert und berücksichtigt worden (zum Beispiel spezielle vertragliche Regelungen mit Auftraggebern).
11	D	Die erforderlichen Regelungen stehen in der Organisation unter Konfigurationsmanagement.
12	D	Die Umsetzung der Regelungen zur Segmentierung von Netzwerken wird konsequent verfolgt, z. B. durch regelmäßige interne Überprüfungen oder Audits. Alle vorher genannten Aspekte müssen erfüllt sein.
13		Das Management der jeweils höheren Ebene und der Auftraggeber wird regelmäßig über Verletzungen und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen informiert und entscheidet über weitere Eskalationen.
14	D	Datenschutzvorfälle und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen werden klassifiziert, bewertet und aufgezeichnet.
15	D	Zu den Aufzeichnungen werden in regelmäßigen und geplanten Abständen Analysen durchgeführt und mögliche Ursachen ermittelt.
16	E	Identifizierte Ursachen für Verletzungen und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an den Regelungen zur Segmentierung von Netzwerken selbst und den Geschäftsprozessen inkl. Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.
17	E	Kennzahlen zu den Regelungen zur Segmentierung von Netzwerken werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt.
18	E	Die Verbesserung der Regelungen zur Segmentierung von Netzwerken ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.
19	E	Ein ausgereiftes Kennzahlensystem zur Segmentierung von Netzwerken ist identifiziert, eingeführt und wird betrieben und ausgewertet.

13.2.2 Schutz von personenbezogenen Daten bei der Datenübermittlung

Frage: Wie stellt die Organisation bei der Übermittlung personenbezogener Daten den Schutz sicher?

Aspekt	Stufe	Argument
0	Null	In der Organisation existieren keine Regelungen zum Schutz personenbezogener Daten bei der Datenübermittlung oder sie sind nicht verabschiedet oder nicht veröffentlicht.
1	A	Regelungen zum Schutz personenbezogener Daten bei der Datenübermittlung sind von der Organisation verabschiedet und veröffentlicht.

Aspekt	Stufe	Argument
2	B	<p>Folgende Inhalte zum Schutz personenbezogener Daten bei der Datenübermittlung müssen geregelt sein:</p> <ul style="list-style-type: none"> ▪ Dienste zur Übermittlung personenbezogener Daten sind ermittelt und freigegeben worden ▪ Je nach Klassifikation der personenbezogenen Daten dürfen entsprechende Dienste eingesetzt werden ▪ Die personenbezogenen Daten sind während der Übermittlung gegen Offenbarung geschützt ▪ Maßnahmen gegen Fehlübermittlung (zum Beispiel Irrläufer) sind getroffen ▪ Verschlüsselungen sind je nach Kritikalität der personenbezogenen Daten etabliert und vorgeschrieben ▪ Kommunikationspartner sind im AV-Vertrag bestimmt
3	B	Für die Regelungen zum Schutz personenbezogener Daten bei der Datenübermittlung sind die Rechte und Pflichten zugewiesen worden.
4	C	Die erforderlichen Regelungen zum Schutz personenbezogener Daten bei der Datenübermittlung sind in die Geschäftsprozesse der Organisation eingearbeitet.
5	C	Für die Umsetzung der Regelungen zum Schutz personenbezogener Daten bei der Datenübermittlung sind notwendigen Ressourcen identifiziert und geplant worden.
6	C	Für die Umsetzung der Regelungen zum Schutz personenbezogener Daten bei der Datenübermittlung sind die notwendigen Ressourcen bewilligt worden und werden planmäßig freigegeben.
7	C	Die relevanten Stakeholder in der Organisation sind in das Themengebiet eingebunden.
8	C	Die erforderlichen Regelungen zum Schutz personenbezogener Daten bei der Datenübermittlung werden den betroffenen Stakeholdern zugänglich gemacht und sind bekannt, z. B. geschult.
9	C	Die Regelungen zum Schutz personenbezogener Daten bei der Datenübermittlung sind dokumentiert und müssen verbindlich umgesetzt werden.
10	C	Besondere Anforderungen sind identifiziert und berücksichtigt worden (zum Beispiel spezielle vertragliche Regelungen mit Auftraggebern).
11	D	Die erforderlichen Regelungen stehen in der Organisation unter Konfigurationsmanagement.
12	D	Die Umsetzung der Regelungen zum Schutz personenbezogener Daten bei der Datenübermittlung wird konsequent verfolgt, z. B. durch regelmäßige interne Überprüfungen oder Audits. Alle vorher genannten Aspekte müssen erfüllt sein.
13	D	Das Management der jeweils höheren Ebene und der Auftraggeber wird regelmäßig über Verletzungen und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen informiert und entscheidet über weitere Eskalationen.
14	D	Datenschutzvorfälle und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen werden klassifiziert, bewertet und aufgezeichnet.
15	D	Zu den Aufzeichnungen werden in regelmäßigen und geplanten Abständen Analysen durchgeführt und mögliche Ursachen ermittelt.
16	E	Identifizierte Ursachen für Verletzungen und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an den Regelungen zum Schutz personenbezogener Daten bei der Datenübermittlung selbst und den Geschäftsprozessen inkl. Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.

Aspekt	Stufe	Argument
17	E	Kennzahlen zu den Regelungen zum Schutz personenbezogener Daten bei der Datenübermittlung werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt.
18	E	Die Verbesserung der Regelungen zum Schutz personenbezogener Daten bei der Datenübermittlung ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.
19	E	Ein ausgereiftes Kennzahlensystem zum Schutz personenbezogener Daten bei der Datenübermittlung ist identifiziert, eingeführt und wird betrieben und ausgewertet.

13.2.3 Vertraulichkeitsvereinbarungen und die Verpflichtung auf das Datengeheimnis

Frage: Wie stellt die Organisation sicher, dass Externe bei der Verarbeitung personenbezogener Daten auf die Vertraulichkeit und das Datengeheimnis verpflichtet worden sind?

Aspekt	Stufe	Argument
0	Null	In der Organisation existieren keine Regelungen zur Verpflichtung von Externen auf die Vertraulichkeit und das Datengeheimnis oder sie sind nicht verabschiedet oder sie sind nicht veröffentlicht.
1	A	Regelungen zur Verpflichtung von Externen auf die Vertraulichkeit und das Datengeheimnis sind von der Organisation verabschiedet und veröffentlicht.
2	B	Folgende Inhalte zur Verpflichtung von Externen auf die Vertraulichkeit und das Datengeheimnis müssen geregelt sein: <ul style="list-style-type: none"> Es gibt mit allen Dienstleistern vertragliche Vereinbarungen zur Vertraulichkeit, alle betroffenen Mitarbeitenden von Dienstleistern sind auf die Vertraulichkeit verpflichtet Es gibt mit allen Dienstleistern vertragliche Vereinbarungen zur Verpflichtung auf das Datengeheimnis, alle betroffenen Mitarbeitenden von Dienstleistern sind auf das Datengeheimnis verpflichtet Es gibt Mustertexte zur Vertraulichkeit und der Verpflichtung auf das Datengeheimnis Die Organisation hat die Möglichkeit die Vertraulichkeitsvereinbarungen und Verpflichtungen auf das Datengeheimnis zu überprüfen
3	B	Für die Regelungen zur Verpflichtung von Externen auf die Vertraulichkeit und das Datengeheimnis sind die Rechte und Pflichten zugewiesen worden.
4	C	Die erforderlichen Regelungen zur Verpflichtung von Externen auf die Vertraulichkeit und das Datengeheimnis sind in die Geschäftsprozesse der Organisation eingearbeitet.
5	C	Für die Umsetzung der Regelungen zur Verpflichtung von Externen auf die Vertraulichkeit und das Datengeheimnis sind notwendigen Ressourcen identifiziert und geplant worden.
6	C	Für die Umsetzung der Regelungen zur Verpflichtung von Externen auf die Vertraulichkeit und das Datengeheimnis sind die notwendigen Ressourcen bewilligt worden und werden planmäßig freigegeben.

Aspekt	Stufe	Argument
7	C	Die relevanten Stakeholder in der Organisation sind in das Themengebiet eingebunden.
8	C	Die erforderlichen Regelungen zur Verpflichtung von Externen auf die Vertraulichkeit und das Datengeheimnis werden den betroffenen Stakeholdern zugänglich gemacht und sind bekannt, z. B. geschult.
9	C	Die Regelungen zur Verpflichtung von Externen auf die Vertraulichkeit und das Datengeheimnis sind dokumentiert und müssen verbindlich umgesetzt werden.
10	C	Besondere Anforderungen sind identifiziert und berücksichtigt worden (zum Beispiel spezielle vertragliche Regelungen mit Auftraggebern).
11	D	Die erforderlichen Regelungen stehen in der Organisation unter Konfigurationsmanagement.
12	D	Die Umsetzung der Regelungen zur Verpflichtung von Externen auf die Vertraulichkeit und das Datengeheimnis wird konsequent verfolgt, z. B. durch regelmäßige interne Überprüfungen oder Audits. Alle vorher genannten Aspekte müssen erfüllt sein.
13	D	Das Management der jeweils höheren Ebene und der Auftraggeber wird regelmäßig über Verletzungen und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen informiert und entscheidet über weitere Eskalationen.
14	D	Datenschutzvorfälle und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen werden klassifiziert, bewertet und aufgezeichnet.
15	D	Zu den Aufzeichnungen werden in regelmäßigen und geplanten Abständen Analysen durchgeführt und mögliche Ursachen ermittelt.
16	E	Identifizierte Ursachen für Verletzungen und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an den Regelungen zur Verpflichtung von Externen auf die Vertraulichkeit und das Datengeheimnis selbst und den Geschäftsprozessen inkl. Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.
17	E	Kennzahlen zu den Regelungen zur Verpflichtung von Externen auf die Vertraulichkeit und das Datengeheimnis werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt.
18	E	Die Verbesserung der Regelungen zur Verpflichtung von Externen auf die Vertraulichkeit und das Datengeheimnis ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.
19	E	Ein ausgereiftes Kennzahlensystem zur Regelungen zur Verpflichtung von Externen auf die Vertraulichkeit und das Datengeheimnis ist identifiziert, eingeführt und wird betrieben und ausgewertet.

13.3 Informationssicherheit bei der Übermittlung von personenbezogenen Daten

Frage: Sind angemessene Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität bei der Übermittlung personenbezogener Daten vorhanden?

Aspekt	Stufe	Argument
0	Null	Es sind keine Maßnahmen zur Informationssicherheit bei der Übermittlung von personenbezogenen Daten definiert oder die Maßnahmen folgen keinem Konzept oder sie folgen keinem (einheitlichen) Sicherheitsstandard.
1	A	Es existieren Maßnahmen zur Informationssicherheit bei der Übermittlung von personenbezogenen Daten.
2	A	In die Anforderungen an die Maßnahmen zur Informationssicherheit bei der Übermittlung von personenbezogenen Daten werden folgende Aspekte einbezogen: <ul style="list-style-type: none"> Die eingesetzten Dienste sind identifiziert (z. B. E-Mail, VoIP) Personenbezogene Daten können von besonderen Kategorien personenbezogener Daten unterschieden werden Maßnahmen zum Schutz personenbezogener Daten vor unberechtigtem Zugriff bei der Übermittlung sind umgesetzt Es wird eine Transportverschlüsselung eingesetzt (TLS)
3	B	In die erweiterten Anforderungen an die Maßnahmen zur Informationssicherheit bei der Übermittlung von personenbezogenen Daten werden folgende Aspekte einbezogen: <ul style="list-style-type: none"> Eine korrekte Adressierung des Empfängers wird sichergestellt Eine elektronische Datenübermittlung erfolgt je nach Klassifikation (personenbezogene Daten und besondere Kategorien) Es werden Signaturen unter Beachtung der rechtlichen Vorgaben eingesetzt Bei externen IT-Systemen werden Kopien personenbezogener Daten angemessen verschlüsselt Schnittstellendefinition und -vereinbarung für Kommunikationsübergänge Ende-zu-Ende-Verschlüsselung
4	C	Die von der Informationssicherheit bei der Übermittlung von personenbezogenen Daten sind in die Geschäftsprozesse der Organisation eingearbeitet.
5	C	Die Mitarbeitenden im Bereich der Informationssicherheit bei der Übermittlung von personenbezogenen Daten sind für ihre Aufgaben qualifiziert und werden regelmäßig weitergebildet. Die Mitarbeitenden, die Prozesse ausführen, die unter dem Regime der Informationssicherheit in Netzwerken stehen, sind in den Prozessen geschult und werden bei Änderungen der Prozesse zeitnah nachgeschult.
6	C	Die Geschäftsprozesse und deren Aktivitäten, die unter dem Regime der Informationssicherheit bei der Übermittlung von personenbezogenen Daten stehen, sind in einer Liste im Anhang der Dokumentation der physischen Sicherheitskonzepte katalogisiert. Die Aspekte der Informationssicherheit bei der Übermittlung von personenbezogenen Daten sind dokumentiert, z. B. integriert in Prozesse.

Aspekt	Stufe	Argument
7	D	Die Dokumentation ist den betroffenen Stakeholdern und Rollen zugänglich und bekannt.
8	D	Die Konzeption der Informationssicherheit bei der Übermittlung von personenbezogenen Daten steht in der Organisation unter Konfigurationsmanagement.
9	D	Die Umsetzung und Einhaltung der Informationssicherheit bei der Übermittlung von personenbezogenen Daten wird konsequent verfolgt, z. B. durch regelmäßige interne Stichproben.
10	E	Kennzahlen zu Verletzungen und Schwachstellen werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt.
11	E	Die Verbesserung der Informationssicherheitsrichtlinie ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.

14 Anschaffung, Entwicklung und Instandhaltung von Systemen

14.1 Sicherheitsanforderungen an Informationssysteme

14.1.1 Anschaffung von Systemen

Frage: Besteht ein Anschaffungsprozess für Systeme und berücksichtigt dieser eine mögliche datenschutzrechtliche Implikation?

Aspekt	Stufe	Argument
0	NULL	Es bestehen keine Vorgaben für die Anschaffung von Systemen.
1	A	Einzelne Bereiche und Prozesse im Unternehmen wurden identifiziert, bei denen im Rahmen der Anschaffung von Systemen datenschutzrechtliche Aspekte zu berücksichtigen sind.
2	A	Für einzelne Abteilungen und Prozesse besteht eine Definition von System(en). Hierbei kann z. B. unterschieden werden zwischen <ul style="list-style-type: none"> ▪ Software, Hardware, Mischsystem ▪ Internes System (Eigenentwicklung), externes System (Fremdentwicklung) ▪ Innerhalb von Software z. B. weitergehend zwischen Programm, Prozess und Script ▪ Innerhalb von Hardware z. B. weitergehend zwischen Komplettsystem und Einzelkomponenten ▪ Standardsystem oder Individualsystem
3	A	Den jeweiligen Systemdefinitionen sind, jedenfalls für einige Bereiche und Prozesse, Vorgaben definiert worden, die bei Anschaffungen erfüllt werden sollten, um datenschutzrechtliche Implikationen zu adressieren.
4	A	Die Definition von Sytem(en) ist dokumentiert.
5	A	Die dokumentierte Definition ist dem erforderlichen Personal zugänglich.
6	B	Für erste Abteilungen und Prozesse besteht die Pflicht, bei der Anschaffung von Systemen die definierten Vorgaben einzuhalten.
7	B	Eine möglicherweise bestehende, datenschutzrechtliche Implikation von Anschaffungen wurde unternehmensweit für alle Bereiche und Prozesse analysiert.
8	B	Die Vorgaben zur Anschaffung adressieren einen sicheren Abnahmeprozess und Prüfroutinen bzgl. der Einhaltung der Anforderungen vor vollständiger Integration des Verarbeitungssystems in die bestehende Infrastruktur.
9	B	Die Bereiche und Prozesse mit identifizierter datenschutzrechtlicher Implikation sind dokumentiert.
10	C	Für alle Bereiche und Prozesse mit identifizierter datenschutzrechtlicher Implikation besteht eine Definition von System(en).
11	C	Die Vorgaben zur Anschaffung adressieren den Einsatz der Verarbeitungssysteme in öffentlichen Netzwerken.
12	C	Für alle Systemdefinitionen wurden Vorgaben definiert, die bei der Anschaffung erfüllt werden sollten.
13	C	Die Einhaltung der Vorgaben bei der Anschaffung ist unternehmensweit verpflichtend.

Aspekt	Stufe	Argument
14	D	Es besteht eine unternehmensweit einheitliche Definition von System(en).
15	D	Die datenschutzrechtliche Implikation ist abhängig von den Bereichen und Prozessen, sowie den Aspekten des anzuschaffenden Systems analysiert und in eine Risikoanalyse überführt worden.
16	D	Die festgestellten Risiken wurden dokumentiert.
17	E	Entsprechend der festgestellten Risiken wurden die definierten Vorgaben für die Anschaffung modifiziert und ggf. erweitert.
18	E	Die Anschaffungsprozesse wurden teilweise so ausgestaltet, dass die etwaig erweiterten Vorgaben für die Anschaffung entsprechend der Risiken beachtet werden.
19	E	Die Anschaffungsprozesse sind dokumentiert und veröffentlicht.
20	F	Die Anschaffungsprozesse wurden unternehmensweit so ausgestaltet, dass etwaig erweiterte Vorgaben für die Anschaffung entsprechend der Risiken beachtet werden.
21	F	Die Anforderungen für die Anschaffung von Verarbeitungssystemen werden regelmäßig kontrolliert und auf ihre Wirksamkeit hin überprüft.
22	F	Verfahren zur Bearbeitung potentieller Vorfälle im Zusammenhang mit der Verarbeitung personenbezogener Daten berücksichtigen auch Korrelationen zur Anschaffung von Verarbeitungssystemen und führen – soweit notwendig – zu veränderten Anforderungen.
23	G	Die Anschaffungsprozesse sind technisch unterstützt und protokolliert.
24	G	Soweit die Anforderungen Freizeichnungen oder Prüfungen vorsehen, ist eine Anschaffung und /oder Integration in bestehende Infrastruktur technisch ausgeschlossen.
25	G	Das mit der Kontrolle und Analyse der dokumentierten Anschaffungsprozesse, Systemdefinitionen und Risiken betraute interne Personal wird regelmäßig geschult.
26	H	Das mit der Kontrolle und Analyse der dokumentierten Anschaffungsprozesse, Systemdefinitionen und Risiken betraute interne Personal berichtet der jeweils nächst höheren Managementebene.
27	H	Verfahren zum Umgang der Ergebnisse der internen Kontrollen und Analysen sehen vor, dass die vom internen Personal vorgeschlagenen notwendigen Änderungen nicht mit qualifizierter Begründung abgelehnt werden können.
28	I	Das mit der Kontrolle und Analyse der dokumentierten Anschaffungsprozesse, Systemdefinitionen und Risiken betraute interne Personal wird durch externe Prüfer komplementiert.
29	I	Eine regelmäßige externe Kontrolle und Analyse der Effektivität der Anschaffungsprozesse, Systemdefinitionen und Risiken findet statt.
30	J	Verfahren zum Umgang der Ergebnisse der externen Kontrollen und Analysen sehen vor, dass die vom externen Personal vorgeschlagenen notwendigen Änderungen nicht mit qualifizierter Begründung abgelehnt werden können.
31	J	Die dokumentierten Anschaffungsprozesse, Systemdefinitionen und Risiken, sowie deren Kontrolle und Analyse sind Bestandteil der in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagements.

14.2 Weiterentwicklung von Systemen

Frage: Besteht ein Prozess für die Weiterentwicklung von Systemen und berücksichtigt dieser etwaige datenschutzrechtliche Implikationen?

Aspekt	Stufe	Argument
0	NULL	Es bestehen keine Vorgaben für die (Weiter-) Entwicklung von Systemen.
1	A	Einzelne Bereiche und Prozesse im Unternehmen wurden identifiziert, bei denen im Rahmen der (Weiter-) Entwicklung von Systemen datenschutzrechtliche Aspekte zu berücksichtigen sind.
2	A	Für einzelne Abteilungen und Prozesse besteht eine Definition von System(en). Hierbei kann z. B. unterschieden werden zwischen <ul style="list-style-type: none"> ▪ Software, Hardware, Mischsystem ▪ Internes System (Eigenentwicklung), externes System (Fremdentwicklung) ▪ Innerhalb von Software z. B. weitergehend zwischen Programm, Prozess und Script ▪ Innerhalb von Hardware z. B. weitergehend zwischen Komplettsystem und Einzelkomponenten ▪ Standardsystem oder Individualsystem
3	A	Den jeweiligen Systemdefinitionen sind, jedenfalls für einige Bereiche und Prozesse, Vorgaben definiert worden, die bei der (Weiter-) Entwicklung erfüllt werden sollten um datenschutzrechtliche Implikationen zu adressieren. Derartige Vorgaben adressieren z. B. <ul style="list-style-type: none"> ▪ Verwendung von Testdaten anstellen von Echtdateien der durchgeführten (Weiter-) Entwicklung ▪ Stabilitäts- und Sicherheitstests
4	A	Die Definition von System(en) ist dokumentiert.
5	A	Die dokumentierte Definition ist dem erforderlichen Personal zugänglich.
6	B	Für erste Abteilungen und Prozesse besteht die Pflicht bei der (Weiter-) Entwicklung von Systemen die definierten Vorgaben einzuhalten.
7	B	Eine möglicherweise bestehende, datenschutzrechtliche Implikation der (Weiter-) Entwicklung von System(en) wurde unternehmensweit für alle Bereiche und Prozesse analysiert.
8	B	Die Vorgaben zur (Weiter-) Entwicklung adressieren einen sicheren Abnahmeprozess und Prüfroutinen bzgl. der Einhaltung der Anforderungen vor vollständiger Integration des Verarbeitungssystems in die bestehende Infrastruktur.
9	B	Die Bereiche und Prozesse mit identifizierter datenschutzrechtlicher Implikation sind dokumentiert.
10	C	Für alle Bereiche und Prozesse mit identifizierter datenschutzrechtlicher Implikation besteht eine Definition von System(en).
11	C	Die Vorgaben zur (Weiter-) Entwicklung adressieren den Einsatz der Verarbeitungssysteme in öffentlichen Netzwerken.
12	C	Für alle Systemdefinitionen wurden Vorgaben definiert, die bei der (Weiter-) Entwicklung erfüllt werden sollten.

Aspekt	Stufe	Argument
13	C	Die Einhaltung der Vorgaben bei der (Weiter-) Entwicklung ist unternehmensweit verpflichtend.
14	D	Es besteht eine unternehmensweit einheitliche Definition von System(en).
15	D	Die datenschutzrechtliche Implikation ist abhängig der Bereiche und des Prozesses sowie der Aspekte des (weiter-) zu-entwickelnden Systems analysiert und in eine Risikoanalyse überführt worden.
16	D	Die festgestellten Risiken wurden dokumentiert.
17	E	Entsprechend den festgestellten Risiken wurden die definierten Vorgaben für die (Weiter-) Entwicklung modifiziert und ggf. erweitert.
18	E	Die (Weiter-) Entwicklungsprozesse wurden teilweise so ausgestaltet, dass die etwaig erweiterten Vorgaben für die (Weiter-) Entwicklung entsprechend der Risiken beachtet werden.
19	E	Die (Weiter-) Entwicklungsprozesse sind dokumentiert und veröffentlicht.
20	F	Die (Weiter-) Entwicklungsprozesse wurden unternehmensweit so ausgestaltet, dass etwaig erweiterten Vorgaben für die (Weiter-) Entwicklung entsprechend der Risiken beachtet werden.
21	F	Die Anforderungen für die (Weiter-) Entwicklung von Verarbeitungssystemen werden regelmäßig kontrolliert und auf ihre Wirksamkeit hin überprüft.
22	F	Verfahren zur Bearbeitung potentieller Vorfälle im Zusammenhang mit der Verarbeitung personenbezogener Daten berücksichtigen auch Korrelationen zur (Weiter-) Entwicklung von Verarbeitungssystemen und führen – soweit notwendig – zu veränderten Anforderungen.
23	G	Die (Weiter-) Entwicklungsprozesse sind technisch unterstützt und protokolliert.
24	G	Soweit die Anforderungen Freizeichnungen oder Prüfungen vorsehen, ist eine (Weiter-) Entwicklung und / oder Integration in bestehende Infrastruktur technisch ausgeschlossen.
25	G	Das mit der Kontrolle und Analyse der dokumentierten (Weiter-) Entwicklungsprozesse, Systemdefinitionen und Risiken betraute interne Personal wird regelmäßig geschult.
26	H	Das mit der Kontrolle und Analyse der dokumentierten (Weiter-) Entwicklungsprozesse, Systemdefinitionen und Risiken betraute interne Personal berichtet der jeweils nächst höheren Managementebene.
27	H	Verfahren zum Umgang der Ergebnisse der internen Kontrollen und Analysen sehen vor, dass die vom internen Personal vorgeschlagenen notwendigen Änderungen nicht mit qualifizierter Begründung abgelehnt werden können.
28	I	Das mit der Kontrolle und Analyse der dokumentierten (Weiter-) Entwicklungsprozesse, Systemdefinitionen und Risiken betraute interne Personal wird durch externe Prüfer komplementiert.
29	I	Eine regelmäßige externe Kontrolle und Analyse der Effektivität der (Weiter-) Entwicklungsprozesse, Systemdefinitionen und Risiken findet statt.
30	J	Verfahren zum Umgang der Ergebnisse der externen Kontrollen und Analysen sehen vor, dass die vom externen Personal vorgeschlagenen notwendigen Änderungen nicht mit qualifizierter Begründung abgelehnt werden können.
31	J	Die dokumentierten (Weiter-) Entwicklungsprozesse, Systemdefinitionen und Risiken sowie deren Kontrolle und Analyse sind Bestandteil der in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagements.

14.2.1 Entwicklung und Wartung von Software für die Verarbeitung personenbezogener Daten: Konzeption und Abnahme

Dieser Abschnitt setzt den Schwerpunkt auf datenschutzrelevante Aspekte der im Hause eines Auftragsverarbeiters (AV) stattfindenden Entwicklung und Wartung von Software zur Erfüllung seiner AV-Tätigkeiten. Das Themengebiet definiert ergänzende Aspekte zu Datenschutz, Informationssicherheit, Informationsrisikomanagement, Benutzerberechtigungsmanagement und IT-Sicherheit an die Prozesse zur Entwicklung und Wartung von Software und setzt auf technischer Ebene Mindestanforderungen und eine professionelle Werkzeugkette zur Unterstützung der Entwicklungs- und Wartungstätigkeiten.

In diesem Themengebiet wird aus Gründen der Übersichtlichkeit der Fokus auf die Konzeption (Anforderungen) und den Abnahmetest bei der Entwicklung und Wartung von Software für die Verarbeitung personenbezogener Daten gesetzt.

Frage: Werden bei der Konzeption von Software-Systemen, welche konkret für die Auftragsverarbeitung eingesetzt werden, Aspekte zu Datenschutz und Informationssicherheit sowie die expliziten Anforderungen des Auftraggebers berücksichtigt?

Aspekt	Stufe	Argument
0	NULL	Keine Berücksichtigung von Aspekten zu Datenschutz und Informationssicherheit in den Entwicklungsprozessen für Software Systeme des AV.
1	A	<p>Datenschutzrechtliche Anforderungen an Software und an die konkret zu entwickelnde beziehungsweise zu modifizierende oder wartende Software werden in den Entwicklungsprozessen für Software im Unternehmen (hier: AV) berücksichtigt. Spezielle Anforderungen an die Software werden ebenfalls berücksichtigt, wie z. B.</p> <ul style="list-style-type: none"> ▪ Zugriffs- und Nutzungsrechte für Daten für Interne und Externe ▪ Behandlung von datenschutzrechtlichen Erlaubnistatbeständen für die Verarbeitung ▪ Aspekte der Informationssicherheit ▪ des Informationssicherheitsmanagements ▪ des Informationsrisikomanagements ▪ des Benutzerberechtigungsmanagements
	A	<p>Darüber hinaus werden weitere relevante nichtfunktionale Anforderungen in Betracht gezogen, z. B.</p> <ul style="list-style-type: none"> ▪ Verfügbarkeit ▪ Zuverlässigkeit ▪ Skalierbarkeit bei der Erhebung von Anforderungen
2	A	Datenschutzrechtliche Anforderungen des Auftraggebers an Software und an die konkret zu entwickelnde bzw. zu modifizierende Software oder – im Fall von multiplen Mandanten – an die allgemein zu erwartenden Anforderungen werden in den Entwicklungsprozessen für Software beim AV berücksichtigt.
3	B	Im Unternehmen (hier: AV) existiert eine Leitlinie oder Ergänzung zu einer Leitlinie zur Softwareentwicklung und Softwarewartung, die die Anforderungen der Organisation an die Berücksichtigung von Aspekten des Datenschutzes und der Informationssicherheit klar formuliert.

Aspekt	Stufe	Argument
4	B	Datenschutzrechtliche Anforderungen an die Software werden im Anforderungserhebungsprozess explizit berücksichtigt. Aus den datenschutzrechtlichen Anforderungen werden explizite Anforderungen an die Umsetzung von Datenschutz, Informationssicherheit und IT-Sicherheit in der Software und der durch sie unterstützten Prozesse abgeleitet. Diese gehen in die Dokumentation der Kundenanforderungen an die Software ein (alternativer Begriff: Lastenheft). Falls ein agiler Entwicklungsprozess im Einsatz ist, werden die relevanten Aspekte bei der Erstellung der Epics mindestens in Form von Constraints berücksichtigt.
5	B	Aus den Kundenanforderungen werden Detailanforderungen entwickelt, in welchen auch die datenschutzrechtlichen Anforderungen an die Software hinsichtlich Datenschutz, Informationssicherheit und IT-Sicherheit detailliert und verfolgbar zu den Kundenanforderungen abgeleitet werden. Diese gehen in die Dokumentation der Detailanforderungen an die Software ein (alternativer Begriff: Pflichtenheft). Falls ein agiler Entwicklungsprozess im Einsatz ist, werden die relevanten Aspekte in die User-Stories aufgenommen und bei Bedarf spezielle User-Stories bezüglich Datenschutz und Informationssicherheit erstellt.
6	B	Die mit Anforderungsmanagement (Erhebung, Modellierung, Dokumentation und Management) betrauten Teammitglieder sind hinsichtlich Datenschutz und Informationssicherheit in der Softwareentwicklung geschult und besitzen Stand-der-Praxis-Wissen in ihrer jeweiligen Disziplin.
7	B	Für die Dokumentation und das Management von Anforderungen wird ein adäquates Werkzeug passend zum grundsätzlichen Typ des Vorgehensmodells der Software Entwicklung und Wartung (wasserfallartig, iterativ, agil) eingesetzt.
8	C	In Abnahmetests (Validierung) werden in die Beschreibung der operativen Szenarien für die Abnahme, die als Grundlage für die Validierung beschrieben werden, für die Nutzung der Software relevante Aspekte aus den datenschutzrechtlichen Anforderungen an die Software mit aufgenommen und ausgeführt. Bei der Durchführung der Validierung beobachtete Anomalien werden dokumentiert, analysiert und ausgewertet. Auf Basis der Ergebnisse werden im Bedarfsfall Korrekturmaßnahmen an der Software vorgenommen. In den Szenarien wird neben der geplanten Verwendung der Software auch relevante (versuchte) missbräuchliche Verwendung der Software berücksichtigt.
9	C	Eine Erfolgskontrolle hinsichtlich Einhaltung von Leitlinien und Regelprozessen wird stichprobenartig, aber regelmäßig, durchgeführt.
10	C	Für die Erhebung und Dokumentation von Anforderungen sowie Abnahmetests von Software existiert ein Regelprozess in der Organisation. Der Regelprozess ist allen in diesem Themenbereich eingesetzten Mitarbeitenden (Stakeholdern) bekannt und sie sind in diesem Bereich geschult und besitzen Stand-der-Praxis-Wissen. Das Management hat den Regelprozess verabschiedet.
11	C	Bei Durchführung der Erhebung und Dokumentation von Anforderungen und dem Abnahmetesten werden die relevanten Stakeholder, z. B. Vertreter des Auftraggebers, Datenschutzbeauftragter, etc. in der Erhebung von Anforderungen und Vertreter der Anwenderseite des Auftraggebers bei der Abnahme, eingebunden.
12	C	Für die Durchführung von Anforderungserhebung und -dokumentation sowie die Durchführung von Abnahmetests werden Ressourcen gemäß Bedarf eingeplant.
13	C	Die eingeplanten Ressourcen werden bereitgestellt.
14	C	Die mit der Abnahme (Erstellung von Szenarien, Ausführung Abnahmetests, Auswertung und Testmanagement) betrauten Teammitglieder sind hinsichtlich Datenschutz und Informationssicherheit in der Software Entwicklung geschult und besitzen Stand-der-Praxis-Wissen in ihrer jeweiligen Disziplin.
15	D	Basierend auf einer Risikoeinschätzung werden Sicherheits- und Penetrationstests als dezidierte Teststufe (oder Teil der Abnahme) zur Sicherstellung von Datenschutz, Informationssicherheit und IT-Sicherheit durchgeführt. Auf Basis der Ergebnisse werden im Bedarfsfall Korrekturmaßnahmen an der Software vorgenommen.

Aspekt	Stufe	Argument
16	D	Es werden Kategorien zur Klassifikation von Testergebnissen und Code-Reviews bzgl. Datenschutz und Informationssicherheit entwickelt, so dass sowohl die Art eines Fehlverhaltens des Systems als auch die Schwere des Fehlverhaltens hinreichend detailliert bewertet werden können. Kategorien für die Testergebnisse können z. B. sein „Unerlaubter Zugriff auf Daten“, „fehlende Verschlüsselung“. Kategorien für die Schwere der Fehlverhalten können z. B. sein „meldepflichtiger Vorfall“, „nicht meldepflichtiger Vorfall“.
17	D	Die in den Abnahmetests identifizierten Fehlverhalten und Fehler werden statistisch hinsichtlich der Kategorien ausgewertet.
18	D	Die Korrektur der in den Abnahmetests identifizierten Anomalien, Fehlverhalten, Fehler und Abweichungen wird durch geeignete Verfolgungssysteme überwacht.
19	D	Es werden regelmäßige Überprüfungen der Umsetzung der Leitlinien zur Entwicklung und Wartung von Software für Datenverarbeitung durchgeführt. Abweichungen werden aufgezeichnet und dem Management zur Kenntnis gebracht.
20	D	Eine Information des höheren Managements über Status und Planabweichungen der Projekte zur Entwicklung und Wartung von Software für Datenverarbeitung findet regelmäßig statt.
21	D	Ursachen für Abweichungen werden ermittelt und gezielte Maßnahmen zur Behebung und Abstellung der Ursachen werden ergriffen und zuende gesteuert.
22	E	Kennzahlen zu Abläufen, z. B. Verletzungen von Leitlinien, Schwachstellen, Erfolge werden im Rahmen eines KVP zielführend eingesetzt.
23	E	Die Kennzahlen werden analysiert um die Identifikation von Verbesserungsmaßnahmen zu unterstützen.
24	E	Die Entwicklungs- und Wartungsprozesse für Software zur Datenverarbeitung sind in einen kontinuierlichen Verbesserungsprozess im Unternehmen integriert.

14.2.2 Entwicklung und Wartung von Software für die Verarbeitung personenbezogener Daten: Technische Umsetzung (Architektur, Code) und Tests bis zur Ebene Systemtests

In diesem Abschnitt wird nach der »Konzeption und Abnahme« aus dem vorigen Abschnitt der Fokus auf die technische Umsetzung (Architektur, Code) und Tests bis zur Ebene von Systemtests bei der Entwicklung und Wartung von Software für die Verarbeitung personenbezogener Daten gesetzt.

Frage: Werden bei der Entwicklung von Software-Systemen, welche konkret für die Auftragsverarbeitung eingesetzt werden, Aspekte zu Datenschutz und Informationssicherheit, insbesondere während der Phasen der Implementation und Tests-Durchführung, berücksichtigt?

Aspekt	Stufe	Argument
0	Null	Keine Berücksichtigung von Aspekten des Datenschutzes und der Informationssicherheit bei der Entwicklung von Software-Systemen, welche konkret für die Auftragsverarbeitung eingesetzt werden.
1	A	In Systemtests (Verifikation) werden Testfälle, die die aus Detailanforderungen abgeleiteten Anforderungen an die Software hinsichtlich Umsetzung von Datenschutz, Informationssicherheit überprüfen, erstellt und ausgeführt, die Ergebnisse dokumentiert und ausgewertet. Auf Basis der Ergebnisse werden im Bedarfsfall Korrekturmaßnahmen an der Software vorgenommen.
2	A	Die Testfälle enthalten sowohl Positiv- als auch Negativtests wie auch Penetrationstests.
3	A	Die mit dem Systemtest (Testfallerstellung, Ausführung, Auswertung und Testmanagement) betrauten Teammitglieder sind hinsichtlich Datenschutz und Informationssicherheit in der Softwareentwicklung geschult und besitzen Stand-der-Praxis-Wissen in ihrer jeweiligen Disziplin.
4	A	Für die Dokumentation, das Management und die Ausführung von Testfällen werden, wo sinnvoll, adäquate Werkzeuge eingesetzt. Dies betrifft grundsätzlich alle Ebenen von Tests wie Unit Test, Integrationstest, Systemtest und an moderne Build-Prozesse gebundene Kombinationen von Tests, die dann beispielsweise als Sanity Checks oder Smoketests fungieren.
5	A	Es existiert ein der Größe, Kritikalität und Komplexität der Software wirtschaftlich angemessener (teil)automatisierter Build-Prozess, der regelmäßige, automatisierte Tests auf funktionale und nichtfunktionale Eigenschaften der Software einbindet.
6	B	Im Rahmen des automatisierten Build-Prozesses werden Prüfungen der Software auf Informations- und IT-Sicherheit, z. B. durch Code-Scans nach bekannten Schwachpunkten oder unsicheren Code Mustern, OWASP Kriterien, etc. durchgeführt.
7	B	Die bestehenden datenschutzrechtlichen Anforderungen an die Software werden bei der Entwicklung und Definition bzw. der Anpassung der Software Architektur und des Software Designs berücksichtigt. Entscheidungen zu Architektur und Design werden dokumentiert. Im Fall, dass Entscheidungen bei Architektur und Design sich aus Anforderungen an Datenschutz und Informationssicherheit ergeben, werden diese Entscheidungen ebenfalls mit Verweis auf die entsprechenden Anforderungen in Architektur und Design dokumentiert.
8	B	Ein Regelprozess für Architektur und Design von Anwendungen zur Verarbeitung personenbezogener Daten existiert. Die mit der Architektur und dem Design (Entwicklung und Dokumentation) betrauten Teammitglieder sind hinsichtlich Datenschutz, Informationssicherheit und IT-Sicherheit in der Softwareentwicklung geschult und besitzen Stand-der-Praxis-Wissen in ihrer jeweiligen Disziplin. Das Management hat den Regelprozess verabschiedet.
9	B	Ein Regelprozess für Integrationstests von Anwendungen zur Verarbeitung personenbezogener Daten existiert. Die mit dem Integrationstest (Testfallerstellung, Ausführung, Auswertung und Testmanagement) betrauten Teammitglieder sind hinsichtlich Datenschutz und Informationssicherheit in der Softwareentwicklung geschult und besitzen Stand-der-Praxis-Wissen in ihrer jeweiligen Disziplin. Das Management hat den Regelprozess verabschiedet.
10	B	Für die Durchführung der Entwicklung von Architektur und Design sowie die Durchführung von Integrationstests und Systemtests werden Ressourcen gemäß Bedarf eingeplant.

Aspekt	Stufe	Argument
11	B	Die eingeplanten Ressourcen werden bereitgestellt.
12	B	Die Implementierung (Coding und Unit Testing) des Designs wird gemäß einem Regelprozess, der auch Coding Guidelines enthält, durchgeführt. Hinsichtlich Regelprozess sind alle involvierten Mitarbeitenden geschult und ihr Wissen entspricht Stand-der-Praxis-Wissen. Der Regelprozess wurde vom Management verabschiedet.
13	B	Für die Durchführung der Implementierung und Entwicklung des Designs (Coding und Unuit Tests) werden Ressourcen gemäß Bedarf eingeplant.
14	B	Die eingeplanten Ressourcen werden bereitgestellt.
15	B	Während der Implementierung des Designs werden die getroffenen Architektur- und Designentscheidungen hinsichtlich Datenschutz und Informationssicherheit umgesetzt und durch Unit Tests verifiziert.
16	B	Der Code der Anwendungen wird in geeigneten Versions- und Konfigurationsmanagementsystemen verwaltet. Zur Verwaltung gehört auch die Konservierung, beziehungsweise Referenzierung der für jeden Softwarestand relevanten begleitenden Dokumentation der Anforderungen, z. B. als Lastenheft / Pflichtenheft, beziehungsweise Epics / User Stories der Architektur, des Designs und der Testfälle.
17	B	Die mit der Implementierung des Designs (Coding, Kommentierung, Unit Tests, technische Dokumentation), betrauten Teammitglieder sind hinsichtlich Datenschutz, Informationssicherheit und IT-Sicherheit in der Softwareentwicklung geschult und besitzen Stand-der-Praxis-Wissen in ihrer jeweiligen Disziplin.
18	B	Auf Basis einer Risikoabschätzung ist eine Architekturschicht für Zugriffs- und Nutzungskontrolle von personenbezogenen Daten als kapselnde Privacy-by-Design-Schicht in der Architektur der Software enthalten.
19	B	In Stichproben werden Code-Reviews zur Sicherstellung der Umsetzung Architektur- und Designentscheidungen hinsichtlich Datenschutz, Informationssicherheit durchgeführt. Auffälligkeiten, d.h. Abweichungen zwischen Design und Code, werden dokumentiert, bewertet und im Bedarfsfall Korrekturmaßnahmen vorgenommen. Kriterien für die Anwendung von stichprobenartigen Code-Reviews sind vorhanden. Kriterien können z. B. sein »Stellen besonderer algorithmischer Komplexität im Code«, »Stellen im Code mit hoher Anzahl von Schnittstellen für Übertragung von personenbezogenen Daten«.
20	B	Eine Erfolgskontrolle hinsichtlich Einhaltung von Leitlinien und Regelprozessen wird stichprobenartig, aber regelmäßig, durchgeführt.
21	C	Es werden Kategorien zur Klassifikation von Testergebnissen und Code-Reviews bzgl. Datenschutz und Informationssicherheit entwickelt, sodass sowohl die Art eines Fehlers oder Fehlverhaltens der Software, als auch die Schwere des Fehlverhaltens hinreichend detailliert bewertet werden kann. Kategorien für die Testergebnisse können z. B. sein »Unerlaubter Zugriff auf Daten« oder »fehlende Verschlüsselung«. Kategorien für die Schwere der Fehlverhalten können z. B. »meldepflichtiger Vorfall«, »nicht meldepflichtiger Vorfall« sein.
22	C	Die in den verschiedenen Teststufen identifizierten Fehlverhalten und Fehler werden statistisch hinsichtlich der Kategorien ausgewertet.
23	C	Die Korrektur der in den verschiedenen Teststufen und Code-Reviews identifizierten Anomalien, Fehlverhalten, Fehler und Abweichungen wird durch geeignete Verfolgungssysteme überwacht.

Aspekt	Stufe	Argument
24	C	Es werden regelmäßige Überprüfungen der Umsetzung der Leitlinien zur Entwicklung und Wartung von Software für Datenverarbeitung durchgeführt. Abweichungen werden aufgezeichnet und dem Management zur Kenntnis gebracht.
25	C	Eine Information des höheren Managements über Status und Planabweichungen der Projekte zur Entwicklung und Wartung von Software für Datenverarbeitung findet regelmäßig statt.
26	D	Ursachen für Abweichungen werden ermittelt und gezielte Maßnahmen zur Behebung und Abstellungen der Ursachen werden ergriffen und zuende gesteuert.
27	D	Kennzahlen zu Abläufen, z. B. Verletzungen von Leitlinien, Schwachstellen, Erfolgen, werden im Rahmen eines KVP zielführend eingesetzt.
28	D	Die Kennzahlen werden analysiert um die Identifikation von Verbesserungsmaßnahmen zu unterstützen.
29	E	Die Entwicklungs- und Wartungsprozesse für Software zur Datenverarbeitung sind in einen kontinuierlichen Verbesserungsprozess im Unternehmen integriert.
30	E	Auf Basis einer Risikobewertung werden Sicherheits- und Penetrations-tests als dezidierte Teststufe zur Sicherstellung von Datenschutz und Informationssicherheit ausgeführt. Auf Basis der Ergebnisse werden im Bedarfsfall Korrekturmaßnahmen an der Software vorgenommen.
31	E	Die mit Sicherheits- und Penetrationstests (Testfallerstellung, Ausführung, Auswertung und Testmanagement) betrauten Teammitglieder sind hinsichtlich Datenschutz, Informationssicherheit in der Software Entwicklung geschult und besitzen Stand-der-Praxis-Wissen in ihrer jeweiligen Disziplin.
32	F	Es werden zur Durchführung von Sicherheits- und Penetrationstests geeignete Werkzeuge, die dem Stand der Praxis entsprechen, eingesetzt.

14.3 Instandhaltung und Wartung von Systemen

Fragen: Besteht – unabhängig etwaiger Weiterentwicklung – ein Prozess zur Wartung und Instandhaltung von Systemen und werden etwaige datenschutzrechtliche Implikationen berücksichtigt?

Aspekt	Stufe	Argument
0	Null	Es sind keine Vorgaben zur Wartung und Instandhaltung vorhanden.
1	A	Es sind jedenfalls abstrakte Wartungspläne vorhanden. Solche Wartungspläne berücksichtigen Aspekte wie z. B. <ul style="list-style-type: none"> ▪ Update-Zyklen ▪ Veröffentlichungs- / Implementierungsphasen ▪ Notfallsysteme, Redundanzen und Wiederherstellbarkeiten ▪ Analyse und Auswertung externer (Fach-) Quellen
2	B	Jedenfalls für Systeme, die personenbezogene Date mit hohem Risiko verarbeiten, bestehen systemspezifische Wartungspläne.
3	B	Soweit Wartungspläne bestehen, sind diese verbindlich einzuhalten.
4	C	Für alle definierten Systeme besteht ein Wartungsplan.
5	C	Die Einhaltung der Wartungspläne wird intern geprüft.
6	D	Die Wartungspläne werden regelmäßig intern evaluiert und angepasst.
7	D	Wartungspläne werden in Rücksprache mit anderen Abteilungen, z. B. Informationssicherheit oder Business Continuity besprochen und entwickelt.
8	D	Die Wartungspläne umfassen mindestens die Aspekte: <ul style="list-style-type: none"> ▪ Update-Zyklen ▪ Veröffentlichungs- / Implementierungsphasen ▪ Notfallsysteme, Redundanzen und Wiederherstellbarkeiten ▪ Analyse und Auswertung externer (Fach-) Quellen ▪ Unversehrtheit und Integrität der Protokolldateien ▪ automatisierte, technisch unterstützte Überwachung von Systemveränderung (Schutz vor Kompromittierung) ▪ Aspekte, die ansonsten als sicherheitsrelevant für ein System definiert wurden
9	E	Die Einhaltung der Wartungspläne wird auch extern geprüft.

15

Lieferantenbeziehungen

15.1 Technische und organisatorische Maßnahmen bei der Auftragsverarbeitung (Organisation als Auftraggeber)

Bei der Beurteilung der technischen und organisatorischen Maßnahmen bei der Auftragsverarbeitung ist nicht nur das Sicherheitsniveau der Verarbeitung beim Auftragnehmer zu beurteilen, auch das Sicherheitsniveau der Verarbeitung bei den Subauftragnehmern.

Hinweis: Für den Vertrag zur Auftragsverarbeitung ist es irrelevant, ob der Vertragstext im Hauptvertrag eingearbeitet ist oder der Vertrag zur Auftragsverarbeitung ein eigenständiges Vertragswerk ist. Es ist nur darauf abzustellen, dass alle gesetzlich geforderten Regelungen getroffen worden sind und die Formvorschriften eingehalten worden sind.

Frage: Wird bei der Zusammenarbeit mit Auftragnehmern im Rahmen einer Auftragsverarbeitung das erforderliche Sicherheitsniveau nach Art. 32 DS-GVO bestimmt, dokumentiert und vereinbart?

Aspekt	Stufe	Argument
0	Null	Vom Auftraggeber wurde kein angemessenes Sicherheitsniveau für die Verarbeitung personenbezogener Daten bei einer Auftragsverarbeitung durch den Auftragnehmer bestimmt.
1	A	Vom Auftraggeber wurde das angemessene Sicherheitsniveau für die Verarbeitung personenbezogener Daten bei einer Auftragsverarbeitung durch den Auftragnehmer bestimmt, verabschiedet und veröffentlicht. Die Bestimmung des angemessenen Sicherheitsniveaus bei der Verarbeitung ist das Ergebnis einer Risikoanalyse (Erwägungsgrund 81, Satz 3: »[...] und das Risiko für die Rechte und Freiheiten der betroffenen Person zu berücksichtigen sind.«).
2	B	Für die Einhaltung der technischen und organisatorischen Maßnahmen zur Einhaltung des erforderlichen Sicherheitsniveaus bei der Verarbeitung durch den Auftragnehmer sind die Rechte und Pflichten zugewiesen worden.
3	C	Ein datenschutzkonformer Vertrag zur Auftragsverarbeitung (Erfüllung der Anforderungen des Art. 28 DS-GVO) ist rechtskonform abgeschlossen worden. Die erforderlichen technischen und organisatorischen Maßnahmen sind im Vertrag dokumentiert und werden regelmäßig auditiert (Art. 32 Abs. 1 lit. d DS-GVO). Das Auditintervall der technischen und organisatorischen Maßnahmen orientiert sich am Risiko der Verarbeitung für die Rechte und Freiheiten der Betroffenen.
4	C	Die vertraglich vereinbarten technischen und organisatorischen Maßnahmen sind beim Auftragnehmer in die Geschäftsprozesse der Organisation eingearbeitet.

Aspekt	Stufe	Argument
5	C	Für die Umsetzung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen sind die notwendigen Ressourcen identifiziert und geplant worden.
6	C	Für die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen sind die notwendigen Ressourcen bewilligt worden und werden planmäßig freigegeben.
7	C	Die beim Auftragnehmer relevanten Stakeholder sind in das Themengebiet eingebunden.
8	C	Die erforderlichen technischen und organisatorischen Maßnahmen werden den beim Auftragnehmer betroffenen Stakeholdern zugänglich gemacht und sind bekannt, z. B. geschult.
9	C	Die erforderlichen technischen und organisatorischen Maßnahmen sind dokumentiert und müssen verbindlich umgesetzt werden.
10	C	Besondere Anforderungen sind identifiziert und berücksichtigt worden.
11	D	Die erforderlichen technischen und organisatorischen Maßnahmen stehen in der Organisation unter Konfigurationsmanagement.
12	D	Die Umsetzung und Einhaltung der Datenschutzmaßnahmen der Informationssicherheit bei der Zusammenarbeit mit Lieferanten wird konsequent verfolgt, z. B. durch regelmäßige Audits.
13	D	Das Management der jeweils höheren Ebene und der Auftraggeber wird regelmäßig über Verletzungen und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen informiert und entscheidet über weitere Eskalationen.
14	D	Datenschutzvorfälle und Schwachstellen bei den vertraglich vereinbarten technischen und organisatorischen Maßnahmen werden klassifiziert, bewertet und aufgezeichnet.
15	D	Zu den Aufzeichnungen werden in regelmäßigen und geplanten Abständen Analysen durchgeführt und mögliche Ursachen ermittelt.
16	E	Identifizierte Ursachen für Datenschutzvorfälle und Schwachstellen werden im Rahmen von Verbesserungsmaßnahmen behandelt. Dabei können sich Änderungen an den technischen und organisatorischen Maßnahmen beim Auftragnehmer selbst und den Geschäftsprozessen inkl. Rollen und Verantwortlichkeiten ergeben. Die Änderungen werden adäquat kommuniziert, z. B. durch Schulungen oder Informationsveranstaltungen, und auch entsprechend der vertraglichen Vereinbarungen dokumentiert. Für die Verbesserungen werden hinreichende Ressourcen bereitgestellt.
17	E	Kennzahlen zu Datenschutzvorfällen und Schwachstellen werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses zielführend eingesetzt. Eine Kennzahl kann sein, die »Summe der Fehlübermittlungen von personenbezogenen Daten pro Jahr zwischen Auftragnehmer und Auftraggeber«.
18	E	Die Verbesserung der technischen und organisatorischen Maßnahmen beim Auftragnehmer ist Teil eines in der Organisation etablierten kontinuierlichen Verbesserungsprozesses und Qualitätsmanagementsystems.
19	E	Ein ausgereiftes Kennzahlensystem ist identifiziert, eingeführt und wird betrieben und ausgewertet.

16 Handhabung von Datenschutzvorfällen

16.1 Mitwirkung des Informationssicherheitsbeauftragten

Der Informationssicherheitsbeauftragte wird installiert, um das Management im Umgang mit Vorfällen und die organisatorische und technische Sicherheit im Informationsverbund unterstützend zu beraten.

Aspekt	Stufe	Argument
0	Null	In der Organisation gibt es keinen Verantwortlichen für Informationssicherheit.
1	A	Es existiert in der Organisation eine verantwortliche Stelle für die Entgegennahme von entdeckten Informationssicherheitsvorfällen.
2	B	Ein Informationssicherheitsbeauftragter ist bestellt. Er informiert und berät, hat entsprechende Audit-Berechtigungen und untersteht in dieser Funktion ausschließlich der Geschäftsführung. Es gibt ein System zur elektronischen Erfassung von Informationssicherheitsvorfällen.
3	C	In der Organisation sind Services zur Erhaltung der Informationssicherheit etabliert. Der Informationssicherheitsbeauftragte ist prozessual in die relevanten Prozesse und Services z. B. BCM, Change-Management, Problem-Management eingebunden. Dies wird regelmäßig durch geeignete Zertifizierung nachgewiesen. Die Organisation nutzt ein System zur Erfassung, Verfolgung und Verwaltung von Informationssicherheitsvorfällen.
4	D	Sämtliche, die Informationssicherheit in der Organisation betreffenden Vorfälle, werden automatisiert und revisionssicher protokolliert. Der Beauftragte wird regelmäßig durch Reports an die Geschäftsführung entlastet.
5	E	Die Sicherheitsreports werden im Management ausgewertet. Abgeleitete Konsequenzen werden im Change-Management berücksichtigt.

16.2 Einrichtung einer Problem-Management-Organisation

Frage: Gibt es in den operativen Services ein Problem-Management mit einem integrierten Incident-Management-Prozess und wie granuliert sind dessen Teilprozesse beschaffen?

Aspekt	Stufe	Argument
0	Null	In der Organisation gibt es keinen Sicherheitsvorfall-Management-Prozess.
1	A	Es existiert in der Organisation eine verantwortliche Stelle für den Umgang mit Sicherheitsvorfällen, welche allen Mitarbeitenden bekannt ist.
2	B	In der Organisation gibt es für den gesamten Informationsverbund einen Service für das Problem-Management. Es ist geregelt, wer für die Annahme und Bearbeitung von Sicherheitsvorfällen verantwortlich ist. Es existiert eine automatisierte Meldekette an den Verantwortlichen und seine Stellvertreter.
3	C	Es existieren Eskalationsprozesse für verschiedene Kategorien von Störungen und Fehlern. Beginnend bei intern festgelegten Eskalationsstufen erfolgen automatisierte Meldungen an den Verantwortlichen für die Informationssicherheit. Gleichzeitig gibt es eine Wissensdatenbank mit Handlungsempfehlungen für bestimmte Kategorien von Vorfällen.
4	D	In der Organisation existiert für alle gemeldeten Sicherheitsvorfälle eine revisionssichere Protokollierung und Verfolgung des Bearbeitungsstatus. Dieses Protokoll wird regelmäßig durch den Verantwortlichen für Informationssicherheit überprüft und ausgewertet und Verbesserungsempfehlungen abgeleitet.
5	E	Die Qualität und Geschwindigkeit der Bearbeitung von gemeldeten Vorfällen wird regelmäßig ausgewertet und bei Bedarf nachgesteuert.

16.3 Datenschutzvorfall- Management-Prozess

Frage: Ist ein Datenschutz-Incident-Management-Prozess bei der Verarbeitung personenbezogener Daten in der Organisation verabschiedet und veröffentlicht?

Aspekt	Stufe	Argument
0	Null	In der Organisation ist kein Prozess für ein Datenschutzvorfall-Management verabschiedet und veröffentlicht.
1	A	In der Organisation ist ein Prozess zum Datenschutzvorfall-Management verabschiedet und veröffentlicht.
2	A	Die Umsetzung des Prozesses zum Datenschutzvorfall-Management wird nicht konsequent verfolgt.
3	B	<p>In der Organisation ist ein Prozess zum Datenschutzvorfall-Management verabschiedet und veröffentlicht worden, der folgende Aspekte abdeckt:</p> <ul style="list-style-type: none"> ▪ Rollen und Verantwortlichkeiten sind klar definiert und dokumentiert ▪ Allen Mitarbeitenden und auch allen anderen involvierten interessierten Parteien sind die Meldewege und Fristen klar ▪ Die Kriterien zur Qualifikation eines Vorfalls als Datenschutzvorfall sind schriftlich formuliert ▪ Die Ansprechpartner zur Meldung eines Datenschutz-Sicherheitsvorfalls im Rahmen einer Auftragsverarbeitung sind schriftlich festgelegt ▪ Die zuständigen Datenschutz-Aufsichtsbehörden sind identifiziert und dokumentiert worden ▪ Ein Datenschutz-Sicherheitsvorfall-Management-Response-Plan ist ausgearbeitet und wird regelmäßig getestet ▪ Die gesetzlichen Voraussetzungen für eine Beweissicherung können eingehalten werden ▪ Die Anforderungen aus einer Auftragsverarbeitung sind im Datenschutz-Sicherheitsvorfall-Management-Response-Plan berücksichtigt ▪ Datenschutz-Sicherheitsvorfall-Meldungen können fristgerecht (72 Stunden) und zumindest im gesetzlich geforderten Umfang erbracht werden ▪ Die Protokollierung des gesamten Prozesses ist vorgeschrieben
4	C	Die Inhalte des Datenschutz-Sicherheitsvorfall-Management-Prozesses werden in der Organisation gelebt.
5		Die bis Stufe 3 beschriebenen Datenschutz-Maßnahmen sind dokumentiert und die Dokumentation ist den betroffenen interessierten Parteien zugänglich.
6		Der Datenschutz-Sicherheitsvorfall-Management-Prozess wird regelmäßig auf Funktion getestet.
7	D	Für die Umsetzung des Datenschutz-Sicherheitsvorfall-Management-Prozesses sind Kennzahlen definiert und werden gemessen, um die Effektivität und Wirksamkeit der Umsetzung zu beschreiben.
8		Aus diesen Kennzahlen werden Ziele zur Verbesserung der Effektivität und Wirksamkeit abgeleitet.

Aspekt	Stufe	Argument
9		Abgeleitet aus den Kennzahlen werden Korrekturmaßnahmen durchgeführt, um die zuvor definierten Datenschutz-Ziele zu erreichen.
10	E	Es werden, zusätzlich zu Stufe 4, Projekte mit eigenen Ressourcen (Personal und Budget) gestartet, um die Einhaltung der Aspekte des Datenschutz-Sicherheitsvorfall-Management-Prozesses fortwährend zu optimieren.
11		Identifizierte Verbesserungen werden getestet, umgesetzt und in der Organisation dokumentiert.

17

Datenschutzaspekte beim Business Conti- nuity Management

Prozesse und Services benötigen in der Regel Technologie, Personal, Organisation und weitere Teilprozesse oder Services. Um bei Störungen an diesen Abhängigkeiten die Funktion des Prozesses oder Services weiterhin ausreichend betreiben zu können, werden im BCM Überkapazitäten bereitgestellt. In diesem Absatz geht es speziell um die Datenschutzbelange im Notfallmanagement.

17.1 Planung zur Aufrechterhaltung des Datenschutzes

Frage: Wurden Maßnahmen zur Aufrechterhaltung des Datenschutzes geplant?

Aspekt	Stufe	Argument
0	Null	Die Anforderungen des Datenschutzes an die Prozesse sind in der Organisation nicht festgelegt und finden in den Planungen für IT-Notfälle keine Anwendung.
1	A	Die Anforderungen des Datenschutzes an die Prozesse sind für den Normalbetrieb festgelegt.
2	A	Es wird versucht, die Anforderungen des Datenschutzes in schwierigen Situationen aufrecht zu erhalten.
3	B	Eine formelle Planung für schwierige Situationen findet statt. Die Anforderungen an die Informationssicherheit werden im Rahmen dieser formellen Planung mit erhoben.
4	B	Bei der Umsetzung von Verfahren in diesen Situationen werden diese Anforderungen umgesetzt.
5	C	Der in Stufe B beschriebene Planungsprozess ist in der Organisation dokumentiert und wird gelebt.
6	D	Zusätzlich zu den Anforderungen der Stufe C werden Kennzahlen definiert und erhoben, wie etwa der Abgleich der benötigten Zeit zum Herunterfahren der Server mit der noch vorhandenen Akkulaufzeit der USV. So kann nachgewiesen werden, dass alle Prozesse und Verfahren für schwierige Situationen auch die Anforderungen an Informationssicherheit erfüllt sind.
7	E	Es wird zusätzlich zur Stufe D ein Prozess zur kontinuierlichen Verbesserung etabliert, um die Einhaltung der Anforderungen des Datenschutzes im IT-Notfallmanagement fortlaufend zu optimieren.

17.2 Umsetzung der Aufrechterhaltung des Datenschutzes

Frage: Sind in der Organisation Prozesse, Verfahren und Maßnahmen festgelegt, dokumentiert und umgesetzt, die das erforderliche Niveau des Datenschutzes in widrigen Situationen aufrechterhalten?

Aspekt	Stufe	Argument
0	Null	In der Organisation existieren keine Prozesse, Verfahren oder Maßnahmen, die das erforderliche Niveau an Informationssicherheit in widrigen Situationen aufrechterhalten.
1	A	In der Organisation sind die Anforderungen an das Niveau des Datenschutzes bei IT-Störungen bekannt.
2	A	Einzelne Prozesse, Verfahren und Maßnahmen sind festgelegt.
3	A	Die Umsetzung liegt in der Verantwortung der operativen Einheiten und ist nicht vollumfänglich gewährleistet.
4	B	In der Organisation sind die Anforderungen an das Niveau des Datenschutzes bei IT-Störungen bekannt.
5	B	Eine Vielzahl von Prozessen und Services wurden im Notfallbewältigungskonzept erfasst und Verfahren und Maßnahmen sind in einem skriptartigen Notfallplan festgelegt.
6	B	Die Umsetzung liegt in der Verantwortung der operativen Einheiten und ist bereits zu einem Großteil gewährleistet.
7	C	In der Organisation sind Prozesse, Verfahren oder Maßnahmen umgesetzt und dokumentiert, wie in den unterschiedlichen widrigen Situationen das erforderliche Niveau des Datenschutzes aufrechterhalten werden kann.
8	C	In den Situationen, in denen das Niveau nicht aufrechterhalten werden könnte, erfolgte zuvor eine Risikoanalyse und die Risiken werden seitens der Geschäftsleitung getragen.
9	C	Die Entscheidung ist ebenfalls dokumentiert.
10	C	Eine auf der Priorität der Prozesse basierende Reihenfolge der Maßnahmen wurde in einem Wiederanlaufplan festgelegt.
11	D	Zusätzlich zur Stufe C finden Untersuchungen statt, wie das getragene Risiko behandelt werden kann und wie auch in diesen widrigen Situationen das Niveau des Datenschutzes gewährleistet werden kann.
12	D	Entsprechende Nachweise der Untersuchung aus Aspekt 12 können geliefert werden.
13	E	Das Notfallvorsorge- und Notfallbewältigungskonzept wird ebenso wie das Notfallhandbuch in einem Managementsystem in der gesamten Organisation gelebt und laufend revisionierbar aktualisiert.
14	E	Die Ergebnisse aus Simulationen fließen stets in die Weiterentwicklung des Systems ein.

17.3 Überprüfen und Bewerten der Aufrechterhaltung des Datenschutzes

Frage: Wird in der Organisation in regelmäßigen Abständen überprüft, ob die umgesetzten Maßnahmen, die den Datenschutz in widrigen Situationen aufrechterhalten, wirksam sind?

Aspekt	Stufe	Argument
0	Null	In der Organisation finden keine oder vereinzelte Überprüfungen statt. Die Überprüfung findet nicht systematisch statt.
1	A	In der Organisation finden systematische Überprüfungen der Wirksamkeit der festgelegten Vorsorge- und Bewältigungsmaßnahmen statt.
2	B	In der Organisation finden bedarfsgerechte systematische Überprüfungen statt.
3	B	Die Untersuchung von Abhängigkeiten der datenschutzrelevanten Prozesse in Bezug auf ihre Services, Personal und Technologie findet statt.
4	C	Es existiert ein dokumentierter Übungsplan, wann und wie die jeweils umgesetzten Maßnahmen, wie etwa die korrekte Startreihenfolge der Server, überprüft werden.
5	C	Die Übungen finden wie geplant statt und zu den einzelnen Übungen werden Übungsprotokolle angefertigt.
6	C	Aufgedeckte Schwachstellen finden im Rahmen der kontinuierlichen Verbesserung Einfluss in die Verbesserung des Datenschutzes bei IT-Notfällen.
7	D	Zusätzlich zur Stufe C finden unangekündigte Überprüfungen statt.
8	D	Aufgedeckte Schwachstellen finden im Rahmen der kontinuierlichen Verbesserung Einfluss in die Verbesserung des Datenschutzniveaus bei IT-Störungen. Anhand von Kennzahlen, wird z. B. die Abhängigkeit von Datenbankservern zu Anmeldediensten, welche bereits vollständig funktionsbereit sein müssen, da sonst keine Anmeldeinformationen für den Datenbankserver abgerufen werden können, überprüft. So wird die Wirksamkeit und Folgerichtigkeit der geplanten Maßnahmen sichergestellt.
9	D	Die Notfallvorsorge- und Notfallbewältigungskonzepte werden nicht nur an den Bedarf, sondern auch an die Ergebnisse der Überprüfungen angepasst.
10	D	Die Maßnahmen werden durch ein Managementsystem gesteuert und gelenkt.
11	E	Zusätzlich zur Stufe D finden entsprechende Simulationen für alle erdenklichen Formen und Kombinationen von IT-Notfällen statt, um das Niveau des Datenschutzes bei Störungen zu verbessern.
12	E	Die Maßnahmen zur Überprüfung der Wirksamkeit des Notfallkonzeptes werden regelmäßig optimiert und aktualisiert.

17.4 Maßnahmen zur Erhöhung der Verfügbarkeit

Frage: Sind in der Organisation informationsverarbeitende Einrichtungen mit ausreichender Redundanz realisiert worden, die die Einhaltung der Verfügbarkeitsanforderungen gewährleisten?

Aspekt	Stufe	Argument
0	Null	Die Verfügbarkeitsanforderungen der Organisationsprozesse sind nicht erfasst worden. Die Systeme werden ohne oder mit punktueller Redundanz betrieben.
1	A	Es gibt ein Bewusstsein für die Notwendigkeit von Ausfallsicherungen und Redundanzen.
2	A	Entsprechende Ausfallsicherungen und Redundanzen sind bereits mehrheitlich in den informationsverarbeitenden Einrichtungen realisiert. Die Verfügbarkeitsanforderungen stammen aus Empfehlungskatalogen oder ähnlichem.
3	A	Die Integration erfolgt bereits strukturiert, orientiert sich aber nicht gezielt an den Bedarfen der informationsverarbeitenden Einrichtung.
4	B	Anforderungen an die Verfügbarkeit der Kern- und Teilprozesse werden weitgehend, aber noch unvollständig erfasst und umgesetzt.
5	B	Wiederanlaufpläne wurden erstellt.
6	C	Ein Prozess zur Ableitung von Verfügbarkeitsanforderungen seitens des Geschäftsbetriebs existiert und ist dokumentiert.
7	C	Die Anforderungen werden bei der Umsetzung und Betrieb aller informationsverarbeitenden Einrichtungen ermittelt und umgesetzt.
8	C	Wiederanlaufpläne wurden unter Berücksichtigung der maximal tolerierbaren Wiederanlaufzeiten der Prozesse erstellt.
9	D	Die Einhaltung der Verfügbarkeitsanforderungen wird mittels geeigneter Kennzahlen, wie etwa der maximal zulässigen Ausfallzeit eines Services im Abgleich mit der tatsächlich benötigten Anlaufzeit der für diesen Service benötigten IT-Systeme, belegt, überprüft und getestet.
10	D	Die Vorgaben der Wiederanlaufpläne werden regelmäßig überprüft und die Maßnahmen werden entsprechend angepasst.
11	E	Maßnahmen werden regelmäßig zur kontinuierlichen Verbesserung durchgeführt, um die Verfügbarkeitsanforderungen, deren Umsetzung und wiederum deren Überwachung fortlaufend zu optimieren.

18 Compliance

Unter Compliance wird im Allgemeinen die Einhaltung von Gesetzen und Regularien verstanden. Dafür können sowohl organisatorische Maßnahmen definiert (z. B. Erstellung von Verträgen), als auch technische Maßnahmen implementiert werden (z. B. Verschlüsselungslösungen um die Vertraulichkeit zu gewährleisten).

Im ersten Unterkapitel wird abgefragt, ob innerhalb der Organisation alle relevanten Gesetze und vertraglichen Anforderungen bekannt sind. Nur wenn ein Überblick über die entsprechenden Anforderungen existiert, können – risikobasiert – geeignete Maßnahmen getroffen werden. Besonders betrachtet werden hier Vorgaben zur Gewährung der geistigen Eigentumsrechte sowie der Schutz von Aufzeichnungen, da eine große Zahl von personenbezogenen Daten in solchen Fällen verarbeitet wird.

Im zweiten Unterkapitel wird beschrieben, wie durch prozessuale oder technische Audits die Wirksamkeit der oben definierten Maßnahmen überprüft, und Maßnahmen eventuell angepasst werden können.

18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen

Frage: Sind in der Organisation informationsverarbeitende Einrichtungen mit ausreichender Redundanz realisiert worden, die die Einhaltung der Verfügbarkeitsanforderungen gewährleisten?

Aspekt	Stufe	Argument
0	Null	Die Verfügbarkeitsanforderungen der Organisationsprozesse sind nicht erfasst worden. Die Systeme werden ohne oder mit punktueller Redundanz betrieben.
1	A	Es gibt ein Bewusstsein für die Notwendigkeit von Ausfallsicherungen und Redundanzen.
2	A	Entsprechende Ausfallsicherungen und Redundanzen sind bereits mehrheitlich in den informationsverarbeitenden Einrichtungen realisiert. Die Verfügbarkeitsanforderungen stammen aus Empfehlungskatalogen oder ähnlichem.
3	A	Die Integration erfolgt bereits strukturiert, orientiert sich aber nicht gezielt an den Bedarfen der informationsverarbeitenden Einrichtung.
4	B	Anforderungen an die Verfügbarkeit der Kern- und Teilprozesse werden weitgehend, aber noch unvollständig erfasst und umgesetzt.
5	B	Wiederanlaufpläne wurden erstellt.
6	C	Ein Prozess zur Ableitung von Verfügbarkeitsanforderungen seitens des Geschäftsbetriebs existiert und ist dokumentiert.
7	C	Die Anforderungen werden bei der Umsetzung und Betrieb aller informationsverarbeitenden Einrichtungen ermittelt und umgesetzt.
8	C	Wiederanlaufpläne wurden unter Berücksichtigung der maximal tolerierbaren Wiederanlaufzeiten der Prozesse erstellt.
9	D	Die Einhaltung der Verfügbarkeitsanforderungen wird mittels geeigneter Kennzahlen, wie etwa der maximal zulässigen Ausfallzeit eines Services im Abgleich mit der tatsächlich benötigten Anlaufzeit der für diesen Service benötigten IT-Systeme, belegt, überprüft und getestet.
10	D	Die Vorgaben der Wiederanlaufpläne werden regelmäßig überprüft und die Maßnahmen werden entsprechend angepasst.
11	E	Maßnahmen werden regelmäßig zur kontinuierlichen Verbesserung durchgeführt, um die Verfügbarkeitsanforderungen, deren Umsetzung und wiederum deren Überwachung fortlaufend zu optimieren.

18.1.1 Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen

Frage: Werden alle gesetzlichen und vertraglichen Anforderungen im Unternehmen umgesetzt?

Aspekt	Stufe	Argument
0	Null	Es gibt keinen Überblick über die Verantwortlichkeiten der verschiedenen Rechtsgebiete und es existiert kein Überblick über die relevanten gesetzlichen oder vertraglichen Anforderungen.
1	A	Es gibt verschiedene Rollen im Unternehmen, die für die unterschiedlichen Rechtsbereiche verantwortlich sind, allerdings existiert keine Dokumentation zu den Verantwortlichkeiten. Weiterhin gibt es keine Dokumentation der rechtlichen oder vertraglichen Anforderungen pro Bereich.
2	B	Es gibt verschiedene Rollen im Unternehmen, die für die unterschiedlichen Rechtsbereiche verantwortlich sind, und es existiert eine Dokumentation, die die Aufteilung dokumentiert. Allerdings gibt es keine der rechtlichen oder vertraglichen Anforderungen pro Bereich.
3	C	Es gibt verschiedene Rollen im Unternehmen, die für die unterschiedlichen Rechtsbereiche verantwortlich sind, und es existiert eine Dokumentation, die die Aufteilung dokumentiert. Für einzelne Bereiche gibt es eine Dokumentation der rechtlichen Vorgaben oder der vertraglichen Vorgaben.
4	C	Es gibt verschiedene Rollen im Unternehmen, die für die unterschiedlichen Rechtsbereiche verantwortlich sind, und es existiert eine Dokumentation, die die Aufteilung dokumentiert. Für einzelne Bereiche gibt es eine Dokumentation der rechtlichen Vorgaben oder der vertraglichen Vorgaben.
5	D	Es gibt verschiedene Rollen im Unternehmen, die für die unterschiedlichen Rechtsbereiche verantwortlich sind, und es existiert eine Dokumentation, die die Aufteilung dokumentiert. Für alle relevanten Bereiche gibt es eine Dokumentation der rechtlichen Vorgaben oder der vertraglichen Vorgaben.
6	D	Es gibt verschiedene Rollen im Unternehmen, die für die unterschiedlichen Rechtsbereiche verantwortlich sind, und es existiert eine Dokumentation, die die Aufteilung dokumentiert. Für alle relevanten Bereiche gibt es eine Dokumentation der rechtlichen und vertraglichen Vorgaben.
7	D	Es gibt einen Prozess zur regelmäßigen Aktualisierung der rechtlichen und vertraglichen Vorgaben pro Bereich.
8	D	Es gibt einen Prozess zur regelmäßigen Aktualisierung der rechtlichen und vertraglichen Vorgaben, welcher zentral koordiniert ist und für alle Bereiche gilt.
9	D	Es gibt einen Auditierungsprozess, welcher die Aktualisierung und Vollständigkeit der für das Unternehmen relevanten rechtlichen und vertraglichen Anforderungen gewährleistet.
10	D	Es gibt einen Auditierungsprozess, welcher die Aktualisierung und Vollständigkeit der für das Unternehmen relevanten rechtlichen und vertraglichen Anforderungen gewährleistet. Basierend auf diesen Ergebnissen werden neue Prozesse und Richtlinien erstellt.
11	D	Es existiert ein Reporting für das Management um die identifizierten Veränderungen vorzustellen und zu entscheiden.

18.1.2 Geistige Eigentumsrechte

Frage: Gibt es Maßnahmen, um die Bewahrung der geistigen Eigentumsrechte zu gewährleisten?

Aspekt	Stufe	Argument
0	Null	Es gibt keine Verantwortlichkeiten und Richtlinien für den Umgang mit den geistigen Eigentumsrechten.
1	A	Es gibt eine Richtlinie, die dem Umgang mit den geistigen Eigentumsrechten regelt (z. B. in Bezug auf Softwareentwicklung oder Lizenzen). Inhalte dieser Richtlinie könnten Maßnahmen zur Beachtung des Urheberrechts und des gewerblichen Rechtsschutzes (wie Patentrecht, Markenrecht, Gebrauchsmusterrecht etc. sein).
2	B	In der Richtlinie zu den geistigen Eigentumsrechten sind Rechte und Pflichten klar zugewiesen.
3	C	Die Umsetzung und Einhaltung der Richtlinie zu den geistigen Eigentumsrechten wird von allen relevanten Bereichen verfolgt.
4	D	Die Richtlinie zum Umgang mit den geistigen Eigentumsrechten wird durch regelmäßige interne Stichproben überprüft.
5	E	Kennzahlen zu Abweichungen und Schwachstellen der Richtlinie werden erhoben und im Rahmen eines kontinuierlichen Verbesserungsprozesses (KVP) eingesetzt.

18.1.3 Schutz vor Aufzeichnungen

Frage: Gibt es Maßnahmen zum Schutz von Aufzeichnungen mit Personenbezug (z. B. Gesprächsaufzeichnungen, Bildschirmaufzeichnungen, Transaktion, Protokollierung, etc.)? Es handelt sich dabei um Maßnahmen gegen Verlust, Zerstörung, unautorisierte Veränderung oder unautorisierten Zugriff.

Aspekt	Stufe	Argument
0	Null	Es gibt keine Verantwortlichkeiten und Richtlinien für den Umgang mit Aufzeichnungen.
1	A	Es gibt einzelne Maßnahmen für den Umgang mit bestimmten Fällen von Aufzeichnungen (z. B. Löschung von Datenträgern oder Maßnahmen für die Protokollierung), welche aber nicht dokumentiert sind.
2	B	<p>Es existieren einzelne dokumentierte Vorgaben (Richtlinien) für den Umgang mit bestimmten Fällen von Aufzeichnungen (Gesprächsaufzeichnungen, Bildschirmaufzeichnungen, Transaktion, Protokollierung etc.). Zu den Vorgaben gehören:</p> <ul style="list-style-type: none"> ▪ Definition der Aufzeichnung (was genau soll aufgezeichnet werden) ▪ Zweckangabe (zu welchem Zweck soll aufgezeichnet werden) ▪ Rollen- und Berechtigungskonzept für die Zugriffe (wer darf auf welchen Daten zugreifen) ▪ Speicherfristen (wie lange sollen die Aufzeichnungen aufbewahrt werden) ▪ Anonymisierung / Pseudonymisierung (können die Daten anonymisiert oder pseudonymisiert werden)

Aspekt	Stufe	Argument
3	C	Es gibt implementierte Schutzmaßnahmen für alle Arten von Aufzeichnungen, diese sind nicht vollständig dokumentiert.
4	D	Es gibt Richtlinien zum Schutz allen Aufzeichnungsarten im Unternehmen.
5	D	Es gibt regelmäßige Audits um die beschriebenen Schutzmaßnahmen zu überprüfen.
6	E	Kennzahlen zu Verletzungen und Schwachstellen der Richtlinien zum Schutz der Aufzeichnungsarten werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses eingesetzt.

18.2 Überprüfungen der Compliance-Anforderungen

18.2.1 Unabhängige Überprüfung der Compliance-Anforderungen

Frage: Werden die Maßnahmen zur Informationssicherheit und Datenschutz von einer unabhängigen Stelle überprüft?

Aspekt	Stufe	Argument
0	Null	Es gibt keine Regelung zur Durchführung von Audits zur Überprüfung des Datenschutzes und Informationssicherheit.
1	A	Es gibt eine Richtlinie, die die Durchführung der Audits regelt. Inhalte der Audits u.a. sind: Scope, Regelmäßigkeit, internes oder externes Audit, Auditplan, Ressourcen, Verantwortlichkeiten, etc.
2	B	Die Richtlinie zur Durchführung von unabhängigen Audits wird verfolgt. Die Audits werden regelmäßig von einem internen Bereich durchgeführt.
3	C	Die Richtlinie zur Durchführung von unabhängigen Audits wird verfolgt. Die Audits werden regelmäßig von einem internen Bereich durchgeführt, welcher weisungsfrei agieren darf.
4	C	Die Richtlinie zur Durchführung von unabhängigen Audits wird verfolgt. Die Audits werden von einem externen Auditor durchgeführt.
5	D	Die Ergebnisse der Audits werden dokumentiert. Abweichungen zu den Richtlinien oder gesetzlichen Vorgaben werden identifiziert, Korrekturmaßnahmen definiert.
6	D	Eventuelle Verbesserungen zu den Richtlinien und den Prozessen werden identifiziert und den Verantwortlichen zwecks Bewertung vorgestellt. Die Bewertungen und Entscheidungen werden dokumentiert.
7	E	Die Verbesserungsvorschläge werden getestet, umgesetzt und in der Organisation dokumentiert.

18.2.2 Optimierung von Datenschutz- und Sicherheitsrichtlinien und -standards

Frage: Gibt es einen unternehmensweiten KVP-Prozess (=kontinuierlicher Verbesserungsprozess)?

Aspekt	Stufe	Argument
0	Null	Es gibt keine Richtlinie zur Durchführung eines unternehmensweiten kontinuierlichen Verbesserungsprozesses (KVP).
1	A	Es gibt teilweise dokumentierte Vorgaben (teilweise in verschiedenen Dokumenten) zu einem KVP-Prozess. Die Inhalte sind hauptsächlich: <ul style="list-style-type: none"> ▪ Angaben zu Verantwortlichkeiten und ▪ Angaben zur Überprüfung von Informationssicherheit- und Datenschutzprozesse
2	B	Es gibt eine Richtlinie zum KVP-Prozess. Sie beinhaltet folgende Vorgaben: <ul style="list-style-type: none"> ▪ Verantwortlichkeiten ▪ Regelmäßige Überprüfung von Informationssicherheit- und Datenschutzprozessen ▪ Identifikation von Abweichungen zu Richtlinien, Prozessen und gesetzlichen Vorgaben ▪ Identifikation und Bewertung von Korrekturmaßnahmen ▪ Implementierung von Korrekturmaßnahmen Überprüfung der neuen Maßnahmen
3	C	Der KVP-Prozess wird in der Organisation gelebt.
4	D	Die Umsetzung des KVP wird dokumentiert, dies beinhaltet im ersten Schritt die Identifikation der Abweichungen sowie abgeleitete Korrekturmaßnahmen und deren Bewertung.
5	D	Die neuen abgeleiteten Korrekturmaßnahmen werden bezüglich Compliance zu den aktuellen Richtlinien, Aufwand, Ressourcen und Ertrag bewertet. Die Ergebnisse werden dem Management vorgestellt. Die Entscheidungen werden dokumentiert.
6	E	Die neuen Korrekturmaßnahmen werden implementiert.
7	F	Kennzahlen zu Verletzungen und Schwachstellen der Richtlinien zum KVP werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses eingesetzt.

18.2.3 Technische Überprüfung der Compliance-Anforderungen

Frage: Werden Überprüfungen/Audits auf technischer Ebene durchgeführt, um die Compliance zu den technischen Maßnahmen zu gewährleisten?

Aspekt	Stufe	Argument
0	Null	Es gibt keine Vorgaben und Verantwortlichkeiten zur technischen Überprüfung von Systemen.
1	A	Es gibt eine Richtlinie zur Überprüfung der Einhaltung der technischen Maßnahmen (Richtlinien) zur Härtung von Systemen.

Aspekt	Stufe	Argument
2	B	Die Richtlinie wird in der Organisation gelebt. Es gibt anlassbezogene Überprüfungen der technischen Sicherheitsmaßnahmen.
3	B	Die Richtlinie wird in der Organisation gelebt. Es gibt unregelmäßige Überprüfungen der technischen Sicherheitsmaßnahmen.
4	C	Es gibt regelmäßige Überprüfungen der technischen Sicherheitsmaßnahmen, welche hauptsächlich manuell durchgeführt werden (z. B. durch Interviews oder Sichtung von Dokumenten). Die Abweichungen werden bewertet und Korrekturmaßnahmen definiert.
5	C	Es gibt regelmäßige Überprüfungen der technischen Sicherheitsmaßnahmen, welche automatisch durchgeführt werden (z. B. durch Einsatz geeigneter Software). Die Abweichungen werden bewertet und Korrekturmaßnahmen definiert.
6	C	Es werden regelmäßig zusätzlich interne Penetrationstests (d. h. automatisierte Simulationen von Angriffsszenarien) durchgeführt. Die Ergebnisse werden bewertet und Korrekturmaßnahmen definiert.
7	D	Es werden regelmäßig zusätzlich externe Penetrationstests durchgeführt. Die Ergebnisse werden bewertet und Korrekturmaßnahmen definiert.
8	E	Es werden regelmäßig Überprüfungen mit Red und Blue Teams (Simulation von Angreifer und Verteidiger) durchgeführt. Die Ergebnisse werden bewertet und Korrekturmaßnahmen definiert.
9	E	Kennzahlen zu Verletzungen und Schwachstellen der Richtlinie werden erhoben und zur Verfolgung und Steuerung eines kontinuierlichen Verbesserungsprozesses eingesetzt.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bitkom e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

[bitkom.org](https://www.bitkom.org)

bitkom