Trusted Site Data Privacy

Kriterienkatalog für Prüfungen der Konformität einer IT-Lösung zur Europäischen Datenschutz-Grundverordnung

Version 2.16 vom 27.01.2026

öffentliche Version

Kriterienkatalog-Version: 2.16

Ansprechpartner:
TÜV NORD CERT GmbH
Zertifizierungsstelle
Am TÜV 1
45307 Essen, Germany

Inhaltsverzeichnis

1. Einleitung und allgemeine Informationen

1.1 Inhaltlicher Fokus

Dieses Dokument beinhaltet die Trusted Site Data Privacy-Zertifizierungskriterien für ein nationales Zertifizierungsprogramm für Deutschland gemäß Art. 42 Abs. 5 DSGVO.

Der vorliegende Kriterienkatalog beschreibt Anforderungen an Verarbeitungsvorgänge, die in Prozessen oder mit Hilfe von mehreren Prozessen/Systemen in einer Funktion als Verantwortlicher oder Auftragsverarbeiter erbracht werden. Die betrachteten Verarbeitungsvorgänge werden dabei als

Datenverarbeitung durch informationsverarbeitende Services (IVS)

bezeichnet. Zur Erbringung der IVS können dabei sowohl Software- als auch kombinierte Software-/ Hardwarelösungen zum Einsatz kommen.

Neben dem IVS selbst wird in den nachfolgenden Kriterien auch seine Einsatzkonzeption[1] betrachtet. Diese wird als immanenter Bestandteil des IVS gesehen, denn sie beschreibt u. U. wichtige Voraussetzungen für die datenschutzkonforme Handhabung der technischen Komponenten des IVS. Entsprechend spielt die Dokumentation des IVS und seiner Einsatzvorgaben eine wesentliche Rolle für die Begutachtung.

Insgesamt sind im Hinblick auf die IVS folgende Komponenten Teil des Evaluierungsgegenstandes:

A Der IVS in seiner technischen Ausprägung als Kombinationen von
A1 Hardware-,
A2 Software-, und
A3 Netzwerkkomponenten sowie
A4 durch diese Komponenten unterstützte Prozesse.

B Die Dokumentation des IVS mit der Beschreibung:
B1 Eigenschaften des IVS (Prozessdokumentation fachlich/technisch),
B2 Benutzungshinweise des IVS (Benutzerdokumentation fachlich/technisch),
B3 ggf. separate Einsatzkonzeption/Betriebskonzept (sofern nicht in B1/B2 enthalten),
B4 Änderungsinformationen.

C Dokumente und sonstige Informationen, die zur Nutzung mit dem IVS bereitgestellt werden:
C1 Formulare,
C2 Informationstexte (z. B. Einwilligungstexte),
C3 Internetseiten,
C4 Vertragstexte (z. B. Vertrag zur Auftragsverarbeitung).

Alle Komponenten des IVS, die nicht Teil des Evaluierungsgegenstandes sind, werden nicht mit in die Evaluierung einbezogen und sind im Kontext der Zertifizierung Out of Scope.

Der IVS soll den Datenschutz und seine Einhaltung durch die Anwender unterstützen und dem Datenschutz widersprechende, abweichende Handhabungen kontrollierbar machen, kann diese jedoch nie vollständig verhindern.

Einschränkung der Gültigkeit dieses Kriterienkataloges

Der vorliegende Kriterienkatalog geht bei der Beschreibung dieser Anforderungen von folgenden Annahmen/Einschränkungen aus:

1. Die Verarbeitungstätigkeiten des IVS betreffen personenbezogene Daten.
2. Der IVS ist als Lösung mit seinen Funktionalitäten eindeutig abgrenzbar.
3. Es erfolgt keine Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO.

[1] Hier wurde der Begriff "Einsatzkonzeption" verwendet. Alternative Begriffe wären "Einsatzkonzept", "Betriebskonzept" oder auch "Nutzungskonzeption".

4. Es erfolgt keine Datenverarbeitung im Beschäftigungskontext (Art. 88 DSGVO).
5. Die Zertifizierung kann nicht als Instrument für die Übermittlung von personenbezogenen Daten an ein Drittland oder eine internationale Organisation gem. Art. 46 Abs. 2 lit. f DSGVO genutzt werden.
6. Die Zertifizierung von Unternehmen, die keine Niederlassung im EWR haben, ist nicht von diesem Kriterienkatalog abgedeckt.
7. Für die Zertifizierung eines Auftragsverarbeiters unter diesem Zertifizierungsprogramm gilt: Antragsteller für eine Zertifizierung im Rahmen dieses Zertifizierungsprogramms müssen Auftragsverarbeiter sein. Dazu gehören Auftragsverarbeiter, die von einem Verantwortlichen direkt mit der Verarbeitung personenbezogener Daten betraut sind, sowie Unterauftragsverarbeiter, die von einem Auftragsverarbeiter gemäß Art. 28 Abs. 2 und 4 DSGVO beauftragt werden. Die Zertifizierung eines Auftragsverarbeiters im Rahmen dieses Zertifizierungsprogramms bedeutet nicht automatisch die Zertifizierung der vom Auftragsverarbeiter beauftragten Unterauftragsverarbeiter. Unterauftragsverarbeiter können jedoch selbst eine Zertifizierung beantragen, die in einem separaten und unabhängigen Verfahren durchgeführt wird.
8. Mit dem vorliegenden Kriterienkatalog können gem. Art. 42 Abs.1 DSGVO nur Verarbeitungsvorgänge zertifiziert werden. In Abgrenzung zu anderen Zertifizierungsverfahren/ -möglichkeiten handelt es sich um ein datenschutzspezifisches Zertifizierungsverfahren, bei der die Konformität der Verarbeitungsvorgänge mit den Anforderungen der DSGVO festgestellt wird. Es handelt sich um keine reine Produkt- oder Dienstzertifizierung. Zudem werden weder Unternehmen, noch reine Datenschutzmanagementsysteme oder Datenschutzbeauftragte zertifiziert Mit dem vorliegenden Kriterienkatalog kann keine gemeinsame Verantwortlichkeit gemäß Artikel 26 DSGVO zertifiziert werden.

1.2 Hinweise zur Darstellung der Programmanforderungen

Kriteriennummer *Anforderungsformulierung*

DS01.01	**Verantwortlicher und Auftragsverarbeiter** Der IVS muss dokumentiert sein, hierbei muss insbesondere vorhanden sein: 1. eine fachliche Prozessbeschreibung ▪ Beschreibung der Funktionen des IVS und der Modalitäten dazu Hauptzielgruppe: (Potentielle) Anwender sowie 2. eine technische Prozessbeschreibung ▪ Beschreibung der technischen Einsatzvoraussetzungen und –merkmale des IVS. Hauptzielgruppe: (Potentielle) Systemadministratoren und technisch versierte Nutzer Für Anwender des IVS werden weiterhin 1. eine fachliche Benutzerdokumentation, ▪ Beschreibung der fachlichen Nutzung des IVS. Hauptzielgruppe: Anwender sowie 2. eine technische Betriebs-/Systemdokumentation ▪ Beschreibung der Wartung und des Managements des IVS inklusive notwendiger technischer Hintergrundinformationen zu seiner Benutzung. Hauptzielgruppe: Systemadministratoren des IVS, technisch versierte Anwender bereitgestellt. Im Kontext von Serviceupdates und Änderungen werden den Anwendern des Services 1. Änderungsinformationen (Releasenotes) ▪ Beschreibung der Änderungen des IVS im Rahmen neuer Versionen / Releases. Hauptzielgruppe: Anwender und Systemadministratoren bereitgestellt. Änderungen am IVS, wie z. B. neue Funktionen, Verbesserungen etc., sind durch den Auftragsverarbeiter gegenüber dem Verantwortlichen mit einer Frist von mindestens 14 Tagen vor der beabsichtigten Implementierung zu kommunizieren. Entsprechende Kommunikationswege müssen festgelegt werden. Dem Verantwortlichen sind hierbei alle Informationen zur Verfügung zu stellen, die er benötigt, um die Auswirkungen der Änderungen auf die Verarbeitungstätigkeiten bewerten zu können, insbesondere konkrete Beschreibung der angestrebten Änderungen, vollständige Liste der Sicherheitsupdates, Veröffentlichungsdatum).
Art der Ermittlung	***DP*** *Prüfung des Vorhandenseins der Informationen zu 1.-6. Bewertung der Qualität, Aktualität und Vollständigkeit der bereitgestellten Dokumentationen durch den Evaluator.*
Nachweis	*Bereitstellung der Einzeldokumente entsprechend 1.-5. und Darstellung, wo und in welcher Form die jeweiligen Informationen enthalten sind. Weiterhin Information, wie die Informationen bereitgestellt werden und wie Betreiber und Betroffene des IVS sich einen Überblick über die Dokumentation verschaffen können.*
Kundenbeschreibung	**Die Umsetzung der jeweiligen Prüfkriterien ist dezidiert und verständlich zu beschreiben. Die reine Verlinkung von Dokumenten ist nicht zulässig. In der Beschreibung sind für aufgeführte Kernaussagen Seitenangaben zu den Nachweisdokumenten erforderlich.**

Benennung vorhandener Nachweise	**Bei allen Nachweisdokumenten handelt es sich um geführte Dokumente mit Versionsangabe, Erstellungsdatum und Änderungshistorie.**

Kriteriennummer

Die Kriteriennummer setzt sich aus dem Katalogkürzel (hier DS für Datenschutz), der Nummer des Abschnitts (hier **DS01**) und der Nummer des Einzelkriteriums (hier 01) zusammen.

Anforderungsformulierung

Die einzelnen Anforderungen spiegeln prüfbare Formulierungen, bezogen auf Merkmale des zu begutachtenden IVS bzw. seiner Einsatzkonzeption wider. Innerhalb der Anforderungsformulierung wird eine Differenzierung zwischen Verantwortlicher und Auftragsverarbeiter vorgenommen. Soweit es sich bei der zu zertifizierenden Stelle um einen Verantwortlichen handelt, finden entsprechend die Anforderungen, welche an Verantwortliche gestellt werden, Anwendung.

Sofern der Dienst einer Auftragsverarbeitung zertifiziert werden soll, sind entsprechend die Anforderungen, welche an Auftragsverarbeiter gestellt werden, zu erfüllen.

Dem Evaluator soll es jeweils möglich sein, diese Formulierungen mit "Ja" oder "Nein" zu beantworten. Im Fall eines "Ja" ist diese Aussage mit einer Nachweisführung zu verbinden, also nachprüfbar zu belegen.

Die Formulierungen orientieren sich dabei stark am Text der DSGVO, sind allerdings meist einfacher formuliert, da eine klare Prüfaussage im Vordergrund steht. Im Zweifelsfall ist also die genaue Formulierung im verwiesenen Artikel der DSGVO zu berücksichtigen.

Art der Ermittlung

Diese Prüfhinweise beschreiben konkrete Nachweisverfahren, die hinsichtlich des Kriteriums zur Anwendung kommen sollen. Dabei beziehen sie sich auf die im Zertifizierungsprogramm[2] bei "Ermittlungsmethoden" genannten Verfahren:

DP Allgemeine Dokumentprüfung
DP_T technische Dokumentprüfung
DP_M methodische Dokumentprüfung
DP_J juristische Dokumentprüfung
AN Analyse
AU Audit der Organisation
IN Inspektion des Evaluierungsgegenstandes
AW Auswertung von Ermittlungen

Prüfhinweis

Im Prüfhinweis werden, sofern erforderlich und sinnvoll, einzelne Evaluierungsanforderungen dezidiert aufgeschlüsselt und konkrete Nachweisverfahren ausführlich beschrieben. Hierdurch werden die einzelnen Anforderungen konkretisiert und zugleich wird hierdurch eine einheitliche Bewertung der Evaluatoren sichergestellt. Die Prüfhinweise sind verpflichtend zu beachten.

Nachweis

Nachweise belegen die Umsetzung des Kriteriums. Zu beachten ist, dass die Verwendung des Wortes "kann" keinesfalls bedeutet, dass an dieser Stelle ein Nachweis optional ist. Vielmehr wird damit zum Ausdruck gebracht, dass alternative Formen von Nachweisen denkbar sind. Grundsätzlich liegt die Akzeptanz von Nachweisen im Urteil des Evaluators. Einzelne Komponenten des Evaluierungsgegenstandes werden im Rahmen einer Vor-Ort-Begehung (Audit) überprüft.

[2] Zertifizierungsprogramm DSGVO der TÜVIT

Votum

Das Votum ist vom Evaluator auszufüllen und bezieht sich auf die Beurteilung der Erfüllung des zu prüfenden Kriteriums.

1.3 Hinweise zum Kriterienkatalog

Der vorliegende Kriterienkatalog wird Bestandteil des Prüfberichtes *Prüfbericht Trusted Site Data Privacy,* Version 2.0.

1.4 Verwendete Abkürzungen

Abs.	Absatz
Art.	Artikel der DSGVO
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGBl.	Bundesgesetzblatt
BKPD	Besondere Kategorien personenbezogener Daten entsprechend [DSGVO] Art. 9 („besondere Kategorien personenbezogener Daten")
BMV-Ä	Bundesmantelvertrag-Ärzte
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
CMEK	Customer Managed Encryption Keys
DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
EDSA	Europäischer Datenschutzausschuss
ENISA	European Union Agency for Cybersecurity
ErwG	Erwägungsgrund
ff.	folgende
gem.	gemäß
GenDG	Gesetz über genetische Untersuchungen bei Menschen
ggf.	gegebenenfalls
Hs.	Hauptsatz
IMSI	International Mobile Subscriber Identity
ISMS	Information Security Management System
IVS	Informationsverarbeitender Service (= Evaluierungsgegenstand)
lit.	litera
o. Ä.	oder Ähnliche(s)
PBD	Personenbezogene Daten
PBDV	Personenbezogene Datenverarbeitung
Rn.	Randnummer
SDM	Standard-Datenschutzmodell
SGB	Sozialgesetzbuch
ToM	technische und organisatorische Maßnahmen
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
TVG	Tarifvertragsgesetz
vgl.	vergleiche

1.5 Verweise auf Gesetze, Vorschriften und Normen

Im Einzelnen besteht bei den einzelnen Kriterienbereichen ein Bezug zu folgenden Gesetzgebungen, Urteilen sowie Beschlüsse / Empfehlungen der Aufsichtsbehörden (DSK, EDSA etc.):

[DSGVO]	Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG
[BDSG]	Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 7 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist
[TDDDG]	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Artikel 8 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist
[FÜ.B]	OKKSA e. V.: Anforderungskatalog für Fachprogramme in der Öffentlichen Verwaltung Teilbereich: Fachübergreifende Serviceanforderungen (Kriterien OKKSA FÜ.B)
[DSK_17067]	Anforderungen an datenschutzrechtliche Zertifizierungsprogramme Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6) Version 2.0 vom 21.06.2022
[SDM]	Das Standard- Datenschutzmodell Eine Methode zur Datenschutzberatung und –prüfung auf der Basis einheitlicher Gewährleistungsziele Version 3.1 vom 14.05.2023
[GL2020-07]	Leitlinien des European Data Protection Board 07/2020 zu den Begriffen des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters in der DSGVO Version 2
[GL2019-04]	Leitlinien 2019-04 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen Version 2
[BSI-TR-02102-1]	Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 1 Stand 24.03.2021
[BSI-TR-02102-2]	Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS) Teil 2 Stand 2021-01
[BSI-200-3]	BSI-Standard 200-3 "Risikoanalyse auf der Basis von IT-Grundschutz"
[DIN ISO 31000]	Risikomanagement-Leitlinien
[ISO/IEC 27005]	Informationssicherheit, Cybersicherheit und Datenschutz - Leitfaden zur Handhabung von Informationssicherheitsrisiken
[DIN EN ISO 14971]	Medizinprodukte - Anwendung des Risikomanagements auf Medizinprodukte

1.6 Evaluierungsgegenstand

Der Evaluationsgegenstand ist das konkrete Objekt einer Evaluation. Bei dem Evaluierungsgegenstand handelt es sich um eine Datenverarbeitung durch informationsverarbeitende Services (IVS). IVS können nur Verarbeitungsvorgänge gemäß Art. 42 Abs. 1 DSGVO sein. Zur Erbringung der IVS können dabei sowohl Software- als auch kombinierte Software- / Hardwarelösungen zum Einsatz kommen.

Neben dem IVS selbst wird in den nachfolgenden Kriterien auch seine Einsatzkonzeption[3] betrachtet. Diese wird als immanenter Bestandteil des IVS gesehen, denn sie beschreibt u. U. wichtige Voraussetzungen für die datenschutzkonforme Handhabung der technischen Komponenten des IVS. Entsprechend spielt die Dokumentation des IVS und seiner Einsatzvorgaben eine wesentliche Rolle für die Begutachtung.

Insgesamt sind im Hinblick auf den IVS folgende Komponenten Teil des Evaluierungsgegenstandes:

A Der IVS in seiner technischen Ausprägung als Kombinationen von
A1 Hardware-,
A2 Software-, und
A3 Netzwerkkomponenten sowie
A4 durch diese Komponenten unterstützte Prozesse.

B Die Dokumentation des IVS mit der Beschreibung:
B1 Eigenschaften des IVS (Prozessdokumentation fachlich/technisch),
B2 Benutzungshinweise des IVS (Benutzerdokumentation fachlich/technisch),
B3 ggf. separate Einsatzkonzeption/Betriebskonzept (sofern nicht in B1/B2 enthalten),
B4 Änderungsinformationen.

C Dokumente und sonstige Informationen, die zur Nutzung mit dem IVS bereitgestellt werden:
C1 Formulare,
C2 Informationstexte (z. B. Einwilligungstexte),
C3 Internetseiten,
C4 Vertragstexte (z. B. Vertrag zur Auftragsverarbeitung).

Zur Bestimmung des Evaluierungsgegenstandes ist seitens des Antragsstellers eine vollständige Datenflussanalyse des IVS unter Berücksichtigung aller an der Verarbeitung personenbezogener Daten beteiligten Akteure, z. B. Auftragsverarbeiter, Subauftragsverarbeiter, gemeinsam Verantwortliche, vorzunehmen und sodann eine im Hinblick auf die Verantwortlichkeit qualifizierte Darstellung des gesamten nach Phasen geordneten Verarbeitungsprozesses inklusive Beschreibung des jeweiligen Akteur- und Rollenmodells (Akteure, Rollen, Beziehungen) für jede Verarbeitungsphase zu erstellen und vorzulegen. Die Darstellung kann entweder durch eine grafische Darstellung (z. B. anhand standardisierter Darstellung wie Business Process Modeling (BPM) oder Unified Modelling Language (UML) oder in textlicher Form erfolgen.

Die qualifizierte Darstellung des Verarbeitungsprozesses muss dabei den vollständigen Lebenszyklus der Verarbeitung von personenbezogenen Daten innerhalb des IVS abbilden.
Die Begriffsbestimmung zur „Verarbeitung“ in Art. 4 Abs. 2 DSGVO listet hierbei nicht abschließend einzelne Verarbeitungsvorgänge auf.

Zudem muss bestimmt und dokumentiert werden, welche Datenverarbeitungsschritte dem erweiterten Verantwortungsbereich des Antragstellers zuzuordnen sind. Hierbei ist auch eindeutig darzulegen, wie die Zugriffsmöglichkeiten der Verantwortlichen und Auftragsverarbeiter in den jeweiligen Datenvorgängen ausgestaltet sind. Alle Datenverarbeitungsschritte und relevante Schnittstellen sind vollständig zu erfassen. Der Antragssteller muss zudem die zu zertifizierenden

[3] Hier wurde der Begriff "Einsatzkonzeption" verwendet. Alternative Begriffe wären "Einsatzkonzept", "Betriebskonzept" oder auch "Nutzungskonzeption".

Verarbeitungsvorgänge, welche Gegenstand der Evaluierung sind, kennzeichnen, sodass dann in Abstimmung mit der Zertifizierungsstelle und unter Berücksichtigung der Angaben gemäß 1.7 bis 1.17 der jeweilige Evaluierungsgegenstand festgelegt werden kann.

Der Antragssteller muss für die Abgrenzung des Evaluierungsgegenstandes vor Aufnahme des Evaluierungsverfahrens ausführliche Angaben gemäß 1.7 bis 1.17 machen. Ausgehend von diesen Angaben wird sodann der Evaluierungsgegenstand ermittelt und entsprechend im Evaluierungsbericht Trusted Site Data Privacy dokumentiert.

1.7 Bezeichnung des Evaluierungsgegenstandes

	Der Evaluierungsgegenstand kann ein Prozess bzw. eine Verarbeitung in einem Produkt, einem System oder innerhalb einer Infrastruktur sein, welcher personenbezogene Daten verarbeitet. Der Evaluierungsgegenstand sollte einen Namen und eine Versionsnummer (oder Datum) besitzen. Während der Prüfung sollte sich die Version möglichst nicht ändern. Das Zertifikat wird für die geprüfte Version ggf. in der geprüften Einsatzumgebung erteilt. Der Name des Evaluierungsgegenstandes kann bis zum Abschluss der Zertifizierung noch geändert werden.

1.7.1. Name und Adresse des Antragstellers

	Bitte Name und Adresse des Antragstellers benennen.

1.7.2. Verarbeitungsvorgänge im Kontext des Evaluierungsgegenstandes

	Beschreibung, welche Verarbeitungsvorgänge mit dem Evaluierungsgegenstand abgedeckt sind.

1.7.3. Zwecke der Verarbeitungsvorgänge im Kontext des Evaluierungsgegenstandes

	Beschreibung, welche Zwecke mit den jeweiligen Verarbeitungsvorgängen abgedeckt sind und weshalb diese Verarbeitungsvorgänge zur Erreichung des Zwecks erforderlich sind.

1.7.4. Einsatzbedingungen

	Darstellung, in welcher IT-Landschaft der Evaluierungsgegenstand eingesetzt wird, in welche anderen Prozesse er eingebunden ist, Einsatz von Verschlüsselung, auf welchen Betriebssystemen es läuft o.Ä.

1.7.5. Beteiligte Stellen

	Für den Evaluierungsgegenstand maßgebliche interne und externe Stellen (Abteilungen, Konzerngesellschaften, Kooperationspartner, Rechenzentrum).

1.7.6. Empfänger bzw. Kategorien von Empfängern

	Für den Evaluierungsgegenstand maßgebliche Empfänger bzw. Kategorien von Empfängern von personenbezogenen Daten.

1.7.7. Antragssteller

	Der Unternehmensname inklusive Anschrift und Rechtsform ist anzugeben. Weiterhin ist anzugeben, ob der Antragssteller als Verantwortlicher gem. Art. 4 Nr. 7 DSGVO oder als Auftragsverarbeiter gem. Art. 4 Nr. 8 DSGVO agiert.

1.7.8. Einsatz von Auftragsverarbeitern bzw. Unterauftragsverarbeitern durch den Antragssteller

	Sofern der Antragssteller als Verantwortlicher agiert: Für den Evaluierungsgegenstand maßgebliche Auftragsverarbeiter und Unterauftragsverarbeiter gem. Art. 4 Nr. 8 DSGVO je Verarbeitungsvorgang des Evaluierungsgegenstandes sind aufzuführen. Sofern der Antragssteller als Auftragsverarbeiter agiert: Für den Evaluierungsgegenstand maßgebliche Unterauftragsverarbeiter gem. Art. 4 Nr. 8 DSGVO je Verarbeitungsvorgang des Evaluierungsgegenstandes sind aufzuführen.

1.7.9. Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen

	Beschreibung, ob im Hinblick auf die Verarbeitungsvorgänge des Evaluierungsgegenstandes eine Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen erfolgt. Hierbei sind alle Übermittlungen zu erfassen, das beinhaltet auch einzelne Support- sowie Wartungs- und Pflegezugriffe und auch mögliche exterritoriale Zugriffe, z. B. aufgrund Geschäftstätigkeit, sowie Weiterübermittlungen durch Auftragsverarbeiter.

1.8 Beschreibung des Evaluierungsgegenstandes

1.8.1. Architektur des Evaluierungsgegenstandes und Zweck der (Teil-)Komponenten

	Beschreibung der Haupt- und Teilkomponenten und ihres Zweckes im Gesamtkontext. Hierbei sind auch die jeweiligen Beteiligten zu nennen, z. B. Kunden, Nutzer, Administratoren etc. Hier und in den nachfolgenden Unterpunkten ist dabei eine technische Beschreibung, die von Datenschutz- und IT-Rechtlern verstanden werden muss, anzugeben. Es soll ein Überblick gegeben werden, der es auch den IT-Spezialisten für die sicherheitstechnische Untersuchung ermöglicht, vertiefende Angaben oder Dokumente gezielt anzufordern.

1.8.2. Datenflüsse zwischen den Komponenten des Evaluierungsgegenstandes

	Darstellung der Datenflüsse zwischen den Haupt- und Teilkomponenten des Evaluierungsgegenstandes unter Nennung der Datenarten und der Beteiligten

1.8.3. Abgrenzung des Evaluierungsgegenstandes

	Für die Prüfung wesentlich ist die Festlegung, welche Komponenten oder Schnittstellen (an der Grenze zu anderen Verfahren oder Systemen) in die Prüfung einbezogen oder nicht geprüft werden sollen (mit Erläuterung, warum die Einbeziehung erfolgen oder nicht erfolgen soll, insbesondere wenn sich die Grenzziehung nicht eindeutig aus der Architektur oder dem Zweck des Evaluierungsgegenstandes ergibt).

1.8.4. Prozesse und Funktionalitäten

	Beschreibung der einzelnen Prozesse und „Funktionalitäten“ z. B. Prozess der Registrierung bei Webanwendungen, detaillierte Beschreibung der Workflows.

1.8.5. Darstellung der gesamten Verarbeitungstätigkeiten innerhalb des Evaluierungsgegenstandes

	Beschreibung auch im Hinblick auf die Verantwortlichkeit der gesamten, nach Phasen geordneten Verarbeitungstätigkeiten sowie des jeweiligen Akteur- und Rollenmodells (Akteure, Rollen, Beziehungen) für jede Verarbeitungsphase.

1.9 Betroffenengruppen, Art der verarbeiteten personenbezogenen Daten, Herkunft der Daten, Zweck ihrer Erhebung, Verarbeitung, Nutzung

Je nach Evaluierungsgegenstand kann sich eine unterschiedliche Struktur dieses Kapitels ergeben, z. B. eingeteilt nach Schnittstellen. Die Angaben sollten möglichst detailliert sein. Nicht ausreichend sind lediglich Angaben wie „Kundendaten zur Kundenbetreuung“ oder „Adressdaten“; hinreichend wäre beispielsweise: „Geburtsdatum (Tag, Monat, Jahr) zur Altersverifikation“ oder „Kundenadresse (Straße, Hausnummer, Adresszusatz, Postleitzahl, Ort, Staat) zum Broschürenversand“.

1.9.1. Betroffenengruppen

	An dieser Stelle sind die von der Datenverarbeitung betroffenen Personengruppen zu benennen.

1.9.2. personenbezogene Daten

	Daten, auf deren Datenverarbeitung Evaluierungsgegenstand abzielt, z. B. Betroffenendaten (Aufschlüsselung aus Datenbank). Es ist anzugeben, welche Daten davon a) besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO sind b) sich auf Kinder im Sinne der DSGVO beziehen.

1.9.3. Herkunft der Daten

	An dieser Stelle ist anzuführen aus welcher Quelle die personenbezogenen Daten stammen.

1.9.4. Zweck der Verarbeitung

	Für die verarbeiteten personenbezogenen Daten bzw. Datenkategorien müssen die Zwecke eindeutig angegeben werden.

1.9.5. Rechtsgrundlagen für die Verarbeitung der personenbezogenen Daten

	Darstellung und ggf. Erläuterung der gesetzlichen Grundlagen zur Verarbeitung personenbezogener Daten in den (Teil-) Komponenten und in Bezug auf die Übermittlung bei Datenflüssen und Datenarten.

1.10 Informationstechnische Geräte einschließlich Standort und Betriebe

	An dieser Stelle sind die für den Evaluierungsgegenstand verwendeten informationstechnischen Geräte einschließlich Standorte und Betriebe zu benennen.

1.11 Service und zur Inbetriebnahme getätigte Schritte

	An dieser Stelle sind die für den Evaluierungsgegenstand verwendeten Service und zur Inbetriebnahme getätigten Schritte zu benennen.

1.12 Netzplan

	Bei vernetzten informationstechnischen Geräten sind die physikalischen und logischen Verbindungen zu anderen informationstechnischen Geräten darzustellen.

1.13 Schnittstellen

	Bei der Überprüfung sind die Schnittstellen von besonderer Bedeutung, an denen Daten in das System/Verfahren einfließen, innerhalb desselben von einer (Haupt-)Komponente zur anderen übertragen werden und das System/Verfahren verlassen. Hier sind alle Schnittstellen, ob elektronischer Art oder in Form von manueller Eingabe oder Eingang von Papierdokumenten aufzuführen und zu beschreiben (welche Datenfelder, zu welchem Zweck, auf welche Weise). Hier sind auch Sicherheitsaspekte aufzuführen, wie z. B. SSL-Verschlüsselung, Einschreibbrief etc. Zu beachten ist, dass auch Administratorzugänge Schnittstellen sind.

1.14 Import der Daten / Eingangsschnittstelle/n

	Erläuterung des Imports der Daten über mögliche Eingangsschnittstellen.

1.15 Interne Schnittstellen

	Hier sind die internen Schnittstellen zu benennen.

1.16 Weitergabe der Daten, Ausgangsschnittstelle/n

	Weitergabe im Sinne von Datenübermittlungen und im Rahmen der Auftragsverarbeitung.

1.17 Zugriffsberechtigungen zu PBD

	Nennung, wer/ welche Personengruppe zugriffsberechtigt auf PBD ist, z. B. Administratoren des Unternehmens.

2. Evaluierungskriterien

DS01 Prozessdokumentation

Die Prozessdokumentation spielt bei der Beurteilung des IVS und seiner Einsatzszenarien vor dem Hintergrund der DSGVO eine herausragende Rolle. Während Teile der Prozessdokumentation, die insbesondere seinen Einsatz beschreiben, in verschiedenen Kriterien dieses Katalogs eine Rolle spielen, finden sich nachfolgend grundsätzliche Anforderungen an die Dokumentation, die Voraussetzung für die klare Beschreibung und die datenschutzgerechte Anwendung des IVS sind.

[DSGVO] Art. 24 Abs. 1

DS01.01	**<u>Verantwortlicher und Auftragsverarbeiter</u>** Das IVS muss dokumentiert sein, hierbei muss insbesondere vorhanden sein: 1. eine fachliche Prozessbeschreibung ▪ Beschreibung der Funktionen des IVS und der Modalitäten dazu Hauptzielgruppe: (Potentielle) Anwender sowie 2. eine technische Prozessbeschreibung ▪ Beschreibung der technischen Einsatzvoraussetzungen und –merkmale des IVS. Hauptzielgruppe: (Potentielle) Systemadministratoren und technisch versierte Nutzer Für Anwender des IVS werden weiterhin 1. eine fachliche Benutzerdokumentation, ▪ Beschreibung der fachlichen Nutzung des IVS. Hauptzielgruppe: Anwender sowie 2. eine technische Betriebs-/Systemdokumentation ▪ Beschreibung der Wartung und des Managements des IVS inklusive notwendiger technischer Hintergrundinformationen zu seiner Benutzung. Hauptzielgruppe: Systemadministratoren des IVS, technisch versierte Anwender bereitgestellt. Im Kontext von Serviceupdates und Änderungen werden den Anwendern des Services 1. Änderungsinformationen (Releasenotes) ▪ Beschreibung der Änderungen des IVS im Rahmen neuer Versionen / Releases. Hauptzielgruppe: Anwender und Systemadministratoren bereitgestellt. Änderungen am IVS, wie z. B. neue Funktionen, Verbesserungen etc., sind durch den Auftragsverarbeiter gegenüber dem Verantwortlichen mit einer Frist von mindestens 14 Tagen vor der beabsichtigten Implementierung zu kommunizieren. Entsprechende Kommunikationswege müssen festgelegt werden. Dem Verantwortlichen sind hierbei alle Informationen zur Verfügung zu stellen, die er benötigt, um die Auswirkungen der Änderungen auf die Verarbeitungstätigkeiten bewerten zu können, insbesondere konkrete Beschreibung der angestrebten Änderungen, vollständige Liste der Sicherheitsupdates, Veröffentlichungsdatum).

[DSGVO] Art. 12 Abs. 1

DS01.02	**Verantwortlicher und Auftragsverarbeiter** Alle Dokumentationsteile des IVS, welche betroffenen Personen zur Verfügung gestellt werden, liegen in Deutsch vor. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. 24 Abs. 1

DS01.03	**Verantwortlicher und Auftragsverarbeiter** Die **technische Betriebsdokumentation / Systemdokumentation** unterstützt den Anwender beim datenschutzgerechten Einsatz des IVS durch Angabe von: 1. Technischen und ggf. organisatorischen Vorrausetzungen zum Betrieb des Services, z. B. ▪ Notwendigkeit einer bestimmten Systemumgebung, ▪ Notwendigkeit bestimmter Zusatzkomponenten im Kontext der nutzbaren Funktionen, ▪ Notwendigkeit von Einweisungen / Schulungen. 2. Grenzwerten der Nutzbarkeit des Service, z. B. ▪ Anzahl der erfassbaren Personendatensätze, ▪ technisch bedingte maximale Vorhaltezeit von Protokollen, ▪ zugesicherte maximale Ausfallrate des Services bei 24/7 Betrieb. 3. Maßgaben zur Einrichtung der Zugriffsverwaltung des Service, z. B. ▪ Angaben dazu, welche Arten von Nutzerrollen für die Nutzung des Services erforderlich sind, ▪ Anleitung zu Einrichtung der Benutzerverwaltung, ▪ Empfehlungen zur datenschutzgerechten Einrichtung der Zugriffstrennung zwischen den Nutzern. 4. Maßgaben zur Nutzung der im IVS verwendeten Sicherheitstechnologien, z. B. ▪ Informationen über eingesetzte Verschlüsselungstechnologien, ▪ Informationen über eingesetzte Signaturkomponenten, ▪ Informationen über die Art der Nutzerauthentifikation. 5. möglichen Risiken für den Schutz der verarbeiteten personenbezogenen Daten, die sich aus der Nutzung des IVS ergeben, z. B. ▪ Risiko der Nicht-Aktualisierung von Softwarekomponenten, ▪ Risiko des Durchbrechens von Zugriffsschranken, ▪ Risiko der Erfassung Daten Dritter.

[DSGVO] Art. 24 Abs. 1, **DS07.01, DS09.04**

DS01.04	**Verantwortlicher und Auftragsverarbeiter** Die zum Service bereitgestellten **Änderungsdokumentationen** enthalten 1. eine vollzählige Auflistung der hinsichtlich der Servicefunktionalität und seiner technischen Einsatzbedingungen relevanten Änderungen, 2. pro Änderung ▪ eine Beschreibung der durchgeführten Änderung,

	▪ ggf. Maßnahmen des Anwenders, welche im Kontext der Serviceänderung erforderlich sind, ▪ ggf. Hinweise zu Einsatzmodalitäten (z. B. genutzte Module), bei denen diese Änderung relevant ist, ▪ Erkennbarkeit von Serviceversion bzw. Datum, ab welcher diese Änderung eingeführt wurde.

DS02 Grundsätze der Verarbeitung

[DSGVO] Art. 5 Abs. 1 lit. a

DS02.01	**Verantwortlicher** Die personenbezogenen Daten müssen in einer für die betroffenen Personen nachvollziehbaren Weise verarbeitet werden (**Transparenzgrundsatz**). Dem Betroffenen werden alle Informationen und Mitteilungen zur Verarbeitung der PBD leicht zugänglich, verständlich sowie in klarer und einfacher Sprache zur Verfügung gestellt, vgl. DS06.01. Hierbei wird insbesondere gewährleistet: • Die Datenschutzinformationen sind klar von anderen Informationen, die sich nicht auf den Datenschutz beziehen, z. B. Vertragsbestimmungen, allgemeine Nutzungsbedingungen, getrennt • Die Datenschutzinformationen sind für einen typischen Angehörigen des Zielpublikums verständlich (Berücksichtigung des Verständnishorizonts der jeweilig betroffenen Personen). • Es ist für die betroffene Person sofort ersichtlich, wo und wie sie auf die Datenschutzinformationen zugreifen kann (leichte Zugänglichkeit) • Sofern das Zielpublikum des Verantwortlichen Kinder sind oder die Waren/Dienstleistungen insbesondere von Kindern genutzt werden, ist die Wortwahl, die Tonalität und der Sprachstil der kindlichen Zielgruppe angepasst • Die erteilten Informationen beinhalten die Angaben gem. Art. 13 bzw. 14 DSGVO, vgl. DS06.04 und DS06.05, sodass sichergestellt ist, dass die betroffene Person den Umfang und die Folgen der Verarbeitung ermitteln kann • Der Verantwortliche stellt die Informationen nach Art. 13 und 14 DSGVO den Betroffenen aktiv bereit oder leitet die Betroffenen direkt an die Stelle wo die Informationen zur Verfügung stehen • Der Betroffene hat dauerhaft Zugang zu den Informationen nach Art. 13 und 14 DSGVO • Der Verantwortliche erinnert den Betroffenen in regelmäßigen Abständen (mindestens jährlich) an die Datenschutzerklärung/-informationen und wo diese zu finden sind • Es wird ein allgemein geläufiger Begriff, wie z. B. „Datenschutz“, „Datenschutzbestimmungen“, „Datenschutzinformationen“, „Datenschutzhinweis“ verwendet • Bei komplexen, technischen oder unerwarteten Verarbeitungsvorgängen erfolgt, neben der Bereitstellung der nach den Art. 13 und 14 DSGVO erforderlichen Informationen, gesondert und eindeutig formuliert eine Darlegung der wichtigsten Folgen der Verarbeitung • Der Verantwortliche nimmt eine dokumentierte Abschätzung vor, ob sich für die durch die Verarbeitung betroffenen Personen besondere Risiken ergeben, die den betroffenen Personen zur Kenntnis gebracht werden sollten. Wenn dies der Fall ist, werden die Betroffenen über diese Risiken aufgeklärt. • Verwendung von Mehrebenen-Datenschutzerklärungen/-informationen, die den Betroffenen das direkte Aufrufen bestimmter Punkte

	ermöglichen, anstatt Darstellung der gesamten Informationen auf dem Bildschirm in Form eines einzigen Hinweises. • Die Informationen werden in einer möglichst einfachen Art und Weise unter Vermeidung komplexer Satz- und sprachlicher Strukturen bereitgestellt • Abstrakte und mehrdeutige Begriffe bzw. Interpretationsspielraum werden vermieden. • Modalverben und -wörter wie „kann“, „könnte“, „manche“, „oft“ und „möglich“ werden vermieden • Absätze und Sätze sind wohl strukturiert und hierarchische Beziehungen werden mit Aufzählungszeichen sowie Einzügen dargestellt. • Die Informationen sind im Aktiv und nicht im Passiv verfasst und übermäßige Substantivierungen werden vermieden • Die Informationen enthalten nicht unverhältnismäßig viele rechtliche, technische oder fachbezogene Formulierungen oder eine entsprechende Terminologie • Sofern das Zielpublikum des Verantwortlichen Kinder sind, ist die Wortwahl, die Tonalität und der Sprachstil der kindlichen Zielgruppe angepasst, sodass der kindliche Empfänger der Informationen auch erkennt, dass die Mitteilung / Information an ihn gerichtet ist • Die Information erfolgt in der Landessprache der jeweiligen Zielgruppe, mithin in Deutsch • Die Übermittlung der Informationen bzgl. der Datenverarbeitung erfolgt schriftlich oder in anderer Form, ggf. auch elektronisch • Die Bereitstellung der Informationen nach Art. 13 und 14 DSGVO nach kann auch in elektronischer Form erfolgen (z. B. auch kontextbezogene „Just-in-time-Pop-up-Hinweise“, 3D Touch-Hinweise sowie Datenschutz-Dashboards, ggfs. Videos und Smartphone- oder IoT-Sprachmeldungen zusätzlich zu Mehrebenen-Datenschutzerklärungen/ -hinweisen) • Für den Fall, dass eine Webseite betrieben wird: Verwendung von Mehrebenen-Datenschutzerklärungen/-hinweisen, die den Betroffenen das direkte Aufrufen bestimmter Punkte ermöglichen, anstatt Darstellung der gesamten Informationen auf dem Bildschirm in Form eines einzigen Hinweises. Weiterhin ist bei der Verwendung von Mehrebenen-Datenschutzerklärungen/-informationen zu gewährleisten: ○ Die Informationen nach Art. 13 und 14 DSGVO werden auch leicht zugänglich an einem einzigen Ort oder in einem Gesamtdokument (digital oder im Papierformat) zur Verfügung gestellt. ○ Die Gestaltung und Gliederung der ersten Ebene der Mehrebenen-Datenschutzerklärung/-informationen muss der betroffenen Person einen Gesamtüberblick über die ihr hinsichtlich der Verarbeitung ihrer personenbezogenen Daten zur Verfügung stehenden Informationen liefen und aufzeigen, wo / wie sie die einzelnen Informationen auf den jeweiligen Ebenen der Datenschutzerklärungen / -hinweise finden kann. ○ Die auf den verschiedenen Ebenen eines Mehrebenen-Hinweises enthaltenen Informationen sind konsistent und unterscheiden sich nicht in widersprüchlicher Weise von Ebene zu Ebene ○ Die erste Ebene von Mehrebenen-Datenschutzerklärungen / -informationen enthält Informationen zu: Verarbeitungszwecken, die Identität des Verantwortlichen sowie eine

	Beschreibung der Rechte der betroffenen Person, Angaben über die Verarbeitung, welche sich am stärksten auf die betroffene Person auswirkt, und die Verarbeitungsvorgänge, mit denen die betroffene Person ggfs. nicht rechnet ○ Die vorstehenden Informationen werden der betroffenen Person direkt zum Zeitpunkt der Erhebung der personenbezogenen Daten zur Kenntnis gebracht werden, z. B. durch die Anzeige auf dem Bildschirm, während die betroffene Person ein Online-Formular ausfüllt ○ Im Hinblick auf den Einsatz des Mehrebenen Ansatzes in einer nicht-digitalen Umgebung: Auf der ersten Ebene werden den Betroffenen zumindest folgende Informationen mitgeteilt: Verarbeitungszwecke, die Identität des Verantwortlichen sowie eine Beschreibung der Rechte der betroffenen Person, Angaben über die Verarbeitung, welche sich am stärksten auf die betroffene Person auswirkt, und die Verarbeitungsvorgänge, mit denen die betroffene Person ggfs. nicht rechnet. Es ist festzulegen und zu dokumentieren, wie die Mitteilung der weiteren nach Art. 13 und 14 DSGVO erforderlichen Informationen erfolgt • Informationen zur Ausübung der Rechte bzgl. der Verarbeitung personenbezogener Daten (Art. 15 – 22 DSGVO) werden der betroffenen Person bereitgestellt • Prozesse bzgl. der Gewährleistung des Rechts auf Auskunft sind etabliert, vgl. **DS06.11** • Die von einer Verletzung des Schutzes der PBD Betroffenen werden benachrichtigt, vgl. **DS09.02** • Unentgeltliche Erteilung der Informationen ○ der Verantwortliche verlangt kein Entgelt für die Erteilung von Informationen nach den Art. 13 und 14 DSGVO oder für Mitteilungen und getroffene Maßnahmen nach den Art. 15 - 22 sowie Art. 34 DSGVO ○ Die Bereitstellung von Informationen ist nicht abhängig von einer finanziellen Transaktion des Betroffenen ○ Nur im Falle von offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder b) sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche muss in diesen Fällen den Nachweis, für den offenkundig unbegründeten oder exzessiven Charakter des Antrags erbringen. • Bezüglich des Zeitpunkts der Informationserteilung werden nachfolgende Fristen eingehalten: a) PBD werden von der betroffenen Person selbst erhoben ○ Die Informationen (Datenschutzinformationen) werden vor der Erhebung der PBD übermittelt, vgl. Art. 13 Abs. 1 DSGVO b) PBD werden nicht bei der betroffenen Person erhoben • Im Hinblick auf den Zeitpunkt der Information des Betroffenen

	sind folgende Fristen gem. Art. 14 Abs. 3 DSGVO einzuhalten ○ Die Informationen (Datenschutzinformationen) werden dem Betroffenen in einer angemessenen Frist nach Erlangung der personenbezogenen Daten „unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten“, längstens innerhalb eines Monats (= äußerste Frist) mitgeteilt (Art. 14 Abs. 3 lit. a DSGVO). Im Hinblick auf die Frist sind folgende Restriktionen zu beachten und entsprechend muss eine frühere Erteilung der Informationen gewährleistet werden. a. Sofern die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden: Die Information muss spätestens zum Zeitpunkt der ersten Kommunikation mit der betroffenen Person erteilt werden (auch wenn die äußerste Frist noch nicht abgelaufen ist) (Art. 14 Abs.3 lit. b DSGVO). b. Sofern eine Offenlegung der personenbezogenen Daten an einen anderen Empfänger beabsichtigt ist: Die Informationen müssen spätestens zum Zeitpunkt dieser Offenlegung erteilt werden (auch wenn die äußerste Frist noch nicht abgelaufen ist) (Art. 14. Abs. 3 lit. c DSGVO) Bei der Entscheidung, wann die Bereitstellung der Informationen nach Art. 14 DSGVO erfolgen soll, sind stets die berechtigten Erwartungen der betroffenen Personen (wie ist das Informationsinteresse der betroffenen Person, d. h. wie dringend wird die Information zur Ausübung ihrer Rechte benötigt), die mögliche Wirkung der Verarbeitung auf Letztere und deren Fähigkeit, ihre Rechte in Bezug auf diese Verarbeitung auszuüben, zu berücksichtigen. Die Entscheidungsgründe, warum die Information zu dem konkret gewählten Zeitpunkt erteilt wurde, sind durch den Verantwortlichen zu dokumentieren. Im Einklang mit dem Grundsatz von Treu und Glauben sind die Informationen so weit wie möglich frühzeitig vor Ablauf der vorgegebenen Fristen zu erteilen. Die Informationspflicht nach Art. 14 Abs. 1 – 4 DSGVO findet in folgenden Fällen keine Anwendung, vgl. Art. 14 Abs. 5 DSGVO: • Der Betroffene verfügt bereits über die Informationen. Der Verantwortliche muss hierbei nachweisen, über welche Informationen der Betroffene bereits verfügt, wie und wann er sie erhalten hat, und diese Informationen in der Zwischenzeit keiner wesentlichen Änderung unterlagen. Nicht wesentliche Änderungen sind beispielsweise Korrekturen von Rechtschreibfehlern oder stilistischen bzw. grammatikalischen Mängel • Die Informationserteilung erweist sich als rechtlich oder tatsächlich unmöglich oder erfordert einen unverhältnismäßigen Aufwand. Die Unmöglichkeit der Informationserteilung betrifft insbesondere Fälle, in denen der Verantwortliche den Betroffenen nicht kennt und die Person deshalb nicht informieren kann. Der Verantwortliche muss die Faktoren darlegen, die ihn daran hindern, den Betroffenen die besagten Informationen zu übermitteln. Bei der Bewertung, ob der Aufwand unverhältnismäßig ist, muss der Verantwortliche eine Abwägung zwischen seinem durch die Information entstehenden Aufwand und den Informationsinteressen des Betroffenen vornehmen und das Ergebnis dokumentieren. Es besteht weiterhin keine Informationspflicht, wenn sich die Erteilung dieser Informationen als unmöglich erweist oder einen

	unverhältnismäßigen Aufwand erfordern würde; dies gilt insbesondere für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke vorbehaltlich der in Art. 89 Abs. 1 DSGVO genannten Bedingungen und Garantien oder soweit die in Art. 14 Abs. 1 DSGVO genannte Pflicht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt. • Es ist sicherzustellen, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Ebenso kann eine Pseudonymisierung zu den geeigneten Maßnahmen gehören, sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen. Sofern die Informationen nach Art. 13 und 14 DSGVO wesentlich oder sachlich geändert werden (insbesondere bei Änderung des Verarbeitungszwecks, der Identität des Verantwortlichen, Änderung der Vorgehensweise, wie die betroffenen Personen ihre Rechte bzgl. der Verarbeitung ausüben können, Erweiterung der Kategorien von Empfängern, zukünftige Übermittlung in ein Drittland) sind die betroffenen Personen frühzeitig vor dem tatsächlichen Wirksamwerden über die Änderungen in Kenntnis zu setzen (mindestens 14 Tage vorher). Keine Informationspflicht besteht bei nicht-wesentlichen Änderungen. Nicht wesentliche Änderungen sind beispielsweise Korrekturen von Rechtschreibfehlern oder stilistischen bzw. grammatikalischen Mängeln. Der Verantwortliche muss sicherstellen, dass die Bekanntgabe der Änderungen in einer Art und Weise erfolgt, die sicherstellt, dass die Mehrzahl der Empfänger ihr auch tatsächlich Beachtung schenkt. Im Hinblick auf Änderungen der Informationen nach Art. 13 und 14 DSGVO hat der Verantwortliche Prozesse implementiert und dokumentiert, welche insbesondere Regelungen treffen zu: • Vorgaben bzgl. der Prüfung und Erfassung etwaiger Anpassungserfordernisse der Datenschutzinformationen bei Änderungen der Verarbeitungstätigkeiten (Festlegung von Zuständigkeiten, Kommunikationswege, Einbindung des Datenschutzbeauftragten, Dokumentation der Anpassungserfordernisse, Sensibilisierung der Beschäftigten • Festlegung von Zuständigkeiten für die Vornahme, Freigabe und Veröffentlichung von Änderungen an den Datenschutzinformationen • Festlegung wie Bekanntgabe der Änderungen erfolgt ○ Es muss sichergestellt sein, dass die Mehrzahl der Empfänger die Änderungsmitteilung zur Kenntnis nimmt (z. B. per E-Mail, per klassischem Brief auf Papier, per Pop-up auf einer Webseite oder auf eine andere Art und Weise, welche der betroffenen Person die Änderungen wirksam zur Kenntnis bringt ○ die Änderungsmitteilung muss separat von anderen Informationen erfolgen ○ Die Information erfolgt in einer präzisen, transparenten, verständlichen und leicht zugänglichen Form und der

	Verwendung einer klaren und einfachen Sprache, vgl. **DS06.01** ○ Dem Betroffenen werden die möglichen Auswirkungen dieser Änderungen erläutert Die Erfüllung des Transparenzgrundsatzes durch den Verantwortlichen ergibt sich aus der gesamtheitlichen Erfüllung der oben referenzierten Einzelanforderungen. Im Hinblick auf die Transparenz der Datenverarbeitung und der Verarbeitung nach Treu und Glauben ist den „Leitlinien für Transparenz gemäß der Verordnung 2016/679 angenommen am 29. November 2017 zuletzt überarbeitet und angenommen am 11. April 2018 der Datenschutzgruppe nach Artikel 29 zu folgen

[DSGVO] Art. 5 Abs. 1 lit. a

DS02.02	**Verantwortlicher** Der Evaluierungsgegenstand ist so ausgestaltet, dass die Verarbeitung nach **Treu und Glauben** erfolgt. Der Verantwortliche verarbeitet die PBD in einer Weise, die für die betroffene Person nicht ungerechtfertigt nachteilig, unrechtmäßig diskriminierend, unerwartet oder irreführend ist. Der Verantwortliche setzt nachfolgende Maßnahmen im Rahmen der Erfüllung des Grundsatzes nach Treu und Glauben um. • Information der Betroffenen über das Bestehen einer Verarbeitung und deren Zwecke, vgl. **DS02.01**, **DS06.01, DS06.04, DS06.05**, sodass diese im Voraus bestimmen können, welchen Umfang und welche Folgen die Verarbeitung hat. Bezüglich des Zeitpunkts der Informationserteilung werden nachfolgende Fristen eingehalten: a) PBD werden von der betroffenen Person selbst erhoben • Die Informationen (Datenschutzinformationen) werden vor der Erhebung der PBD übermittelt, vgl. Art. 13 Abs. 1 DSGVO b) PBD werden nicht bei der betroffenen Person erhoben • Im Hinblick auf den Zeitpunkt der Information des Betroffenen sind folgende Fristen gem. Art. 14 Abs. 3 DSGVO einzuhalten: ○ Die Informationen (Datenschutzinformationen) werden dem Betroffenen in einer angemessenen Frist nach Erlangung der personenbezogenen Daten „unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten“, längstens innerhalb eines Monats (= äußerste Frist) mitgeteilt (Art. 14 Abs. 3 lit. a DSGVO). Im Hinblick auf die Frist sind folgende Restriktionen zu beachten und entsprechend muss eine frühere Erteilung der Informationen gewährleistet werden. ○ Sofern die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden: Die Information muss spätestens zum Zeitpunkt der ersten Kommunikation mit der betroffenen Person erteilt werden (auch wenn die äußerste Frist noch nicht abgelaufen ist) (Art. 14 Abs.3 lit. b DSGVO).

	○ Sofern eine Offenlegung der personenbezogenen Daten an einen anderen Empfänger beabsichtigt ist: Die Informationen müssen spätestens zum Zeitpunkt dieser Offenlegung erteilt werden (auch wenn die äußerste Frist noch nicht abgelaufen ist) (Art. 14. Abs. 3 lit. c DSGVO) ○ Bei der Entscheidung, wann die Bereitstellung der Informationen nach Art. 14 DSGVO erfolgen soll, sind stets die berechtigten Erwartungen der betroffenen Personen (wie ist das Informationsinteresse der betroffenen Person, d. h. wie dringend wird die Information zur Ausübung ihrer Rechte benötigt), die mögliche Wirkung der Verarbeitung auf Letztere und deren Fähigkeit, ihre Rechte in Bezug auf diese Verarbeitung auszuüben, zu berücksichtigen. Die Entscheidungsgründe, warum die Information zu dem konkret gewählten Zeitpunkt erteilt wurde, sind durch den Verantwortlichen zu dokumentieren. Im Einklang mit dem Grundsatz von Treu und Glauben sind die Informationen so weit wie möglich frühzeitig vor Ablauf der vorgegebenen Fristen zu erteilen. Die Informationspflicht nach Art. 14 Abs. 1 – 4 DSGVO findet in folgenden Fällen keine Anwendung, vgl. Art. 14 Abs. 5 DSGVO: ○ Der Betroffene verfügt bereits über die Informationen. Der Verantwortliche muss hierbei nachweisen, über welche Informationen bereits verfügt, wie und wann er sie erhalten hat, und diese Informationen in der Zwischenzeit keiner wesentlichen Änderung unterlagen. Nicht wesentliche Änderungen sind beispielsweise Korrekturen von Rechtschreibfehlern oder stilistischen bzw. grammatikalischen Mängeln. ○ Die Informationserteilung erweist sich als rechtlich oder tatsächlich unmöglich oder erfordert einen unverhältnismäßigen Aufwand. Die Unmöglichkeit der Informationserteilung betrifft insbesondere Fälle, in denen der Verantwortliche den Betroffenen nicht kennt und die Person deshalb nicht informieren kann. Der Verantwortliche muss die Faktoren darlegen, die ihn daran hindern, den Betroffenen die besagten Informationen zu übermitteln. Bei der Bewertung, ob der Aufwand unverhältnismäßig ist, muss der Verantwortliche eine Abwägung zwischen seinem durch die Information entstehenden Aufwand und den Informationsinteressen des Betroffenen vornehmen und das Ergebnis dokumentieren. ○ Es besteht weiterhin keine Informationspflicht, wenn die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erfolgt. Voraussetzung dafür ist jedoch, dass die in Art. 89 Abs. 1 DSGVO genannten Bedingungen und Garantien erfüllt sind. Es ist sicherzustellen, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Ebenso kann eine Pseudonymisierung zu den geeigneten

	Maßnahmen gehören, sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen. • Der Verantwortliche stellt Informationen bzgl. der Datenverarbeitung in objektiver und neutraler Weise unter Vermeidung jeglicher irreführender oder manipulativer Sprache oder Gestaltung bereit, vgl. Anforderungen in **DS06.01**. ○ Die Informationen werden hierbei in einer möglichst einfachen Art und Weise unter Vermeidung komplexer Satz- und sprachlicher Strukturen bereitgestellt ○ Abstrakte und mehrdeutige Begriffe bzw. Interpretationsspielraum werden vermieden. ○ Insbesondere die Zwecke und die Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten sind klar dargelegt sein. ○ Modalverben und -wörter wie „kann“, „könnte“, „manche“, „oft“ und „möglich“ werden vermieden. ○ Absätze und Sätze sind wohl strukturiert und hierarchische Beziehungen werden mit Aufzählungszeichen sowie Einzügen dargestellt. ○ Die Informationen sind im Aktiv und nicht im Passiv verfasst und übermäßige Substantivierungen werden vermieden ○ Die Informationen enthalten nicht unverhältnismäßig viele rechtliche, technische oder fachbezogene Formulierungen oder eine entsprechende Terminologie ○ Sofern das Zielpublikum des Verantwortlichen Kinder sind, ist die Wortwahl, die Tonalität und der Sprachstil der kindlichen Zielgruppe angepasst, sodass der kindliche Empfänger der Informationen auch erkennt, dass die Mitteilung / Information an ihn gerichtet ist ○ Die Informationen bzgl. der Datenverarbeitung sind von anderen Informationen, die sich nicht auf den Datenschutz beziehen, z. B. Vertragsbestimmungen, Nutzungsbedingungen, getrennt ○ Verwendung eines gemeinhin geläufigen Begriffs, wie z. B. „Datenschutz“, „Datenschutzbestimmungen“, „Datenschutzinformationen“, „Datenschutzhinweis“ ○ Die Information erfolgt in der Landessprache der jeweiligen Zielgruppe, mithin in Deutsch • Die Verarbeitung der PBD beruht auf einer Rechtsgrundlage, vgl. **DS03.01** • Die einschlägigen Rechtsgrundlagen werden konkret gegenüber den Betroffenen kommuniziert. • Der Verantwortliche hat Prozesse bzgl. der Änderungen der Information nach Art. 13 und 14 DSGVO implementiert, vgl. **DS06.01** • Der Verantwortliche ergreift Maßnahmen, um ein angemessenes Gleichgewicht zwischen seinen geschäftlichen Interessen und den Rechten und Erwartungen der betroffenen Personen herzustellen, insbesondere bei Online-Diensten im Zusammenhang mit Online-Diensten, die ohne Bezahlung angeboten werden und bei denen die Nutzer häufig nicht wissen, wie und in welchem Umfang ihre

	personenbezogenen Daten verarbeitet werden (sofern der Verantwortliche seine Datenverarbeitung auf ein berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DSGVO stützt), vgl. Anforderungen in **DS03.07** Der Verantwortliche hat Prozesse etabliert, die es dem Betroffenen ermöglichen, seine Rechte in Bezug auf die verarbeiteten PBD auszuüben: ○ Recht auf Auskunft, vgl. **DS06.02, DS06.07, DS06.08, DS06.09** ○ Recht auf Berichtigung, vgl. **DS06.02**, **DS06.11** ○ Recht auf Löschung, vgl. **DS06.02**, **DS06.11** ○ Recht auf Einschränkung, vgl. **DS06.02, DS06.11**, **DS06.13** ○ Recht auf Datenübertragbarkeit, vgl. **DS06.02, DS06.14** ○ Recht auf Widerspruch, vgl. **DS06.02, DS06.15**, **DS06.16** ○ Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, vgl. **DS06.17** • Der Verantwortliche stellt sicher, dass er Betroffene nicht in unlauterer Weise[4] an seinen Dienst bindet (sog. Lock-In). Im Zuge eines Anbieterwechsels muss er Betroffenen ermöglichen, ihre personenbezogenen Daten zu einem anderen Verantwortlichen übertragen zu können, ohne dass dies mit besonderem Aufwand und ggf. Datenverlusten verbunden ist, vgl. die Anforderungen in **DS06.14**. • sofern relevant: im Rahmen einer dokumentierten Abwägung nach Art. 6 Abs. 1 lit. f DSGVO werden die vernünftigen Erwartungen der Betroffenen durch den Verantwortlichen berücksichtigt. Im Hinblick auf die vernünftigen Erwartungen sind dabei zu berücksichtigen: ○ a) ob eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht (vgl. ErwG 47 Satz 1 und 2 DSGVO). Hierbei sind insbesondere folgende Elemente bei der Bewertung der Beziehung zur betroffenen Person zu berücksichtigen: ○ Bestehen einer Beziehung zur betroffenen Person (z. B. ist zwischen Kunden und Nicht-Kunden zu unterschieden), einschließlich des Datums der Beendigung der Beziehung, falls eine solche bestand ○ Nähe der Beziehung (z. B. Fälle, in denen ein für die Verarbeitung Verantwortlicher Teil einer Unternehmensgruppe mit einer einzigen Marke ist, im Vergleich zu einer Unternehmensgruppe, die nur wirtschaftliche Verbindungen hat, die dem durchschnittlichen Kunden unbekannt sind, da im letzteren Fall die betroffene Person weniger wahrscheinlich erwarten kann, dass Daten zwischen den Unternehmen der Gruppe ausgetauscht werden) ○ Ort und Kontext der Datenerhebung (z. B. erwarten die Betroffenen vielleicht eine Videoüberwachung in einer Bank, nicht aber in Sanitär- oder Saunaeinrichtungen)

[4] Geschäftliche Handlungen, die sich an Verbraucher richten oder diese erreichen, sind unlauter, wenn sie nicht der unternehmerischen Sorgfalt entsprechen und dazu geeignet sind, das wirtschaftliche Verhalten des Verbrauchers wesentlich zu beeinflussen.

	○ Art und Merkmale der Dienstleistung (z. B. haben ein Stammkunde und ein bloßer Interessent, der nur einen Newsletter abonniert hat, unterschiedliche angemessene Erwartungen) ○ Anwendbare rechtliche Anforderungen im jeweiligen Kontext (z. B. Vertraulichkeitsanforderungen, die für die betreffende Beziehung gelten) ○ b) ob die Betroffenen zum Zeitpunkt der Erhebung der PBD und der Umstände der Verarbeitung, vernünftigerweise absehen können, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird (ErwG 47 Satz 3 DSGVO), d.h., dass die Verarbeitung nicht überraschend oder unwahrscheinlich ist, vgl. Anforderungen in **DS03.07**. ○ Die bloße Erfüllung der in den Art. 12, 13 und 14 DSGVO festgelegten Informationspflichten sind nicht ausreichend, um davon auszugehen, dass die betroffenen Personen vernünftigerweise eine bestimmte Verarbeitung erwarten können, können die Erwartung des Betroffenen aber zu einem gewissen Maß beeinflussen. ○ Bei der Abwägung ist die „durchschnittliche“ betroffene Person zu betrachten, es sei denn die Verarbeitung wird wahrscheinlich verschiedene Gruppen von betroffenen Personen mit unterschiedlichen Merkmalen betreffen. Hierbei sind nachfolgende Merkmale zu berücksichtigen: ○ Alter der betroffenen Person (die berechtigten Erwartungen von Minderjährigen können anders sein als die von Erwachsenen) ○ Ausmaß, in dem die betroffene Person eine Person des öffentlichen Lebens ist ○ Die (berufliche) Stellung, die die betroffene Person innehat, und der Grad des Verständnisses und der Kenntnis der geplanten Verarbeitung, die sie in einem bestimmten Kontext haben dürfte (z. B. würde das Personal, das an einem Bewerbungsgespräch beteiligt ist, häufig erwarten, dass einige seiner personenbezogenen Daten mit den Bewerbern ausgetauscht werden). ○ Sofern relevant: Im Falle einer Zweckänderung/Weiterverarbeitung sind bei der Kompatibilitätsprüfung nach Art. 6 Abs. 4 DSGVO die vernünftigen Erwartungen der betroffenen Person zu berücksichtigen (ErwG 50 Satz 6), vgl. die Anforderungen in **DS03.08** • sofern relevant: Sofern die Verarbeitung von PBD auf der Grundlage von Algorithmen erfolgt, informiert der Verantwortliche den Betroffenen über den Umstand, dass mithilfe der Algorithmen Analysen oder Prognosen über sie erstellt werden. Der Verantwortliche prüft regelmäßig, ob die Algorithmen zweckentsprechend funktionieren. Hierfür sind entsprechende Zuständigkeiten, Prüfungsintervalle und die Prüfungsmethodik durch den Verantwortlichen festzulegen. Sofern Fehler festgestellt werden, sind diese zu beheben. • Der Verantwortliche sieht für den Fall, dass automatisierte Entscheidungen im Einzelfall einschließlich Profiling betrieben wird, ein qualifiziertes menschliches Eingreifen vor, um Fehler aufzudecken, die durch Maschinen entstehen können, vgl. **DS06.17**.

	Die Erfüllung des Grundsatzes zur Verarbeitung nach Treu und Glauben durch den Verantwortlichen ergibt sich aus der gesamtheitlichen Erfüllung der oben referenzierten Einzelanforderungen.

[DSGVO] Art. 5 Abs. 1 lit. a

DS02.03	**Verantwortlicher** Der Evaluierungsgegenstand ist so ausgestaltet, dass die **Datenverarbeitung unter Zugrundelegung einer Rechtsgrundlage** (Grundsatz der Rechtmäßigkeit) erfolgt. Hierzu muss der Verantwortliche eine gültige Rechtsgrundlage für die Verarbeitung PBD festlegen. 1. Für die Datenverarbeitung muss der Verantwortliche die korrekte Rechtsgrundlage heranziehen. Hierbei sind folgende Rechtsgrundlagen zu berücksichtigen: a) die betroffene Person hat ihre Einwilligung erteilt (Art. 6 Abs. 1 lit. a DSGVO). Die Einwilligung muss freiwillig für den bestimmten Fall, in Kenntnis der Sachlage und unmissverständlich erteilt werden. Besondere Aufmerksamkeit soll der Frage gewidmet werden, ob Kinder und Jugendliche in der Lage sind, ihren Willen in Kenntnis der Sachlage zu bekunden, vgl. die Anforderungen in **DS03.02, DS04 und DS04.09** (Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft) b) die Verarbeitung erfolgt für die Erfüllung eines Vertrages oder die Durchführung einer vorvertraglichen Maßnahme (Art. 6 Abs. 1 lit. b DSGVO), vgl. die Anforderungen in **DS03.03** c) die Verarbeitung erfolgt zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, vgl. die Anforderungen in **DS03.04** d) die Verarbeitung erfolgt, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen, vgl. die Anforderungen in **DS03.05** e) die Verarbeitung erfolgt für die Wahrnehmung einer Aufgabe, die erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde (Art. 6 Abs. 1 lit. e DSGVO), vgl. die Anforderungen in **DS03.06** f) die Verarbeitung erfolgt zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 lit. f DSGVO), vgl. die Anforderungen in **DS03.07** g) sofern relevant: die Voraussetzungen an eine zweckändernde Weiterverarbeitung erfüllt sind (Art. 6 Abs. 4 DSGVO), vgl. die Anforderungen in **DS03.08** 2. Sofern die Voraussetzungen für die Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 DSGVO erfüllt sind, muss der Verantwortliche die Anforderungen in **DS05** umsetzen 3. Der Verantwortliche dokumentiert die Rechtsgrundlagen sowie den Umstand, weshalb die Rechtsgrundlagen für die konkrete Verarbeitung einschlägig sind, vgl. Anforderungen in **DS03.01**. 4. Der Verantwortliche informiert Betroffene über die einschlägigen Rechtsgrundlagen, vgl. Anforderungen in **DS06.01**.

	5. Der Verantwortliche differenziert bei der Auswahl korrekter Rechtsgrundlagen nach einzelnen Verarbeitungstätigkeiten, vgl. Anforderungen in **DS03.01**. 6. Der Verantwortliche stellt sicher, dass die Rechtsgrundlage in einem klaren Zusammenhang zu dem Zweck der Verarbeitung steht und die Verarbeitung notwendig ist und nicht an Bedingungen geknüpft ist, vgl. Anforderungen in **DS02.06**. 7. Der Verantwortliche legt vor Beginn der Verarbeitung die Rechtsgrundlage fest, vgl. Anforderungen in **DS03.01**. 8. Der Verantwortliche stellt die Verarbeitung ein, sobald die Rechtsgrundlage entfällt und löscht die PBD, vgl. Anforderungen in **DS02.08** 9. Der Verantwortliche stellt sicher, dass der Betroffene die Kontrolle über die PBD im Rahmen der Rechtsgrundlage so autonom wie möglich ausüben kann. 10. Wenn eine Einwilligung Rechtsgrundlage für die Verarbeitung ist, muss der Verantwortliche den Widerruf der Einwilligung durch den Betroffenen ermöglichen. Ein Widerruf der Einwilligung ist so einfach zu ermöglichen wie ihre Erteilung, vgl. **DS04.06.** 11. Wenn berechtigte Interessen die Rechtsgrundlage sind, muss der Verantwortliche eine ausgewogene Interessenabwägung vornehmen und dabei insbesondere das Ungleichgewicht der Kräfte berücksichtigen, vor allem dann, wenn Kinder im Alter von bis zu 18 Jahren und andere schutzbedürftige Gruppen betroffen sind. Es werden Maßnahmen und Garantien zur Reduzierung der negativen Auswirkungen auf die betroffenen Personen umgesetzt, vgl. **DS03.07**. Die Erfüllung des Grundsatzes zur Rechtmäßigkeit durch den Verantwortlichen ergibt sich aus der gesamtheitlichen Erfüllung der oben referenzierten Einzelanforderungen.

[DSGVO] Art. 5 Abs. 1 lit. b

DS02.04	**<u>Verantwortlicher</u>** Der Verantwortliche stellt sicher, dass die Zwecke, zu denen die PBD verarbeitet werden, festgelegt, eindeutig und legitim sind **(Zweckbindung).** Der Zweck der Verarbeitung steht vor der Erhebung personenbezogener Daten fest. Der Verantwortliche dokumentiert den Zweck der Datenverarbeitung. Zweckänderungen darf der Verantwortliche nur unter Einhaltung der Ausnahmeregelungen des Art. 6 Abs. 4 DSGVO vornehmen (vgl. **DS03.08**). Der Verantwortliche verfügt über dokumentierte Prozesse zur Auswahl und Umsetzung technischer und organisatorischer Maßnahmen, um eine zweckgebundene Datenverarbeitung sicherzustellen. Die Prozesse regeln insbesondere: 1. Der Verantwortliche legt die Zwecke vor der Datenverarbeitung fest und bewertet, zu welchen Zwecken die Datenverarbeitung erfolgen soll. Die Zuständigkeiten und der Ablauf der Bewertung sind festzulegen und zu dokumentieren. Abgeleitet aus dem definierten Zweck, stellt der Verantwortliche fest, welche personenbezogenen Daten für die Verarbeitung erforderlich sind. 2. Der Verantwortliche dokumentiert die Zwecke in einer Weise, dass es Dritten möglich ist, diese nachzuvollziehen. Dabei berücksichtigt der Verantwortliche Folgendes: ▪ Der Zweck muss konkret bestimmt sein, zu allgemeine Angaben wie beispielsweise „für Marketing-Zwecke“, „Verbesserung der Nutzererfahrungen“, IT-Sicherheitszwecke“, „zukünftige Forschung“ sind ohne weitere Detailangaben nichtkonkret bestimmt. Wie detailliert ein Zweck angegeben werden sollte, hängt von dem besonderen Kontext ab, in dem die Daten erhoben werden, und von den betroffenen personenbezogenen Daten. ▪ Abstrakte und mehrdeutige Begriffe bzw. Begriffe mit Interpretationsspielraum sind zu vermeiden. ▪ Die Zweckbeschreibung darf nicht unverhältnismäßig viele rechtliche, technische oder fachbezogene Formulierungen oder eine entsprechende Terminologie enthalten. 3. Der Verantwortliche legt die Zwecke eindeutig fest (Spezifizität) 4. Der Verantwortliche prüft und stellt sicher, dass die Verarbeitung zu den festgelegten Zwecken rechtlich zulässig ist (Legitimität), vgl. Anforderungen in **DS02.03**. 5. Der Verantwortliche implementiert technische und organisatorische Maßnahmen, die eine Nichtverkettung von Datensätzen, d. h. Zusammenführung von Datensätzen sicherstellen und die eine Weiterverarbeitung für neue mit dem ursprünglichen Zweck nicht zu vereinbarenden Zwecken verhindern. 6. Der Verantwortliche implementiert technische und organisatorische Maßnahmen, die die Wiederverwendung personenbezogener Daten einschränken, z. B. vertragliche Verpflichtung der eingesetzten Auftragsverarbeiter, Schulung der Beschäftigten 7. Der Verantwortliche legt anhand des Zwecks fest, welche personenbezogenen Daten für die Verarbeitung notwendig sind. Der Verantwortliche überprüft regelmäßig, ob die Verarbeitung für die Zwecke, für die die Daten erhoben wurden, erforderlich ist. Hierfür implementiert er

	entsprechende Prozesse (Zuständigkeiten, Prüfintervalle, Prüfmethodik). 8. Der Verantwortliche implementiert Prozesse, die sicherstellen, dass die PBD, die für eine oder mehrere Zwecke erhoben wurden, nicht in einer mit diesen Zwecken nicht vereinbarenden Weise weiterverarbeitet werden. Jeder neue Zweck muss mit dem ursprünglichen Zweck, für den die Daten erhoben wurden, vereinbar sein und bei Veränderungen der Gestaltung berücksichtigt werden, vgl. die Anforderungen in **DS03.08** 9. Der Verantwortliche wendet technische Maßnahmen unter anderem Hashing und Verschlüsselung an, um die Möglichkeit einzuschränken, dass PBD einem neuen Zweck zugeführt werden. Der Verantwortliche soll organisatorische Maßnahmen anwenden, die die Wiederverwendung personenbezogener Daten einschränken, und z. B. Strategien und vertragliche Verpflichtungen festlegen. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

DSGVO] Art. 5 Abs. 1 lit. b

DS02.05	**Verantwortlicher** Eine **Weiterverarbeitung von personenbezogenen Daten für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke** oder für **statistische Zwecke** gilt gemäß Art. 89 Abs. 1 DSGVO nicht als unvereinbar mit dem ursprünglichen Zweck (Art. 5 Abs. 1 lit. b Hs.2 DSGVO, Fiktion der Zweckidentität). 1. Der Verantwortliche muss eine vorgelagerte Überprüfung durchführen, ob sich die im öffentlichen Interesse liegenden Archivzwecke, wissenschaftlichen oder historischen Forschungszwecke oder statistische Zwecke mit anonymisierten Daten verwirklichen lassen. Das Ergebnis der Überprüfung ist zu dokumentieren. Zuständigkeiten für die Überprüfung sind festzulegen. 2. Der Verantwortliche muss die Zwecke der Weiterverarbeitung dokumentieren und darlegen, dass diese für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gem. Art. 89 Abs. 1 DSGVO erfolgt. 3. Der Verantwortliche muss, sofern sich die Zwecke nicht mir anonymisierten Daten verwirklichen lassen, darlegen, dass gem. Art. 89 Abs. 1 DSGVO technische und organisatorische Maßnahmen (geeignete Garantien) bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird, vgl. **DS02.06**. Zudem sind auch Maßnahmen zu berücksichtigen, die auf eine Gewährleistung anderer Datenschutzgrundsätze abzielen, z. B Zweckbindung, Vertraulichkeit und Integrität von Daten, vgl. **DS02.04**, **DS02.09, DS08.03**. Die technischen und organisatorischen Maßnahmen müssen dokumentiert sein. 4. Der Verantwortliche muss die Sicherstellung der Betroffenenrechte unter Berücksichtigung der Ausnahmetatbestände gem. Art. 89 Abs. 2, 3 und 4 DSGVO gewährleisten. a) Der Verantwortliche muss dokumentieren, welche Regelungen aus dem Unionsrecht oder dem deutschen Recht gem. Art. 89 Abs. 2 und 3 im Hinblick auf Ausnahmen von den Rechten gem. Art. 15, 16, 18, 19, 20 DSGVO herangezogen werden.

	b) Der Ausnahmetatbestand findet gem. Art. 89 Abs. 4 DSGVO nur Anwendung für die Datenverarbeitung zu Archiv-, Forschungs- oder statistischen Zwecken. Sofern darüber hinaus noch andere Zwecke verfolgt werden, gelten für diese Zwecke die Ausnahmen von den Betroffenenrechten nicht. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. 5 Abs. 1 lit. c

DS02.06	**Verantwortlicher** Der Verantwortliche stellt sicher, dass die verarbeiteten PBD dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind (Grundsatz der Datenminimierung). Der Verantwortliche muss zunächst festlegen, ob die Verarbeitung von PBD für ihre entsprechenden Zwecke überhaupt erforderlich ist. Der Verantwortliche erfüllt den Grundsatz der Datenminimierung insbesondere durch folgende Aspekte: • Prüfung, ob die entsprechenden Zwecke durch die Verarbeitung einer kleineren Zahl von personenbezogenen Daten erfüllt werden können, • Prüfung, ob weniger stark untergliederte oder aggregierte personenbezogene Daten herangezogen werden können • Der Verantwortliche verzichtet auf die Verarbeitung PBD, sofern es bei dem entsprechenden Zweck möglich ist. • Der Verantwortliche beschränkt die Menge der erhobenen PBD auf das für den Zweck notwendige Maß. Die personenbezogenen Daten müssen für die betreffende Verarbeitung relevant sein, und der Verantwortliche muss diese Relevanz nachweisen können. Der Verantwortliche muss dokumentieren warum die Daten zur Erreichung der Zwecke erforderlich sind und muss hierbei darlegen, warum die Zwecke oder die Verarbeitung ohne diese PDB nicht erfüllbar wären (Erforderlichkeitsprüfung). Die Darstellung der Erforderlichkeit der Verarbeitung muss den gesamten Lebenszyklus der Datenverarbeitung berücksichtigen. • Der Verantwortliche muss dokumentieren, warum die Zwecke der Verarbeitung nicht in zumutbarer Weise durch andere datensparsamere Mittel in gleichem Maße erreicht werden kann. • Sofern innerhalb des Evaluierungsgegenstandes die Möglichkeit besteht, dass Betroffene Personen ihre PBD gegenüber anderen Nutzern oder Dritten sichtbar machen, z. B. Informationen aus Social Media Profilen, abgegebene Kommentare, stellt der Verantwortliche sicher, dass per Voreinstellungen eine Sichtbarmachung nicht standardmäßig erfolgt und dass die PBD nicht ohne Eingreifen der betroffenen Person einer unbestimmten Anzahl von natürlichen Personen zugänglich gemacht werden. Vielmehr können Betroffene den Umfang der Sichtbarkeit ihrer PBD und der von ihnen geteilten Inhalte selbst festlegen. • Der Verantwortliche stellt technische Möglichkeiten bzgl. der Minimierung der verarbeiteten PBD in Abhängigkeit von der jeweiligen Verarbeitungssituation bereit. So sind beispielsweise Pflichtfelder und optionale Felder für die Abfrage von PBD vom Betroffenen vorhanden. • Der Verantwortliche stellt sicher, dass eine möglichst geringe Zahl von Personen für die Ausführung ihrer Aufgaben Zugang zu

	personenbezogenen Daten haben muss und der Zugang entsprechend beschränkt wird. Hierfür ist ein Rollen- und Berechtigungskonzept implementiert, welches sicherstellt, dass ein Zugriff nach dem Need-to-Know-Prinzip erfolgt, vgl. die Anforderungen in **DS08.03** • Die Mechanismen, z. B. technische Systemkonfigurationen, die zur Gewährleistung der Datenminimierung implementiert sind, sind dokumentiert. • Der Verantwortliche verwendet nach Möglichkeit aggregierte Daten • Der Verantwortliche pseudonymisiert PBD, sobald keine Notwendigkeit mehr für direkt identifizierbare personenbezogene Daten besteht, und speichert Identifizierungsschlüssel separat. Sofern Pseudonymisierungstechniken eingesetzt werden, ist die konkrete Umsetzung beschrieben. • Sofern der Verantwortliche PBD nicht oder nicht mehr für den Zweck benötigt, anonymisiert oder löscht er diese, vgl. die Anforderungen in **DS02.08**. Die Löschung muss auch etwaige Backups berücksichtigen. • Sofern Anonymisierungstechniken eingesetzt werden, ist die konkrete Umsetzung beschrieben. • Der Verantwortliche erstellt bei einer Datenübermittlung nicht mehr Kopien als notwendig. • Sofern der Verantwortliche selbst Software, die innerhalb des Evaluierungsgegenstandes eingesetzt wird, entwickelt, wird der Grundsatz der Datenminimierung bereits bei der Entwicklung dieser Software berücksichtigt. Der Verantwortliche sensibilisiert Mitarbeiter und die Beachtung des Grundsatzes der Datenminimierung im Entwicklungsprozess ist verbindlich in den Anforderungen bzgl. der Entwicklung von Software festgelegt, z. B. Privacy by Design Richtlinie, Coding Richtlinie, Datenschutzrichtlinie. • Wenn im Rahmen des Evaluierungsgegenstandes durch den Verantwortlichen Datenabfragefelder, z. B. in Formularen, genutzt werden, werden über Pflichtfelder nur diejenigen PBD abgefragt, die für die Erreichung der Zwecke erforderlich sind. Freitextfelder werden vermieden. Sofern Freitextfelder genutzt werden, handelt es sich nur in Ausnahmenfällen um Pflichtfelder, weil die Angabe weiterer Informationen zwingend zur Zweckerreichung erforderlich ist. Der Verantwortliche muss dokumentieren, warum die Nutzung von verpflichtenden Freitextfeldern Daten zur Erreichung der Zwecke erforderlich ist, und muss hierbei darlegen, warum die Zwecke oder die Verarbeitung ohne diese ergänzenden Informationen nicht erfüllbar wären (Erforderlichkeitsprüfung). Es ist dem Betroffenen transparent zu erläutern warum das Freitextfeld existiert und es ist darauf hinzuweisen, welche Informationen erwünscht sind und welche nicht, z. B. das der Betroffene keine personenbezogenen Daten eingeben soll. • Sofern Waren oder Dienstleistungen im Onlinehandel durch den Verantwortlichen angeboten werden, muss den Betroffenen ein Gastzugang (Online-Geschäft ohne Anlegung eines fortlaufenden Nutzerkontos) bzw. eine Nutzung des IVS ohne Registrierung angeboten werden. Sofern kein Gastzugang angeboten wird, sind die Gründe hierfür zu dokumentieren. • Der Zugriff auf externe Ressourcen durch das IVS (wie z. B. Kamera, Kalender, Adressbuch, externe Geräte) muss für die Zweckerreichung erforderlich sein. Es muss durch technische Maßnahmen sichergestellt sein, dass der Zugriff nur in dem für die Zweckerreichung notwendigen Maß erfolgt, d. h. nur auf für die Verarbeitungszwecke erforderliche Datensätze, innerhalb der externen Ressource zugegriffen wird. Der Betroffene muss über den Zugriff auf externe Ressourcen informiert werden und diesem

	Zugriff zustimmen. Es müssen Prozesse implementiert sein, die eine regelmäßige Überprüfung des Erfordernisses des Zugriffs auf externe Ressourcen und deren datensparsame Umsetzung sicherstellen (Festlegung von Zuständigkeiten, Häufigkeit der Überprüfung, Art der Überprüfung). • Der Verantwortliche verarbeitet und speichert Daten nur im datensparsamsten Format, mit dem sich die Verarbeitungszwecke erfüllen lassen (z.B. Erfassung Altersgruppe anstelle des genauen Geburtsdatums, Erfassung Berufsfeld anstatt konkrete Berufsbezeichnung) • Es sind technische und organisatorische Maßnahmen vorhanden, die eine Nichtverkettung von Datensätzen, d. h. Zusammenführung von Datensätzen sicherstellen. Es sind Prozesse (Festlegung von Zuständigkeiten, Art und Weise der Überprüfung, Häufigkeit) zu implementieren, die eine regelmäßige Prüfung (mindestens jährlich oder anlassbezogen), ob die verarbeiteten PBD noch angemessen, relevant und notwendig sind, oder ob die Daten gelöscht oder anonymisiert werden müssen. Es sind Zuständigkeiten für die Überprüfung festzulegen. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. 5 Abs. 1 lit. d

DS02.07	**Verantwortlicher** Der Verantwortliche muss PBD sachlich richtig und immer auf dem neuesten Stand halten (**Grundsatz der Richtigkeit**). Hierbei schafft der Verantwortliche Kontroll- und Eingriffsmöglichkeiten zur Feststellung der Richtigkeit PBD und unterstützt die Korrektur sowie Löschung unrichtiger Daten. Der Verantwortliche erfüllt den Grundsatz der Richtigkeit, indem er nachfolgende Maßnahmen ergreift. • Der Verantwortliche verwendet verlässliche Quellen, was die Richtigkeit der verarbeiteten PBD betrifft. • Der Verantwortliche muss unter Berücksichtigung der Art der PBD und deren typischer Änderungshäufigkeit begründet dokumentieren, in welchen zeitlichen Abständen und auf welche Weise, der Betroffene aufgefordert wird, die Richtigkeit der personenbezogenen Daten zu überprüfen. • Der Verantwortliche informiert Betroffene nach den Art. 12 bis 15 DSGVO über die verarbeiteten PBD und gewährt den Betroffenen den tatsächlichen Zugang zu diesen Daten, um die Richtigkeit zu kontrollieren und bei Bedarf Berichtigungen vorzunehmen. • Der Verantwortliche verfügt über Prozesse bzgl. Berichtigungs-, Lösch- und Einschränkungsanträgen, vgl. die Anforderungen in **DS06.11** • Der Verantwortliche überprüft regelmäßig die Richtigkeit sowie Aktualität der Datenbestände. Hierfür sind Zuständigkeiten, Art und Weise der Überprüfung sowie Fristen der Überprüfung festzulegen. • Der Verantwortliche mindert die Auswirkungen eines kumulierten Fehlers in der Verarbeitungskette. Hierzu soll er die Verarbeitungskette in allen Systemen nachverfolgen können. • Die Struktur der Daten bzw. der Datenbank muss so ausgestaltet sein, dass einzelne Datenfelder, Datensätze oder Gruppen von Daten berichtigt werden können, z. B. auch durch die betroffene Person selbst. • Der Verantwortliche aktualisiert PBD, falls es für den Zweck erforderlich ist.

	• Die technischen Systeme müssen so ausgestaltet sein, dass Berichtigungs- oder Löschvorgänge technisch realisiert werden können, und dass die Daten in Zweifelsfällen für die weitere Verarbeitung eingeschränkt werden können. • Die technischen Systeme müssen so ausgestaltet sein, dass Berichtigungen oder Löschungen durchgeführt werden können, ohne die Integrität des unverändert verbleibenden Datenbestandes zu beeinträchtigen. • Der Verantwortliche dokumentiert wer für die Prüfung, Anordnung und Durchführungen von Berichtigungen bzw. Löschungen verantwortlich ist • Es muss durch ein Berechtigungs- und Rollenkonzept sichergestellt werden, dass unbefugte Berichtigungen oder Löschungen verhindert oder nachträglich erkannt werden können. • Der Verantwortliche stellt sicher, dass berichtigte bzw. gelöschte Datensätze bei der Wiederherstellung von Backups berücksichtigt werden, sodass wirksam ausgeschlossen ist, dass unrichtige Daten wieder für die Verarbeitung herangezogen werden. • Der Verantwortliche führt eine Dokumentation aller angefertigten Kopien und deren Erstellungsdatum. • Der Verantwortliche dokumentiert alle Berichtigungs- bzw. Löschvorgänge. • Der Verantwortliche stellt eine konsistente Weiterverarbeitung der berichtigten Daten sicher • Der Verantwortliche verwendet technische und organisatorische Gestaltungsmerkmale, um die Fehlerhaftigkeit von Datensätzen zu reduzieren, z. B. sollten knapp formulierte vorgegebene Antwortmöglichkeiten anstelle von Freitextfeldern verwendet werden.

[DSGVO] Art. 5 Abs. 1 lit. e, Art. 11, [DSK_17067] zu Art 5 Abs. 1 lit. e

DS02.08	**Verantwortlicher** Der Verantwortliche muss sicherstellen, dass die PBD nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (**Grundsatz der Speicherbegrenzung**). Eine **Identifizierung des Betroffenen** bei der Speicherung seiner personenbezogenen Daten ist nur so lange möglich, wie es für die Verarbeitungszwecke erforderlich ist. Die personenbezogenen Daten müssen in einer Form gespeichert werden, welche die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Anschließend sind die Daten zu löschen (im physikalischen Sinn) oder irreversibel zu anonymisieren. Sofern eine Anonymisierung erfolgt, muss diese vollständig unumkehrbar sein. Der Verantwortliche verfügt über ein Löschkonzept, z. B. nach DIN 66398-2016, welches insbesondere Folgendes regelt: • Anwendungsbereich des Löschkonzeptes (z. B. welche IT-Systeme und Datenbestände) • Festlegung von Löschfristen • Festlegung und konkrete Beschreibung von Löschmechanismen (Dokumentation der einzelnen Vorgänge bzw. Umsetzungsvorgaben) ○ Bei der Festlegung der Mindestanforderungen an Verfahren

	zur Löschung sind die Vorgaben des IT-Grundschutzkompendiums CON.6 Löschen und Vernichten umzusetzen • Festlegung von Zuständigkeiten und Meldewege bzgl. der Vornahme von Löschungen • Der Verantwortliche muss rechtfertigen können, warum die Dauer der Speicherung für den Zweck und in Bezug auf die betreffenden personenbezogenen Daten erforderlich ist, und er muss die Begründung und die Rechtsgrundlage für die Speicherfrist angeben können • Sofern ein Auftragsverarbeiter durch den Verantwortlichen eingesetzt wird: Darlegung inwieweit Löschpflichten durch den Auftragsverarbeiter zu erfüllen sind • Zuständigkeiten bzgl. der Überwachung der Löschprozesse • Überprüfung der tatsächlichen Umsetzung bzw. Wirksamkeit der Löschung • Festlegung wie Durchführung von Löschungsmaßnahmen dokumentiert werden • Berücksichtigung der Datenlöschung in Backups und Archiven • Regelmäßige Evaluierung (mindestens jährlich), ob die gewählten Löschmechanismen noch dem Stand der Technik entsprechen • Der Verantwortliche soll nach Möglichkeit automatisierte Löschverfahren implementieren • Der Verantwortliche legt fest, welche personenbezogenen Daten und welche Speicherdauer für Backups und Logdateien notwendig sind Es muss sichergestellt sein, dass Löschungen durchgeführt werden können, ohne die Integrität des verbleibenden Datenbestandes zu beinträchtigen. Als Maßstab für die Beurteilung, ob eine wirksame faktische Anonymisierung vorliegt, ist der Stellungnahme 5/2014 der Artikel 29-Gruppe zu Anonymisierungstechniken, WP 216, zu folgen. Hiernach darf es nach einer Anonymisierung personenbezogener Daten, keiner Partei möglich sein, • eine Person aus einem Datenbestand herauszugreifen, • eine Person betreffende Datensätze miteinander zu verknüpfen, bspw. eine Verbindung zwischen zwei Datensätzen eines Datenbestands (oder zwischen zwei unabhängigen Datenbeständen) herzustellen, oder • durch Inferenz, Informationen aus einem solchen Datenbestand über eine Person abzuleiten. Aufgrund des technologischen Fortschritts besteht das Risiko, dass anonymisierte Daten de-anonymisiert werden, sodass die Anonymisierung fortwährend auf ihre Validität überprüft werden muss. Entsprechende Prozesse müssen implementiert und dokumentiert sein. Die Prozesse müssen insbesondere Festlegungen treffen zu: Zuständigkeiten für die Überprüfung der Validität der Anonymisierungsverfahren, Art und Weise der Überprüfung (z. B. Vornahme von Re-Identifizierungsangriffen), Umfang der Überprüfung (stichprobenartig oder vollumfänglich) Häufigkeit der Überprüfung (mindestens jährlich oder anlassbezogen), Dokumentation der Überprüfung, Festlegung von Verfahren, wenn das Vorliegen einer De-Anonymisierung festgestellt wird.

	Es bestehen klare Regelungen zwischen Auftragsverarbeiter und Verantwortlichem, vgl. Art 28 Abs. 3 lit. g DSGVO, **DS07.09**, was mit den PBD nach Beendigung des Auftrags geschehen soll (Löschung, Rückgabe). Es ist ein Prozess bzgl. der Aushändigung der PBD an den Verantwortlichen bzw. Löschung der PBD nach Beendigung des Vertrags vorhanden (insbesondere Festlegung von Zuständigkeiten, Art und Weise der Aushändigung der PDB oder Löschung). Hierbei werden auch sämtliche PBD bei etwaigen weiteren Auftragsverarbeitern berücksichtigt. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. 5 Abs. 1 lit. f

DS02.09	**Verantwortlicher** Die PBD werden in einer Weise verarbeitet, die eine angemessene Sicherheit der PBD gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch Einsatz geeigneter technischer und organisatorischer Maßnahmen, vgl. die Anforderungen in **DS08**.

[DSGVO] Art. 5 Abs. 2

DS02.10	**Verantwortlicher** Der Verantwortliche muss die Einhaltung der vorgenannten Kriterien im Rahmen seiner Rechenschaftspflicht nachweisen können. Die Maßnahmen zur Einhaltung der Vorgaben der Kriterien **DS02.01** bis **DS02.09** sind dokumentiert Die Verantwortlichkeitsstruktur innerhalb des etablierten Datenschutzmanagementsystems respektive der einzelnen Prozessbeschreibungen ist dokumentiert, vgl. die einzelnen Anforderungen in **DS09**.

DS03 Rechtmäßigkeit der Verarbeitung

[DSGVO] Art. 6 Abs. 1

DS03.01	**Verantwortlicher** Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist: 1. die Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben, 2. die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen, 3. die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt, 4. die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen, 5. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, 6. die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Der Verantwortliche hat Prozesse implementiert, die eine vorgelagerte Prüfung des Vorhandenseins einer Rechtsgrundlage sicherstellen. Diese Prozesse treffen insbesondere Festlegungen zu: • Festlegung von Zuständigkeiten für die Durchführung der Überprüfung inklusive Einbeziehung bestimmter Fachbereiche • Festlegung wie die Rechtmäßigkeitsüberprüfung erfolgt: Aus der Rechtmäßigkeitsprüfung soll erkennbar sein, dass der Verantwortliche alle in Art. 6 Abs. 1 lit. a – f DSGVO genannten Bedingungen auf Einschlägigkeit überprüft und zu einem Ergebnis gelangt. Aus dem Prozess soll die Regelmäßigkeit zur Überprüfung der Rechtmäßigkeit hervorgehen und folgende inhaltliche Aspekte berücksichtigen: ○ das anwendbare nationale Datenschutzrecht ○ die Erforderlichkeit der Datenverarbeitung im Hinblick auf den Umstand, ob die Daten zur Erreichung des Zweckes notwendig sind und der Zweck der Verarbeitung nicht in zumutbarer Weise auch durch andere Mittel erreicht werden kann ○ eine ggf. bestehende gemeinsame Verantwortlichkeit nach Art. 26 DSGVO ○ involvierte Auftragsverarbeiter nach Art. 28 DSGVO ○ involvierte Datenempfänger. • Dokumentation der Rechtsgrundlage Es müssen Prozesse implementiert sein, die sicherstellen, dass eine

	Datenverarbeitung erst erfolgt, wenn der jeweilige Auftragsverarbeitungsvertrag wirksam abgeschlossen wurde. Hierfür ist mindestens geregelt: • Dokumentation wie Auftragsvergabe erfolgt (Beschaffungswege/ -prozess) • Richtlinien für die Beauftragung von Dienstleistern (z. B. Einkaufspolicy) • Festlegung wann Datenschutzbeauftragte einzubeziehen ist • Vorhandensein von Muster-Auftragsverarbeitungsverträgen • Festlegung von Zuständigkeiten bzgl. der Überprüfung, ob ein Auftragsverarbeitungsvertrag geschlossen werden muss • Festlegung von Zuständigkeiten bzgl. der Prüfung von Auftragsverarbeitungsverträgen • Festlegung von Zuständigkeiten für den Abschluss des Auftragsverarbeitungsvertrages (Unterschriftenregelung) • Dokumentation des Abschlusses des Auftragsverarbeitungsvertrages • Dokumentation des Auftragsverarbeitungsvertrages gemäß etablierten Dokumentenmanagement Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

Die nachfolgenden Kriterien beschreiben die einzelnen Grundlagen der rechtmäßigen Verarbeitung und sind je nach Grundlage der Verarbeitung anzuwenden bzw. obsolet. Sie verweisen ggf. auf weitere relevante Kriterien dieses Dokumentes.

[DSGVO] Art. 6 Abs. 1 a

DS03.02	**Verantwortlicher** Sofern die Verarbeitung auf Basis einer Einwilligung erfolgt (Art. 6 Abs. 1 lit. a DSGVO) müssen die Rechtmäßigkeitsvoraussetzungen gemäß **DS04** erfüllt werden. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. 6 Abs. 1 lit. b i. V. m. Art. 5 Abs. 1 lit. c

DS03.03	**Verantwortlicher** Sofern die Verarbeitung für die **Erfüllung eines Vertrages** oder **die Durchführung einer vorvertraglichen Maßnahme erfolgt** (Art. 6 Abs. 1 lit. b DSGVO) müssen nachfolgende Rechtmäßigkeitsvoraussetzungen vorliegen. 1. Der Vertrag mit der betroffenen Person, auf den sich die Verarbeitung bezieht, muss a) tatsächlich wirksam bestehen oder b) es muss sich um ein vorvertragliches Verhältnis auf Anfrage der betroffenen Person handeln. 2. Die Verarbeitungszwecke im Rahmen einer Vertragsbeziehung sind klar festgelegt und werden der betroffenen Person mitgeteilt. 3. Die Datenverarbeitung muss a) für die Erfüllung eines Vertrages mit einer betroffenen Person objektiv erforderlich sein oder b) objektiv zur Durchführung vorvertraglicher Maßnahmen, die auf

	Anfrage der betroffenen Person erfolgen, erforderlich sein. Hierbei werden nur diejenigen personenbezogenen Daten verarbeitet, die für die Erfüllung eines Vertrages oder für die Durchführung vorvertraglicher Maßnahmen zwingend erforderlich sind (vgl. **DS02.06**, Art. 5 Abs. 1 lit. c DSGVO). Ferner sind alle Verarbeitungsvorgänge für die Erfüllung eines Vertrages oder für die Durchführung vorvertraglicher Maßnahmen erforderlich. Es ist nachzuweisen, inwieweit der Hauptgegenstand des Vertrages mit der betroffenen Person tatsächlich nicht erfüllt werden kann, wenn die spezifische Verarbeitung der fraglichen personenbezogenen Daten nicht erfolgt. 4. Die Strukturen und Abläufe, die zu einem Vertragsschluss oder einem vorvertraglichen Verhältnis führen, sind dokumentiert. 5. Sofern Art. 6 Abs. 1 lit. b DSGVO die Grundlage für einige oder alle Verarbeitungsvorgänge bildet, sind im Hinblick auf etwaige Vertragskündigungen Prozesse bzgl. der sich daraus ergebenden Folgen für die Datenverarbeitung vorhanden. Hierbei sind Regelungen in Bezug auf die Einstellung der Verarbeitung, Löschung der Daten (vgl. Art. 17 Abs. 1 lit. a DSGVO) sowie auf etwaige bestehende Ausnahmen von der Löschpflicht, z. B. Erfüllung einer rechtlichen Verpflichtung gem. Art. 17 Abs. 3 lit. e DSGVO, zu treffen. Die Anforderungen gem. **DS02.08** sind entsprechend zu berücksichtigen. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. 6 Abs. 1 lit. c i. V. m. Art. 5 Abs. 1 lit. c, Art. 6 Abs. 2, 3

DS03.04	**<u>Verantwortlicher</u>** Sofern die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erfolgt, der der Verantwortliche unterliegt (Art. 6 Abs. 1 lit. c DSGVO) müssen nachfolgende Rechtmäßigkeitsvoraussetzungen vorliegen. 1. Vorliegen einer rechtlichen Verpflichtung des Verantwortlichen und die Verpflichtung muss sich unmittelbar auf die Datenverarbeitung beziehen. 2. Die Verpflichtung weist einen Bezug zu der betroffenen Person auf. 3. Die rechtliche Verpflichtung muss sich aus dem Unionsrecht oder dem deutschen Recht ergeben, dem der Verantwortliche unterworfen ist. Die rechtliche Verpflichtung muss den Anforderungen des Art. 6 Abs. 2 und 3 DSGVO bzw. eventuell bestehender Sonderregelungen (z. B. rechtliche Verpflichtungen in Kollektivvereinbarungen) genügen. 4. Es muss dokumentiert sein, welche Rechtsgrundlage aus dem Unionsrecht oder dem deutschen Recht i. V. m. Art. 6 Abs. 1 lit. c DSGVO herangezogen wird. 5. Die Verarbeitung muss zur Erfüllung der rechtlichen Verpflichtung erforderlich sein (vgl. **DS02.06**, Art. 5 Abs. 1 lit. c DSGVO). Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. 6 Abs. 1 lit. d i. V. m. Art. 5 Abs. 1 lit. c

DS03.05	**<u>Verantwortlicher</u>** Sofern die Verarbeitung erfolgt, um lebenswichtige Interessen der

	betroffenen Person oder einer anderen natürlichen Person zu schützen (Art. 6 Abs. 1 lit. d DSGVO), müssen nachfolgende Rechtmäßigkeitsvoraussetzungen vorliegen. 1. Vorliegen lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person. 2. Es muss dokumentiert sein wessen und welche lebenswichtigen Interessen betroffen sind. 3. Die Verarbeitung muss für den Schutz der lebenswichtigen Interessen erforderlich sein (vgl. (vgl. **DS02.06**, Art. 5 Abs. 1 lit. c DSGVO). 4. Eine andere Rechtsgrundlage ist nicht einschlägig. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. 6 Abs. 1 lit. e i. V. m. Art. 5 Abs. 1 lit. c, Art. 6 Abs. 2, 3

DS03.06	**Verantwortlicher** Sofern die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (Art. 6 Abs. 1 lit. e DSGVO), müssen nachfolgende Rechtmäßigkeitsvoraussetzungen vorliegen. 1. Dem Verantwortlichen wurde a) die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe übertragen oder b) in Ausübung öffentlicher Gewalt erfolgende Aufgaben übertragen. Die Bedingungen der Aufgabenerfüllung, ihr Umfang und die Umstände, die zu einem Wegfall der Rechtsgrundlage führen, müssen dokumentiert sein 2. Die Rechtsgrundlage für die Datenverarbeitung muss sich aus dem Unionsrecht oder dem deutschen Recht ergeben, dem der Verantwortliche unterworfen ist. Die Rechtsgrundlage muss den Anforderungen des Art. 6 Abs. 2 und 3 DSGVO und eventuell bestehenden Sonderregelungen (in Abhängigkeit des Anwendungskontextes) genügen. 3. Es muss dokumentiert sein, welche Rechtsgrundlage aus dem Unionsrecht oder dem deutschen Recht i. V. m. Art. 6 Abs. 1 lit. e DSGVO herangezogen wird. 4. Die Verarbeitung muss zur Wahrnehmung der Aufgabe erforderlich sein (vgl. **DS02.06**, Art. 5 Abs. 1 lit. c DSGVO). Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. 6 Abs. 1 lit. f

DS03.07	**Verantwortlicher** Sofern die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erfolgt (Art. 6 Abs. 1 lit. f DSGVO), müssen nachfolgende Rechtmäßigkeitsvoraussetzungen vorliegen. 1. Die Verarbeitung muss im berechtigten Interesse des a) Verantwortlichen oder b) eines Dritten liegen. 2. Es handelt sich nicht um von einer Behörde in Erfüllung ihrer Aufgaben vorgenommene Verarbeitungen. 3. Die Datenverarbeitung muss für den angestrebten Zweck erforderlich sein. 4. Die Verarbeitung ist zur Wahrung der berechtigten Interessen des

Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

5. Die vernünftigen Erwartungen der Betroffenen sind zu berücksichtigen
Im Hinblick auf die vernünftigen Erwartungen sind dabei zu berücksichtigen:

a) ob eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht (vgl. ErwG 47 Satz 1 und 2 DSGVO). Hierbei sind insbesondere Elemente bei der Bewertung der Beziehung zur betroffenen Person zu berücksichtigen:

- Bestehen einer Beziehung zur betroffenen Person (z. B. ist zwischen Kunden und Nicht-Kunden zu unterschieden), einschließlich des Datums der Beendigung der Beziehung, falls eine solche bestand
- Nähe der Beziehung (z. B. Fälle, in denen ein für die Verarbeitung Verantwortlicher Teil einer Unternehmensgruppe mit einer einzigen Marke ist, im Vergleich zu einer Unternehmensgruppe, die nur wirtschaftliche Verbindungen hat, die dem durchschnittlichen Kunden unbekannt sind, da im letzteren Fall die betroffene Person weniger wahrscheinlich erwarten kann, dass Daten zwischen den Unternehmen der Gruppe ausgetauscht werden)
- Ort und Kontext der Datenerhebung (z. B. erwarten die Betroffenen vielleicht eine Videoüberwachung in einer Bank, nicht aber in Sanitär- oder Saunaeinrichtungen)
- Art und Merkmale der Dienstleistung (z. B. haben ein Stammkunde und ein bloßer Interessent, der nur einen Newsletter abonniert hat, unterschiedliche angemessene Erwartungen)
- Anwendbare rechtliche Anforderungen im jeweiligen Kontext (z. B. Vertraulichkeitsanforderungen, die für die betreffende Beziehung gelten

b) ob die Betroffenen zum Zeitpunkt der Erhebung der PBD und der Umstände der Verarbeitung, vernünftigerweise absehen können, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird (ErwG 47 Satz 3 DSGVO), d.h., dass die Verarbeitung nicht überraschend oder unwahrscheinlich ist.

- Die bloße Erfüllung der in den Art. 12, 13 und 14 DSGVO festgelegten Informationspflichten sind nicht ausreichend, um davon auszugehen, dass die betroffenen Personen vernünftigerweise eine bestimmte Verarbeitung erwarten können.
- Bei der Abwägung ist die „durchschnittliche“ betroffene Person zu betrachten, es sei denn die Verarbeitung wird wahrscheinlich verschiedene Gruppen von betroffenen Personen mit unterschiedlichen Merkmalen betreffen. Hierbei sind nachfolgende Merkmale zu berücksichtigen:
  - Alter der betroffenen Person (die berechtigten Erwartungen von Minderjährigen können anders sein als die von Erwachsenen)
  - Ausmaß, in dem die betroffene Person eine Person des

	öffentlichen Lebens ist ○ Die (berufliche) Stellung, die die betroffene Person innehat, und der Grad des Verständnisses und der Kenntnis der geplanten Verarbeitung, die sie in einem bestimmten Kontext haben dürfte (z. B. würde das Personal, das an einem Bewerbungsgespräch beteiligt ist, häufig erwarten, dass einige seiner personenbezogenen Daten mit den Bewerbern ausgetauscht werden). 6. Die Interessen müssen durch Berücksichtigung zusätzlicher Schutzmaßnahmen ausgeglichen werden. 7. Die Interessenabwägung muss transparent und adressatengerecht dokumentiert werden. 8. Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, Widerspruch einzulegen. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. 6 Abs. 4

DS03.08	**Verantwortlicher** Sofern der Verantwortliche intendiert, PBD zu einem anderen Zweck als zu demjenigen, zu dem die PBD erhoben wurden, zu verarbeiten, muss er alle Zweckänderungen mit Begründung dokumentieren. Hierbei muss ersichtlich sein, was der ursprüngliche Zweck war und welcher Zweck nun mit der Verarbeitung verfolgt wird. Der Verantwortliche verfügt über dokumentierte Prozesse im Hinblick auf die Überprüfung der Rechtmäßigkeit einer Zweckänderung und im Hinblick auf weitere Maßnahmen (z. B. Einholung weiterer Einwilligungen). In diesem Zusammenhang sind Zuständigkeiten für die Überprüfung der Rechtmäßigkeit einer Zweckänderung, die Art und Weise der Überprüfung (Dokumentation des Vorgehens der Überprüfung unter Berücksichtigung nachfolgend aufgeführter Prüfschritte), Sensibilisierung der Beschäftigten bzgl. des Umgangs mit etwaigen Zweckänderungen, Einbindung des Datenschutzbeauftragten, sowie die Dokumentation der Durchführung der Überprüfung festgelegt. Sofern der Verantwortliche eine Zweckänderung vornehmen möchte, muss er prüfen, ob die Verarbeitung zu einem anderen Zweck **rechtmäßig** erfolgt. Hierzu verfügt er über einen dokumentierten Prüfprozess (Anforderungen an den Prozess siehe vorstehend), bei dem er sicherstellt, dass nachfolgende Prüfschritte durchgeführt werden: a) Überprüfung, ob eine entsprechende Einwilligung des Betroffenen vorliegt, vgl. Anforderungen in **DS04** b) Überprüfung, ob eine Rechtsvorschrift der Union bzw. einer deutschen Rechtsvorschrift anwendbar ist • Die Zweckänderung kann ihre Rechtsgrundlage in einer Rechtsvorschrift der Union bzw. Deutschlands haben, wenn diese eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz der Gemeinschaftsgüter des Art. 23 Abs. 1 DSGVO darstellt. Sofern es sich um eine deutsche Regelung handelt, muss Deutschland auch für die Erstverarbeitung eine Regelungsbefugnis zukommen (also insbesondere auf Grundlage der Art. 6 Abs. 1 lit. c und lit e i. V. m. Abs. 2 und 3 DSGVO; vgl. **DS03.05**

	und **DS03.06**. Sofern die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, nicht auf einer Einwilligung oder einer Rechtsvorschrift der Union bzw. einer deutschen Rechtsvorschrift beruht, führt der Verantwortliche eine **dokumentierte Abwägung** nach Art. 6 Abs. 4 DSGVO durch **(Kompatibilitätstest)** und berücksichtigt dabei folgende Prüfschritte: **1. Zweckbindung überprüfen** Verbindung zwischen den Zwecken für die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung • Erfassung des ursprünglichen Zwecks der Datenerhebung • Feststellung, ob der neue Verarbeitungszweck mit dem ursprünglichen Zweck vereinbar ist Eine enge Zweckbindung kann insbesondere dann angenommen werden, wenn der ursprüngliche Zweck den neuen Zweck der Weiterverarbeitung als logischen nächsten Schritt bereits impliziert hat. **2. Zusammenhang der Datenverarbeitung überprüfen** Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses bzw. Beziehung (z. B. Käufer und Verkäufer, Arbeitgeber und Beschäftigter) zwischen den betroffenen Personen und dem Verantwortlichen • Prüfung, ob innerhalb der Erstinformation umfassend auf mögliche Szenarien der Weiterverwendung hingewiesen worden ist. • Prüfung, ob die Zweckänderung aus der Perspektive der betroffenen Person als erwartbar angesehen werden kann. Dabei sind die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen in Bezug auf die weitere Verwendung dieser Daten, zu berücksichtigen (vgl. ErwG 50 Satz 6 DSGVO). Dabei ist zu berücksichtigen: ○ Befindet sich die betroffene Person in einem näheren Verhältnis zum Verantwortlichen (z. B. Kundenbeziehung, Arbeitsverhältnis) einschließlich des Datums der Beendigung der Beziehung, falls eine solche bestand ○ Nähe der Beziehung (z. B. Fälle, in denen ein für die Verarbeitung Verantwortlicher Teil einer Unternehmensgruppe mit einer einzigen Marke ist, im Vergleich zu einer Unternehmensgruppe, die nur wirtschaftliche Verbindungen hat, die dem durchschnittlichen Kunden unbekannt sind, da im letzteren Fall die betroffene Person weniger wahrscheinlich erwarten kann, dass Daten zwischen den Unternehmen der Gruppe ausgetauscht werden) ○ Verbindung zwischen dem ursprünglichen Verarbeitungszweck zum Zeitpunkt der Datenerhebung und den Zwecken der geplanten Weiterverarbeitung (ist die Verarbeitung im ursprünglichen Zweck schon implizit enthalten und kann sie als logischer nächster Schritt gesehen werden) ○ entspricht die Weiterverarbeitung der in diesem Zusammenhang allgemein üblichen Praxis in dem Umfeld, sodass die Verarbeitung nicht überraschend und unvorhersehbar ist (Kontext der Weiterverarbeitung)

	○ beruht die weitere Verarbeitung auf einer gesetzlichen Bestimmung ○ Transparenz der Weiterverarbeitung (einschließlich Art und Inhalt der Informationen, die der betroffenen Person ursprünglich oder später bereitgestellt wurden Die bloße Erfüllung der in den Art. 12, 13 und 14 DSGVO festgelegten Informationspflichten sind allerdings nicht ausreichend, um davon auszugehen, dass die betroffenen Personen vernünftigerweise eine bestimmte Verarbeitung erwarten können, können die Erwartung des Betroffenen aber zu einem gewissen Maß beeinflussen. ○ Anwendbare rechtliche Anforderungen im jeweiligen Kontext (z. B. Vertraulichkeitsanforderungen, die für die betreffende Beziehung gelten) **3. Berücksichtigung der Art PBD** Sofern besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO verarbeitet werden sollen, besteht ein erhöhtes Rechtfertigungsbedürfnis im Rahmen der Kompatibilitätsprüfung nach Art. 6 Abs. 4 DSGVO (ggf. i. V. m. Art. 5 Abs. 1 lit. b DSGVO). Auch sonstige sensible Daten, wie z. B. personenbezogene Daten von Kindern, Älteren, besonders im Rahmen des Kompatibilitätstests sind zu berücksichtigen. **4. Folgen für die betroffene Person** Eine Zweckänderung kann das Risiko für die Rechte und Freiheiten der betroffenen Personen erhöhen. • Erfordernis zur Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO überprüfen • Gegenüberstellung positiver sowie negativer Folgen für die betroffene Person (z. B. wirtschaftliche sowie gesellschaftliche Vor- und Nachteile) • Berücksichtigung, ob die Weiterverarbeitung durch den Verantwortlichen, der die Daten bereits erhoben hat oder ein Dritter durch die Weiterverarbeitung Kenntnis von den personenbezogenen Daten erhält. Das Bestehen eines erhöhten Risikos bei Übermittlung der personenbezogenen Daten an Dritte, die Daten zu einem anderen Zweck verarbeiten könnte z. B. durch unkontrollierbare Parallelspeicherungen für die Schutzmaßnahmen wie Zugriffsbeschränkungen und Sperrungen verloren gehen • Überprüfung, ob die Systeme und Prozesse nach der Zweckänderung weiterhin die Ausübung der Betroffenenrechte gem. Kapitel 3 DSGVO gewährleisten • Aktualisierung der Informationen an den Betroffenen i.S.d. Art. 13 bzw. 14 DSGVO (z. B. Datenschutzerklärung) • Überprüfung der Auswirkungen auf bestehende Auftragsverarbeitungsverhältnisse und ggf. Anpassung der einschlägigen Auftragsverarbeitungsverträge Je schwerer es für die betroffene Person ist, die Weiterverarbeitung im Einzelnen nachzuvollziehen und die Folgen abzuschätzen, desto eher muss eine Zweckkompatibilität abgelehnt werden. **5. Vorhandensein geeigneter Garantien**

	Durch die Implementierung geeigneter technischer und organisatorischer Maßnahmen kann eine Kompensation für die mit einer Zweckänderung einhergehenden Risiken erfolgen. Folgende beispielhafte Maßnahmen können als geeignete Garantien herangezogen werden: • Überprüfung, ob durch Verschlüsselung oder Pseudonymisierung der gleiche Zweck mit einer Weiterverarbeitung erreicht werden kann • Anonymisierung personenbezogener Daten • Aggregation personenbezogener Daten • Implementierung von Privacy Enhancing Technologies • Datenschutzfreundliche Voreinstellungen

DS04 Einwilligung

[DSGVO] Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a, Art. 7

DS04.01	**A) Verantwortlicher** Sofern der Verantwortliche eine Verarbeitung von personenbezogenen Daten auf der Grundlage einer Einwilligung durchführt, muss die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten für einen oder mehrere Zwecke eingewilligt haben. Die Einwilligung wird für einen bestimmten Fall abgegeben: • die Einwilligung der betroffenen Person wird für „einen oder mehrere bestimmte“ Zwecke erteilt und die betroffene Person hat in Bezug auf jeden dieser Zwecke eine Wahlmöglichkeit • Die Zwecke werden durch den Verantwortlichen vorab bestimmt, vgl. DS02.04 • Die Einwilligung bezieht sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommenen Verarbeitungsvorgänge • Wenn die Verarbeitung mehreren Zwecken dient, kann der Betroffene zu verschiedenen Verarbeitungsvorgängen von PBD gesondert eine Einwilligung erteilen • Der Verantwortliche erteilt mit jedem Ersuchen um gesonderte Einwilligung spezifische Informationen über die Daten, die für jeden Zweck verarbeitet werden, sodass den betroffenen Personen die Auswirkungen der unterschiedlichen Wahlmöglichkeiten verdeutlicht werden Nachfolgende Wirksamkeitsvoraussetzungen der Einwilligung werden durch den Verantwortlichen erfüllt. Die spezifische Überprüfung erfolgt in den nachfolgenden Zertifizierungskriterien. 1. Freiwillig abgegebene Willenserklärung, vgl. die Anforderungen in DS04.02 2. für den bestimmten Fall abgegebene Willenserklärung, DS04.03 3. in informierter Weise abgegebene Willenserklärung, DS04.03 4. unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, DS04.04 **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen seiner Weisungsgebundenheit bzgl. der Einholung einer Einwilligung, sofern der Verantwortliche den Auftragsverarbeiter ausdrücklich die Weisung erteilt hat (vgl. die Anforderungen in DS07.04, DS07.10), dass dieser für die Einholung der Einwilligung von den Betroffenen im Namen des Verantwortlichen zuständig ist. Sofern eine entsprechende Weisung nicht vorliegt, ist dieses Kriterium nicht einschlägig. Die inhaltliche Gestaltung der Einwilligungsformulierung obliegt dem Verantwortlichen und ist durch den Auftragsverarbeiter umzusetzen. Sofern der Auftragsverarbeiter der Auffassung ist, dass die Weisung des Verantwortlichen gegen die DSGVO-Anforderungen oder gegen andere Datenschutzbestimmungen verstößt, informiert der Auftragsverarbeiter unverzüglich den Verantwortlichen. Die Zuständigkeiten und

	Kommunikationswege hierfür sind zu dokumentieren.

[DSGVO] Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a, Art. 7 Abs. 4

DS04.02	**Verantwortlicher** Die **Einwilligung wird** durch den Betroffenen **freiwillig erteilt.** Im Hinblick auf die Beurteilung der Freiwilligkeit der Einwilligung ist insbesondere zu berücksichtigen: • Der Betroffene hat eine echte und freie Wahl und ist in der Lage, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile (d. h., dass nicht das Risiko einer Täuschung, Einschüchterung, Nötigung, sonstige beträchtliche nachteilige Folgen (z. B. Zusatzkosten) besteht) zu erleiden. Dies muss der Verantwortliche nachweisen. • Eine Freiwilligkeit ist dann nicht gegeben, wenn sich der Betroffene in einer Situation der Abhängigkeit von dem Verantwortlichen befindet, die in der Natur ihres Verhältnisses oder aufgrund besonderer Umstände beruht, vgl. die Anmerkungen im Prüfhinweis zu etwaigen Machtasymmetrien. • Der Zugang zu Diensten und Funktionen wird nicht von der Einwilligung eines Betroffenen in die Speicherung von Informationen in seinem Gerät oder den Zugang zu bereits darin gespeicherten Informationen abhängig gemacht werden (sog. Cookie-Banner oder Cookie-Walls). • Der Prozess/das Verfahren für das Einholen der Einwilligung muss den Betroffenen ermöglichen, zu verschiedenen Verarbeitungsvorgängen und Verarbeitungszwecken von PBD gesondert eine Einwilligung zu erteilen (d. h. nur für einige Verarbeitungsvorgänge bzw. Zwecke und für andere nicht). • Der Verantwortliche muss nachweisen können, dass der Betroffene freiwillig in die Verarbeitung der PBD eingewilligt hat. Die Gründe, die für eine Freiwilligkeit der Einwilligungserteilung sprechen, sind zu dokumentieren. • Der Verantwortliche muss nachweisen, dass das Widerrufen der Einwilligung nicht zu Kosten für die betroffene Person führt und folglich zu einem eindeutigen Nachteil für diejenigen, die die Einwilligung widerrufen. • Eine Freiwilligkeit ist nicht gegeben, wenn die Ablehnung einer Einwilligung mit einem Mehraufwand für den Betroffenen verbunden ist, z. B. an Klicks oder Aufmerksamkeit, Unterzeichnung eines zusätzlichen Formulars für Verweigerung der Einwilligung, wenn Ablehnung von Cookies erst auf der zweiten Cookie-Banner-Ebene möglich ist, wenn für Verweigerung der Einwilligung eine extra Schaltfläche betätigt werden muss. • Eine Freiwilligkeit ist nicht gegeben, wenn ein Cookie-Banner oder sonstiges grafisches Element zur Einwilligungsabfrage den Zugriff auf das IVS insgesamt oder Teile des Inhalts verdeckt und das Cookie-Banner nicht einfach ohne Entscheidung geschlossen werden kann. • Eine Freiwilligkeit ist nicht gegeben, wenn ein Opt-out durch den Betroffenen vorgenommen werden muss. • Eine Freiwilligkeit ist nicht gegeben, wenn sämtliche Cookies bereits vorausgewählt sind und durch die Betätigung eines Buttons „Cookies“ zulassen aktiviert werden. • Eine Freiwilligkeit ist nicht gegeben, wenn der Betroffene durch

	manipulative Farbkombinationen oder kompliziert gestaltete Auswahlprozesse (Nudging bzw. Dark Pattern) zu einer Einwilligungserteilung gedrängt wird. • Eine Freiwilligkeit ist nicht gegeben, wenn Informationen missverständlich formuliert sind, eine bewusst verharmlosende Sprache genutzt wird oder der Betroffene mit Informationen überfrachtet wird. • Eine Freiwilligkeit ist nicht gegeben, wenn die Möglichkeit der Verweigerung einer Einwilligung für den Betroffenen nicht deutlich erkennbar ist, weil diese bspw. außerhalb des Einwilligungsbanners platziert ist oder nur schwer lesbar ist. • Bei der Beurteilung der Freiwilligkeit ist zu berücksichtigen, ob die Erfüllung eines Vertrages davon abhängig gemacht wird, dass in eine Datenverarbeitung eingewilligt wird, die für die Vertragserfüllung nicht erforderlich ist. Sofern dies der Fall ist, führt dies regelmäßig dazu, dass die Einwilligung nicht als freiwillig angesehen werden kann. • Die Einwilligung wird für einen bestimmten Fall abgegeben: ○ die Einwilligung der betroffenen Person wird für „einen oder mehrere bestimmte“ Zwecke erteilt und die betroffene Person hat in Bezug auf jeden dieser Zwecke eine Wahlmöglichkeit ○ Die Einwilligung bezieht sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommenen Verarbeitungsvorgänge ○ Wenn die Verarbeitung mehreren Zwecken dient, kann der Betroffene kann zu verschiedenen Verarbeitungsvorgängen von PBD gesondert eine Einwilligung erteilen, ○ Der Verantwortliche erteilt mit jedem Ersuchen um gesonderte Einwilligung spezifische Informationen über die Daten, die für jeden Zweck verarbeitet werden, sodass den betroffenen Personen die Auswirkungen der unterschiedlichen Wahlmöglichkeiten verdeutlicht werden

[DSGVO] Art. 4 Nr. 11, Art. 7 Abs. 2

DS04.03	**A) <u>Verantwortlicher</u>** Die **Einwilligung erfolgt in informierter Weise**. Den Betroffen werden mindestens folgende Informationen innerhalb der Einwilligungserklärung bereitgestellt, bevor ihre Einwilligung eingeholt wird: 1. zur Identität des Verantwortlichen, 2. zu den verarbeitenden Datenkategorien, 3. zu den Phasen der Verarbeitung der jeweiligen PBD, 4. zu geplanten Übermittlungen und Empfängern der Übermittlung, 5. zum Zweck der Datenverarbeitung, 6. zur Freiwilligkeit, 7. zur Widerrufbarkeit und den sich aus einem Widerruf ergebenden Konsequenzen. 8. sofern relevant: Angaben zu möglichen Risiken von Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien nach Art. 46 DSGVO 9.sofern relevant: ggf. über die Verwendung der Daten für eine automatisierte Entscheidungsfindung Die Informationen werden insbesondere als schriftliche oder mündliche

	Erklärungen oder als Audio- oder Videonachrichten zur Verfügung gestellt. Im Hinblick auf die Informiertheit der Einwilligung können in Abhängigkeit von den Umständen und dem Kontext des jeweiligen Falls möglicherweise mehr Informationen erforderlich sein, vgl. die Anforderungen zu Art. 13 DSGVO in **DS06.04**. Die Bereitstellung von Informationen erfolgt hierbei: 1. in verständlicher und leicht zugänglicher Form • Die Informationen sind nicht versteckt, d. h. die betroffene Person darf nicht gezwungen sein, die Informationen selbst ausfindig zu machen. • Es ist für betroffene Personen leicht zu erkennen sein, wer der Verantwortliche ist. • Die Einwilligungserklärung ist als solche bezeichnet. Missverständliche Überschriften, durch die Betroffene über den tatsächlichen Inhalt getäuscht werden, werden nicht genutzt. • Manipulative Farbkombinationen oder kompliziert gestaltete Auswahlprozesse (Nudging bzw. Dark Pattern), durch die Betroffene zu einer Einwilligungserteilung gedrängt werden, werden nicht genutzt. • Eine jederzeitige Abrufbarkeit des Inhalts ist sichergestellt. • Die Informationen, die für die Entscheidung in informierter Weise maßgeblich sind, sind nicht in Allgemeinen Geschäftsbedingungen versteckt. • Soll die Einwilligung elektronisch erteilt werden, so erfolgt die Aufforderung in klarer und knapper Form. Mehrschichtige und gesonderte Informationen sind möglich, um die doppelte Verpflichtung zu erfüllen, auf der einen Seite präzise und vollständig und auf der anderen Seite verständlich zu sein. • Sofern die Aufforderung zur Einwilligung auf elektronischem Weg erfolgt, so erfolgt die Aufforderung zu Einwilligung in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung gegeben wird. 2. in einer klaren und einfachen Sprache, vgl. **DS06.01** • Die Wahl der Formulierungen ist der jeweiligen Zielgruppe angepasst. Wenn zur Zielgruppe minderjährige betroffene Personen zählen, müssen die Informationen in einer dergestalt klaren und einfachen Sprache erfolgen, dass ein Kind sie verstehen kann. Hierbei ist sicherzustellen, dass die Wortwahl, die Tonalität und der Sprachstil der kindlichen Zielgruppe angepasst sind. • Die Einwilligungserklärung ist in der Landessprache des Staates formuliert, an dessen Bewohner sich der Verantwortliche mit seinem Einwilligungsbegehren wendet. Mithin muss die Einwilligungserklärung in Deutsch verfasst sein. • Die Informationen werden in einer möglichst einfachen Art und Weise unter Vermeidung komplexer Satz- und sprachlicher Strukturen bereitgestellt. • Abstrakte und mehrdeutige Begriffe bzw. Interpretationsspielraum werden vermieden.

	• Modalverben und -wörter wie „kann“, „könnte“, „manche“, „oft“ und „möglich“ werden vermieden. • Absätze und Sätze sind wohl strukturiert sein und hierarchische Beziehungen werden mit Aufzählungszeichen sowie Einzügen dargestellt. • Die Informationen sind im Aktiv und nicht im Passiv verfasst und übermäßige Substantivierungen werden vermieden. • Die Informationen enthalten nicht unverhältnismäßig viele rechtliche, technische oder fachbezogene Formulierungen oder eine entsprechende Terminologie • Es ist klar erkennbar sein, wer der Verantwortliche ist. • Der Zweck der Datenverarbeitung, für den die Datenverarbeitung erfolgen soll, wird deutlich erklärt • Die Einwilligungserklärung wird als solche bezeichnet 3. sichtbar getrennt von anderen Sachverhalten. • Sofern die Einwilligung noch andere Sachverhalte betrifft, erfolgt das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache, sodass eine klare Unterscheidung von anderen Sachverhalten besteht • Wenn im Rahmen eines Vertrags (in Schriftform) um Einwilligung ersucht wird, ist das Ersuchen um Einwilligung von den anderen Sachverhalten klar zu unterscheiden. ○ Enthält der schriftliche Vertrag viele Aspekte, die mit der Frage der Einwilligung in die Verwendung der PBD nicht in Zusammenhang stehen, wird die Frage der Einwilligung entweder in einem anderen Dokument oder auf eine Weise behandelt werden, die sich deutlich abhebt • Die Informationen, die für die Entscheidung in informierter Verweise maßgeblich sind, sind für den Betroffenen leicht zu erkennen und nicht versteckt (z. B. in Allgemeinen Geschäftsbedingungen), insbesondere durch eine hervorgehobene graphische Gestaltung, wie Umrandung, farbige oder graue Unterlegung der Einwilligungserklärung, die Verwendung von besonderen Schriften und Schriftgestaltungen (fett; kursiv) oder andere Gestaltungsmerkmale, die die Einwilligungserklärung deutlich hervorgehoben, nicht Versteckt in allgemeinen Geschäftsbedingungen • Wenn die Aufforderung zur Einwilligung elektronisch gestellt wird, erfolgt sie nach ErwG 32 DSGVO in gesonderter und klarer Form und ist nicht lediglich ein Absatz in den Geschäftsbedingungen. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen seiner Weisungsgebundenheit bzgl. der Einholung einer Einwilligung, sofern der Verantwortliche den Auftragsverarbeiter ausdrücklich die Weisung erteilt hat, dass dieser für die Einholung der Einwilligung von den Betroffenen im Namen des Verantwortlichen verantwortlich ist. Sofern eine entsprechende Weisung nicht vorliegt, ist dieses Kriterium nicht einschlägig. Die Art und Weise wie die Einwilligungserklärung zugänglich und sichtbar gemacht wird, ergibt sich aus der Weisung des Verantwortlichen, welche entsprechen durch den Auftragsverarbeiter umzusetzen ist. Sofern der Auftragsverarbeiter der Auffassung ist, dass die Weisung des Verantwortlichen gegen die DSGVO-Anforderungen oder gegen andere

	Datenschutzbestimmungen verstößt, informiert der Auftragsverarbeiter unverzüglich den Verantwortlichen. Die Zuständigkeiten und Kommunikationswege hierfür sind zu dokumentieren.

[DSGVO] Art. 4 Nr. 11

DS04.04	**A) <u>Verantwortlicher</u>** Die Erteilung einer Einwilligung erfolgt durch eine Erklärung oder eindeutig bestätigende Handlung des Betroffenen. • Erteilung der Einwilligung erfolgt in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann oder einer mündlichen Erklärung oder durch eine andere Erklärung oder Verhaltensweise, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert, z. B. Anklicken eines Kästchens, Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft • Stillschweigen, bereits angekreuzte Kästchen, Opt-out-Konstruktionen, bloße Information und die Weiternutzung des IVS, oder Untätigkeit stellen keine Einwilligung dar. • Die Einwilligung in die Verarbeitung von PBD erfolgt separat von einem Vorgang, mit dem einem Vertrag oder den allgemeinen Geschäftsbedingungen zugestimmt wird. • Die Einwilligung wird eingeholt bevor mit der Verarbeitung der PBD begonnen wird. **<u>B) Auftragsverarbeiter</u>** Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen seiner Weisungsgebundenheit bzgl. der Einholung einer Einwilligung, sofern der Verantwortliche den Auftragsverarbeiter ausdrücklich die Weisung erteilt hat, dass dieser für die Einholung der Einwilligung von den Betroffenen im Namen des Verantwortlichen verantwortlich ist. Sofern eine entsprechende Weisung nicht vorliegt, ist dieses Kriterium nicht einschlägig. Die Art und Weise wie die Einwilligung eingeholt wird, ergibt sich aus der Weisung des Verantwortlichen, welche entsprechen durch den Auftragsverarbeiter umzusetzen ist. Sofern der Auftragsverarbeiter der Auffassung ist, dass die Weisung des Verantwortlichen gegen die DSGVO-Anforderungen oder gegen andere Datenschutzbestimmungen verstößt, informiert der Auftragsverarbeiter unverzüglich den Verantwortlichen. Die Zuständigkeiten und Kommunikationswege hierfür sind zu dokumentieren.

[DSGVO] Art. 7 Abs. 1

DS04.05	**A) Verantwortlicher** Sofern eine Verarbeitung mit Einwilligung der betroffenen Person erfolgt, kann der Verantwortliche nachweisen, dass die betroffene Person ihre Einwilligung zu dem Verarbeitungsvorgang gegeben hat. Der Verantwortliche kann hierbei insbesondere nachweisen: • Inhalt der Einwilligungserklärung (in welche Verarbeitung welcher Daten zu welchem Zweck wurde durch den Betroffenen eingewilligt) • Nachweis, dass der betroffenen Person vor Erteilung der Einwilligung alle erforderlichen Informationen gegeben wurden, damit diese ihre Entscheidung auf der Basis von umfassenden Informationen treffen konnte • Verfahren wie die Einwilligung zustande kam inklusive Angabe welche Informationen den Betroffenen zur Verfügung gestellt wurden • Nachweis, dass alle Kriterien für eine gültige Einwilligung erfüllt wurden (Dokumentation der einzelnen Abläufe im Hinblick auf die Erteilung einer Einwilligung zum Zeitpunkt der Abgabe dieser und Dokumentation der Informationen, die der betroffenen Person zu dem Zeitpunkt vorgelegt wurden) Bei der Erbringung des Nachweises, dass eine gültige Einwilligung eingeholt wurde, werden nur diejenigen Daten erfasst werden, die erforderlich sind, um eine Verbindung zur Verarbeitung, in die der Betroffene eingewilligt hat, nachweisen zu können, vgl. **DS02.06**. Die Pflicht zum Nachweis besteht so lange wie Datenverarbeitungstätigkeit andauert. Nachdem die Verarbeitungstätigkeit beendet wurde, wird der Einwilligungsnachweis nur so lange aufbewahrt, als es zur Erfüllung einer rechtlichen Verpflichtung oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen gemäß Artikel 17 Abs. 3 lit. b) und e) erforderlich ist. Hierfür sind entsprechende Löschprozesse etabliert, welche insbesondere Festlegungen treffen zu: • Aufbewahrungsdauer des Einwilligungsnachweises • Zuständigkeiten für Löschung • Verfahren für Umsetzung der Löschung • Zuständigkeiten für Überprüfung der Vornahme von Löschungen inklusive Festlegung Art und Weise der Überprüfung und Häufigkeit der Überprüfung **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen seiner Weisungsgebundenheit bzgl. der Erbringung des Nachweises über die Erteilung einer Einwilligung durch den Betroffenen, sofern der Verantwortliche den Auftragsverarbeiter ausdrücklich die Weisung erteilt hat (vgl. die Anforderungen in **DS07.04, DS07.10**), dass dieser für die Einholung der Einwilligung von den Betroffenen im Namen des Verantwortlichen und deren Dokumentation verantwortlich ist. Sofern eine entsprechende Weisung nicht vorliegt, ist dieses Kriterium nicht einschlägig.

[DSGVO] Art. 7 Abs. 3

DS04.06	**A) Verantwortlicher** Der **Widerruf der Einwilligung** wird ebenso einfach wie die Einwilligung ermöglicht. Im Hinblick auf die Vornahme des Widerrufs sind folgende Anforderungen durch den Verantwortlichen umzusetzen: • Sofern die Einwilligung mittels elektronischer Mittel lediglich durch einen Mausklick, Wischvorgang oder Tastenanschlag erteilt wird, muss für den Betroffenen die Möglichkeit bestehen, seinen Widerruf auf die entsprechende Art und Weise vorzunehmen. • Wird die Einwilligung unmittelbar bei der Nutzung des IVS erteilt, muss auch deren Widerruf auf diesem Weg möglich sein. • Wird die Einwilligung über eine dienstleistungsspezifische Nutzerschnittfläche (beispielsweise über eine Website, eine App, ein Konto, in das sich der Betroffene einloggt, die Schnittstelle eines Gerätes des Internet der Dinge oder eine E-Mail) erteilt, muss der Betroffene die Möglichkeit haben, seine Einwilligung über dieselbe elektronische Schnittstelle zu widerrufen. Ausschließliche Widerrufsmöglichkeiten über andere Kommunikationswege wie E-Mail, Fax oder Brief sind unzulässig. Ein ausschließlicher Hinweis auf ein Kontaktformular ist ebenfalls unzulässig. • Sofern eine Einwilligung mittels Banner o. Ä. abgefragt, ist es unzulässig, wenn zunächst eine Datenschutzerklärung aufgerufen und dann in dieser zu der richtigen Stelle gescrollt werden muss, um zu einer Widerrufsmöglichkeit zu gelangen. • Eine Platzierung der Widerrufsmöglichkeit in der Datenschutzerklärung ist nur zulässig, sofern Verlinkungen in der Datenschutzerklärung den Betroffenen direkt an die Stelle zur Möglichkeit des Widerrufs leiten und keine Suchvorgänge notwendig sind (direkt auffindbare Widerrufsmöglichkeit). • Der Betroffene muss seine Einwilligung widerrufen können, ohne Nachteile zu erleiden, d. h. der Widerruf muss kostenfrei möglich sein und ohne Absenkung des Leistungsniveaus • Die einzelnen Schritte wie ein Betroffener seine Einwilligung widerrufen kann, sind durch den Verantwortlichen zu dokumentieren. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt den Verantwortlichen, im Rahmen seiner Weisungsgebundenheit dabei, dass der Widerruf der Einwilligung so einfach, wie die Erteilung der Einwilligung ist. Hierfür muss der Verantwortliche den Auftragsverarbeiter ausdrücklich die Weisung erteilt haben (vgl. die Anforderungen in **DS07.04, DS07.10**), dass dieser für die Umsetzung des Widerrufsrechts verantwortlich ist. Sofern eine entsprechende Weisung nicht vorliegt, ist dieses Kriterium nicht einschlägig.

[DSGVO] Art. 7 Abs. 3

DS04.07	**A) Verantwortlicher** Der Verantwortliche informiert die betroffene Person vor Abgabe der Einwilligung darüber, dass die Rechtmäßigkeit, der aufgrund der Einwilligung **bis zum Widerruf erfolgten Verarbeitung** nicht durch den Widerruf der Einwilligung berührt wird. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen seiner Weisungsgebundenheit dabei, die betroffene Person vor Abgabe der Einwilligung darüber zu informieren, dass die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht durch den Widerruf der Einwilligung berührt wird.

[DSGVO] Art. 7 Abs. 3

DS04.08	**A) Verantwortlicher** Die Prozesse zur **Behandlung des Widerrufs** der Einwilligung stellen sicher, dass die betroffenen Verarbeitungstätigkeiten eingestellt werden. Sofern keine anderweitige Rechtsgrundlage für die Verarbeitung vorliegt und die fortgesetzte Speicherung nicht durch einen weiteren Zweck gerechtfertigt wird, sind die PBD, die auf der Grundlage der Einwilligung verarbeitet werden, zu löschen. Hierfür sind entsprechende Prozesse implementiert und dokumentiert, vgl. die Anforderungen in **DS02.08**, **DS06.12**. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt den Verantwortlichen, im Rahmen seiner Weisungsgebundenheit dabei, dass in Folge eines Widerrufs, die betroffenen Verarbeitungstätigkeiten eingestellt und die PBD gelöscht werden. Hierfür muss der Verantwortliche den Auftragsverarbeiter ausdrücklich die Weisung erteilt haben (vgl. die Anforderungen in **DS07.04, DS07.10**), dass dieser für die Behandlung von Widerrufen des Betroffenen verantwortlich ist und wie er diese konkret zu behandeln hat. Sofern eine entsprechende Weisung nicht vorliegt, ist dieses Kriterium nicht einschlägig. Sofern der Auftragsverarbeiter seitens das Verantwortlichen mit der Behandlung von Widerrufen beauftragt wurde, hat er Prozesse zur Gewährleistung, dass die betroffenen Verarbeitungstätigkeiten eingestellt und die PBD gelöscht werden, implementiert. Diese Prozesse treffen insbesondere Festlegungen zu: • Zuständigkeiten und Kommunikationswege bzgl. der Behandlung des Widerrufs und der Vornahme der Löschungen • Festlegung und konkrete Beschreibung von Löschmechanismen (Dokumentation der einzelnen Vorgänge bzw. Umsetzungsvorgaben) ○ Bei der Festlegung der Mindestanforderungen an Verfahren zur Löschung sind die Vorgaben des IT-Grundschutzkompendiums CON.6 Löschen und Vernichten umzusetzen • Zuständigkeiten bzgl. der Überwachung der Löschprozesse • Überprüfung der tatsächlichen Umsetzung bzw. Wirksamkeit der Löschung • Festlegung wie Durchführung von Löschungsmaßnahmen

	dokumentiert werden • Berücksichtigung der Datenlöschung in Backups und Archiven • Regelmäßige Evaluierung (mindestens jährlich), ob die gewählten Löschmechanismen noch dem Stand der Technik entsprechen

[DSGVO] Art. 6 Abs. 1 lit. a, Art. 8

DS04.09	**A) Verantwortlicher** Gilt die Einwilligung gem. Artikel 6 Abs. 1 lit. a DSGVO (vgl. die Anforderungen in **DS04.01** bis **DS04.08**) bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, so ist die Verarbeitung der personenbezogenen Daten des Kindes nach Art. 8 Abs. 1 DSGVO rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat Sofern das Kind noch nicht das sechzehnte Lebensjahr vollendet hat, ist diese Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird. Im Hinblick auf die allgemeine Wirksamkeit der Einwilligung finden die Anforderungen in **DS04.01 bis DS04.08** Anwendung. Ergänzend muss sichergestellt sein, dass die Wortwahl, Tonalität und Sprachstil der kindlichen Zielgruppe angepasst ist. Im Hinblick auf die spezifischen Bedingungen des Art. 8 DSGVO ist unter Berücksichtigung der verfügbaren Technik durch den Verantwortlichen zu evaluieren: a) Ob das Alter des Minderjährigen, welcher den Dienst der Informationsgesellschaft nutzt, eine Einwilligung oder Zustimmung des Trägers der elterlichen Verantwortung entbehrlich macht (Altersverifikation). Hierfür sind entsprechende Prozesse zu implementieren, welche mindestens folgendes berücksichtigen: • Es müssen Systeme zur Altersverifikation implementiert sein. Hierbei muss sichergestellt sein, dass nur diejenigen Daten verarbeitet werden, die für die Altersverifikation zwingend erforderlich sind. • Im Rahmen der Auswahl des jeweiligen Systems zur Altersverifikation ist eine Bewertung des Risikos der damit verbundenen Datenverarbeitung vorzunehmen und zu dokumentieren. • Es muss sichergestellt sein, dass die im Rahmen der Altersverifikation gewonnenen Daten nicht für kommerzielle Zwecke verwendet werden. • Sofern das Kind angibt, dass es die Altersgrenze (Alter der digitalen Mündigkeit) noch nicht erreicht hat, kann der Verantwortliche diese Angabe ohne weitere Überprüfungen akzeptieren, muss aber sicherstellen, dass eine erforderliche Einwilligung bzw. Zustimmung des Trägers der elterlichen Verantwortung vorliegt (siehe nachfolgend). b) Sofern das Kind das 16. Lebensjahr noch nicht vollendet hat, ob eine erforderliche Einwilligung bzw. Zustimmung zur Datenverarbeitung des Trägers der elterlichen Sorge vorliegt und tatsächlich von diesen abgegeben wurde (Authentifizierung). Hierfür sind entsprechende Prozesse zu implementieren, welche mindestens folgendes berücksichtigen: • Eine Bestätigung des Kindes, seine Eltern hätten zugestimmt, ist nicht ausreichend, sondern es müssen Maßnahmen zur

	Altersverifikation umgesetzt werden: Unter Berücksichtigung der verfügbaren Technologie, der Angemessenheit und der mit der Verarbeitung einhergehenden Risiken (vgl. Risikobewertung) muss der Verantwortliche Maßnahmen bzgl. der Einholung der Einwilligung durch den Träger der elterlichen Verantwortung bzw. dessen Zustimmung implementiert haben. Hierfür sind entsprechende Maßnahmen zu implementieren (z. B. Double-Opt-in-Verfahren, ein von den Eltern unterschriebenes Dokument (per Post, Fax, elektronischem Scan), Rückgriff auf Kreditkarten der Eltern zur Legitimation von Transaktionen, Telefongespräch oder Videokonferenz mit den Eltern unter einer kostenlosen Nummer etc.) • Bei der Auswahl der jeweiligen Maßnahmen ist sicherzustellen, dass nur diejenige Daten verarbeitet werden, die hierfür zwingend erforderlich sind. • Die Prozesse bzw. implementierten Maßnahmen sind kontinuierlich zu überprüfen. Hierfür sind entsprechende Zuständigkeiten festzulegen. • Es muss sichergestellt sein, dass die Einwilligung bzw. die Zustimmungserklärung vor Beginn der Datenverarbeitung erfolgt. • Der Verantwortliche muss das Kind gem. Art. 7 Abs. 3 Satz 3 DSGVO das Kind über die erteilte Einwilligung durch die Träger der elterlichen Sorge informieren. Hierfür müssen entsprechende Prozesse implementiert sein (Zuständigkeiten, Kommunikationswege). • Nachdem das Kind das Alter der digitalen Mündigkeit erreicht hat, kann die Einwilligung in die Verarbeitung der personenbezogenen Daten durch den Träger der elterlichen Verantwortung bzw. dessen Zustimmung in die Datenverarbeitung durch das Kind bestätigt, geändert oder widerrufen werden. Der Verantwortliche muss das Kind nach Erreichung der Altersgrenze hierüber informieren und eine entsprechende Maßnahme des Kindes fordern. Hierbei ist das Kind darüber in Kenntnis zu setzen, dass es die Möglichkeit hat, selbst die Einwilligung in Übereinstimmung mit Art. 7 Abs. 3 DSGVO zu widerrufen. Zudem ist es auf das Recht auf Vergessenwerden gem. Art. 17 DSGVO hinzuweisen. Hierfür sind entsprechende Prozesse (Zuständigkeiten, Prozesse bzgl. der Überprüfung des Eintritts der Altersgrenze, Kommunikationswege, Festlegung des weiteren Vorgehens, wenn das Kind keine geforderte Maßnahme ergreift) zu implementieren und zu dokumentieren. Die Ergebnisse der Überprüfung sind zu dokumentieren. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen. **B) Auftragsverarbeiter** Sofern es sich um einen Dienst der Informationsgesellschaft handelt, der einem Kind direkt angeboten wird, ist die Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat und das Kind die Einwilligung zur Verarbeitung erteilt hat. Sofern das Kind noch nicht das sechzehnte Lebensjahr vollendet hat, ist diese Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind

	oder mit dessen Zustimmung erteilt wird. Der Auftragsverarbeiter unterstützt den verantwortlichen im Rahmen seiner Weisungsgebundenheit bei der Erfüllung der vorstehenden Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft. Der Auftragsverarbeiter stellt dem Verantwortlichen in diesem Zusammenhang entweder einen Muster-Einwilligungstext oder ein Hilfsdokument zur Formulierung einer Einwilligung nach Maßgabe des Art. 8 Abs. 1 DSGVO bereit. Im Hinblick auf die allgemeine Wirksamkeit der Einwilligung finden die Anforderungen in **DS04** Anwendung. Sofern der Auftragsverarbeiter per Weisung durch den Verantwortlichen verpflichtet wird, die Einwilligung nach Art. 8 Abs. 1 DSGVO selbst einzuholen, sind alle Anforderungen zu Abschnitt *A) Verantwortlicher* durch den Auftragsverarbeiter zu erfüllen und nachzuweisen.

DS05 Verarbeitung besonderer Kategorien personenbezogener Daten

[DSGVO] Art. 9 Abs. 1, 2 ggf. i. V. m. landes- oder bundesrechtlichen Normen, wie [BDSG] §§ 22, 27 Abs. 1

DS05.01	**A) Verantwortlicher** Zusätzlich zu den in DS03 und DS04 genannten Anforderungen, sind nachfolgende Anforderungen zu erfüllen, wenn „besondere Kategorien personenbezogener Daten“ (BKPD) verarbeitet werden: 1. Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem deutschen Recht kann das Verbot nach Art. 9 Abs. 1 DSGVO durch die Einwilligung der betroffenen Person nicht aufgehoben werden (Art. 9 Abs. 2 lit. a DSGVO) Neben den Anforderungen an eine Einwilligung nach Art. 7 DSGVO (vgl. DS04) muss sich die ausdrückliche Einwilligung explizit auf die Verarbeitung besonderer Kategorien PBD beziehen und die verwendeten Daten sowie den Verwendungszweck konkret benennen. Eine konkludente oder stillschweigende Erklärung ist nicht zulässig. 2. die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem deutschen Recht oder einer Kollektivvereinbarung nach dem deutschen Recht, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist (Art. 9 Abs. 2 lit. b DSGVO) Hierzu muss der Verantwortliche im Hinblick auf den Umfang der Verarbeitung zunächst prüfen und dokumentieren, ob sich ein Verarbeitungserfordernis aus konkreten unionsrechtlichen oder einzelstaatlichen Normen, z. B. zu Zwecken der Renten- und Sozialversicherung, Krankenversicherung, Sozialhilfe, Wohnungs-, Familien- oder Ausbildungsförderung, die in den jeweiligen Spezialgesetzen verankert sein müssen, ergibt. Hierzu können auch Betriebsvereinbarungen und Tarifverträge zählen. 3. die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben (Art. 9 Abs. 2 lit. c DSGVO) Der Verantwortliche muss sich bei Prüfung der Anwendbarkeit von lit. c vergewissern, dass sich die Einholung einer Einwilligung als (faktisch) unmöglich erweist, z. B. weil der Betroffene bewusstlos ist oder infolge physischer Abwesenheit nicht erreicht werden kann und die Verarbeitung offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann. 4. die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf

	Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden (Art. 9 Abs. 2 lit. d DSGVO). Der Verantwortliche muss sicherstellen, dass die Verarbeitung im Rahmen der Zwecksetzung der jeweiligen Organisation und auf Grundlage geeigneter Garantien erfolgt, wozu vor allem hinreichende technisch-organisatorische Maßnahmen zählen (vgl. **DS08**). Es ist zu prüfen, ob die Verarbeitung zweckmäßige Tätigkeiten umfasst, die für die spezifische Ausrichtung der Organisation erforderlich sind. Die Verarbeitung darf sich nur auf eigene Mitglieder, ehemalige Mitglieder sowie Personen beziehen, die in Bezug auf ihren jeweiligen Tätigkeitszweck in regelmäßigem Kontakt mit der Organisation stehen. Nach außen offen gelegt werden dürfen die personenbezogenen Daten nur mit ausdrücklicher Einwilligung der Betroffenen. 5. die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat (Art. 9 Abs. 2 lit. e DSGVO). Es ist sicherzustellen, dass die Veröffentlichung auf einen bewussten Willensakt des Betroffenen zurückzuführen ist, die Veröffentlichung demnach unzweifelhaft von der betroffenen Person herrührt oder eindeutig von ihr veranlasst wurde. Der Verantwortliche muss nachweisen können, dass die PBD offensichtlich öffentlich gemacht wurden. 6. die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich (Art. 9 Abs. 2 lit. f DSGVO). Der Verantwortliche muss dokumentieren, weshalb ein Erfordernis für die Verarbeitung der PBD bei der Ausübung oder Verteidigung von Rechtsansprüchen vorliegt. Eine willkürliche Offenlegung der besonderen Kategorien PBD, die mit dem Streitinhalt in keiner Verbindung stehen, ist unzulässig. 7. die Verarbeitung ist auf der Grundlage des Unionsrechts oder des deutschen Rechts, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich (Art. 9 Abs. 2 lit. g DSGVO) Der Verantwortliche muss dokumentieren, ob und welches erhebliche öffentliche Interesse vorliegt. Dabei ist sicherzustellen, dass die Verarbeitung verhältnismäßig ist, die Maßnahmen zur Erreichung des Ziels daher geeignet und erforderlich sind und die Nachteile für den Betroffenen in einem angemessenen Verhältnis zum Ziel stehen. 8. die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des deutschen Rechts oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Abs. 3 genannten Bedingungen und Garantien erforderlich (Art. 9 Abs. 2 lit. h DSGVO)

	Der Verantwortliche muss darlegen, auf Basis welcher gesetzlichen Erlaubnis eine solche Verarbeitung aus dem Unionsrecht oder aus dem deutschen Recht oder eines Vertrags mit einem Angehörigen eines Gesundheitsberufs (z. B. Ärzte, Ärztepersonal) erfolgt. Der Verantwortliche muss zudem sicherstellen, dass die Verarbeitung zu den in Abs. 2 lit. h DSGVO genannten Zwecken „im Interesse einzelner natürlicher Personen und der Gesellschaft insgesamt“ erforderlich ist. Ferner ist die Verarbeitung nur zulässig, wenn diese von Fachpersonal oder unter dessen Verantwortung vorgenommen wird und dieses Fachpersonal gesetzlich einem Berufsgeheimnis unterliegt oder die verarbeitende Person anderweitig einer Geheimhaltungspflicht durch Unionsrecht, dem deutschen Recht oder den Vorschriften einer nationalen zuständigen Stelle unterliegt. 9. Die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des deutschen Rechts, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich ist (Art. 9 Abs. 2 lit. i DSGVO). Der Verantwortliche hat zu dokumentieren, welche Norm aus dem Recht der Union oder dem deutschen Recht die Verarbeitung besonderer Kategorien PBD für die in lit. i) genannten Zwecke legitimiert. 10. die Verarbeitung ist auf der Grundlage des Unionsrechts oder des deutschen Rechts, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Art. 89 Abs. 1 DSGVO erforderlich (Art. 9 Abs. 2 lit. j DSGVO). Der Verantwortliche muss dokumentieren auf welche Norm des Unionsrechts oder des deutschen Rechts er sich bezieht und hat sicherzustellen, dass sich das Erfordernis eines öffentlichen Interesses auf alle in lit. j genannten Alternativen bezieht. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen seiner Weisungsgebundenheit bzgl. der Einholung einer Einwilligung, sofern der Verantwortliche den Auftragsverarbeiter ausdrücklich die Weisung erteilt hat (vgl. die Anforderungen in **DS07.04, DS07.10**), dass dieser für die Einholung der Einwilligung von den Betroffenen im Namen des Verantwortlichen verantwortlich ist. Sofern ei-ne entsprechende Weisung nicht vorliegt, ist dieses Kriterium nicht einschlägig. Die inhaltliche Gestaltung der Einwilligungsformulierung obliegt dem Verantwortlichen und ist durch den Auftragsverarbeiter umzusetzen. Sofern der Auftragsverarbeiter der Auffassung ist, dass die Weisung des Verantwortlichen gegen die DSGVO-Anforderungen oder gegen andere

	Datenschutzbestimmungen verstößt, informiert der Auftragsverarbeiter unverzüglich den Verantwortlichen. Die Zuständigkeiten und Kommunikationswege hierfür sind zu dokumentieren.

[DSGVO] Art. 9 Abs. 3 ggf. i. V. m. landes- oder bundesrechtlichen Normen, wie [BDSG] §§ 22, 27 Abs. 1 i. V. m. [BDSG]

DS05.02	**A) Verantwortlicher** Falls besondere Kategorien personenbezogener Daten zu Zwecken von Art. 9 Abs. 2 lit. h DSGVO verarbeitet werden, stellt der Verantwortliche sicher, dass diese Daten von **Fachpersonal** oder unter deren Verantwortung verarbeitet werden und dieses Fachpersonal oder auch andere die Daten verarbeitende Personen einem gesetzlichen Berufsgeheimnis unterliegen. Die jeweilige Datenverarbeitung aufgrund eines Vertrages mit einem Angehörigen eines Gesundheitsberufes muss erforderlich sein. **B) Auftragsverarbeiter** Falls besondere Kategorien personenbezogener Daten zu Zwecken von Art. 9 Abs. 2 lit. h DSGVO verarbeitet werden, stellt der Auftragsverarbeiter sicher, dass diese Daten von **Fachpersonal** oder unter deren Verantwortung verarbeitet werden und dieses Fachpersonal oder auch andere die Daten verarbeitende Personen einem gesetzlichen Berufsgeheimnis unterliegen. Der Auftragsverarbeiter weist dem Verantwortlichen nach, dass alle Personen, die im Rahmen der beauftragten Tätigkeit eingesetzt werden, einem Berufsgeheimnis unterliegen und alle Personen auf die Geheimhaltung von Berufsgeheimnissen verpflichtet sind.

[DSGVO] Art. 9 Abs. 4

DS05.03	**Verantwortlicher und Auftragsverarbeiter** Sofern eine **Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten** erfolgt, kann die Verarbeitung durch deutsches Recht gesondert geregelt sein. Der Verantwortliche muss zunächst prüfen und dokumentieren, ob derartige deutsche Normen einschlägig sind und welche zusätzlichen Bedingungen und Beschränkungen sich aus diesen im Hinblick auf die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten ergeben. Der Verantwortliche muss dokumentieren auf welche Norm er sich bezieht. Es sind die zusätzlichen Bedingungen einschließlich der Beschränkungen, welche sich aus der nationalen Regelung ergeben, zu erfüllen. Die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten muss zu den Verarbeitungszwecken erfolgen, welche in der nationalen Regelung vorgesehen sind. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

DS06 Rechte der Betroffenen

[DSGVO] Art. 12 Abs. 1

DS06.01	**A) Verantwortlicher** Mit Hilfe geeigneter Maßnahmen werden den Betroffenen die Informationen gemäß den Art. 13 und 14 DSGVO sowie alle Mitteilungen gemäß den Art. 15 – 22 und Art. 34 DSGVO 1. in präziser, transparenter, verständlicher und leicht zugänglicher Form: • Die Datenschutzinformationen sind klar von anderen Informationen, die sich nicht auf den Datenschutz beziehen, z. B. Vertragsbestimmungen, allgemeine Nutzungsbedingungen, getrennt • Die Datenschutzinformationen sind für einen typischen Angehörigen des Zielpublikums verständlich (Berücksichtigung des Verständnishorizonts der jeweilig betroffenen Personen). • Es ist für die betroffene Person sofort ersichtlich, wo und wie sie auf die Datenschutzinformationen zugreifen kann (leichte Zugänglichkeit) • Sofern das Zielpublikum des Verantwortlichen Kinder sind oder die Waren/Dienstleistungen insbesondere von Kindern genutzt werden, ist die Wortwahl, die Tonalität und der Sprachstil der kindlichen Zielgruppe angepasst • Der Verantwortliche stellt die Informationen nach Art. 13 und 14 DSGVO den Betroffenen aktiv bereit oder leitet die Betroffenen direkt an die Stelle wo die Informationen zur Verfügung stehen • Der Betroffene hat dauerhaft Zugang zu den Informationen nach Art. 13 und 14 DSGVO • Der Verantwortliche erinnert den Betroffenen in regelmäßigen Abständen (mindestens jährlich) an die Datenschutzerklärung/-informationen und wo diese zu finden sind • Es wird ein allgemein geläufiger Begriff, wie z. B. „Datenschutz“, „Datenschutzbestimmungen“, „Datenschutzinformationen“, „Datenschutzhinweis“ verwendet • Bei komplexen, technischen oder unerwarteten Verarbeitungsvorgängen erfolgt, neben der Bereitstellung der nach den Art. 13 und 14 DSGVO erforderlichen Informationen, gesondert und eindeutig formuliert eine Darlegung der wichtigsten Folgen der Verarbeitung • Der Verantwortliche nimmt eine dokumentierte Abschätzung vor, ob sich für die durch die Verarbeitung betroffenen Personen besondere Risiken ergeben, die den betroffenen Personen zur Kenntnis gebracht werden sollten. Wenn dies der Fall ist, werden die Betroffenen über diese Risiken aufgeklärt. • Verwendung von Mehrebenen-Datenschutzerklärungen/-informationen, die den Betroffenen das direkte Aufrufen bestimmter Punkte ermöglichen, anstatt Darstellung der ge-samten Informationen auf dem Bildschirm in Form eines einzigen Hinweises. 2. in einer klaren, einfachen Sprache • Die Informationen werden in einer möglichst einfachen Art und Weise unter Vermeidung komplexer Satz- und sprachlicher Strukturen bereitgestellt • Abstrakte und mehrdeutige Begriffe bzw. Interpretationsspielraum

	werden vermieden. • Modalverben und -wörter wie „kann“, „könnte“, „manche“, „oft“ und „möglich“ werden vermieden • Absätze und Sätze sind wohl strukturiert und hierarchische Beziehungen werden mit Aufzählungszeichen sowie Einzügen dargestellt. • Die Informationen sind im Aktiv und nicht im Passiv verfasst und übermäßige Substantivierungen werden vermieden • Die Informationen enthalten nicht unverhältnismäßig viele rechtliche, technische oder fachbezogene Formulierungen oder eine entsprechende Terminologie • Sofern das Zielpublikum des Verantwortlichen Kinder sind, ist die Wortwahl, die Tonalität und der Sprachstil der kindlichen Zielgruppe angepasst, sodass der kindliche Empfänger der Informationen auch erkennt, dass die Mitteilung / Information an ihn gerichtet ist • Die Information erfolgt in der Landessprache der jeweiligen Zielgruppe, mithin in Deutsch 3. schriftlich oder in anderer Form, ggf. auch elektronisch • Die Übermittlung der Informationen gem. den Art. 13 und 14 DSGVO und alle Mitteilungen gemäß den Art. 15 bis 22 und Art. 34 DSGVO, erfolgt schriftlich oder in anderer Form, ggf. auch elektronisch • Sofern die betroffene Person, den Antrag bzgl. Wahrnehmung ihrer Betroffenenrechte in elektronischer Form gestellt hat, erfolgt die Kommunikation nach Möglichkeit auf elektronischem Weg, es sei denn, die Person wünscht einen anderen Kommunikationsweg. • Die Bereitstellung der Informationen nach Art. 13 und 14 DSGVO nach kann auch in elektronischer Form erfolgen (z. B. auch kontextbezogene „Just-in-time-Pop-up-Hinweise“, 3D Touch-Hinweise sowie Datenschutz-Dashboards, ggfs. Videos und Smartphone- oder IoT-Sprachmeldungen zusätzlich zu Mehrebenen-Datenschutzerklärungen/ -hinweisen) • Für den Fall, dass eine Webseite betrieben wird: Verwendung von Mehrebenen-Datenschutzerklärungen/-hinweisen, die den Betroffenen das direkte Aufrufen bestimmter Punkte ermöglichen, anstatt Darstellung der gesamten Informationen auf dem Bildschirm in Form eines einzigen Hinweises. Weiterhin ist bei der Verwendung von Mehrebenen-Datenschutzerklärungen/-informationen zu gewährleisten: ○ Die Informationen nach Art. 13 und 14 DSGVO werden auch leicht zugänglich an einem einzigen Ort oder in einem Gesamtdokument (digital oder im Papierformat) zur Verfügung gestellt. ○ Die Gestaltung und Gliederung der ersten Ebene der Mehrebenen-Datenschutzerklärung/-informationen muss der betroffenen Person einen Gesamtüberblick über die ihr hinsichtlich der Verarbeitung ihrer personenbezogenen Daten zur Verfügung stehenden Informationen liefen und aufzeigen, wo / wie sie die einzelnen Informationen auf den jeweiligen Ebenen der Datenschutzerklärungen / -hinweise finden kann. ○ Die auf den verschiedenen Ebenen eines Mehrebenen-Hinweises enthaltenen Informationen sind konsistent und unterscheiden sich nicht in widersprüchlicher Weise von Ebene zu Ebene ○ Die erste Ebene von Mehrebenen-Datenschutzerklärungen / -informationen enthält Informationen zu:

	Verarbeitungszwecken, die Identität des Verantwortlichen sowie eine Beschreibung der Rechte der betroffenen Person, Angaben über die Verarbeitung, welche sich am stärksten auf die betroffene Person auswirkt, und die Verarbeitungsvorgänge, mit denen die betroffene Person ggfs. nicht rechnet ○ Die vorstehenden Informationen werden der betroffenen Person direkt zum Zeitpunkt der Erhebung der personenbezogenen Daten zur Kenntnis gebracht werden, z. B. durch die Anzeige auf dem Bildschirm, während die betroffene Person ein Online-Formular ausfüllt ○ Im Hinblick auf den Einsatz des Mehrebenen Ansatzes in einer nicht-digitalen Umgebung: Auf der ersten Ebene werden den Betroffenen zumindest folgende Informationen mitgeteilt: Verarbeitungszwecke, die Identität des Verantwortlichen sowie eine Beschreibung der Rechte der betroffenen Person, Angaben über die Verarbeitung, welche sich am stärksten auf die betroffene Person auswirkt, und die Verarbeitungsvorgänge, mit denen die betroffene Person ggfs. nicht rechnet. Es ist festzulegen und zu dokumentieren, wie die Mitteilung der weiteren nach Art. 13 und 14 DSGVO erforderlichen Informationen erfolgt • Falls es von der betroffenen Person verlangt wird, können die Information gem. den Art. 13 und 14 und alle Mitteilungen gem. den Art. 15 bis 22 und Art. 34, mündlich erteilt werden. Im Hinblick auf die Ausübung der Betroffenenrecht nach Art. 15 bis 22 DSGVO muss die Identität der betroffenen Person allerdings in anderer Form nachgewiesen wurde. Der Verantwortliche muss festlegen, wie ein entsprechender Identitätsnachweis erfolgen kann. ○ Im Fall der mündlichen Bereitstellung der Informationen nach Art. 13 und 14 DSGVO mittels Nachrichtenaufzeichnung ermöglicht der Verantwortliche, dass der Betroffene die aufgezeichnete Nachricht mehrmals abhören kann ○ Der Verantwortliche dokumentiert: das Verlangen nach Information in mündlicher Form, das Verfahren, mit dem ggf. die Identität der betroffenen Person überprüft wurde, die Tatsache, dass der betroffenen Person die Information erteilt wurde • Der Verantwortliche kann die Informationen gem. Art. 13 und 14 DSGVO in Kombination mit standardisierten Bildsymbolen bereitstellen ○ verwendeten Bildsymbole müssen standardisiert sein ○ Die Bildsymbole werden ergänzend zu den ausgeschriebenen Datenschutzinformationen genutzt ○ Werden die Bildsymbole in elektronsicher Form bereitgestellt, müssen sie maschinenlesbar sein 4. unentgeltlich • der Verantwortliche verlangt kein Entgelt für die Erteilung von Informationen nach den Art. 13 und 14 DSGVO oder für Mitteilungen und getroffene Maßnahmen nach den Art. 15 - 22 sowie Art. 34 DSGVO • Die Bereitstellung von Informationen ist nicht abhängig von einer finanziellen Transaktion des Betroffenen übermittelt. • Nur im Falle von offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer

	betroffenen Person kann der Verantwortliche entweder a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder b) sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche muss in diesen Fällen den Nachweis, für den offenkundig unbegründeten oder exzessiven Charakter des Antrags erbringen. • Der Verantwortliche muss dokumentieren, welche Modalitäten und Formate für die Informationsübermittlung genutzt werden Bezüglich des Zeitpunkts der Mitteilung der Informationen nach Art. 13 und 14 DSGVO werden nachfolgende Fristen eingehalten: a) PBD werden von der betroffenen Person selbst erhoben • Die Informationen (Datenschutzinformationen) werden vor der Erhebung der PBD übermittelt, vgl. Art. 13 Abs. 1 DSGVO b) PBD werden nicht bei der betroffenen Person erhoben • Im Hinblick auf den Zeitpunkt der Information des Betroffenen sind folgende Fristen gem. Art. 14 Abs. 3 DSGVO einzuhalten: ○ Die Informationen (Datenschutzinformationen) werden dem Betroffenen in einer angemessenen Frist nach Erlangung der personenbezogenen Daten „unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten“, längstens innerhalb eines Monats (= äußerste Frist) mitgeteilt (Art. 14 Abs. 3 lit. a DSGVO). Im Hinblick auf die Frist sind folgende Restriktionen zu beachten und entsprechend muss eine frühere Erteilung der In-formationen gewährleistet werden. ○ Sofern die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden: Die Information muss spätestens zum Zeitpunkt der ersten Kommunikation mit der betroffenen Person erteilt werden (auch wenn die äußerste Frist noch nicht abgelaufen ist) (Art. 14 Abs.3 lit. b DSGVO). ○ Sofern eine Offenlegung der personenbezogenen Daten an einen anderen Empfänger beabsichtigt ist: Die Informationen müssen spätestens zum Zeitpunkt dieser Offenlegung erteilt werden (auch wenn die äußerste Frist noch nicht ab-gelaufen ist) (Art. 14. Abs. 3 lit. c DSGVO) ○ Bei der Entscheidung, wann die Bereitstellung der Informationen nach Art. 14 DSGVO erfolgen soll, sind stets die berechtigten Erwartungen der betroffenen Personen (wie ist das Informationsinteresse der betroffenen Person, d. h. wie dringend wird die Information zur Ausübung ihrer Rechte benötigt), die mögliche Wirkung der Verarbeitung auf Letztere und deren Fähigkeit, ihre Rechte in Bezug auf diese Verarbeitung auszuüben, zu berücksichtigen. Die Entscheidungsgründe, warum die Information zu dem konkret ge-wählten Zeitpunkt erteilt wurde, sind durch den Verantwortlichen zu dokumentieren. Im Einklang mit dem Grundsatz von Treu und Glauben sind die Informationen so weit wie möglich frühzeitig vor Ablauf der vorgegebenen Fristen zu erteilen. • Die Informationspflicht nach Art. 14 Abs. 1 – 4 DSGVO findet in folgenden Fällen keine Anwendung, vgl. Art. 14 Abs. 5 DSGVO:

	○ Der Betroffene verfügt bereits über die Informationen. Der Verantwortliche muss hierbei nachweisen, über welche In-formationen bereits verfügt, wie und wann er sie erhalten hat, und diese Informationen in der Zwischenzeit keiner wesentlichen Änderung unterlagen. Nicht wesentliche Änderungen sind beispielsweise Korrekturen von Rechtschreib-fehlern oder stilistischen bzw. grammatikalischen Mängeln. ○ Die Informationserteilung erweist sich als rechtlich oder tatsächlich unmöglich oder erfordert einen unverhältnismäßigen Aufwand. Die Unmöglichkeit der Informationserteilung betrifft insbesondere Fälle, in denen der Verantwortliche den Betroffenen nicht kennt und die Person deshalb nicht informieren kann. Der Verantwortliche muss die Faktoren darlegen, die ihn daran hindern, den Betroffenen die besagten Informationen zu übermitteln. Bei der Bewertung, ob der Aufwand unverhältnismäßig ist, muss der Verantwortliche eine Abwägung zwischen seinem durch die Information entstehenden Aufwand und den Informationsinteressen des Betroffenen vornehmen und das Ergebnis dokumentieren. ○ Es besteht weiterhin keine Informationspflicht, wenn die Verarbeitung für im öffentlichen Interesse liegende Archiv-zwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erfolgt. Voraussetzung dafür ist jedoch, dass die in Art. 89 Abs. 1 DSGVO genannten Bedingungen und Garantien erfüllt sind. Es ist sicherzustellen, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Ebenso kann eine Pseudonymisierung zu den geeigneten Maßnahmen gehören, sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen. • Sofern die Informationen nach Art. 13 und 14 DSGVO wesentlich oder sachlich geändert werden (insbesondere bei Änderung des Verarbeitungszwecks, der Identität des Verantwortlichen, Änderung der Vorgehensweise, wie die betroffenen Personen ihre Rechte bzgl. der Verarbeitung ausüben können, Erweiterung der Kategorien von Empfängern, zukünftige Übermittlung in ein Drittland) sind die betroffenen Personen frühzeitig vor dem tatsächlichen Wirksamwerden über die Änderungen in Kenntnis zu setzen (mindestens 14 Tage vorher). Keine Informationspflicht besteht bei nicht-wesentlichen Änderungen. Nicht wesentliche Änderungen sind beispielsweise Korrekturen von Rechtschreibfehlern oder stilistischen bzw. grammatikalischen Mängeln. Der Verantwortliche muss sicherstellen, dass die Bekanntgabe der Änderungen in einer Art und Weise erfolgt, die sicherstellt, dass die Mehrzahl der Empfänger ihr auch tatsächlich Beachtung schenkt. Im Hinblick auf Änderungen der Informationen nach Art. 13 und 14 DSGVO hat der Verantwortliche Prozesse implementiert und dokumentiert, welche insbesondere Regelungen treffen zu: ○ Vorgaben bzgl. der Prüfung und Erfassung etwaiger Anpassungserfordernisse der Datenschutzinformationen bei Änderungen der Verarbeitungstätigkeiten (Festlegung von Zuständigkeiten, Kommunikationswege, Einbindung des Datenschutzbeauftragten, Dokumentation der

	Anpassungserfordernisse, Sensibilisierung der Beschäftigten ○ Festlegung von Zuständigkeiten für die Vornahme, Freigabe und Veröffentlichung von Änderungen an den Datenschutzinformationen ○ Festlegung wie Bekanntgabe der Änderungen erfolgt ▪ Es muss sichergestellt sein, dass die Mehrzahl der Empfänger die Änderungsmitteilung zur Kenntnis nimmt (z. B. per E-Mail, per klassischem Brief auf Papier, per Pop-up auf einer Webseite oder auf eine andere Art und Weise, welche der betroffenen Person die Änderungen wirksam zur Kenntnis bringt ▪ die Änderungsmitteilung muss separat von anderen Informationen erfolgen ▪ Die Information erfolgt in einer präzisen, transparenten, verständlichen und leicht zugänglichen Form unter der Verwendung einer klaren und einfachen Sprache, vgl. **DS06.01** ▪ Dem Betroffenen werden die möglichen Auswirkungen dieser Änderungen erläutert • Bezüglich der Wahrnehmung von Betroffenenrechten gem. Art. 15 bis 22 DSGVO berücksichtigen die implementierten Prozesse folgende Fristen: ○ Der Verantwortliche stellt der betroffenen Person Informationen über die nach den Artikel 15 bis 22 DSGVO ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags der betroffenen Person zur Verfügung. Ebenso wird eine eventuelle Fristverlängerung um weitere zwei Monate nach Art. 12 Abs. 3 S. 2 und 3 DSGVO in dem Prozess berücksichtigt, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Die betroffene Person wird innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung informiert. Hierfür sind Musterdokumente vorhanden. Sofern der Verantwortliche auf Antrag der betroffenen Person nicht tätig wird, unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen. Hierfür sind ebenfalls Musterdokumente vorhanden. Es sind Zuständigkeiten für die Überwachung der Einhaltung der Fristen dokumentiert. • Jeder Antragseingang sowie die Bearbeitung wird durch den Verantwortlichen dokumentiert Sofern die Pflichten nach Art 12 bis 22 und Art. 34 DSGVO sowie Art. 5 DSGVO seitens des Verantwortlichen gem. Art. 23 DSGVO aufgrund einer Rechtsvorschrift der Union oder Deutschlands nicht erfüllt werden, muss dokumentiert sein, welche Rechtsgrundlage aus dem Unionsrecht oder dem deutschen Recht i. V. m. Art. 23 DSGVO herangezogen wir und inwieweit eine entsprechende Beschränkung der Rechte und Pflichten

	besteht. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt gem. Art. 28 Abs. 3 Satz 2 lit. e DSGVO den Verantwortlichen soweit möglich und im Rahmen seiner Weisungsgebundenheit mit geeigneten technischen und organisatorischen Maßnahmen dabei, der Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person nachzukommen. Die Einzelheiten der vom Auftragsverarbeiter zu leistenden Unterstützung müssen im Auftragsverarbeitungsvertrag oder in einem Anhang zu diesem Vertrag aufgeführt sein. Die Unterstützungsleistung umfasst insbesondere die Bereitstellung von Informationen und Unterlagen, die der Verantwortliche zur Beantwortung von Anträgen heranziehen kann. Im Rahmen der Unterstützungsfunktion benennt der Auftragsverarbeiter eine Ansprechperson für den für die Verarbeitung Verantwortlichen.

[DSGVO] Art. 12 Abs. 3

DS06.02	**A) Verantwortlicher** Der Verantwortliche verfügt über dokumentierte Prozesse zur Bereitstellung von Informationen an den Betroffenen zu den Maßnahmen, die er auf Basis eines Betroffenenantrags gemäß den Art. 15 - 22 DSGVO ergriffen hat. Die Prozesse berücksichtigen insbesondere: • Die Vorgehensweise bzgl. der Prüfung, ob PBD der anfragenden Person verarbeitet werden und die Informationsbereitstellung unter Benennung der jeweiligen beteiligten Stellen muss festgelegt sein. • Sensibilisierung der Beschäftigten bzgl. der Handhabung von Betroffenenanfragen • Abwesenheits- und Vertretungsregelung, um Einhaltung bestehender Fristen gewährleisten zu können, sind etabliert • Zuständigkeiten für die Prüfung der Betroffenenanfrage und Bereitstellung der Informationen und Regelungen für die Kommunikationswege mit den Betroffenen sind klar zu definieren. Bei der Auswahl der Kommunikationswege muss sichergestellt sein, dass eine sichere Übertragung der Daten (z. B. per Ende-zu-Ende-verschlüsselter E-Mail bzw. mithilfe verschlüsselter Dokumente, Nutzung einer Dokumentenaustauschplattform) erfolgt. • Festlegung wie die Kommunikation mit der Betroffenen Person erfolgt: Sofern die betroffene Person, den Antrag in elektronischer Form gestellt hat, erfolgt die Kommunikation nach Möglichkeit auf elektronischem Weg, es sei denn, die Person wünscht einen anderen Kommunikationsweg. ○ Falls es von der betroffenen Person verlangt wird, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde. Der Verantwortliche muss festlegen, wie ein entsprechender Identitätsnachweis erfolgen kann. ○ Der Verantwortliche dokumentiert: das Verlangen nach Information in mündlicher Form, das Verfahren, mit dem ggf.

	die Identität der betroffenen Person überprüft wurde, die Tatsache, dass der betroffenen Person die Information erteilt wurde • Es wird sichergestellt, dass alle Beschäftigten beim Verantwortlichen Betroffenenanfragen, unabhängig vom Eingangskanal, als solche erkennen und der Prozess im Umgang mit solchen Anfragen allen bekannt ist. • Festlegung wie eingehende Betroffenenanfragen dokumentiert werden. • Festlegung wie lange Betroffenenanfragen gespeichert werden und Information der Anfragenden über diese Speicherdauer. • Berücksichtigung der Authentisierung der Betroffene, vgl. **DS06.03**. • Es sind Zuständigkeiten bzgl. der Überwachung der Einhaltung der Bearbeitungsdauer und -qualität festzulegen • Der Prozess muss berücksichtigen, dass sofern keine PBD des Anfragenden verarbeitet werden, eine Negativauskunft erteilt wird, vgl. **DS06.09.**Es muss sichergestellt sein, dass die Ausübung der Rechte durch betroffene Personen die Rechte und Freiheiten anderer Personen nicht beeinträchtigt. Hierfür sind entsprechende Prüfungen etabliert inklusive Festlegung von Zuständigkeiten und Festlegung wie ggf. Unkenntlichmachung bestimmter Informationen erfolgt. Soweit erforderlich erfolgt eine Unkenntlichmachung von Informationen (z. B. Schwärzung) zur Wahrung der Rechte und Freiheiten anderer Personen. • Die implementierten Prozesse berücksichtigen folgende Fristen: ○ Der Verantwortliche stellt der betroffenen Person Informationen über die nach den Artikel 15 bis 22 DSGVO ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags der betroffenen Person zur Verfügung. Ebenso wird eine eventuelle Fristverlängerung um weitere zwei Monate nach Art. 12 Abs. 3 S. 2 und 3 DSGVO in dem Prozess berücksichtigt, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Die betroffene Person wird innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung informiert. Hierfür sind Musterdokumente vorhanden. Sofern der Verantwortliche auf Antrag der betroffenen Person nicht tätig wird, unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen. Hierfür sind ebenfalls Musterdokumente vorhanden. Es sind Zuständigkeiten für die Überwachung der Einhaltung der Fristen dokumentiert. • Jeder Antragseingang sowie die Bearbeitung dessen wird durch den Verantwortlichen dokumentiert. • Die Information des Betroffenen erfolgt in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten, vgl. die

	Anforderungen in **DS06.01.** • Für die Beantwortung der Betroffenenanfrage sind Musterdokumente vorhanden. • Die Information der Betroffenen erfolgt unentgeltlich. Nur im Falle von offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder b) sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche muss in diesen Fällen den Nachweis, für den offenkundig unbegründeten oder exzessiven Charakter des Antrags erbringen. Sofern die Pflichten nach Art. 12 bis 22 DSGVO seitens des Verantwortlichen gem. Art. 23 DSGVO aufgrund einer Rechtsvorschrift der Union oder Deutschlands nicht erfüllt werden, muss dokumentiert sein, welche Rechtsgrundlage aus dem Unionsrecht oder dem deutschen Recht i. V. m. Art. 23 DSGVO herangezogen wir und inwieweit eine entsprechende Beschränkung der Rechte und Pflichten aus Art. 12 bis 22 DSGVO besteht. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt gem. Art. 28 Abs. 3 Satz 2 lit. e DSGVO den Verantwortlichen soweit möglich und im Rahmen seiner Weisungsgebundenheit dabei, den Betroffenen über die auf den Antrag nach Art. 15 – 22 DSGVO hin ergriffenen Maßnahmen zu informieren. Sofern der Antrag des Betroffenen PBD betrifft, auf die der Auftragsverarbeiter nur Zugriff gewähren kann, hält der Auftragsverarbeiter eine Kontaktstelle bereit, die eine Umsetzung des Anliegens gewährleistet. Einzelheiten zur Unterstützungspflicht des Auftragsverarbeiters im Zuge der Bearbeitung von Anträgen nach den Art. 15 – 22 DSGVO ergeben sich aus **DS06.08, DS06.09, DS06.11, DS06.12, DS06.13, DS06.14, DS06.15, DS06.16, DS06.17**. Der Auftragsverarbeiter agiert im Rahmen seiner Befugnisse, die sich aus dem zugrundeliegenden Auftragsverarbeitungsvertrag ergeben. Die vom Verantwortlichen erhaltenen Weisungen und ergriffenen Unterstützungsleistungen dokumentiert der Auftragsverarbeiter. Im Rahmen der Unterstützungsfunktion benennt der Auftragsverarbeiter eine Ansprechperson für den für die Verarbeitung Verantwortlichen.

[DSGVO] Art. 12 insb. Abs. 6

DS06.03	**A) Verantwortlicher** Es sind Prozesse implementiert, die eine sichere und datensparsame **Authentisierung der Betroffenen im Rahmen einer Antragstellung gemäß den Artikeln 15 – 21 DSGVO** ermöglichen. Die Prozesse treffen zumindest Regelungen zu: ▪ Zuständigkeiten für die Vornahme der Authentisierung ▪ Schulung der Beschäftigten im Hinblick auf die Authentisierung von auskunftsberechtigten Personen

	▪ Im Falle von Anfragen Dritter für den Betroffenen: Sicherstellung, der Überprüfung, dass sich die Vollmacht auch auf die Einholung datenschutzrechtlicher Auskünfte bezieht. Hierfür sind entsprechende Arbeitsanweisungen zu dokumentieren. ▪ Bei begründeten Zweifeln an der Identität der natürlichen Person, sind zusätzliche Informationen zur Bestätigung der Identität des Betroffenen anzufordern. Es ist festzulegen, welche zusätzlichen Informationen angefordert werden. ▪ Festlegung der Authentisierungsmethode unter Berücksichtigung des Risikos für die Rechte und Freiheiten der betroffenen Personen (z. B. Abfrage von zusätzlichen Informationen, Übermittlung eines Ausweisdokumentes, Identifizierung über eIDAS-Dienst, Post-/Video-Ident-Identifizierung, Identifizierung über Nutzerkonto) mit entsprechenden Arbeitsanweisungen. Hierbei ist sicherzustellen, dass der Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit. c DSGVO eingehalten wird. ▪ Dokumentation von Art und Datum der Authentisierung des Antragsstellers **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt den Verantwortlichen, sofern möglich und im Rahmen seiner Weisungsgebundenheit, bei einer sicheren und datensparsamen **Authentisierung der Betroffenen** im Rahmen einer Antragstellung gemäß den Artikeln 15 – 21 DSGVO**.** Hierzu leitet der Auftragsverarbeiter etwaige Anträge gemäß den Artikeln 15 – 21 DSGVO an den Verantwortlichen weiter und informiert den Betroffenen hierüber. Sofern der Auftragsverarbeiter per Weisung durch den Verantwortlichen verpflichtet wird, die Authentisierung der Betroffenen im Zuge einer Antragstellung gemäß den Artikeln 15 – 21 DSGVO teilweise oder gänzlich selbst vorzunehmen, muss der Auftragsverarbeiter Prozesse bzgl. der Authentisierung etabliert haben, welche insbesondere Festlegungen treffen zu: Zuständigkeiten für die Vornahme der Authentisierung, Schulung der Beschäftigten im Hinblick auf die Authentisierung von auskunftsberechtigten Personen, Festlegung der Authentisierungsmethode unter Berücksichtigung des Risikos für die Rechte und Freiheiten der betroffenen Personen, Dokumentation von Art und Datum der Authentisierung des Betroffenen. Im Rahmen der Unterstützungsfunktion benennt der Auftragsverarbeiter eine Ansprechperson für den für die Verarbeitung Verantwortlichen.

[DSGVO] Art. 13 Abs. 1, 2, 4

DS06.04	**A) Verantwortlicher** Bei der Erhebung der PBD **direkt beim Betroffenen** werden diesem folgende Informationen vor der Erhebung nach Art. 13 DSGVO mitgeteilt: 1. Namen und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters (Art. 13 Abs. 1 lit. a DSGVO), 2. ggf. Kontaktdaten des Datenschutzbeauftragten (Art. 13 Abs. 1 lit. b DSGVO), 3. Zwecke und Rechtsgrundlage der Verarbeitung (Art. 13 Abs. 1 lit. c DSGVO), 4. ggf. berechtigte Interessen des Verantwortlichen oder eines Dritten (Art. 13 Abs. 1 lit. d DSGVO), 5. ggf. Empfänger oder Kategorien von Empfängern der PBD (Art. 13 Abs. 1 lit. e DSGVO), 6. ggf. die Absicht des Verantwortlichen, die PBD an ein Drittland oder eine internationale Organisation zu übermitteln (Art. 13 Abs. 1 lit. f DSGVO), 7. Dauer der Speicherung der PBD oder, falls nicht möglich, die Kriterien für die Festlegung dieser Dauer (Art. 13 Abs. 2 lit. a DSGVO), 8. Bestehen des Rechts auf Auskunft (Art. 13 Abs. 2 lit. b DSGVO), 9. Bestehen des Rechts auf Berichtigung, Löschung oder Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung (Art. 13 Abs. 2 lit. b DSGVO), 10. Bestehen des Rechts auf Datenübertragbarkeit (Art. 13 Abs. 2 lit. b DSGVO), 11. ggf. Bestehen der Möglichkeit des Widerrufs der Einwilligung (Art. 13 Abs. 2 lit. c DSGVO), 12. Bestehen des Beschwerderechts und Angabe der Aufsichtsbehörde (Art. 13 Abs. 2 lit. d DSGVO), 13. ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte (Art. 13 Abs. 2 lit. e DSGVO), 14. das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person (Art. 13 Abs. 2 lit. f DSGVO). • Die Informationen (Datenschutzinformationen) werden vor der Erhebung der PBD übermittelt, vgl. Art. 13 Abs. 1 DSGVO. • Die Information erfolgt in einer präzisen, transparenten, verständlichen und leicht zugänglichen Form und der Verwendung einer klaren und einfachen Sprache; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten, vgl. **DS06.01** • Die Datenschutzinformationen sind klar von anderen Informationen, die sich nicht auf den Datenschutz beziehen, z. B.

	Vertragsbestimmungen, allgemeine Nutzungsbedingungen, getrennt • Die Information erfolgt in der Landessprache der jeweiligen Zielgruppe, mithin in Deutsch • Sofern das Zielpublikum des Verantwortlichen Kinder sind oder die Waren/Dienstleistungen insbesondere von Kindern genutzt werden, muss die Wortwahl, die Tonalität und der Sprachstil der kindlichen Zielgruppe angepasst sein • Der Verantwortliche stellt die Informationen nach Art. 13 DSGVO den Betroffenen aktiv bereit oder leitet die Betroffenen direkt an die Stelle wo die Informationen zur Verfügung stehen • Der Betroffene hat dauerhaft Zugang zu den Informationen nach Art. 13 DSGVO • Der Verantwortliche erinnert den Betroffenen in regelmäßigen Abständen (mindestens jährlich) an die Datenschutzerklärung/-informationen und wo diese zu finden sind • Es wird ein allgemein geläufiger Begriff, wie z. B. „Datenschutz“, „Datenschutzbestimmungen“, „Datenschutzinformationen“, „Datenschutzhinweis“ verwendet • Bei komplexen, technischen oder unerwarteten Verarbeitungsvorgängen erfolgt, neben der Bereitstellung der nach 14 DSGVO erforderlichen Informationen, gesondert und eindeutig formuliert eine Darlegung der wichtigsten Folgen der Verarbeitung • Verwendung von Mehrebenen-Datenschutzerklärungen/-informationen, die den Betroffenen das direkte Aufrufen bestimmter Punkte ermöglichen, anstatt Darstellung der ge-samten Informationen auf dem Bildschirm in Form eines einzigen Hinweises. • Die Information erfolgt schriftlich oder in anderer Form, ggf. auch elektronisch o Die Bereitstellung kann auch in elektronischer Form erfolgen (z. B. auch kontextbezogene „Just-in-time-Pop-up-Hinweise“, 3D Touch-Hinweise sowie Datenschutz-Dashboards, ggfs. Videos und Smartphone- oder IoT-Sprachmeldungen zusätzlich zu Mehrebenen-Datenschutzerklärungen/ -hinweisen) o Für den Fall, dass eine Webseite betrieben wird: Verwendung von Mehrebenen-Datenschutzerklärungen/-hinweisen, die den Betroffenen das direkte Aufrufen bestimmter Punkte ermöglichen, anstatt Darstellung der gesamten Informationen auf dem Bildschirm in Form eines einzigen Hinweises. Weiterhin ist bei der Verwendung von Mehrebenen-Datenschutzerklärungen/-informationen zu gewährleisten: o Die Informationen nach Art. 13 DSGVO werden auch leicht zugänglich an einem einzigen Ort oder in einem Gesamtdokument (digital oder im Papierformat) zur Verfügung gestellt. o Die Gestaltung und Gliederung der ersten Ebene der Mehrebenen-Datenschutzerklärung/-informationen muss der betroffenen Person einen Gesamtüberblick über die ihr hinsichtlich der Verarbeitung ihrer personenbezogenen Daten zur Verfügung stehenden Informationen liefen und aufzeigen, wo / wie sie die einzelnen Informationen auf den jeweiligen Ebenen der Datenschutzerklärungen / -informationen finden kann. o Die auf den verschiedenen Ebenen eines Mehrebenen-

	Hinweises enthaltenen Informationen sind konsistent und unterscheiden sich nicht in widersprüchlicher Weise von Ebene zu Ebene ○ Die erste Ebene von Mehrebenen-Datenschutzerklärungen / -informationen enthält Informationen zu: Verarbeitungszwecken, die Identität des Verantwortlichen sowie eine Beschreibung der Rechte der betroffenen Person, Angaben über die Verarbeitung, welche sich am stärksten auf die betroffene Person auswirkt, und die Verarbeitungsvorgänge, mit denen die betroffene Person ggfs. nicht rechnet ○ Die vorstehenden Informationen werden der betroffenen Person direkt zum Zeitpunkt der Erhebung der personenbezogenen Daten zur Kenntnis gebracht werden, z. B. durch die Anzeige auf dem Bildschirm, während die betroffene Person ein Online-Formular ausfüllt ○ Im Hinblick auf den Einsatz des Mehrebenen Ansatzes in einer nicht-digitalen Umgebung: Auf der ersten Ebene werden den Betroffenen zumindest folgende Informationen mitgeteilt: Verarbeitungszwecke, die Identität des Verantwortlichen sowie eine Beschreibung der Rechte der betroffenen Person, Angaben über die Verarbeitung, welche sich am stärksten auf die betroffene Person auswirkt, und die Verarbeitungsvorgänge, mit denen die betroffene Person ggfs. nicht rechnet. Es ist festzulegen und zu dokumentieren, wie die Mitteilung der weiteren nach Art. 13 DSGVO erforderlichen Informationen erfolgt ○ Falls es von der betroffenen Person verlangt wird, können die Information gem. den Art. 13 DSGVO mündlich erteilt werden. Der Verantwortliche muss festlegen, wie ein entsprechender Identitätsnachweis erfolgen kann. ▪ Im Fall der mündlichen Bereitstellung der Informationen nach Art. 13 DSGVO mittels Nachrichtenaufzeichnung ermöglicht der Verantwortliche, dass der Betroffene die aufgezeichnete Nachricht mehrmals abhören kann ▪ Der Verantwortliche dokumentiert: das Verlangen nach Information in mündlicher Form, die Tatsache, dass der betroffenen Person die Information erteilt wurde ○ Der Verantwortliche kann die Informationen gem. Art. 13 DSGVO in Kombination mit standardisierten Bildsymbolen bereitstellen ▪ Die verwendeten Bildsymbole müssen standardisiert sein ▪ Die Bildsymbole werden ergänzend zu den ausgeschriebenen Datenschutzinformationen genutzt ▪ Werden die Bildsymbole in elektronsicher Form bereitgestellt, müssen sie maschinenlesbar sein • Die Information erfolgt unentgeltlich, vgl. **DS06.01** Sofern der Betroffene bereits über die oben genannten Informationen verfügt, findet keine der in den Abs. 1–3 geregelten Informationspflichten Anwendung. In diesem Fall trägt der Verantwortliche hierfür die Beweislast und muss darüber Rechenschaft ablegen können, über welche

	Informationen der Betroffene bereits verfügt und wann er diese erhalten hat, und dass diese Informationen in der Zwischenzeit keiner wesentlichen Änderung unterlagen. Nicht wesentliche Änderungen sind beispielsweise Korrekturen von Rechtschreibfehlern oder stilistischen bzw. grammatikalischen Mängeln. Der Verantwortliche informiert betroffene Personen über etwaige Änderungen der Informationen nach den Art. 13 DSGVO. Sofern die Informationen nach Art. 13 wesentlich oder sachlich geändert werden (insbesondere bei Änderung des Verarbeitungszwecks, der Identität des Verantwortlichen, Änderung der Vorgehensweise, wie die betroffenen Personen ihre Rechte bzgl. der Verarbeitung ausüben können, Erweiterung der Kategorien von Empfängern, zukünftige Übermittlung in ein Drittland) werden die betroffenen Personen frühzeitig vor dem tatsächlichen Wirksamwerden über die Änderungen in Kenntnis gesetzt (mindestens 14 Tage vorher). Keine Informationspflicht besteht bei nicht-wesentlichen Änderungen. Nicht wesentliche Änderungen sind beispielsweise Korrekturen von Rechtschreibfehlern oder stilistischen bzw. grammatikalischen Mängeln. Der Verantwortliche muss sicherstellen, dass die Bekanntgabe der Änderungen in einer Art und Weise erfolgt, die sicherstellt, dass die Mehrzahl der Empfänger ihr auch tatsächlich Beachtung schenkt. Im Hinblick auf Änderungen der Informationen nach Art. 13 hat der Verantwortliche Prozesse implementiert und dokumentiert, welche insbesondere Regelungen treffen zu: • Vorgaben bzgl. der Prüfung und Erfassung etwaiger Anpassungserfordernisse der Datenschutzinformationen bei Änderungen der Verarbeitungstätigkeiten (Festlegung von Zuständigkeiten, Kommunikationswege, Einbindung des Datenschutzbeauftragten, Dokumentation der Anpassungserfordernisse, Sensibilisierung der Beschäftigten) • Festlegung von Zuständigkeiten für die Vornahme, Freigabe und Veröffentlichung von Änderungen an den Datenschutzinformationen • Festlegung wie Bekanntgabe der Änderungen erfolgt: ○ Es muss sichergestellt sein, dass die Mehrzahl der Empfänger die Änderungsmitteilung zur Kenntnis nimmt (z. B. per E-Mail, per klassischem Brief auf Papier, per Pop-up auf einer Webseite oder auf eine andere Art und Weise, welche der betroffenen Person die Änderungen wirksam zur Kenntnis bringt ○ die Änderungsmitteilung muss separat von anderen Informationen erfolgen ○ Die Information erfolgt in einer präzisen, transparenten, verständlichen und leicht zugänglichen Form unter der Verwendung einer klaren und einfachen Sprache vgl. **DS06.01** ○ Dem Betroffenen werden die möglichen Auswirkungen dieser Änderungen erläutert **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt gem. Art. 28 Abs. 3 Satz 2 lit. e DSGVO den Verantwortlichen soweit möglich und im Rahmen seiner Weisungsgebundenheit dabei, dass den Betroffenen des IVS die Informationen nach Art. 13 DSGVO mitgeteilt werden können. Hierfür hat der Auftragsverarbeiter dem Verantwortlichen die erforderlichen Informationen zu der Datenverarbeitung im Kontext des IVS zur

	Verfügung zu stellen und im Rahmen seiner Dokumentation nachzuweisen, dass interne Prozesse vorhanden sind, die eine Unterstützung bei der Informationspflicht ermöglichen. Aus der Prozessdokumentation sollte hervorgehen, welche internen Stellen an der Unterstützungspflicht beteiligt sind und als Anlaufstelle für den Verantwortlichen dienen. Der Auftragsverarbeiter sollte erfolgte Unterstützungsleistungen dokumentieren bzw. Nutzeraktionen protokollieren, sofern Weisungen automatisiert umgesetzt werden. Im Rahmen der Unterstützungsfunktion benennt der Auftragsverarbeiter eine Ansprechperson für den für die Verarbeitung Verantwortlichen.

[DSGVO] Art. 14 Abs. 1,2

DS06.05	**A) Verantwortlicher** Werden PBD **nicht direkt beim Betroffenen** erhoben, sind diesem folgende Informationen zur Verfügung zu stellen: 1. Namen und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters (Art. 14 Abs. 1 lit. a DSGVO), 2. Kontaktdaten des Datenschutzbeauftragten (Art. 14 Abs. 1 lit. b DSGVO), 3. Zwecke und Rechtsgrundlage der Verarbeitung (Art. 14 Abs. 1 lit. c DSGVO), 4. Kategorien der PBD, die verarbeitet werden (Art. 14 Abs. 1 lit. d DSGVO), 5. ggf. Empfänger oder Kategorien von Empfängern der PBD (Art. 14 Abs. 1 lit. e DSGVO), 6. ggf. die Absicht des Verantwortlichen, die PBD an ein Drittland oder eine internationale Organisation zu übermitteln (Art. 14 Abs. 1 lit. f DSGVO), 7. Dauer der Speicherung der PBD oder, falls nicht möglich, die Kriterien für die Festlegung dieser Dauer (Art. 14 Abs. lit. a DSGVO), 8. ggf. berechtigte Interessen des Verantwortlichen oder eines Dritten (Art. 14 Abs. 2 lit. b DSGVO), 9. Bestehen des Rechts auf Auskunft (Art. 14 Abs. 2 lit. c DSGVO), 10. Bestehen des Rechts auf Berichtigung, Löschung oder Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung (Art. 14 Abs. 2 lit. c DSGVO), 11. Bestehen des Rechts auf Datenübertragbarkeit (Art. 14 Abs. 2 lit. c DSGVO), 12. ggf. Bestehen der Möglichkeit des Widerrufs der Einwilligung (Art. 14 Abs. 2 lit. d DSGVO), 13. Bestehen des Beschwerderechts und Angabe der Aufsichtsbehörde (Art. 14 Abs. 2 lit. e DSGVO), 14. Quelle der personenbezogenen Daten (Art. 14 Abs. 2 lit. f DSGVO), 15. das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person(Art. 14 Abs. 2 lit. g DSGVO).

	• Die Information erfolgt in einer präzisen, transparenten, verständlichen und leicht zugänglichen Form und der Verwendung einer klaren und einfachen Sprache, dies gilt insbesondere für Informationen, die sich speziell an Kinder richten, vgl. **DS06.01**
	• Die Datenschutzinformationen sind klar von anderen Informationen, die sich nicht auf den Datenschutz beziehen, z. B. Vertragsbestimmungen, allgemeine Nutzungsbedingungen, getrennt
	• Sofern das Zielpublikum des Verantwortlichen Kinder sind oder die Waren/Dienstleistungen insbesondere von Kindern genutzt werden, muss die Wortwahl, die Tonalität und der Sprachstil der kindlichen Zielgruppe angepasst sein
	• Der Verantwortliche stellt die Informationen nach Art. 14 DSGVO den Betroffenen aktiv bereit oder leitet die Betroffenen direkt an die Stelle wo die Informationen zur Verfügung stehen
	• Die Information erfolgt in der Landessprache der jeweiligen Zielgruppe, mithin in Deutsch
	• Der Betroffene hat dauerhaft Zugang zu den Informationen nach Art. 14 DSGVO
	• Der Verantwortliche erinnert den Betroffenen in regelmäßigen Abständen (mindestens jährlich) an die Datenschutzerklärung/-informationen und wo diese zu finden sind
	• Es wird ein allgemein geläufiger Begriff, wie z. B. „Datenschutz“, „Datenschutzbestimmungen“, „Datenschutzinformationen“, „Datenschutzhinweis“ verwendet
	• Bei komplexen, technischen oder unerwarteten Verarbeitungsvorgängen erfolgt, neben der Bereitstellung der nach 14 DSGVO erforderlichen Informationen, gesondert und eindeutig formuliert eine Darlegung der wichtigsten Folgen der Verarbeitung
	• Verwendung von Mehrebenen-Datenschutzerklärungen/-informationen, die den Betroffenen das direkte Aufrufen bestimmter Punkte ermöglichen, anstatt Darstellung der ge-samten Informationen auf dem Bildschirm in Form eines einzigen Hinweises.
	• Die Information erfolgt schriftlich oder in anderer Form, ggf. auch elektronisch
	  ○ Die Bereitstellung kann auch in elektronischer Form erfolgen (z. B. auch kontextbezogene „Just-in-time-Pop-up-Hinweise“, 3D Touch-Hinweise sowie Datenschutz-Dashboards, ggfs. Videos und Smartphone- oder IoT-Sprachmeldungen zusätzlich zu Mehrebenen-Datenschutzerklärungen/ -hinweisen)
	  ○ Für den Fall, dass eine Webseite betrieben wird: Verwendung von Mehrebenen-Datenschutzerklärungen/-hinweisen, die den Betroffenen das direkte Aufrufen bestimmter Punkte ermöglichen, anstatt Darstellung der gesamten Informationen auf dem Bildschirm in Form eines einzigen Hinweises. Weiterhin ist bei der Verwendung von Mehrebenen-Datenschutzerklärungen/-informationen zu gewährleisten:
	  ○ Die Informationen nach Art. 14 DSGVO werden auch leicht zugänglich an einem einzigen Ort oder in einem Gesamtdokument (digital oder im Papierformat) zur Verfügung gestellt.
	  ○ Die Gestaltung und Gliederung der ersten Ebene der Mehrebenen-Datenschutzerklärung/-informationen muss der

	betroffenen Person einen Gesamtüberblick über die ihr hinsichtlich der Verarbeitung ihrer personenbezogenen Daten zur Verfügung stehenden Informationen liefen und aufzeigen, wo / wie sie die einzelnen Informationen auf den jeweiligen Ebenen der Datenschutzerklärungen / -informationen finden kann. ○ Die auf den verschiedenen Ebenen eines Mehrebenen-Hinweises enthaltenen Informationen sind konsistent und unterscheiden sich nicht in widersprüchlicher Weise von Ebene zu Ebene ○ Die erste Ebene von Mehrebenen-Datenschutzerklärungen / -informationen enthält Informationen zu: Verarbeitungszwecken, die Identität des Verantwortlichen sowie eine Beschreibung der Rechte der betroffenen Person, Angaben über die Verarbeitung, welche sich am stärksten auf die betroffene Person auswirkt, und die Verarbeitungsvorgänge, mit denen die betroffene Person ggfs. nicht rechnet ○ Die vorstehenden Informationen werden der betroffenen Person direkt zum Zeitpunkt der Erhebung der personenbezogenen Daten zur Kenntnis gebracht werden, z. B. durch die Anzeige auf dem Bildschirm, während die betroffene Person ein Online-Formular ausfüllt ○ Im Hinblick auf den Einsatz des Mehrebenen Ansatzes in einer nicht-digitalen Umgebung: Auf der ersten Ebene werden den Betroffenen zumindest folgende Informationen mitgeteilt: Verarbeitungszwecke, die Identität des Verantwortlichen sowie eine Beschreibung der Rechte der betroffenen Person, Angaben über die Verarbeitung, welche sich am stärksten auf die betroffene Person auswirkt, und die Verarbeitungsvorgänge, mit denen die betroffene Person ggfs. nicht rechnet. Es ist festzulegen und zu dokumentieren, wie die Mitteilung der weiteren nach Art. 14 DSGVO erforderlichen Informationen erfolgt ○ Falls es von der betroffenen Person verlangt wird, können die Information gem. den Art. 14 DSGVO mündlich erteilt werden. Der Verantwortliche muss festlegen, wie ein entsprechender Identitätsnachweis erfolgen kann. ○ Im Fall der mündlichen Bereitstellung der Informationen nach Art. 14 DSGVO mittels Nachrichtenaufzeichnung ermöglicht der Verantwortliche, dass der Betroffene die aufgezeichnete Nachricht mehrmals abhören kann ○ Der Verantwortliche dokumentiert: das Verlangen nach Information in mündlicher Form, die Tatsache, dass der betroffenen Person die Information erteilt wurde ○ Der Verantwortliche kann die Informationen gem. Art. 14 DSGVO in Kombination mit standardisierten Bildsymbolen bereitstellen ▪ Die verwendeten Bildsymbole müssen standardisiert sein ▪ Die Bildsymbole werden ergänzend zu den ausgeschriebenen Datenschutzinformationen genutzt ▪ Werden die Bildsymbole in elektronsicher Form bereitgestellt, müssen sie maschinenlesbar sein • Die Information erfolgt unentgeltlich, vgl. **DS06.01**

Im Hinblick auf den Zeitpunkt der Information des Betroffenen werden folgende Fristen gem. Art. 14 Abs. 3 DSGVO eingehalten:

- Die vorstehenden Informationen werden dem Betroffenen in einer angemessenen Frist nach Erlangung der personenbezogenen Daten „unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten“, längstens innerhalb eines Monats (= äußerste Frist) mitgeteilt (Art. 14 Abs. 3 lit. a DSGVO). Im Hinblick auf die Frist sind folgende Restriktionen zu beachten und entsprechend muss eine frühere Erteilung der Informationen gewährleistet werden.
    - Sofern die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden: Die Information muss spätestens zum Zeitpunkt der ersten Kommunikation mit der betroffenen Person erteilt werden (auch wenn die äußerste Frist noch nicht abgelaufen ist) (Art. 14 Abs.3 lit. b DSGVO).
    - Sofern eine Offenlegung der personenbezogenen Daten an einen anderen Empfänger beabsichtigt ist: Die Informationen müssen spätestens zum Zeitpunkt dieser Offenlegung erteilt werden (auch wenn die äußerste Frist noch nicht abgelaufen ist) (Art. 14. Abs. 3 lit. c DSGVO)

Bei der Entscheidung, wann die Bereitstellung der Informationen nach Art. 14 DSGVO erfolgen soll, sind stets die berechtigten Erwartungen der betroffenen Personen (wie ist das Informationsinteresse der betroffenen Person, d. h. wie dringend wird die Information zur Ausübung ihrer Rechte benötigt), die mögliche Wirkung der Verarbeitung auf Letztere und deren Fähigkeit, ihre Rechte in Bezug auf diese Verarbeitung auszuüben, zu berücksichtigen. Die Entscheidungsgründe, warum die Information zu dem konkret gewählten Zeitpunkt erteilt wurde, sind durch den Verantwortlichen zu dokumentieren. Im Einklang mit dem Grundsatz von Treu und Glauben sind die Informationen so weit wie möglich frühzeitig vor Ablauf der vorgegebenen Fristen zu erteilen. Die Informationspflicht nach Art. 14 Abs. 1 – 4 DSGVO findet in folgenden Fällen keine Anwendung, vgl. Art. 14 Abs. 5 DSGVO:

- Der Betroffene verfügt bereits über die Informationen. Der Verantwortliche muss hierbei nachweisen, über welche Informationen bereits verfügt, wie und wann er sie erhalten hat, und diese Informationen in der Zwischenzeit keiner wesentlichen Änderung unterlagen. Nicht wesentliche Änderungen sind beispielsweise Korrekturen von Rechtschreibfehlern oder stilistischen bzw. grammatikalischen Mängeln.
- Die Informationserteilung erweist sich als rechtlich oder tatsächlich unmöglich oder erfordert einen unverhältnismäßigen Aufwand. Die Unmöglichkeit der Informationserteilung betrifft insbesondere Fälle, in denen der Verantwortliche den Betroffenen nicht kennt und die Person deshalb nicht informieren kann. Der Verantwortliche muss die Faktoren darlegen, die ihn daran hindern, den Betroffenen die besagten Informationen zu übermitteln. Bei der Bewertung, ob der Aufwand unverhältnismäßig ist, muss der Verantwortliche eine Abwägung zwischen seinem durch die Information entstehenden Aufwand und den Informationsinteressen des Betroffenen vornehmen und das Ergebnis dokumentieren.
- Es besteht weiterhin keine Informationspflicht, wenn die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für

	wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erfolgt. Voraussetzung dafür ist jedoch, dass die in Art. 89 Abs. 1 DSGVO genannten Bedingungen und Garantien erfüllt sind. Es ist sicherzustellen, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Ebenso kann eine Pseudonymisierung zu den geeigneten Maßnahmen gehören, sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen. • Die Erlangung oder Offenlegung der personenbezogenen Daten, über deren Verarbeitung der Betroffene grundsätzlich informiert werden soll, ist durch mitgliedstaatliches Recht oder Unionsrecht ausdrücklich geregelt. • Die Informationen unterliegen nach dem Recht der Mitgliedstaaten oder der Union dem Berufsgeheimnis (z. B. einer nach Gesetz oder Berufsordnung schweigepflichtigen Person, z. B. einem Arzt, Rechtsanwalt oder Steuerberater). Sofern der Verantwortliche eine Ausnahme nach Art. 14 Abs. 5 DSGVO geltend macht, sind die jeweiligen Faktoren, für das Vorliegen eines Ausnahmetatbestandes zu dokumentieren. Sofern die Informationen nach Art. 14 wesentlich oder sachlich geändert werden (insbesondere bei Änderung des Verarbeitungszwecks, der Identität des Verantwortlichen, Änderung der Vorgehensweise, wie die betroffenen Personen ihre Rechte bzgl. der Verarbeitung ausüben können, Erweiterung der Kategorien von Empfängern, zukünftige Übermittlung in ein Drittland) werden die betroffenen Personen frühzeitig vor dem tatsächlichen Wirksamwerden über die Änderungen in Kenntnis gesetzt (mindestens 14 Tage vorher). Keine Informationspflicht besteht bei nicht-wesentlichen Änderungen. Nicht wesentliche Änderungen sind beispielsweise Korrekturen von Rechtschreibfehlern oder stilistischen bzw. grammatikalischen Mängeln. Der Verantwortliche muss sicherstellen, dass die Bekanntgabe der Änderungen in einer Art und Weise erfolgt, die sicherstellt, dass die Mehrzahl der Empfänger ihr auch tatsächlich Beachtung schenkt. Im Hinblick auf Änderungen der Informationen nach Art. 14 DSGVO hat der Verantwortliche Prozesse implementiert und dokumentiert, welche insbesondere Regelungen treffen zu: • Vorgaben bzgl. der Prüfung und Erfassung etwaiger Anpassungs-erfordernisse der Datenschutzinformationen bei Änderungen der Verarbeitungstätigkeiten (Festlegung von Zuständigkeiten, Kommunikationswege, Einbindung des Datenschutzbeauftragten, Dokumentation der Anpassungserfordernisse, Sensibilisierung der Beschäftigten) • Festlegung von Zuständigkeiten für die Vornahme, Freigabe und Veröffentlichung von Änderungen an den Datenschutzinformationen • Festlegung wie Bekanntgabe der Änderungen erfolgt: ○ Es muss sichergestellt sein, dass die Mehrzahl der Empfänger die Änderungsmitteilung zur Kenntnis nimmt (z. B. per E-Mail, per klassischem Brief auf Papier, per Pop-up auf einer Webseite oder auf eine andere Art und Weise, welche der betroffenen Person die Änderungen wirksam zur Kenntnis bringt ○ die Änderungsmitteilung muss separat von anderen Informationen erfolgen

	• Die Information erfolgt in einer präzisen, transparenten, verständlichen und leicht zugänglichen Form unter der Verwendung einer klaren und einfachen Sprache, vgl. **DS06.01** • Dem Betroffenen werden die möglichen Auswirkungen dieser Änderungen erläutert **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt gem. Art. 28 Abs. 3 Satz 2 lit. e DSGVO den Verantwortlichen soweit möglich und im Rahmen seiner Weisungsgebundenheit dabei, dass den Betroffenen die Informationen nach Art. 14 DSGVO mitgeteilt werden können. Hierfür hat der Auftragsverarbeiter dem Verantwortlichen die erforderlichen Informationen zu der Datenverarbeitung im Kontext der IVS zur Verfügung zu stellen und im Rahmen seiner Dokumentation nachzuweisen, dass interne Prozesse vorhanden sind, die eine Unterstützung bei der Informationspflicht ermöglichen. Aus der Prozessdokumentation sollte hervorgehen, welche internen Stellen an der Unterstützungspflicht beteiligt sind und als Anlaufstelle für den Verantwortlichen dienen. Der Auftragsverarbeiter sollte erfolgte Unterstützungsleistungen dokumentieren bzw. Nutzeraktionen protokollieren, sofern Weisungen automatisiert umgesetzt werden. Im Rahmen der Unterstützungsfunktion benennt der Auftragsverarbeiter eine Ansprechperson für den für die Verarbeitung Verantwortlichen.

[DSGVO] Art. 13 Abs. 3, Art. 14 Abs. 4; [BDSG] § 32 Abs. 1, § 33 Abs. 1

DS06.06	**A) Verantwortlicher** Sofern der Verantwortliche beabsichtigt, die PBD für einen anderen Zweck weiterzuverarbeiten als den, für den die PBD erhoben wurden, • stellt er denjenigen Betroffenen, deren PBD zu einem anderen Zweck als dem ursprünglichen Erhebungszweck verarbeitet werden sollen, Informationen nach **DS06.04** bzw. **DS06.05** sowie entsprechende Informationen über den anderen Zweck bereit • dokumentiert eine Abwägung in der er dargelegt, dass die Verarbeitung zu dem anderen Zweck mit demjenigen, zudem die PBD ursprünglich erhoben wurden, vereinbar ist, vgl. Anforderung **DS03.08** **B) Auftragsverarbeiter** Im Falle einer Zweckerweiterung unterstützt der Auftragsverarbeiter den Verantwortlichen gem. Art. 28 Abs. 3 Satz 2 lit. e DSGVO soweit möglich und im Rahmen seiner Weisungsgebundenheit dabei, den Betroffenen über diesen anderen Zweck mit allen maßgeblichen Informationen entsprechend der vorgenannten Kriterien zu informieren. Im Rahmen der Unterstützungsfunktion benennt der Auftragsverarbeiter eine Ansprechperson für den für die Verarbeitung Verantwortlichen.

[DSGVO] Art. 12 Abs. 3, Art. 15 Abs. 1, 2

DS06.07	**A) Verantwortlicher** Der betroffenen Person wird eine Bestätigung erteilt, ob durch den Verantwortlichen sie betreffende personenbezogene Daten verarbeitet werden oder nicht. Gemäß Art. 15 Abs. 1 DSGVO werden folgende Informationen dem Betroffenen mitgeteilt: 1. Namen und Kontaktdaten des Verantwortlichen, 2. Verarbeitungszwecke (Art. 15 Abs. 1 lit. a DSGVO), 3. Kategorien der verarbeiteten personenbezogenen Daten (Art. 15 Abs. 1 lit. b DSGVO), 4. Empfänger bzw. Kategorien von Empfängern der PBD (Art. 15 Abs. 1 lit. c DSGVO), 5. Dauer der Speicherung der PBD oder, falls nicht möglich, die Kriterien für die Festlegung dieser Dauer (Art. 15 Abs. 1 lit. d DSGVO), 6. das Bestehen des Rechts auf Berichtigung und Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung (Art. 15 Abs. 1 lit. e DSGVO), 7. das Bestehen des Beschwerderechts bei der Aufsichtsbehörde (Art. 15 Abs. 1 lit. f DSGVO), 8. wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten (Art. 15 Abs. 1 lit. g DSGVO), 9. das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person (Art. 15 Abs. 1 lit. h DSGVO). • Werden keine PBD zu einer anfragenden Person verarbeitet, muss der Verantwortliche ihn hierüber ebenfalls informieren (vgl. **DS06.09**) • Die Information erfolgt in einer präzisen, transparenten, verständlichen und leicht zugänglichen Form und der Verwendung einer klaren und einfachen Sprache, dies gilt insbesondere für Informationen, die sich speziell an Kinder richten, vgl. die Anforderungen, vgl. **DS06.01** • Für die Beantwortung der Betroffenenanfrage sind Musterdokumente vorhanden. • Die Information der Betroffenen erfolgt unentgeltlich. Nur im Falle von offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder b) sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche muss in diesen Fällen den Nachweis, für den offenkundig unbegründeten oder exzessiven Charakter des Antrags erbringen. • Sofern die betroffene Person, den Antrag in elektronischer Form

gestellt hat, erfolgt die Kommunikation nach Möglichkeit auf elektronischem Weg, es sei denn, die Person wünscht einen anderen Kommunikationsweg.

  - Falls es von der betroffenen Person verlangt wird, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde. Der Verantwortliche muss festlegen, wie ein entsprechender Identitätsnachweis erfolgen kann.
  - Der Verantwortliche dokumentiert: das Verlangen nach Information in mündlicher Form, das Verfahren, mit dem ggf. die Identität der betroffenen Person überprüft wurde, die Tatsache, dass der betroffenen Person die Information erteilt wurde

- Der Verantwortliche stellt der betroffenen Person die Informationen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags der betroffenen Person zur Verfügung. Im Hinblick auf eine etwaige Fristverlängerung um weitere zwei Monate nach Art. 12 Abs. 3 S. 2 und 3 DSGVO, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist, wird sichergestellt, dass die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung, informiert wird. Hierfür sind Musterdokumente vorhanden. Sofern der Verantwortliche auf Antrag der betroffenen Person nicht tätig wird, unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen. Hierfür sind ebenfalls Musterdokumente vorhanden. Es sind Zuständigkeiten für die Überwachung der Einhaltung der Fristen dokumentiert.
- Jeder Antragseingang sowie die Bearbeitung wird durch den Verantwortlichen dokumentiert.

Sofern die Pflichten nach Art. 15 DSGVO seitens des Verantwortlichen gem. Art. 23 DSGVO aufgrund einer Rechtsvorschrift der Union oder Deutschlands nicht erfüllt werden, muss dokumentiert sein, welche Rechtsgrundlage aus dem Unionsrecht oder dem deutschen Recht i. V. m. Art. 23 DSGVO herangezogen wir und inwieweit eine entsprechende Beschränkung der Rechte und Pflichten aus Art. 15 DSGVO besteht.

B) Auftragsverarbeiter

Der Auftragsverarbeiter unterstützt den Verantwortlichen gem. Art. 28 Abs. 3 Satz 2 lit. e DSGVO soweit möglich und im Rahmen seiner Weisungsgebundenheit dabei, gegenüber Betroffenen die Auskunft über die PBDV entsprechend Art. 15 Abs. 1 DSGVO zu erteilen. Hierzu leitet der Auftragsverarbeiter etwaige Anträge gemäß den Artikeln 15 – 21 DSGVO an den Verantwortlichen weiter und informiert den Betroffenen hierüber.

Der Service erleichtert den Verantwortlichen die Einhaltung der Verpflichtung, den Betroffenen Zugang zu ihren PBD gem. obenstehender Informationen zu gewähren. Die Unterstützungspflicht kann dadurch erfüllt werden, dass der Auftragsverarbeiter die Zusammenstellung der personenbezogenen Daten, die vom Verantwortlichen gem. Art. 15 DSGVO zu beauskunften sind, technisch ermöglicht z. B. Extrahierungsmöglichkeit, Oberfläche zur Verwaltung der personenbezogenen Daten.

	Im Rahmen der Unterstützungsfunktion benennt der Auftragsverarbeiter eine Ansprechperson für den für die Verarbeitung Verantwortlichen.

[DSGVO] Art. 15 Abs. 3

DS06.08	**A) Verantwortlicher** Es ist ein Prozess vorhanden, der die Bereitstellung einer **Kopie der gespeicherten PBD** an Betroffene unterstützt. Der Prozess regelt mindestens: 1. definierte Zuständigkeiten inklusive Fristen und Kommunikationswege im Hinblick auf die Erstellung und Bereitstellung der Kopie der PBD 2. Sicherstellung der Vollständigkeit, Originaltreue und Verständlichkeit der Kopie der PBD 3. Festlegung wie Bereitstellung der Kopie der PBD erfolgt, z. B. durch gesicherten Zugang. Hierbei sind folgende Anforderungen umzusetzen: - Bereitstellung der Kopie der Daten in einer konkreten, dauerhaften Form (Text, elektronisch), sodass die Person sie leicht herunterladen kann. - Der betroffenen Person ist eine originalgetreue und verständliche Reproduktion der PBD auszuhändigen. Die Auflistung der PBD in aggregierter Form ist nicht ausreichend, sofern der Kontext der Datenverarbeitung nicht ersichtlich wird. Der betroffenen Person sind Auszüge aus Dokumenten oder ganzen Dokumenten sowie Auszüge aus Datenbanken, die die PBD enthalten, zur Verfügung zu stellen, wenn dies notwendig ist, um ihre Betroffenenrechte wirksam ausüben zu können, insbesondere wenn Daten aus anderen Daten generiert werden oder wenn sie auf freien Feldern beruhen und die Zurverfügungstellung einer solchen Kopie erforderlich ist, um der betroffenen Person die Überprüfung der Richtigkeit und Vollständigkeit der Daten zu ermöglichen und die Verständlichkeit der Daten zu gewährleisten. Dabei sind die Rechte und Freiheiten anderer Personen zu berücksichtigen (vgl. Nr. 4). Der Verantwortliche muss Prozesse im Hinblick auf die Überprüfung des Umfangs der herauszugebenden Daten festgelegt haben (Verantwortlichkeiten bzgl. Prüfung von Erforderlichkeit und Umfang der Zurverfügungstellung einer Kopie der Dokumente sowie Auszüge aus Datenbanken, Sensibilisierung der Beschäftigten bzgl. der Bereitstellung der Kopie der PBD).Sofern die betroffene Person den Antrag elektronisch stellt, sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt. - Schriftliche Informationen, auch in elektronischer Form, sind anderen Formen vorzuziehen. - Das Format muss eine verständliche und leicht zugängliche Darstellung der Informationen ermöglichen. - Im Fall der elektronischen/digitalen Übermittlung muss die betroffene Person in der Lage sein, ihre Daten in einem gängigen elektronischen Format herunterzuladen. - Eine sichere Übertragung der Daten (z. B. per Ende-zu-Ende-verschlüsselter E-Mail bzw. mithilfe verschlüsselter Dokumente, Nutzung einer Dokumentenaustauschplattform) muss

	sichergestellt sein. 4. Überprüfung, dass durch die Datenkopie die Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden, ggf. Vornahme von Schwärzungen 5. Kostenlose Bereitstellung der ersten Kopie der PBD Der Verantwortliche stellt der betroffenen Person die Informationen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags der betroffenen Person zur Verfügung. Im Hinblick auf ei-ne etwaige Fristverlängerung um weitere zwei Monate nach Art. 12 Abs. 3 S. 2 und 3 DSGVO, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist, wird sicher-gestellt, dass die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung, informiert wird. Hierfür sind Musterdokumente vorhanden. Sofern der Verantwortliche auf Antrag der betroffenen Person nicht tätig wird, unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechts-behelf einzulegen. Hierfür sind ebenfalls Musterdokumente vorhanden. Es sind Zuständigkeiten für die Überwachung der Einhaltung der Fristen dokumentiert. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt den Verantwortlichen gem. Art. 28 Abs. 3 Satz 2 lit. e DSGVO bei der Erfüllung von Betroffenenrechten im Rahmen seiner Weisungsgebundenheit. Hierzu leitet der Auftragsverarbeiter etwaige Anträge auf Bereitstellung einer Kopie an den Verantwortlichen weiter und informiert den Betroffenen hierüber. Zudem kann die Unterstützungspflicht dadurch erfüllt werden, dass der Auftragsverarbeiter die Bereitstellung von Kopien technisch ermöglicht, z. B. durch Implementierung einer Extrahierungsmöglichkeit. Im Rahmen der Unterstützungsfunktion benennt der Auftragsverarbeiter eine Ansprechperson für den für die Verarbeitung Verantwortlichen.

[DSGVO] Art. 15 Abs. 1, [BDSG] § 34

DS06.09	**A) Verantwortlicher**
	Der Verantwortliche verfügt über einen Prozess, der potenziell Betroffene darüber informiert, dass keine personenbezogenen Daten verarbeitet werden (sog. Negativauskunft).
	Der Prozess trifft insbesondere Festlegungen zu:
	• Zuständigkeiten im Hinblick auf die Erteilung der Negativauskunft
	• Sofern die betroffene Person, den Antrag in elektronischer Form gestellt hat, erfolgt die Kommunikation nach Möglichkeit auf elektronischem Weg, es sei denn, die Person wünscht einen anderen Kommunikationsweg.
	  ○ Falls es von der betroffenen Person verlangt wird, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde. Der Verantwortliche muss festlegen, wie ein entsprechender Identitätsnachweis erfolgen kann.
	  ○ Der Verantwortliche dokumentiert: das Verlangen nach Information in mündlicher Form, das Verfahren, mit dem ggf. die Identität der betroffenen Person überprüft wurde, die Tatsache, dass der betroffenen Person die Information erteilt wurde
	• Festlegung wie Erteilung der Negativauskunft erfolgt. Eine sichere Übertragung der Daten (z. B. per Ende-zu-Ende-verschlüsselter E-Mail bzw. mithilfe verschlüsselter Dokumente, Nutzung einer Dokumentenaustauschplattform) muss sichergestellt sein.
	• Werden personenbezogene Daten zu einem Betroffenen verarbeitet, sind die Informationen gem. Art. 15 Abs. 1 DSGVO zu erteilen (vgl. DS06.07).
	• Der Verantwortliche stellt der betroffenen Person die Informationen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags der betroffenen Person zur Verfügung. Im Hinblick auf eine etwaige Fristverlängerung um weitere zwei Monate nach Art. 12 Abs. 3 S. 2 und 3 DSGVO, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist, wird sichergestellt, dass die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung, informiert wird. Hierfür sind Musterdokumente vorhanden. Sofern der Verantwortliche auf Antrag der betroffenen Person nicht tätig wird, unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen. Hierfür sind ebenfalls Musterdokumente vorhanden. Es sind Zuständigkeiten für die Überwachung der Einhaltung der Fristen dokumentiert.
	• Die Information des Betroffenen erfolgt in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten, vgl. die Anforderungen in DS06.01.
	• Jeder Antragseingang sowie die Bearbeitung wird durch den Verantwortlichen dokumentiert.
	• Für die Beantwortung der Betroffenenanfrage sind Musterdokumente vorhanden.

	• Die Information der Betroffenen erfolgt unentgeltlich. Nur im Falle von offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder b) sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche muss in diesen Fällen den Nachweis, für den offenkundig unbegründeten oder exzessiven Charakter des Antrags erbringen. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt den Verantwortlichen gem. Art. 28 Abs. 3 Satz 2 lit. e DSGVO soweit möglich und im Rahmen seiner Weisungsgebundenheit bei der Erteilung der Information gegenüber einem potenziellen Betroffenen, dass keine personenbezogenen Daten verarbeitet werden (sog. Negativauskunft). Im Rahmen der Unterstützungsfunktion benennt der Auftragsverarbeiter eine Ansprechperson für den für die Verarbeitung Verantwortlichen.

[BDSG] § 34 Abs. 2

DS06.10	**Verantwortlicher** Die **zum Zweck der Auskunftserteilung an die betroffene Person und zu deren Vorbereitung gespeicherten Daten** dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verarbeitet werden; für andere Zwecke ist die Verarbeitung nach Maßgabe des Art. 18 DSGVO einzuschränken. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. 16, Art. 17, Art. 18, Art. 19

DS06.11	**A) Verantwortlicher** Es ist ein Prozess zur Annahme und Verarbeitung von **Berichtigungs-, Lösch- und Einschränkungsanträgen** der Betroffenen vorhanden. Der Prozess zur Berichtigung, Löschung und Einschränkung der Verarbeitung der verarbeiteten PBD beinhaltet: 1. Prozesse zur Authentisierung von Betroffenen, 2. Der Verantwortliche muss Prozesse bzgl. der Identitätsprüfung des Betroffenen etabliert und dokumentiert haben (Authentifizierung), vgl. die Anforderungen in **DS06.03** 3. definierte Zuständigkeiten inklusive Fristen und Kommunikationswege für die durchzuführenden Vorgänge, 4. Abwesenheits- und Vertretungsregelung, um Einhaltung bestehender Fristen gewährleisten zu können, sind etabliert 5. Sensibilisierung der Beschäftigten bzgl. der Handhabung von Berichtigungs-, Lösch- und Einschränkungsanträgen 6. Mitteilung gem. Art. 19 DSGVO an alle Empfänger, denen personenbezogene Daten offengelegt wurden, über jede Berichtigung oder Löschung

	der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach Art. 16 DSGVO, Art. 17 Abs.1 DSGVO und Art. 18 DSGVO, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden., 7. Berücksichtigung von eventuellen Veröffentlichungen der Daten, 8. korrekte Berücksichtigung der Maßgaben und Ausnahmen zur Löschung entsprechend Art. 17 Abs. 1 und 3, 9. sichere technische Umsetzung unter Berücksichtigung a) der Irreversibilität von Löschungen, b) Einbeziehung von Backups in die Vorgänge, 10. Unterrichtung der betroffenen Person über Empfänger, denen personenbezogenen Daten offengelegt wurden, wenn die betroffene Person dies verlangt. • Für die Beantwortung der Betroffenenanfrage sind Musterdokumente vorhanden. • Die Bearbeitung des Antrags und Information der Betroffenen Information der Betroffenen erfolgt unentgeltlich. Nur im Falle von offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder b) sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche muss in diesen Fällen den Nachweis, für den offenkundig unbegründeten oder exzessiven Charakter des Antrags erbringen. • Sofern die betroffene Person, den Antrag in elektronischer Form gestellt hat, erfolgt die Kommunikation nach Möglichkeit auf elektronischem Weg, es sei denn, die Person wünscht einen anderen Kommunikationsweg. ○ Falls es von der betroffenen Person verlangt wird, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde. Der Verantwortliche muss festlegen, wie ein entsprechender Identitätsnachweis erfolgen kann. ○ Der Verantwortliche dokumentiert: das Verlangen nach Information in mündlicher Form, das Verfahren, mit dem ggf. die Identität der betroffenen Person überprüft wurde, die Tatsache, dass der betroffenen Person die Information erteilt wurde • Der Verantwortliche informiert den Betroffenen über getroffene Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags der betroffenen Person zur Verfügung. Im Hinblick auf eine etwaige Fristverlängerung um weitere zwei Monate nach Art. 12 Abs. 3 S. 2 und 3 DSGVO, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist, wird sichergestellt, dass die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung, informiert wird. Hierfür sind Musterdokumente vorhanden. Sofern der Verantwortliche auf Antrag der betroffenen Person nicht tätig wird, unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach

	Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen. Hierfür sind ebenfalls Musterdokumente vorhanden. Es sind Zuständigkeiten für die Überwachung der Einhaltung der Fristen dokumentiert. • Die Information des Betroffenen erfolgt in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten, vgl. **DS06.01.** • Jeder Antragseingang sowie die Bearbeitung dessen wird durch den Verantwortlichen dokumentiert. Sofern die Pflichten nach Art 16, 17, 18 DSGVO seitens des Verantwortlichen gem. Art. 23 DSGVO aufgrund einer Rechtsvorschrift der Union oder Deutschlands nicht erfüllt werden, muss dokumentiert sein, welche Rechtsgrundlage aus dem Unionsrecht oder dem deutschen Recht i. V. m. Art. 23 DSGVO herangezogen wir und inwieweit eine entsprechende Beschränkung der Rechte und Pflichten aus Art. 16, 17, 18 DSGVO besteht. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt den Verantwortlichen gem. Art. 28 Abs. 3 Satz 2 lit. e DSGVO soweit möglich und im Rahmen seiner Weisungsgebundenheit bei der Bearbeitung von **Berichtigungs-, Lösch- und Einschränkungsanträgen.** Die entsprechenden Weisungen sind zu dokumentieren. Hierzu leitet der Auftragsverarbeiter etwaige Berichtigungs-, Lösch- und Einschränkungsanträge an den Verantwortlichen weiter und informiert den Betroffenen hierüber. Sofern die Löschung, Berichtigung oder Einschränkung der Verarbeitung durch den Verantwortlichen nicht selbst möglich ist, benennt der Auftragsverarbeiter eine Ansprechperson, die die Umsetzung vornehmen kann, vgl. die Anforderungen in **DS06.12, DS06.13**. Im Rahmen der Unterstützungsfunktion benennt der Auftragsverarbeiter eine Ansprechperson für den für die Verarbeitung Verantwortlichen.

[DSGVO] Art. 17

DS06.12	**A) Verantwortlicher** Der Verantwortliche löscht die personenbezogenen Daten auf Verlangen des jeweiligen Betroffenen. Hierfür ist ein Löschkonzept, z. B. nach DIN 66398-2016, dokumentiert, welches insbesondere regelt: ▪ Anwendungsbereich des Löschkonzeptes (z. B. welche IT-Systeme und Datenbestände) ▪ Festlegung von Löschfristen ▪ Festlegung und konkrete Beschreibung von Löschmechanismen (Dokumentation der einzelnen Vorgänge bzw. Umsetzungsvorgaben) - Bei der Festlegung der Mindestanforderungen an Verfahren zur Löschung sind die Vorgaben des IT-Grundschutzkompendiums CON.6 Löschen und Vernichten umzusetzen ▪ Festlegung von Zuständigkeiten und Meldewege bzgl. der Vornahme von Löschungen ▪ Sofern ein Auftragsverarbeiter durch den Verantwortlichen eingesetzt

	wird: Darlegung inwieweit Löschpflichten durch den Auftragsverarbeiter zu erfüllen sind ▪ Zuständigkeiten bzgl. der Überwachung der Löschprozesse ▪ Überprüfung der tatsächlichen Umsetzung bzw. Wirksamkeit der Löschung ▪ Festlegung wie Durchführung von Löschungsmaßnahmen dokumentiert werden ▪ Berücksichtigung der Datenlöschung in Backups und Archiven ▪ Regelmäßige Evaluierung (mindestens jährlich), ob die gewählten Löschmechanismen noch dem Stand der Technik entsprechen Es muss sichergestellt sein, dass Löschungen durchgeführt werden können, ohne die Integrität des verbleibenden Datenbestandes zu beinträchtigen. Eine Ausnahme von der Löschpflicht besteht für den Verantwortlichen, sofern die Verarbeitung zu einem der in Art. 17 Abs. 3 DSGVO dargelegten Gründen erforderlich ist. Der Verantwortliche hat im Falle einer Ausnahme von der Löschpflicht darzulegen, aus welchem der in Art. 17 Abs. 3 DSGVO benannten Gründen keine Löschung von personenbezogenen Daten erfolgt. Sofern Betroffene eine Löschung ihrer Daten selbständig vornehmen können, stellt der Verantwortliche eine entsprechende Information zur Verfügung. • Der Verantwortliche informiert den Betroffenen über getroffene Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags. Im Hinblick auf eine etwaige Fristverlängerung um weitere zwei Monate nach Art. 12 Abs. 3 S. 2 und 3 DSGVO, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist, wird sichergestellt, dass die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung, informiert wird. Hierfür sind Musterdokumente vorhanden. Sofern der Verantwortliche auf Antrag der betroffenen Person nicht tätig wird, unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen. Hierfür sind ebenfalls Musterdokumente vorhanden. Es sind Zuständigkeiten für die Überwachung der Einhaltung der Fristen dokumentiert. • Die Bearbeitung des Antrags und Information der Betroffenen erfolgt unentgeltlich. Nur im Falle von offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder b) sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche muss in diesen Fällen den Nachweis, für den offenkundig unbegründeten oder exzessiven Charakter des Antrags erbringen. • Sofern die betroffene Person, den Antrag in elektronischer Form gestellt hat, erfolgt die Kommunikation nach Möglichkeit auf elektronischem Weg, es sei denn, die Person wünscht einen anderen Kommunikationsweg.

	○ Falls es von der betroffenen Person verlangt wird, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde. Der Verantwortliche muss festlegen, wie ein entsprechender Identitätsnachweis erfolgen kann. ○ Der Verantwortliche dokumentiert: das Verlangen nach Information in mündlicher Form, das Verfahren, mit dem ggf. die Identität der betroffenen Person überprüft wurde, die Tatsache, dass der betroffenen Person die Information erteilt wurde • Die Information des Betroffenen erfolgt in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten, vgl. **DS06.01.** • Jeder Antragseingang sowie die Bearbeitung dessen wird durch den Verantwortlichen dokumentiert. Sofern die Pflichten nach Art 17 DSGVO seitens des Verantwortlichen gem. Art. 23 DSGVO aufgrund einer Rechtsvorschrift der Union oder Deutschlands nicht erfüllt werden, muss dokumentiert sein, welche Rechtsgrundlage aus dem Unionsrecht oder dem deutschen Recht i. V. m. Art. 23 DSGVO herangezogen wir und inwieweit eine entsprechende Beschränkung der Rechte und Pflichten aus Art. 17 DSGVO besteht. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt den Verantwortlichen gem. Art. 28 Abs. 3 Satz 2 lit. e DSGVO im Rahmen seiner Weisungsgebundenheit soweit möglich bei der Löschung gespeicherter PBD. Die entsprechenden Weisungen sind zu dokumentieren. Der Auftragsverarbeiter leitet etwaige Löschanträge an den Verantwortlichen weiter und informiert den Betroffenen hierüber. Zudem kann eine Unterstützungspflicht auch dadurch erfüllt werden, dass der Verantwortliche durch technische Maßnahmen in die Lage versetzt wird, die Daten direkt zu löschen. Sofern die Löschung durch den Verantwortlichen nicht selbst möglich ist, benennt der Auftragsverarbeiter eine Ansprechperson für den für die Verarbeitung Verantwortlichen, die die Umsetzung der Löschung umsetzen kann. Hierfür sind entsprechende Prozesse etabliert, welche insbesondere Festlegungen trifft zu: Zuständigkeiten und Meldewege bzgl. der Vornahme von Löschungen, Löschmechanismen inklusive Dokumentation der einzelnen Vorgänge bzw. Umsetzungsvorgaben (bei der Festlegung der Mindestanforderungen an Verfahren zur Löschung sind die Vorgaben des BSI IT-Grundschutzkompendiums CON.6 Löschen und Vernichten umzusetzen), Zuständigkeiten bzgl. der Überwachung der Löschprozesse, Überprüfung der tatsächlichen Umsetzung bzw. Wirksamkeit der Löschung, Festlegung wie Durchführung von Löschungsmaßnahmen dokumentiert werden, Berücksichtigung der Datenlöschung in Backups und Archiven, regelmäßige Evaluierung (mindestens jährlich), ob die gewählten Löschmechanismen noch dem Stand der Technik entsprechen. Im Rahmen der Unterstützungsfunktion benennt der Auftragsverarbeiter eine Ansprechperson für den für die Verarbeitung Verantwortlichen. Sofern Betroffene eine Löschung ihrer Daten selbständig vornehmen können, unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erstellung einer entsprechenden Beschreibung zum Vorgehen, die dem Betroffenen zur Verfügung gestellt wird.

[DSGVO] Art. 18

DS06.13	**A) Verantwortlicher** Der Verantwortliche nimmt eine Einschränkung der Verarbeitung von PBD auf Verlangen des jeweiligen Betroffenen vor. Der Verantwortliche prüft hierbei zunächst, ob eine der folgenden Voraussetzungen erfüllt ist: a. der Betroffene bestreitet die Richtigkeit der vom Verantwortlichen verarbeiteten PBD b. der Betroffene verlangt statt der Löschung eine Einschränkung der Verarbeitung aufgrund einer unrechtmäßigen Verarbeitung c. der Betroffene benötigt die PBD zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen d. der Betroffene hat einer Verarbeitung gem. Art. 21 Abs. 1 DSGVO widersprochen und es erfolgt eine Prüfung, ob berechtigte Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen. Die Einschränkung erfolgt durch 1. Vermerk der Gründe zur Einschränkung der Verarbeitung (s. Art. 18 Abs. 1 DSGVO), 2. Kennzeichnung von Datensätzen, 3. abweichende Verarbeitungsoptionen für entsprechend gekennzeichnete Datensätze im IVS, 4. Protokollierung der vorgenommenen Kennzeichnungen. • Der Verantwortliche informiert den Betroffenen über getroffene Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags. Im Hinblick auf eine etwaige Fristverlängerung um weitere zwei Monate nach Art. 12 Abs. 3 S. 2 und 3 DSGVO, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist, wird sichergestellt, dass die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung, informiert wird. Hierfür sind Musterdokumente vorhanden. Sofern der Verantwortliche auf Antrag der betroffenen Person nicht tätig wird, unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen. Hierfür sind ebenfalls Musterdokumente vorhanden. Es sind Zuständigkeiten für die Überwachung der Einhaltung der Fristen dokumentiert. • Die Bearbeitung des Antrags und Information der Betroffenen erfolgt unentgeltlich. Nur im Falle von offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder b) sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche muss in diesen Fällen den Nachweis, für den offenkundig unbegründeten oder exzessiven Charakter des Antrags erbringen. • Sofern die betroffene Person, den Antrag in elektronischer Form gestellt hat, erfolgt die Kommunikation nach Möglichkeit auf elektronischem Weg, es sei denn, die Person wünscht einen anderen

	Kommunikationsweg. ○ Falls es von der betroffenen Person verlangt wird, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde. Der Verantwortliche muss festlegen, wie ein entsprechender Identitätsnachweis erfolgen kann. ○ Der Verantwortliche dokumentiert: das Verlangen nach Information in mündlicher Form, das Verfahren, mit dem ggf. die Identität der betroffenen Person überprüft wurde, die Tatsache, dass der betroffenen Person die Information erteilt wurde • Jeder Antragseingang sowie die Bearbeitung dessen wird durch den Verantwortlichen dokumentiert. Sofern die Pflichten nach Art 18 DSGVO seitens des Verantwortlichen gem. Art. 23 DSGVO aufgrund einer Rechtsvorschrift der Union oder Deutschlands nicht erfüllt werden, muss dokumentiert sein, welche Rechtsgrundlage aus dem Unionsrecht oder dem deutschen Recht i. V. m. Art. 23 DSGVO herangezogen wir und inwieweit eine entsprechende Beschränkung der Rechte und Pflichten aus Art. 18 DSGVO besteht. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt den Verantwortlichen gem. Art. 28 Abs. 3 Satz 2 lit. e DSGVO im Rahmen seiner Weisungsgebundenheit soweit möglich bei der Einschränkung der Verarbeitung der PBD. Die entsprechenden Weisungen sind zu dokumentieren. In der Dokumentation zum Evaluierungsgegenstand beschreibt der Auftragsverarbeiter, wie die Verarbeitung von PBD eingeschränkt werden kann. Der Auftragsverarbeiter leitet etwaige Anträge zur Einschränkung der Verarbeitung PBD an den Verantwortlichen weiter und informiert den Betroffenen hierüber. Zudem kann eine Unterstützungspflicht auch dadurch erfüllt werden, dass der Verantwortliche durch technische Maßnahmen in die Lage versetzt wird, die Verarbeitung der Daten einzuschränken. Sofern die Einschränkung der Verarbeitung durch den Verantwortlichen nicht selbst möglich ist, benennt der Auftragsverarbeiter eine Ansprechperson für den für die Verarbeitung Verantwortlichen, die die Einschränkung der Verarbeitung vornehmen kann. Im Rahmen der Unterstützungsfunktion benennt der Auftragsverarbeiter eine Ansprechperson für den für die Verarbeitung Verantwortlichen.

[DSGVO] Art. 20

DS06.14	**A) Verantwortlicher** Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem **strukturierten, gängigen und maschinenlesbaren Format** zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern die Verarbeitung der PBD auf einer Einwilligung gem. Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a oder auf einem Vertrag gem. Art. 6 Abs. 1 lit. b DSGVO beruht und die

	Verarbeitung mithilfe automatisierter Verfahren erfolgt. . Hierfür hat der Verantwortliche Prozesse implementiert, welche mindestens regeln: 1. definierte Zuständigkeiten inklusive Fristen und Kommunikationswege im Hinblick auf die Bearbeitung von Anfragen zur Datenübertragbarkeit 2. Abwesenheits- und Vertretungsregelung, um Einhaltung bestehender Fristen gewährleisten zu können, sind etabliert 3. Sensibilisierung der Beschäftigten bzgl. der Handhabung von Anfragen bzgl. der Datenübertragbarkeit 4. Bei der Umsetzung des Rechts auf Datenübertragbarkeit muss der Verantwortliche folgende Voraussetzungen prüfen – die Prüfschritte sind zu dokumentieren: a) Der Betroffene muss seine PBD dem Verantwortlichen bereitgestellt haben. Die folgenden Datenkategorien können als „von der betroffenen Person bereitgestellt“ betrachtet werden: ○ aktiv und willentlich von dem Betroffenen bereitgestellte Date ○ Beobachtete Daten, die von dem Betroffenen durch die Nutzung des IVS bereitgestellt werden b) Die an den Verantwortlichen bereitgestellten PBD müssen sich auf den Betroffenen selbst beziehen c) Die Verarbeitung durch den Verantwortlichen erfolgt auf Basis einer Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO oder Art. 9 Abs. 2 lit. a DSGVO oder auf einem Vertrag gemäß Art. 6 Abs.1 lit. b DSGVO d) Die Verarbeitung der PBD erfolgt mithilfe automatisierter Verfahren e) Es handelt sich um keine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde 5. Prüfung der Identität der anfragenden Person (Authentifizierung), vgl. die Anforderungen in **DS06.03** 6. Der Prozess berücksichtigt folgende Fristen: Der Verantwortliche stellt der betroffenen Person die PBD unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags der betroffenen Person zur Verfügung. Ebenso wird eine eventuelle Fristverlängerung um weitere zwei Monate nach Art. 12 Abs. 3 S. 2 und 3 DSGVO in dem Prozess berücksichtigt, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Die betroffene Person wird innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung informiert. Hierfür sind Musterdokumente vorhanden. Sofern der Verantwortliche auf Antrag der betroffenen Person nicht tätig wird, unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen. Hierfür sind ebenfalls Musterdokumente vorhanden. Es sind Zuständigkeiten für die Überwachung der Einhaltung der Fristen dokumentiert. 7. Die Information des Betroffenen erfolgt in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten, vgl. die Anforderungen in

	DS06.01. 8. Jeder Antragseingang sowie die Bearbeitung wird durch den Verantwortlichen dokumentiert. 9. Es muss sichergestellt sein, dass die Ausübung der Rechte durch betroffene Personen die Rechte und Freiheiten anderer Personen nicht beeinträchtigt. Hierfür sind entsprechende Prüfungen etabliert inklusive Festlegung von Zuständigkeiten und Festlegung wie ggf. Unkenntlichmachung bestimmter Informationen erfolgt. Soweit erforderlich erfolgt eine Unkenntlichmachung von Informationen (z. B. Schwärzung) zur Wahrung der Rechte und Freiheiten anderer Personen. 10. Sofern keine PBD durch den Verantwortlichen verarbeitet werden und mithin keine Daten übertragen werden können, wird der Betroffene hierüber in Kenntnis gesetzt. 11. Die Datenübertragung erfolgt unentgeltlich. Nur im Falle von offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder b) sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche muss in diesen Fällen den Nachweis, für den offenkundig unbegründeten oder exzessiven Charakter des Antrags erbringen. 12. Es ist sichergestellt, dass die betroffene Person, die sie betreffenden PBD, in einem strukturierten (Darstellung der Daten in strukturierter Weise), gängigen (Format ist allgemein gebräuchlich) und maschinenlesbaren Format (wenn es „in einem Dateiformat vorliegt, das so strukturiert ist, dass Softwareanwendungen die konkreten Daten einfach identifizieren, erkennen und extrahieren können. erfasst werden sowohl digitale als auch papierbasierte, einscanbare Formate, die eine software- bzw. computergesteuerte Verarbeitung ermöglichen) erhält. Bei der Bestimmung des Formats, in welchem die PBD bereitgestellt werden, ist eine Orientierung am branchen- und regionsspezifischen Kontext notwendig, wobei insbesondere XML, JSON, CSV-Formate zu bevorzugen sind. Das gewählte Format ist zu dokumentieren. 13. Die direkte Übertragung an einen anderen Verantwortlichen wird, soweit technisch möglich, unterstützt (Art. 20 Abs. 2 DSGVO). Sofern die Pflichten nach Art 20 DSGVO seitens des Verantwortlichen gem. Art. 23 DSGVO aufgrund einer Rechtsvorschrift der Union oder Deutschlands nicht erfüllt werden, muss dokumentiert sein, welche Rechtsgrundlage aus dem Unionsrecht oder dem deutschen Recht i. V. m. Art. 23 DSGVO herangezogen wir und inwieweit eine entsprechende Beschränkung der Rechte und Pflichten aus Art. 20 DSGVO besteht. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt den Verantwortlichen gem. Art. 28 Abs. 3 Satz 2 lit. e DSGVO soweit möglich und im Rahmen seiner Weisungsgebundenheit bei der Übertragung der PBD in einem strukturierten, gängigen und **maschinenlesbaren Format**. Die entsprechenden Weisungen sind zu dokumentieren. Der Auftragsverarbeiter leitet etwaige Anträge zur Übertragung der PBD in ein strukturiertes, gängiges und

	maschinenlesbares Format an den Verantwortlichen weiter und informiert den Betroffenen hierüber. Zudem kann die Unterstützungspflicht dadurch erfüllt werden, dass der Auftragsverarbeiter es technisch ermöglich, die personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesen Format zu extrahieren und zu übertragen, z. B. durch Implementierung einer Exportfunktion im XML-, CSV- oder JSON-Format. Im Rahmen der Unterstützungsfunktion benennt der Auftragsverarbeiter eine Ansprechperson für den für die Verarbeitung Verantwortlichen und stellt dem Verantwortlichen alle Informationen zur Verfügung, damit der Verantwortliche das Recht auf Datenübertragbarkeit umsetzen kann.

[DSGVO] Art. 21 Abs. 1

DS06.15	**A) Verantwortlicher** Der Verantwortliche muss dem Antrag eines Betroffenen auf Ausübung seines Widerspruchsrechts gegen die Verarbeitung ihn betreffender PBD nachkommen. In diesem Zusammenhang ergreift der Verantwortliche folgende Maßnahmen, die eine Umsetzung des Widerspruchsrechts sicherstellen. a) Widerspruchsrecht gegen Verarbeitungen nach Art. 6 Abs. 1 UAbs. 1 lit. e oder f DSGVO (Art. 21 Abs. 1 DSGVO): 1. Bereitstellung entsprechender Kommunikationswege bzw. Bereitstellung von technischen Funktionen, die die jederzeitige Vornahme eines Widerspruchs sicherstellen 2. Der Verantwortliche muss sicherstellen, dass betroffene Personen ihre Rechte auf sämtlichen ihnen gegenüber verwendeten Kommunikationswegen effektiv geltend machen können. 3. Unterrichtung der betroffenen Personen über das Bestehen des Widerspruchsrechts, vgl. die Anforderungen in **DS06.16**. 4. Festlegung von Zuständigkeiten bzgl. der Bearbeitung von Widersprüchen gegen die Verarbeitung 5. Sensibilisierung der Beschäftigten bzgl. des Widerspruchsrechts 6. Abwesenheits- und Vertretungsregelung, um Einhaltung bestehender Fristen gewährleisten zu können, sind etabliert 7. Der Widerspruch muss auf Gründen, die sich aus der besonderen Situation der betroffenen Person ergeben, fußen • Die betroffene Person muss Gründe vortragen, die sich aus ihrer besonderen Situation ergeben. Ein entsprechender Hinweis an den Betroffenen erfolgt. 8. Prüfung der Begründetheit des Widerspruchs und des Vorhandenseins etwaiger Ausnahmen vom Widerspruchsrecht. Sofern der Verantwortliche schutzwürdige Gründe hat, die einer Umsetzung des Widerspruchsrechts entgegenstehen, führt er eine Interessenabwägung durch, in welcher er seine schutzwürdigen Gründe für die Verarbeitung nachweist, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder er macht geltend, dass die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient. Musterdokumente für die Vornahme der Interessensabwägung sind vorhanden.

	9. Der Prozess berücksichtigt folgende Fristen: Der Verantwortliche entscheidet und informiert den Betroffenen unverzüglich über die getroffenen Maßnahmen, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags der betroffenen Person. Ebenso wird eine eventuelle Fristverlängerung um weitere zwei Monate nach Art. 12 Abs. 3 S. 2 und 3 DSGVO in dem Prozess berücksichtigt, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Die betroffene Person wird innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung informiert. Hierfür sind Musterdokumente vorhanden. Sofern der Verantwortliche auf Antrag der betroffenen Person nicht tätig wird, unterrichtet er gem. Art. 12 Abs. 4 DSGVO die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen. Hierfür sind ebenfalls Musterdokumente vorhanden. Es sind Zuständigkeiten für die Überwachung der Einhaltung der Fristen dokumentiert. Eine ablehnende Entscheidung ist gem. Art. 12 Abs. 4 DSGVO zu begründen und der Betroffene ist über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen. zu informieren. Hierfür sind Musterdokumente vorhanden. 10. Die Information des Betroffenen erfolgt in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten, vgl. **DS06.01**. 11. Jeder Antragseingang sowie die Bearbeitung dessen wird durch den Verantwortlichen dokumentiert. 12. Festlegung wie die Kommunikation mit der Betroffenen Person erfolgt: Sofern die betroffene Person, den Antrag in elektronischer Form gestellt hat, erfolgt die Kommunikation nach Möglichkeit auf elektronischem Weg, es sei denn, die Person wünscht einen anderen Kommunikationsweg. • Falls es von der betroffenen Person verlangt wird, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde. Der Verantwortliche muss festlegen, wie ein entsprechender Identitätsnachweis erfolgen kann. • Der Verantwortliche dokumentiert: das Verlangen nach Information in mündlicher Form, das Verfahren, mit dem ggf. die Identität der betroffenen Person überprüft wurde, die Tatsache, dass der betroffenen Person die Information erteilt wurde 13. Sofern die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat und noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber der betroffenen Person überwiegen, wird die Verarbeitung nach Art. 18 Abs. 1 lit. d DSGVO eingeschränkt, vgl. **DS06.11**. 14. Sofern kein Grund für die Weiterverarbeitung vorliegt und der Widerspruch wirksam war, beendet der Verantwortliche die Verarbeitungsmaßnahmen unverzüglich und löscht die PBD (vgl. Art. 17 Abs. 1 lit. c Var. 1 DSGVO) Hierfür sind technische Funktionen zur Beendigung der mit dem Widerspruch verbundenen Verarbeitung sowie bzgl. der Löschung der PBD, vgl. die Anforderungen in **DS06.11**, vorhanden.

	15. Hat der Verantwortliche die personenbezogenen Daten öffentliche gemacht, informiert er Dritte, welche die Daten verarbeiten, über das Löschungsverlangen (Art. 17 Abs. 2 DSGVO). Hierfür sind entsprechende Prozesse (Zuständigkeiten, Kommunikationswege) vorhanden, vgl. die Anforderungen in **DS06.11**. 16. Die Umsetzung des Widerspruchsrechts erfolgt unentgeltlich. Nur im Falle von offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder b) sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche muss in diesen Fällen den Nachweis, für den offenkundig unbegründeten oder exzessiven Charakter des Antrags erbringen b) Widerspruchsrecht gegen Datennutzung für Direktwerbung (Art. 21 Abs. 2 und 3 DSGVO) Sofern die betroffene Person der Verarbeitung für Zwecke der Direktwerbung (Werbewiderspruch) einschließlich des Profilings, sofern dies mit dieser Direktwerbung zusammenhängt, widerspricht, ist sichergestellt, dass die Daten nicht mehr für diese Zwecke verarbeitet werden, Art. 21 Abs. 3 DSGVO. Hierfür sind entsprechende Prozesse vorhanden, welche mindestens vorsehen: 1. Bereitstellung entsprechender Kommunikationswege bzw. Bereitstellung von technischen Funktionen, die die jederzeitige Vornahme eines Werbewiderspruchs sicherstellen 2. Unterrichtung der betroffenen Personen über das Bestehen des Widerspruchsrechts, vgl. die Anforderungen in **DS06.16**. 3. Festlegung von Zuständigkeiten bzgl. der Bearbeitung von Werbewidersprüchen, die eine die eine unverzügliche Bearbeitung sicherstellen 4. Der Prozess berücksichtigt folgende Fristen: Der Verantwortliche entscheidet und informiert den Betroffenen unverzüglich über die getroffenen Maßnahmen, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags der betroffenen Person. Ebenso wird eine eventuelle Fristverlängerung um weitere zwei Monate nach Art. 12 Abs. 3 S. 2 und 3 DSGVO in dem Prozess berücksichtigt, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Die betroffene Person wird innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung informiert. Hierfür sind Musterdokumente vorhanden. Sofern der Verantwortliche auf Antrag der betroffenen Person nicht tätig wird, unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen. Hierfür sind ebenfalls Musterdokumente vorhanden. Es sind Zuständigkeiten für die Überwachung der Einhaltung der Fristen dokumentiert. Eine ablehnende Entscheidung ist gem. Art. 12 Abs. 4 DSGVO zu begründen und der Betroffene ist über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen. zu informieren. Hierfür sind Musterdokumente vorhanden. 5. Die Information des Betroffenen erfolgt in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen

	Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten, vgl. **DS06.01**. 6. Jeder Antragseingang sowie die Bearbeitung dessen wird durch den Verantwortlichen dokumentiert. 7. Festlegung wie die Kommunikation mit der Betroffenen Person erfolgt: Sofern die betroffene Person, den Antrag in elektronischer Form gestellt hat, erfolgt die Kommunikation nach Möglichkeit auf elektronischem Weg, es sei denn, die Person wünscht einen anderen Kommunikationsweg. • Falls es von der betroffenen Person verlangt wird, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde. Der Verantwortliche muss festlegen, wie ein entsprechender Identitätsnachweis erfolgen kann. • Der Verantwortliche dokumentiert: das Verlangen nach Information in mündlicher Form, das Verfahren, mit dem ggf. die Identität der betroffenen Person überprüft wurde, die Tatsache, dass der betroffenen Person die Information erteilt wurde 8. Für die Information des Betroffenen sind Musterdokumente vorhanden bzw. Sicherstellung durch technische Umsetzung. 9. Vornahme des Werbewiderspruchs kann ohne Begründung erfolgen. Eine Begründung des Betroffenen wird nicht gefordert 10. Vornahme des Werbewiderspruchs kann ohne zusätzliche Hürden bzw. Erschwernisse erfolgen 11. Sofern möglich, wird eine sofortige Ausübung des Widerspruchsrechts ermöglicht, z. B. durch Checkbox oder Verlinkung, einer Widerspruchsmöglichkeit, Einstellungen im Kundenportal. 12. Implementierung von technischen und organisatorischen Maßnahmen, die sicherstellen, dass die PBD nicht mehr zu Direktwerbungszwecken genutzt werden, 13. Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten unverzüglich nicht mehr zum Zweck der Direktwerbung verarbeitet inklusive Abstellung etwaiger Profilingmaßnahmen und die mit der Verarbeitung zum Zwecke der Direktwerbung verwendeten Datensätze werden unverzüglich gelöscht. Hierfür sind technischen Funktionen zur Beendigung der Direktwerbung sowie die Löschung der PBD vorhanden, vgl. die Anforderungen in **DS02.08, DS06.11, DS06.12**. 14. Aufnahme der PBD in eine Werbesperrdatei, die die Datenverwendung für Direktwerbezwecke in Zukunft unterbindet. 15. Gewährleistung, dass jederzeit aktuelle Datenbestände genutzt werden 16. Sofern die PBD in eine Werbesperrdatei aufgenommen werden, werden die betroffenen Personen über den Sinn und Zweck der Aufnahme ihrer Daten in eine Sperrdatei unterrichtet werden. Die Umsetzung des Widerspruchsrechts erfolgt unentgeltlich. Nur im Falle von offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder b) sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche muss in diesen Fällen den Nachweis, für den offenkundig unbegründeten oder exzessiven Charakter des Antrags erbringen.

	c) Widerspruchsrecht gegen Datennutzung zu wissenschaftlichen, historischen oder statistischen Zwecken (Art. 21 Abs. 6 DSGVO) Die betroffene Person kann der Verarbeitung sie betreffender PBD zu wissenschaftlichen, historischen oder statistischen Zwecken im Sinne des Art. 89 Abs. 1 DSGVO widersprechen. Hierbei sind folgende Voraussetzungen zu erfüllen: 1. Verarbeitung erfolgt zu wissenschaftlichen, historischen oder statistischen Zwecken gem. Art. 89 Abs. 1 DSGVO 2. Der Widerspruch muss auf Gründen, die sich aus der besonderen Situation der betroffenen Person ergeben, fußen. Die betroffene Person muss Gründe vortragen, die sich aus ihrer besonderen Situation ergeben und welche noch nicht im Rahmen des Art. 6 Abs. 1 lit. e DSGVO bzw. Art. 89 Abs. 1 DSGVO berücksichtigt wurden. Die betroffenen Personen werden diesbezüglich sensibilisiert. 3. Der Verantwortliche muss eine Abwägung der entgegenstehenden Interessen vornehmen, in der er nachweist, dass die Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist. Hierfür sind entsprechende Zuständigkeiten festgelegt und Musterdokumente für die Vornahme der Interessensabwägung vorhanden. 4. Als Einwendung gegen den Widerspruch kann seitens des Verantwortlichen vorgebracht werden, dass die Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist, vgl. die Anforderungen in **DS03.06**, oder weil weitere Ausnahmen nach Art. 89 Abs. 2 und 3 DSGVO sowie Art. 23 DSGVO vorliegen 5. Vorhandensein von technischen Funktionen zur Beendigung der mit dem Widerspruch verbundenen Verarbeitung sowie bzgl. der Löschung der PBD, vgl. die Anforderungen in **DS02.08**, **DS06.11, DS06.12** 6. Bestätigung eines wirksamen Widerspruchs gegenüber der betroffenen Person 7. Die Information des Betroffenen erfolgt in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten, **vgl. DS06.01**. 8. Festlegung wie die Kommunikation mit der Betroffenen Person erfolgt: Sofern die betroffene Person, den Antrag in elektronischer Form gestellt hat, erfolgt die Kommunikation nach Möglichkeit auf elektronischem Weg, es sei denn, die Person wünscht einen anderen Kommunikationsweg. • Falls es von der betroffenen Person verlangt wird, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde. Der Verantwortliche muss festlegen, wie ein entsprechender Identitätsnachweis erfolgen kann. • Der Verantwortliche dokumentiert: das Verlangen nach Information in mündlicher Form, das Verfahren, mit dem ggf. die Identität der betroffenen Person überprüft wurde, die Tatsache, dass der betroffenen Person die Information erteilt wurde. Für die Information des Betroffenen sind Musterdokumente vor-handen. 9. Jeder Antragseingang sowie die Bearbeitung dessen wird durch den Verantwortlichen dokumentiert. 10. Die Umsetzung des Widerspruchsrechts erfolgt unentgeltlich. Nur im Falle von offenkundig unbegründeten oder – insbesondere im Fall von

	häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder b) sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche muss in diesen Fällen den Nachweis, für den offenkundig unbegründeten oder exzessiven Charakter des Antrags erbringen. Sofern die Pflichten nach Art 21 DSGVO seitens des Verantwortlichen gem. Art. 23 DSGVO aufgrund einer Rechtsvorschrift der Union oder Deutschlands nicht erfüllt werden, muss dokumentiert sein, welche Rechtsgrundlage aus dem Unionsrecht oder dem deutschen Recht i. V. m. Art. 23 DSGVO herangezogen wir und inwieweit eine entsprechende Beschränkung der Rechte und Pflichten aus Art. 21 DSGVO besteht. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt den Verantwortlichen gem. Art. 28 Abs. 3 Satz 2 lit. e DSGVO soweit möglich und im Rahmen seiner Weisungsgebundenheit bei der Verarbeitung von Widersprüchen gegen die Verarbeitung von PBD. Die Unterstützungspflicht wird insbesondere umgesetzt durch: 1. Vorhandensein von Prozessen, die eine Weiterleitung von Widersprüchen gegen die Verarbeitung an den Verantwortlichen sicherstellen, sofern diese an den Auftragsverarbeiter gerichtet werden. In diesem Zusammenhang sind Ansprechpersonen für den für die Verarbeitung Verantwortlichen benannt, Kommunikationswege und Zuständigkeiten für die Bearbeitung entsprechender Betroffenenanfragen festgelegt. Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, damit dieser das Widerrufsrecht umsetzen kann. 2. Die Dokumentation des IVS, welche dem Verantwortlichen zur Verfügung gestellt wird, enthält einen Hinweis darauf, dass der Verantwortliche verpflichtet ist, auf Widersprüche der betroffenen Person gegen die Verarbeitung zu reagieren. Im Rahmen der Unterstützungsfunktion benennt der Auftragsverarbeiter eine Ansprechperson für den für die Verarbeitung Verantwortlichen.

[DSGVO] Art. 21 Abs. 4

DS06.16	**A) Verantwortlicher** Der Verantwortliche informiert Betroffene zum Zeitpunkt der Erhebung von PBD über das Bestehen eines Widerspruchsrechts nach Art. 21 Abs. 1 DSGVO. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt den Verantwortlichen gem. Art. 28 Abs. 3 Satz 2 lit. e DSGVO soweit möglich und im Rahmen seiner Weisungsgebundenheit bei der Erteilung der Information über das Bestehen eines **Widerspruchsrechts** entsprechend Art. 21 Abs.1 DSGVO. Hierzu

	stellt er eine Dokumentation des IVS bereit, welche darüber informiert, dass der Verantwortliche verpflichtet ist, Betroffene auf das Bestehen und die Ausübung ihres Widerspruchsrechts hinzuweisen. Im Rahmen der Unterstützungsfunktion benennt der Auftragsverarbeiter eine Ansprechperson für den für die Verarbeitung Verantwortlichen.

[DSGVO] Art. 22

DS06.17	**A) Verantwortlicher** Der Betroffene hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihm gegenüber rechtliche Wirkung entfaltet oder ihn in ähnlicher Weise erheblich beeinträchtigt. 1. Dies gilt nicht, wenn die Entscheidung a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist. • Die automatisierte Entscheidung muss für den Abschluss oder die Erfüllung eines Vertrages mit einer betroffenen Person objektiv erforderlich sein. Die Erforderlichkeit ist eng auszulegen. • Der Verantwortliche muss nachweisen können, dass die automatisierte Entscheidung erforderlich ist, insbesondere dass Verträge ohne den Einsatz von automatisierten Verfahren nicht bewältigt werden können. • Die Erforderlichkeit ist zu dokumentieren. b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten • Vorliegen einer rechtlichen Verpflichtung des Verantwortlichen und die Verpflichtung muss sich unmittelbar auf automatisierte Entscheidungen beziehen. • Die Verpflichtung weist einen Bezug zu der betroffenen Person auf. • Die rechtliche Verpflichtung muss sich aus dem Unionsrecht oder dem deutschen Recht ergeben, dem der Verantwortliche unterworfen ist. • Es muss dokumentiert sein, welche Rechtsgrundlage aus dem Unionsrecht oder dem deutschen Recht i. V. m. Art. 22 Abs. 2 lit. b DSGVO herangezogen wird. • Die einschlägigen Rechtsvorschriften müssen angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten (insbesondere spezifische Unterrichtung der betroffenen Person, Anspruch auf direktes Eingreifen einer Person, Darlegung des eigenen Standpunktes durch die betroffene Person, Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung, Recht auf Anfechtung der Entscheidung) c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt, vgl. die Anforderungen an Anforderungen an eine Einwilligung in **DS04**. • Die Einwilligung muss in informierter Weise erfolgen. Der betroffenen Person sind Informationen über den Zweck des

	automatisierten Entscheidungsverfahrens (vgl. **DP06.04** und **DP06.05**) mitzuteilen. Zudem sind Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer automatisierten Entscheidungsfindung für die betroffene Person anzugeben. • Die Einwilligungserklärung muss ausdrücklich erteilt werden, d. h. sie muss sich ausdrücklich darauf beziehen, dass die betreffende Entscheidung ausschließlich auf einer automatisierten Entscheidung beruht. • Die Einwilligung muss freiwillig erteilt werden. • Die Einwilligungserklärung muss sich explizit auf das Einverständnis mit der automatisierten Entscheidung beziehen. • Die Einwilligung ist zu dokumentieren. • Es muss möglich sein, die Einwilligung zu widerrufen, vgl. die Anforderungen in **DS04.06, DS04.07, DS04.08**. Bezüglich der Anforderungen an eine Einwilligung ist den Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, angenommen am 4. Mai 2020, des EDSA zu folgen. 2. Der Verantwortliche muss die Datenschutzgrundsätze gem. Art. 5 DSGVO bei sämtlichen Profiling-Tätigkeiten und automatisierten Entscheidungen umsetzen, vgl. die jeweiligen Anforderungen in **DS02**. 3. Der Verantwortliche muss die betroffenen Personen über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gem. Art. 22 Abs. 1 und 4 DSGVO informieren und hat – zumindest in diesen Fällen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person zur Verfügung zu stellen (Art. 13 Abs. 2 lit. f DSGVO, Art. 14 Abs. 2 lit. g DSGVO), vgl. die Anforderungen in **DS06.04** und **DS06.05**. Den betroffenen Personen muss klar und einfach erläutert werden, wie Profiling bzw. automatisierte Entscheidungen funktionieren. 4. Die betroffenen Personen müssen, sofern relevant, über ihre Rechte nach Art. 22 Abs. 3 DSGVO informiert werden. 5. Die betroffene Person hat das Recht, Auskunft zu den zwecks Profiling verwendeten PBD zu erlangen, einschließlich der zur Profilerstellung verwendeten Datenkategorien, vgl. die Anforderungen in **DS06.07**. Zudem sind die zur Profilerstellung verwendeten Eingabedaten zur Verfügung zu stellen und Informationen zum Profil und Details zu den Segmenten, in die die betroffene Person eingeteilt wurde, mitzuteilen, Art. 15 Abs. 3 DSGVO. 6. Es sind Prozesse bzgl. Berichtigungs-, Lösch- und Einschränkungsanträgen im Hinblick auf das Profiling zu implementieren, vgl. die Anforderungen in **DS06.11.** 7. Es werden geeignete mathematische oder statistische Verfahren verwendet sowie technische und organisatorische Maßnahmen eingesetzt mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird, und personenbezogene Daten in einer Weise sichern, dass den potenziellen Bedrohungen für die Interessen und Rechte der betroffenen Person Rechnung getragen wird und unter anderem verhindern, dass es gegenüber natürlichen Personen aufgrund von Rasse, ethnischer Herkunft, politischer Meinung, Religion oder Weltanschauung,

	Gewerkschaftszugehörigkeit, genetischer Anlagen oder Gesundheitszustand sowie sexueller Orientierung zu diskriminierenden Wirkungen oder zu einer Verarbeitung kommt, die eine solche Wirkung hat, vgl. ErwG 71 DSGVO. 8. Die Mindestanforderungen gem. Art. 22 Abs. 3 DSGVO werden erfüllt: Die betroffene Person muss die Möglichkeit haben, dem Verantwortlichen ihren Standpunkt darzulegen, die Entscheidung durch eine natürliche Person überprüfen zu lassen und die getroffene Entscheidung anzufechten. Mithin muss der Verantwortliche Prozesse implementiert haben, die sicherstellen, dass eine automatisiert herbeigeführte Entscheidung ergebnisoffen und anhand des konkreten individuellen Sachverhaltes durch eine natürliche Person seitens des Verantwortlichen überprüft wird, sofern die betroffene Person dies verlangt. Hierbei ist der Standpunkt der betroffenen Person zu berücksichtigen. Die implementierten Prozesse müssen insbesondere Festlegungen treffen zu: detaillierte Information der betroffenen Personen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung und ihre Rechte nach Art. 22 Abs. 3 DSGVO, Kommunikationswegen für die betroffene Person, Festlegung von Zuständigkeiten für die Befassung mit dem Sachverhalt durch eine natürliche Person (ggf. unter Berücksichtigung des Standpunkts der betroffenen Person, Dokumentation der Überprüfung, auf Verlangen sind der betroffenen Person die wesentlichen Gründe der Ablehnung ihres Begehrens mitzuteilen, Art und Weise der Erläuterung der nach der Bewertung getroffenen Entscheidung, Angebot von Maßnahmen, die es der betroffenen Person ermöglicht, korrigierend einzuwirken). 9. Im Regelfall sind Kinder nicht von einer ausschließlich automatisierten Entscheidungsfindung betroffen. Lediglich in Ausnahmefällen wird eine Verarbeitung der Daten von Kindern auf der Grundlage der Ausnahmen in Art. 22 Abs. 2 lit. a, b, c DSGVO durchgeführt. In diesem Fall müssen geeignete Garantien vorhanden sein (siehe vorstehende Anforderungen), die sicherstellen, dass die Rechte, Freiheiten und berechtigten Interessen der Kinder, deren Daten verarbeitet werden, mit diesen Garantien wirksam geschützt werden. 10. Eine automatisierte Entscheidung, die besondere Kategorien von PBD umfasst ist gem. Art. 22 Abs. 4 DSGVO nur bei Vorliegen nachfolgender kumulativer Bedingungen zulässig und wenn der Verantwortliche angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen hat. a) Es gilt eine Ausnahme nach Art. 22 Abs. 2 DSGVO, siehe vorstehende Ausführungen b) Es findet Art. 9 Abs. 2 lit. a DSGVO (ausdrückliche Einwilligung der betroffenen Person in die Verarbeitung besonderer Kategorien von PBD) Anwendung, vgl. die Anforderungen in **DS05.01** c) oder Art. 9 Abs. 2 lit. g DSGVO findet Anwendung (die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats aus Gründen eines erheblichen öffentlichen Interesses erforderlich), vgl. die Anforderungen in **DS05.01** ▪ Es sind angemessene Maßnahmen getroffen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu schützen (Mindestanforderungen gem. Art. 22 Abs. 3 DSGVO (vgl. die Anforderungen unter Ziffer 8), Erfüllung der Informationspflichten (vgl. die Anforderungen unter

	Ziffer 3), Transparenz der involvierten Logik, Verwendung geeigneter mathematischer oder statistischer Verfahren (vgl. die Anforderungen in Ziffer 7). 11. Eine Datenschutz-Folgenabschätzung wurde durchgeführt, vgl. die Anforderungen in **DS10.** Es ist den Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, angenommen am 3. Oktober 2017 (WP251rev.01), gebilligt vom EDSA, zuletzt überarbeitet und angenommen am 6. Februar 2018, der Datenschutzgruppe nach Artikel 29, gebilligt vom EDSA, zu folgen. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt den Verantwortlichen gem. Art. 28 Abs. 3 Satz 2 lit. e DSGVO soweit möglich und im Rahmen seiner Weisungsgebundenheit im Hinblick auf die Beantwortung von Anträgen von betroffenen Personen im Zusammenhang mit Art. 22 DSGVO. Hierzu stellt er eine Dokumentation des IVS bereit, welche den Verantwortlichen darüber informiert, dass er verpflichtet ist, den Betroffenen über das Bestehen des Rechts zu informieren, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden. Im Rahmen der Unterstützungsfunktion benennt der Auftragsverarbeiter eine Ansprechperson für den für die Verarbeitung Verantwortlichen.

DS07 Verantwortlicher und Auftragsverarbeiter

[DSGVO] Art. 24 Abs. 1, 2

DS07.01	**Verantwortlicher** Die mit dem IVS verbundenen Prozesse enthalten **Vorgaben für geeignete technische und organisatorische Maßnahmen,** die die Einhaltung der Datenschutzanforderungen sicherstellen. Hierbei sind insbesondere sicherzustellen, vgl. insbesondere auch die Anforderungen in DS07.02: • Durchführung einer Risikoanalyse, vgl. die Anforderungen an diese in DS02.07 sowie DS07.02 • Führen des Verzeichnisses von Verarbeitungstätigkeiten, vgl. die Anforderungen in DS07.11 • Benennung eines Datenschutzbeauftragten, vgl. DS09.03 • Implementierung von Prozessen bzgl. der Sicherstellung der Betroffenenrechte, vgl. DS06 • Implementierung von Prozessen bzgl. des Umgangs mit Verletzungen des Schutzes personenbezogener Daten, vgl. die Anforderungen in DS09.01 sowie DS09.02 • Festlegung von festen Ansprechpartnern der Organisationseinheiten eines Unternehmens für den Datenschutzbeauftragten und die Beschäftigten der jeweiligen Organisationseinheiten in Sachen Datenschutz • Vorhandensein von Vertretungsregelungen für abwesende Mitarbeiter • Sofern innerhalb des Evaluierungsgegenstandes die Möglichkeit besteht, dass Betroffene Personen ihre PBD gegenüber anderen Nutzern oder Dritten sichtbar machen, z. B. Informationen aus Social Media Profilen, abgegebene Kommentare, stellt der Verantwortliche sicher, dass per Voreinstellungen eine Sichtbarmachung nicht standardmäßig erfolgt und dass die PBD nicht ohne Eingreifen der betroffenen Person einer unbestimmten Anzahl von natürlichen Personen zugänglich gemacht werden. Vielmehr können Betroffene den Umfang der Sichtbarkeit ihrer PBD und der von ihnen geteilten Inhalte selbst festlegen. Es ist eine Funktion implementiert, die es der betroffenen Person ermöglicht, ihre gespeicherten PBD einzusehen. • Es ist eine Funktion implementiert, die es gewährleistet, dass der Person eine Kopie der PBD zur Verfügung gestellt wird. • Es ist eine Funktion bzgl. der Übertragbarkeit der Daten implementiert. • Durchführung von Datenschutzschulungen für die Beschäftigten, vgl. die Anforderungen in DS09.08 • Verpflichtung der Beschäftigten zur Wahrung der Vertraulichkeit und des Datenschutzes • Verschlüsselung von Datenträgern, vgl. auch die Anforderungen in DS08 • Vorhandensein von Passwortrichtlinien, vgl. auch die Anforderungen in DS08 • Protokollierung von Zugriffen, vgl. auch die Anforderungen in DS08 • Einrichtung und Kontrolle von Berechtigungen, vgl. auch die Anforderungen in DS08 • Implementierung automatischer Sperr- und Löschroutinen,

	Pseudonymisierungs- und Anonymisierungsverfahren • Es werden technische Maßnahmen, z. B. Hashing und Verschlüsselung, angewendet, um die Möglichkeit einzuschränken, dass personenbezogene Daten einem neuen Zweck zugeführt werden. Es werden organisatorische Maßnahmen angewendet, die die Wiederverwendung personenbezogener Daten einschränken, z. B. vertragliche Verpflichtungen. • Es finden regelmäßige Überprüfungen statt, ob die Verarbeitung für die Zwecke, für die die Daten erhoben wurden, erforderlich ist und die Verarbeitung unter Beachtung des Aspekts der Zweckbindung erfolgt. • Es werden technische Möglichkeiten bzgl. der Minimierung der verarbeiteten PBD in Abhängigkeit von der jeweiligen Verarbeitungssituation bereitgestellt. • Personenbezogene Daten werden pseudonymisiert, sobald keine Notwendigkeit mehr für direkt identifizierbare personenbezogene Daten besteht und die Identifizierungsschlüssel sollten separat gespeichert werden. • Personenbezogene Daten werden anonymisiert oder gelöscht, wenn sie nicht oder nicht mehr für den Zweck notwendig sind. • Nach Möglichkeit werden aggregierte Daten verwendet. • Festlegung eines Rechte-Rollen-Konzeptes nach dem Erforderlichkeitsprinzip • Es sind Verfahren und Funktionen für die Löschung und/ oder Anonymisierung von PBD implementiert, vgl. die Anforderungen in **DS02.08** • Ein Löschkonzept ist vorhanden, vgl. die Anforderungen in **DS02.08** • Durch ein Zugriffs- und Berechtigungskonzept wird sichergestellt, dass eine möglichst geringe Zahl von Personen für die Ausführung ihrer Aufgaben Zugang zu den PBD haben. • Sofern Pseudonymisierungstechniken eingesetzt werden, ist die konkrete Umsetzung beschrieben. • Sofern Anonymisierungstechniken eingesetzt werden, ist die konkrete Umsetzung beschrieben. • Die Struktur der Daten bzw. der Datenbank muss so ausgestaltet sein, dass einzelne Datenfelder, Datensätze oder Gruppen von Daten berichtigt werden können, z. B. auch durch die betroffene Person selbst. • Alle Berichtigungs- bzw. Löschvorgänge müssen dokumentiert werden. • Es sind technische und organisatorische Maßnahmen implementiert, die die PBD vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung schützen, vgl. auch die Anforderungen in **DS08**. • Die Wirksamkeit der Umsetzung der Sicherheitsanforderungen wird regelmäßig überprüft. Hierfür sind entsprechende Zuständigkeiten und die Art und Weise der Überprüfung festgelegt. • Datenübertragungen werden vor unbefugtem und unbeabsichtigtem Zugriff und vor unbefugten und unbeabsichtigten Änderungen geschützt, vgl. auch die Anforderungen in **DS08**. • Datenspeicher sind vor unbefugtem Zugriff und unbefugten

	Änderungen geschützt, vgl. auch die Anforderungen in **DS08**. ▪ Backups und Logdateien sind vor unbefugtem und unbeabsichtigtem Zugang und vor unbefugten und unbeabsichtigten Änderungen geschützt, vgl. auch die Anforderungen in **DS08**. Teil dieser Konzeption sind regelmäßige und anlassbezogene Überprüfungen der getroffenen Maßnahmen.

[DSGVO] Art. 25 Abs. 1 i. V. m. Art. 5 Abs. 1

DS07.02	**Verantwortlicher** Der Verantwortliche muss geeignete technische und organisatorische Maßnahmen bei der wirksamen Umsetzung der Datenschutzgrundsätze gem. Art. 5 Abs. 1 DSGVO ergreifen und notwendige Garantien in die Verarbeitung aufnehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Personen zu schützen. Hierbei muss er den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen, berücksichtigen. Der Verantwortliche muss im Hinblick auf die Umsetzung geeigneter Maßnahmen im Zusammenhang mit **Datenschutz durch Technikgestaltung (privacy by design)** die Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Version 2.0, angenommen am 20. Oktober 2020, des EDSA berücksichtigen. Hierbei ist insbesondere durch den Verantwortlichen sicherzustellen: 1. Datenschutzaspekte sind bereits in der Anfangsphase der Planung eines Verarbeitungsvorgangs zu berücksichtigen, noch vor der Festlegung der Verarbeitungsmittel. Hierfür sind entsprechende Prozesse bzw. Arbeitsanweisungen, z. B. Datenschutzleitfaden für die IT-Entwickler, zu implementieren. 2. Der Verantwortliche stellt sicher, dass der Datenschutzbeauftragte in die Beschaffungs- und Entwicklungsverfahren sowie während des gesamten Verarbeitungszyklus involviert wird. Hierfür sind entsprechende Prozesse zu implementieren (Festlegung von Zuständigkeiten, Festlegung, wie und wann der Datenschutzbeauftragte einzubeziehen ist, Festlegung, welche Informationen dem Datenschutzbeauftragten zur Verfügung gestellt werden). 3. Maßnahmen, welche die Einhaltung des Datenschutzes im Betrieb gewährleisten, wenn bspw. Änderungen im Datenschutzrecht oder in den IT-Verfahren stattfinden, z. B. Durchführung anlassbezogener Kontrollen, Prozesse bzgl. der frühzeitigen Einbeziehung des Datenschutzbeauftragten (Festlegung wie und wann der Datenschutzbeauftragte einzubeziehen ist, Beteiligung des Datenschutzbeauftragten an Führungskreistreffen, regelmäßige Treffen des Datenschutzbeauftragten mit IT-Beauftragten und Informationssicherheitsbeauftragten) sind etabliert. 4. Die Einhaltung des Grundsatzes Datenschutz durch Technikgestaltung muss während des gesamten Lebenszyklus der Verarbeitung berücksichtigt werden. 5. Der Verantwortliche dokumentiert die umgesetzten technischen und organisatorischen Maßnahmen. Neben den konkreten Maßnahmen sind auch die Entscheidungsfindung einschließlich der Aspekte und Gründe

	warum bestimmte Maßnahmen umgesetzt oder nicht umgesetzt wurden, zu dokumentieren. 6. Bei der Auswahl der technischen und organisatorischen Maßnahmen sind nachfolgende Aspekte durch den Verantwortlichen zu berücksichtigen: der Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zweck der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen. 7. Der Verantwortliche muss Leistungsindikatoren etablieren, um die Wirksamkeit der umgesetzten Maßnahmen nachzuweisen. 8. Die Datenschutzgrundsätze gem. Art. 5 DSGVO und ErwG 39 DSGVO bei der Verarbeitung personenbezogener Daten müssen im Wege des Datenschutzes durch Technikgestaltung umgesetzt werden. Die Verantwortlichen müssen prüfen, wie die Wahrung der Datenschutzgrundsätze bei dem jeweiligen konkreten Verarbeitungsvorgang zu gewährleisten ist. a) Transparenz, vgl. die Anforderungen in **DS02.01** b) Rechtmäßigkeit, vgl. die Anforderungen in **DS02.03** c) Verarbeitung nach Treu und Glauben, vgl. die Anforderungen in **DS02.02** d) Zweckbindung, vgl. die Anforderungen in **DS02.04** e) Datenminimierung, vgl. die Anforderungen in **DS02.06** f) Richtigkeit, vgl. die Anforderungen in **DS02.07, DS06.11** g) Speicherbegrenzung, vgl. die Anforderungen in **DS02.08** h) Integrität und Vertraulichkeit, vgl. die Anforderungen in **DS02.09, DS08** i) Rechenschaftspflicht, vgl. die Anforderungen in **DS02.10** 9. Die Umsetzung der Datenschutzgrundsätze und der Rechte der betroffenen Personen ist beschrieben (Rechenschaftspflicht), vgl. die Anforderungen in **DS02.10,** und die Umsetzung innerhalb der Organisation wird gefordert, z. B. interne Richtlinie oder Datenschutzkonzept. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. 25 Abs. 2

DS07.03	**<u>Verantwortlicher</u>** Der IVS unterstützt den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen (vgl. die nachfolgenden Anforderungen Nr. 1 bis 8), die sicherstellen, dass durch standardmäßige Voreinstellungen personenbezogene Daten nur soweit verarbeitet werden, wie es für den jeweiligen Zweck erforderlich ist. Dies gilt im Hinblick auf: • Menge der erhobenen PBD • Umfang der Verarbeitung der PBD, • Speicherfrist der verarbeiteten PBD, • Zugänglichkeit zu PBD Im Hinblick auf die Umsetzung des **Prinzips „Privacy by default – datenschutzfreundliche Voreinstellungen**“ ist den Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Version 2.0, Angenommen am 20. Oktober 2020, des EDSA zu folgen. Hierbei ist insbesondere sicherzustellen: 1. Datenschutzfreundliche Voreinstellungen sind bereits in der

	Anfangsphase der Planung eines Verarbeitungsvorgangs zu berücksichtigen, noch vor der Festlegung der Verarbeitungsmittel. Hierfür sind entsprechende Prozesse bzw. Arbeitsanweisungen, z. B. Datenschutzleitfaden für die IT-Entwickler, zu implementieren. 2. Der Datenschutzbeauftragte ist in die Beschaffungs- und Entwicklungsverfahren sowie während des gesamten Verarbeitungszyklus einzubeziehen. Hierfür sind entsprechende Prozesse zu implementieren (Festlegung von Zuständigkeiten, Festlegung, wie und wann der Datenschutzbeauftragte einzubeziehen ist, Festlegung, welche Informationen dem Datenschutzbeauftragten zur Verfügung gestellt werden). 3. Die Einhaltung des Grundsatzes Datenschutz durch Voreinstellungen muss während des gesamten Lebenszyklus der Verarbeitung berücksichtigt werden. 4. Die Verarbeitungszwecke sind eindeutig festzulegen und zu dokumentieren. 5. Die umgesetzten technischen und organisatorischen Maßnahmen müssen dokumentiert sein. 6. Die Umsetzung des Datenschutzes durch datenschutzfreundliche Voreinstellungen ist beschrieben und die Umsetzung innerhalb der Organisation wird gefordert, z. B. interne Richtlinie oder Datenschutzkonzept. 7. Durch datenschutzfreundliche Voreinstellungen wird die Erhebung, Verarbeitung und Weitergabe personenbezogener Daten auf das für den angestrebten Zweck erforderliche Mindestmaß begrenzt (Erforderlichkeit). Die Verarbeitungszwecke sind eindeutig festzulegen und die Erforderlichkeit der Verarbeitung ist zu dokumentieren. Nachfolgend sind zentrale Aspekte des Datenschutzes durch datenschutzfreundliche Voreinstellungen aufgelistet. Allerdings ist diese Auflistung nicht abschließend und lediglich beispielhaft. a) Menge und Umfang der Verarbeitung ▪ Es werden nur personenbezogene Daten verarbeitet, die angemessen, relevant und auf das für den Zweck Notwendige beschränkt sind. ▪ Es werden technische Möglichkeiten bzgl. der Minimierung der verarbeiteten PBD in Abhängigkeit von der jeweiligen Verarbeitungssituation bereitgestellt. ▪ Personenbezogene Daten werden pseudonymisiert, sobald keine Notwendigkeit mehr für direkt identifizierbare personenbezogene Daten besteht und die Identifizierungsschlüssel sollten separat gespeichert werden. ▪ Freitextfelder werden sparsam verwendet und jedes Freitextfeld sollte mit einer Zweckbeschreibung versehen sein. ▪ Pflichtfelder werden sparsam verwendet und es erfolgt eine deutliche Kennzeichnung der Pflichtfelder. ▪ Durch ein Zugriffs- und Berechtigungskonzept wird sichergestellt, dass eine möglichst geringe Zahl von Personen für die Ausführung ihrer Aufgaben Zugang zu den PBD haben. ▪ Sofern eine Optionalität im Hinblick auf die Erhebung und Verarbeitung von personenbezogenen Daten gegeben ist, ist jede Option standardmäßig deaktiviert. ▪ Vor der Erhebung und Verarbeitung von personenbezogenen Daten jede Option standardmäßig deaktiviert und ▪ Sollte nur durch ausdrückliche Wahl der betroffenen Person aktiviert werden. ▪ Bestimmte Funktionen sind per default deaktiviert oder

	eingeschränkt, z. B. Kamera- und Mikrofonfunktionen ■ Assistenzsysteme sind per default deaktiviert oder eingeschränkt. ■ Autostartfunktionen sind deaktiviert oder eingeschränkt. ■ Der automatische Verbindungsaufbau zu Netzwerken oder dem Internet ist per default deaktiviert oder eingeschränkt. ■ Benutzerflächen, z. B. bzgl. Größe, Form, Farbe von Schaltflächen, sind so gestaltet, dass die Wahrnehmung und Entscheidung der betroffenen Personen nicht in eine bestimmte Richtung gelegt werden, sog. Dark Patterns. ■ Es sind Voreinstellungen implementiert, die Verknüpfungsmöglichkeiten minimieren und einschränken. ■ Es werden Entpersonalisierungs- oder andere Datensparsamkeitstechniken eingesetzt. ■ Sofern Pseudonymisierungstechniken eingesetzt werden, ist die konkrete Umsetzung beschrieben. ■ Sofern Anonymisierungstechniken eingesetzt werden, ist die konkrete Umsetzung beschrieben. ■ Die Mechanismen, z. B. technische Systemkonfigurationen, die zur Gewährleistung der Datenminimierung implementiert sind, sind dokumentiert. b) Speicherfrist der verarbeiteten PBD ■ Speicherfristen werden durch Voreinstellungen möglichst kurz gehalten. ■ Es ist ein Löschkonzept implementiert, dass sicherstellt, dass PBD nach Ablauf der Speicherfrist automatisiert gelöscht werden. ■ Personenbezogene Daten werden anonymisiert oder gelöscht, wenn sie nicht oder nicht mehr für den Zweck notwendig sind. ■ Nach Möglichkeit werden aggregierte Daten verwendet. ■ Es sind Verfahren und Funktionen für die Löschung und/oder Anonymisierung von PBD implementiert. ■ Ein Löschkonzept ist vorhanden. ■ Es ist sichergestellt, dass anonymisierte Daten nicht wieder identifizierbar gemacht und gelöschte Daten nicht wiederhergestellt werden können und es werden entsprechende Tests durchführt. ■ Die Löschung bestimmter PBD erfolgt automatisiert. ■ Die jeweilige Speicherdauer, sofern möglich inklusive Angabe der entsprechenden Rechtsgrundlage, ist dokumentiert. ■ Das Löschkonzept berücksichtigt Backups und Logdateien. ■ Es sind Prozesse im Hinblick auf die Überprüfung der Vornahme und Wirksamkeit der Löschungen implementiert (Zuständigkeiten für Überprüfung der Vornahme von Löschungen inklusive Festlegung Art und Weise der Überprüfung und Häufigkeit der Überprüfung). c) Zugänglichkeit der PBD ■ Ein Rollen- und Berechtigungskonzept ist implementiert, welches sicherstellt, dass ein Zugriff nach dem Need-to-Know-Prinzip erfolgt. ■ Es ist ein Berechtigungskonzept implementiert, dass sicherstellt, dass der Zugriff auf besonders schützenswerte Daten nur unter Einhaltung des Vier-Augen-Prinzips erfolgt. ■ Einrichtung eines voreingestellten starken Zugriffschutzes, z.

	B. Passwortvorgaben ▪ Es sind technische und organisatorische Maßnahmen implementiert, die die PBD vor unbefugter oder unrechtmäßiger Verarbeitung schützen, vgl. auch die Anforderungen in **DS08**. ▪ Datenübertragungen werden vor unbefugtem und unbeabsichtigtem Zugriff und vor unbefugten und unbeabsichtigten Änderungen geschützt. ▪ Datenspeicher sind vor unbefugtem Zugriff und unbefugten Änderungen geschützt. ▪ Die Stärke von gewählten Passwörtern wird gemessen und angezeigt, um eine sichere Passwortvergabe zu unterstützen. d) Zugänglichmachen einer unbestimmten Zahl von Personen ▪ Sofern PBD einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden sollen, ist ein bewusstes Konfigurieren bzw. Eingreifen der betroffenen Person erforderlich. Entsprechende Eingriffsmöglichkeiten sind zu implementieren, z. B. Einholung einer Einwilligung in die Bereitstellung der PBD für eine unbestimmte Anzahl von Personen, Vorhandensein entsprechender Privatsphäreeinstellungen per default. 8. Die Umsetzung des Prinzips „Privacy by default – datenschutzfreundliche Voreinstellungen“ ist beschrieben (Rechenschaftspflicht), vgl. die Anforderungen in **DS02.10,** und die Umsetzung innerhalb der Organisation wird gefordert, z. B. interne Richtlinie oder Datenschutzkonzept. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. 28 DSGVO

DS07.04	**A) Verantwortlicher** Alle eingesetzten Auftragsverarbeiter inklusive Unterauftragsverarbeiter sind dokumentiert. Hierbei ist darzulegen, dass es sich bei diesen auch tatsächlich um Auftragsverarbeiter handelt. Im Rahmen einer Einzelfallanalyse ist hierbei zu beurteilen, in welchem Maße jede Stelle tatsächlich Einfluss auf die Zwecke und Mittel der Verarbeitung hat. Dabei ist für die Einstufung als Verantwortlicher oder Auftragsverarbeiter eine Prüfung der konkreten Datensätze oder Vorgänge vorzunehmen und dies entsprechend zu dokumentieren. Es ist hierbei insbesondere zu belegen, dass jeweils die nachfolgenden Voraussetzungen im Hinblick auf das Vorliegen einer Auftragsverarbeitung erfüllt werden. 1. Der Auftragsverarbeiter bzw. Unterauftragsverarbeiter ist eine vom Verantwortlichen getrennte Stelle, d. h. die Verarbeitungstätigkeit wird ganz oder teilweise an eine externe Organisation delegiert. 2. Die jeweilige Datenverarbeitung erfolgt im Auftrag des Verantwortlichen. 3. Personenbezogene Daten werden nur auf Weisungen des Verantwortlichen verarbeitet und entsprechend ist sichergestellt, dass der Auftragsverarbeiter/Unterauftragsverarbeiter nicht über den Zweck und wesentlichen Mittel der Datenverarbeitung entscheidet. Im Hinblick auf die Beurteilung der Wesentlichkeit der Mittel gilt der Maßstab des EDSA gem. Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.0, angenommen am 7.Juli 2021 (vgl. Prüfhinweis).

	4. Der Auftragsverarbeiter darf keine Verarbeitung für seine eigenen Zwecke vornehmen. Vom Verantwortlichen ist ferner darzulegen, ob für den Einsatzbereich des IVS bereichsspezifische Vorschriften bestehen, die besondere Voraussetzungen für eine Auftragsverarbeitung vorsehen oder diese insgesamt ausschließen. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen. **B) Auftragsverarbeiter** Alle eingesetzten Auftragsverarbeiter inklusive Unterauftragsverarbeiter sind dokumentiert. Hierbei ist darzulegen, dass es sich auch tatsächlich um Auftragsverarbeiter handelt. Im Rahmen einer Einzelfallanalyse ist hierbei zu beurteilen, im welchem Maße jede Stelle tatsächlich Einfluss auf die Zwecke und Mittel der Verarbeitung hat. Dabei ist für die Einstufung als Verantwortlicher oder Auftragsverarbeiter eine Prüfung der konkreten Datensätze oder Vorgänge vorzunehmen und dies entsprechend zu dokumentieren. Es ist hierbei insbesondere zu belegen, dass jeweils die nachfolgenden Voraussetzungen im Hinblick auf das Vorliegen einer Auftragsverarbeitung erfüllt werden. 1. Der Auftragsverarbeiter bzw. Unterauftragsverarbeiter ist eine vom Verantwortlichen getrennte Stelle, d. h. die Verarbeitungstätigkeit wird ganz oder teilweise an eine externe Organisation delegiert. 2. Die jeweilige Datenverarbeitung erfolgt im Auftrag des Verantwortlichen. 3. Personenbezogene Daten werden nur auf Weisungen des Verantwortlichen verarbeitet und entsprechend ist sichergestellt, dass der Auftragsverarbeiter/Unterauftragsverarbeiter nicht über den Zweck und wesentliche Mittel der Datenverarbeitung entscheidet. Im Hinblick auf die Beurteilung der Wesentlichkeit der Mittel gilt der Maßstab gem. Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.0, angenommen am 7.Juli 2021 (vgl. Prüfhinweis). 4. Der Auftragsverarbeiter darf keine Verarbeitung für seine eigenen Zwecke vornehmen. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. 28 Abs. 1

DS07.05	**Verantwortlicher** Der Verantwortliche arbeitet nur mit Auftragsverarbeitern, die **hinreichend Garantien** dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO – auch in Bezug auf die Sicherheit der Verarbeitung - erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet. Bei der Beurteilung, ob die Garantien des Auftragsverarbeiters hinreichend sind, sind vom Verantwortlichen folgende Elemente zu berücksichtigen:

	a) Eignung der angebotenen technischen und organisatorischen Maßnahmen b) Fachwissen des Auftragsverarbeiters c) Zuverlässigkeit des Auftragsverarbeiters d) Ressourcen des Auftragsverarbeiters Der Datenschutzbeauftragte ist frühzeitig in den Auswahlprozess einzubeziehen. Der Verantwortliche hat fortlaufend während des Auftragsverhältnisses sicherzustellen, dass hinreichende Garantien des Auftragsverarbeiters vorliegen. Hierbei sind entsprechende Prozesse bzgl. der Kontrolle der Auftragsverarbeiter zu implementieren und zu dokumentieren. Es müssen Zuständigkeiten, die Art und Weise der Überprüfung (z. B. Vorlage von Zertifikaten, aktuelles Sicherheitskonzept, Auskünfte des Auftragsverarbeiters z. B. in einem Fragebogen, Vor-Ort-Kontrolle, Berichte der Wirtschaftsprüfer, der Internen Revision oder des Datenschutzbeauftragten) sowie Fristen der Überprüfung (in Abhängigkeit des mit der Verarbeitung verbundenen Risikos, in der Regel jährlich, sofern von dieser Frist abgewichen wird, ist dies begründet zu dokumentieren) festgelegt werden. Die Durchführung der Überprüfung ist zu dokumentieren. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. 28 Abs. 2

DS07.06	**Verantwortlicher und Auftragsverarbeiter** 1. Sofern der Auftragsverarbeiter beabsichtigt, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) zu beauftragen, muss er eine schriftliche, gesonderte oder allgemeine Genehmigung des Verantwortlichen einholen. Der Verantwortliche und Auftragsverarbeiter müssen hierbei das Vorgehen im Hinblick auf die Genehmigung des Einsatzes von Unterauftragsverarbeitern festlegen. 2. Anhand der dem IVS zugeordneten Vereinbarungen und Beschreibungen ist die Rolle der einzelnen Unterauftragsverarbeiter klar erkennbar. Eine Übersicht der genehmigten Unterauftragsverarbeiter ist in die Vereinbarung zwischen Verantwortlichen und Auftragsverarbeiter (Auftragsverarbeitungsvertrag) oder einen Anhang dazu aufgenommen und ist stets auf dem neuesten Stand zu halten. 3. Im Falle der allgemeinen Genehmigung muss der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Unterauftragsverarbeiter informieren. Der Verantwortliche muss hierdurch die Möglichkeit erhalten, gegen derartige Änderungen Einspruch zu erheben. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. 28 Abs. 4

DS07.07	**Auftragsverarbeiter** 1. Der Auftragsverarbeiter muss allen **Unterauftragsverarbeiter** im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem

	Unionsrecht oder dem Recht des betreffenden Mitgliedstaats **dieselben Datenschutzpflichten** auferlegen, zu denen er sich der Auftragsverarbeiter gegenüber dem Verantwortlichen verpflichtet hat. **2.** Der Auftragsverarbeiter arbeitet nur mit **Unterauftragsverarbeitern,** die **hinreichend Garantien** dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO – auch in Bezug auf die Sicherheit der Verarbeitung - erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet. Bei der Beurteilung, ob die Garantien des Unterauftragsverarbeiters hinreichend sind, sind vom Verantwortlichen folgende Elemente zu berücksichtigen: a) Eignung der angebotenen technischen und organisatorischen Maßnahmen b) Fachwissen des Unterauftragsverarbeiters c) Zuverlässigkeit des Unterauftragsverarbeiters d) Ressourcen des Unterauftragsverarbeiters Der Datenschutzbeauftragte ist frühzeitig in den Auswahlprozess einzubeziehen. Der Auftragsverarbeiters hat fortlaufend während des Auftragsverhältnisses sicherzustellen, dass hinreichende Garantien des Unterauftragsverarbeiters vorliegen. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. 28 Abs. 4

DS07.08	**Unterauftragsverarbeiter** Nimmt ein Auftragsverarbeiter gem. Art. 28 Abs. 4 DSGVO die Dienste eines weiteren Auftragsverarbeiters (Unterauftragsverarbeiters) in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, sind folgende Bedingungen zu erfüllen: 1. Der Verantwortliche muss eine schriftliche, gesonderte oder allgemeine Genehmigung zur Inanspruchnahme des Unterauftragsverarbeiters erteilt haben, vgl. **DS07.06**. 2. Diesem Unterauftragsverarbeiter sind im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem deutschen Recht dieselben Datenschutzpflichten auferlegen, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gem. Art. 28 Abs. 3 DSGVO festgelegt sind (vgl. **DS07.09**) (inklusive vom Unterauftragsverarbeiter angebotene Garantien für technische und organisatorische Maßnahmen zur Sicherstellung, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO – auch in Bezug auf die Sicherheit der Verarbeitung erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet). Die Auferlegung derselben Datenschutzpflichten ist hierbei formal auszulegen, d. h. es ist sicherzustellen, dass die Verpflichtungen materiell identisch sind. Sofern der Auftragsverarbeiter dem Unterauftragsverarbeiter einen Teil der Verarbeitung überträgt, für den einige der zwischen dem Verantwortlichen und Auftragsverarbeiter vereinbarten Verpflichtungen nicht gelten, sind diese nicht standardmäßig in den Vertrag mit dem Unterauftragsverarbeiter aufzunehmen (z. B. Meldung einer Verletzung des

	Schutzes personenbezogener Daten durch einen Unterauftragsverarbeiter direkt an den Verantwortlichen, Weiterleitung von Betroffenenanfragen direkt an den Verantwortlichen). In diesem Zusammenhang sind Festlegungen zu treffen, wie die Unterstützungspflichten gem. Art. 28 Abs. 3 lit. e und f DSGVO seitens des Unterauftragsverarbeiters zu erfüllen sind. Hierbei sind Festlegungen zwischen dem Auftragsverarbeiter und Unterauftragsverarbeiter zu treffen, ob der Unterauftragsverarbeiter im Falle von Betroffenenanfragen zunächst den Auftragsverarbeiter hierüber in Kenntnis setzen soll, welcher sodann den Verantwortlichen informiert, oder ob der Unterauftragsverarbeiter den Verantwortlichen über die Betroffenenanfrage direkt in Kenntnis setzen soll. Zudem sind Festlegungen zwischen dem Auftragsverarbeiter und Unterauftragsverarbeiter zu treffen, ob der Unterauftragsverarbeiter im Falle einer Verletzung des Schutzes personenbezogener Daten zunächst den Auftragsverarbeiter hierüber in Kenntnis setzen soll, welcher sodann den Verantwortlichen informiert, oder ob der Unterauftragsverarbeiter den Verantwortlichen über die Verletzung des Schutzes personenbezogener Daten direkt in Kenntnis setzen soll. Sofern die Meldung einer Verletzung des Schutzes personenbezogener Daten oder eine Weiterleitung einer Betroffenenanfrage durch den Unterauftragsverarbeiter direkt an den Verantwortlichen erfolgen soll, hat der Unterauftragsverarbeiter Prozesse implementiert haben, eine Benachrichtigung des Verantwortlichen sicherstellen (Festlegung von Zuständigkeiten und Kommunikationswegen, Festlegung, welche Informationen dem Verantwortlichen mitgeteilt werden). Sofern die Meldung einer Verletzung des Schutzes personenbezogener Daten oder eine Weiterleitung einer Betroffenenanfrage durch den Unterauftragsverarbeiter direkt an den Verantwortlichen erfolgen soll, müssen sowohl der Verantwortliche, der Auftragsverarbeiter als auch der Unterauftragsverarbeiter zustimmen. Sofern eine direkte Benachrichtigung des Verantwortlichen durch den Unterauftragsverarbeiter vereinbart ist, ist der Auftragsverarbeiter durch den Unterauftragsverarbeiter über jede Meldung zu informieren und an diesen eine Kopie der Meldung zu übermitteln. Hierfür sind Kommunikationswege und Zuständigkeiten festzulegen. Sofern eine Meldung von Datenschutzverletzungen bzw. Betroffenenanfragen durch den Unterauftragsverarbeiter an den Auftragsverarbeiter vereinbart wurde, hat der Unterauftragsverarbeiter Prozesse implementiert, die eine Benachrichtigung des Auftragsverarbeiters sicherstellen (Festlegung von Zuständigkeiten und Kommunikationswegen, Festlegung, welche Informationen dem Auftragsverarbeiter mitgeteilt werden). 3. Der Vertrag oder das andere Rechtsinstrument nach dem Unionsrecht oder dem deutschen Recht muss gem. Art. 28 Abs. 9 DSGVO schriftlich abgefasst sein, was auch in einem elektronischen Format erfolgen kann. vgl. **DS07.09**. 4. Da der Auftragsverarbeiter verpflichtet ist, dem Verantwortlichen alle Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung zu stellen, muss der Unterauftragsverarbeiter dem Auftragsverarbeiter entsprechende Informationen bereitstellen, wie die Verarbeitungstätigkeit durchgeführt wird (z. B. Sicherheitskonzept, Offenlegung von Berichten der Wirtschaftsprüfer, der Internen Revision oder des Datenschutzbeauftragten des Auftragsverarbeiters oder die Mitteilung der Ergebnisse von Datenschutzaudits oder Zertifizierungen). Zudem muss der Unterauftragsverarbeiter

	Überprüfungen, die von dem Auftragsverarbeiter selbst oder einem von diesem beauftragten Prüfer durchgeführt werden, ermöglichen. Weiterhin muss der Unterauftragsverarbeiter Überprüfungen, die von dem Verantwortlichen selbst oder einem von diesem beauftragten Prüfer durchgeführt werden, ermöglichen. 5. Der Unterauftragsarbeiter muss verpflichtet werden, sicherzustellen, dass die Verarbeitung durch weitere von ihm eingesetzte Unterauftragsverarbeiter ebenfalls auf der Grundlage eines Vertrages oder das andere Rechtsinstrument nach dem Unionsrecht oder dem deutschen Recht erfolgt und ihnen wiederum dieselben Datenschutzpflichten auferlegt werden. 6. Es sind Prozesse implementiert, die sicherstellen, dass eine Datenverarbeitung durch den Unterauftragsverarbeiter erst erfolgt, wenn der jeweilige Auftragsverarbeitungsvertrag wirksam abgeschlossen wurde. Hierfür ist mindestens geregelt: • Dokumentation wie Auftragsvergabe erfolgt (Beschaffungswege/ -prozess) • Richtlinien für die Beauftragung von Dienstleistern (z. B. Einkaufspolicy) • Festlegung wann Datenschutzbeauftragte einzubeziehen ist • Vorhandensein von Muster-Auftragsverarbeitungsverträgen • Festlegung von Zuständigkeiten bzgl. der Überprüfung, ob ein Auftragsverarbeitungsvertrag geschlossen werden muss • Festlegung von Zuständigkeiten bzgl. der Prüfung von Auftragsverarbeitungsverträgen • Festlegung von Zuständigkeiten für den Abschluss des Auftragsverarbeitungsvertrages (Unterschriftenregelung) • Dokumentation des Abschlusses des Auftragsverarbeitungsvertrages • Dokumentation des Auftragsverarbeitungsvertrages gemäß etabliertem Dokumentenmanagement **Einsatz weiterer Unterauftragsverarbeiter** Sofern der Unterauftragsverarbeiter wiederum einen weiteren Unterauftragsverarbeiter in Anspruch nimmt, so muss er sicherstellen, dass 1. Der Verantwortliche eine schriftliche, gesonderte oder allgemeine Genehmigung zur Inanspruchnahme des weiteren Unterauftragsverarbeiters erteilt hat, vgl. **DS07.06**. 2. Der Unterauftragsverarbeiter alle weiteren Unterauftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem deutschen Recht dieselben Datenschutzpflichten auferlegt, zu denen er sich gegenüber dem Auftragsverarbeiter verpflichtet hat, vgl. vorstehende Ausführungen und **DS07.09**. 3. Der Vertrag oder das andere Rechtsinstrument nach dem Unionsrecht oder dem deutschen Recht gem. Art. 28 Abs. 9 DSGVO schriftlich abgefasst ist, was auch in einem elektronischen Format erfolgen kann. vgl. **DS07.09**. 4. Der Unterauftragsverarbeiter nur mit weiteren Unterauftragsverarbeitern arbeitet, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO – auch in Bezug auf die Sicherheit der Verarbeitung - erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet, vgl. **DS07.07**.

	5. Der Unterauftragsverarbeiters fortlaufend sicherstellt, dass während des Auftragsverhältnisses hinreichende Garantien des weiteren Unterauftragsverarbeiters vorliegen, vgl. **DS07.07**. 6. Der weitere Unterauftragsarbeiter muss verpflichtet werden, sicherzustellen, dass die Verarbeitung durch weitere von ihm eingesetzte Unterauftragsverarbeiter ebenfalls auf der Grundlage eines Vertrages oder das andere Rechtsinstrument nach dem Unionsrecht oder dem deutschen Recht erfolgt und ihnen wiederum dieselben Datenschutzpflichten auferlegt werden. 7. Festlegungen getroffen werden, wie die Unterstützungspflichten gem. Art. 28 Abs. 3 lit. e und f DSGVO seitens des weiteren Unterauftragsverarbeiters zu erfüllen sind., vgl. vorstehende Anforderungen. Es sind Prozesse implementiert, die sicherstellen, dass eine Datenverarbeitung durch den weiteren Unterauftragsverarbeiter erst erfolgt, wenn der jeweilige Auftragsverarbeitungsvertrag wirksam abgeschlossen wurde. Hierfür ist mindestens geregelt: • Dokumentation wie Auftragsvergabe erfolgt (Beschaffungswege/ -prozess) • Richtlinien für die Beauftragung von Dienstleistern (z. B. Einkaufspolicy) • Festlegung wann Datenschutzbeauftragte einzubeziehen ist • Vorhandensein von Muster-Auftragsverarbeitungsverträgen • Festlegung von Zuständigkeiten bzgl. der Überprüfung, ob ein Auftragsverarbeitungsvertrag geschlossen werden muss • Festlegung von Zuständigkeiten bzgl. der Prüfung von Auftragsverarbeitungsverträgen • Festlegung von Zuständigkeiten für den Abschluss des Auftragsverarbeitungsvertrages (Unterschriftenregelung) • Dokumentation des Abschlusses des Auftragsverarbeitungsvertrages • Dokumentation des Auftragsverarbeitungsvertrages gemäß etablierten Dokumentenmanagement

[DSGVO] Art. 28 Abs. 3, 9 [GL2020-07] Abschnitt 1.3, 1.4

DS07.09	**A) Verantwortlicher** Der Verantwortliche hat mit allen im Kontext der IVS eingesetzten Auftragsverarbeitern einen Vertrag zur Auftragsverarbeitung gem. Art. 28 DSGVO geschlossen. Alle eingesetzten Auftragsverarbeiter inklusive Unterauftragsverarbeiter sind dokumentiert. Der **Vertrag zur Auftragsverarbeitung** enthält entsprechend Art. 28 DSGVO konkrete Maßgaben zur Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter: 1. Gegenstand der Verarbeitung (Art. 28 Abs. 3 DSGVO), 2. Dauer der Verarbeitung (Art. 28 Abs. 3 DSGVO), 3. Dokumentation der Art der Verarbeitung (Art. 28 Abs. 3, Art. 28 Abs. 3 lit. a DSGVO), 4. ggf. rechtliche Grundlagen der Verarbeitung (Art. 28 Abs. 3 lit. a DSGVO), 5. Verpflichtung des Auftragsverarbeiters, Daten nur auf dokumentierte Weisung - auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation - zu

	verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 lit. a DSGVO) 6. Zweck der Verarbeitung (Art. 28 Abs. 3 DSGVO), 7. Art der verarbeiteten personenbezogenen Daten (Art. 28 Abs. 3 DSGVO), 8. Kategorien der betroffenen Personen (Art. 28 Abs. 3 DSGVO), 9. Pflichten und Rechte der Verantwortlichen (Art. 28 Abs. 3 DSGVO), 10. Verpflichtung der befugten Mitarbeiter des Auftragsverarbeiters zur Vertraulichkeit und Verschwiegenheit bzw. Verweis auf eine eventuell bestehende gesetzliche Verschwiegenheitspflicht (Art. 28 Abs. 3 lit. b DSGVO), 11. Ergreifung aller Maßnahmen zur Sicherheit der Verarbeitung nach Art. 32 DSGVO (Art. 28 Abs. 3 lit. c DSGVO), 12. Festlegung, dass der Auftragsverarbeiter keine weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch nimmt (Art. 28 Abs. 2 DSGVO) und dass der Auftragsverarbeiter die Bedingungen gem. Art. 28 Abs. 2 und 4 DSGVO für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält (Art. 28 Abs. 3 lit. d DSGVO), 13. Unterstützung des Verantwortlichen bei der Bearbeitung von Anträgen betroffener Personen (Art. 28 Abs. 3 lit. e DSGVO), 14. Unterstützung des Verantwortlichen bei der Erfüllung der Pflichten nach Art. 32 bis 36 durch den Auftragsverarbeiter (Art. 28 Abs. 3 lit. f DSGVO, detailliertere Anforderungen dazu in den nachfolgenden Kriterien), 15. Löschung bzw. Rückgabe der PBD nach Abschluss der Erbringung der Verarbeitungsleistungen (Art. 28 Abs. 3 lit. g DSGVO), 16. Bereitstellung der Informationen zum Nachweis der Erfüllung der hier genannten Verpflichtungen (Art. 28 Abs. 3 lit. h DSGVO), 17. Ermöglichen und Unterstützen von Prüfungen zum Nachweis der Erfüllung der hier genannten Verpflichtungen (Art. 28 Abs. 3 lit. h DSGVO), 18. Informationspflicht des Auftragsverarbeiters gegenüber dem Verantwortlichen über das Bestehen einer widerrechtlichen Anweisung (Art. 28 Abs. 3 Satz 3 DSGVO). Der jeweilige Gegenstand der Auftragsverarbeitungen (Leistungsbeschreibung) ist definiert. Es sind Prozesse im Hinblick auf die Auswahl und Überprüfung der eingesetzten Auftragsverarbeiter implementiert. Diesbezüglich gelten die Anforderungen von **DS07.05.** Der Vertrag oder das andere Rechtsinstrument nach dem Unionsrecht oder dem deutschen Recht ist gem. Art. 28 Abs. 9 DSGVO schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann. Der Vertrag oder das andere Rechtsinstrument muss für den Auftragsverarbeiter in Bezug auf den Verantwortlichen verbindlich sein, d. h. er muss

	dem Auftragsverarbeiter Verpflichtungen auferlegen, die nach dem Unionsrecht oder dem Recht der Mitgliedstaaten verbindlich sind. Zudem müssen darin die Pflichten des Verantwortlichen niedergelegt werden. Es sind Prozesse implementiert, die sicherstellen, dass eine Datenverarbeitung erst erfolgt, wenn der jeweilige Auftragsverarbeitungsvertrag wirksam abgeschlossen wurde. Hierfür ist mindestens geregelt: • Dokumentation wie Auftragsvergabe erfolgt (Beschaffungswege/ -prozess) • Richtlinien für die Beauftragung von Dienstleistern (z. B. Einkaufspolicy) • Festlegung wann Datenschutzbeauftragte einzubeziehen ist • Vorhandensein von Muster-Auftragsverarbeitungsverträgen • Festlegung von Zuständigkeiten bzgl. der Überprüfung, ob ein Auftragsverarbeitungsvertrag geschlossen werden muss • Festlegung von Zuständigkeiten bzgl. der Prüfung von Auftragsverarbeitungsverträgen • Festlegung von Zuständigkeiten für den Abschluss des Auftragsverarbeitungsvertrages (Unterschriftenregelung) • Dokumentation des Abschlusses des Auftragsverarbeitungsvertrages • Dokumentation des Auftragsverarbeitungsvertrages gemäß etablierten Dokumentenmanagement Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen. **B) Auftragsverarbeiter** Der Auftragsverarbeiter hat mit allen im Kontext der IVS eingesetzten Unterauftragsverarbeiter einen Vertrag zur Auftragsverarbeitung gem. Art. 28 DSGVO geschlossen. Alle eingesetzten Unterauftragsverarbeiter sind dokumentiert. Der jeweilige Gegenstand der Auftragsverarbeitung (Leistungsbeschreibung) ist definiert. Der **Vertrag zur Auftragsverarbeitung** enthält entsprechend Art. 28 DSGVO konkrete Maßgaben zur Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter: 1. Gegenstand der Verarbeitung (Art. 28 Abs. 3 DSGVO), 2. Dauer der Verarbeitung (Art. 28 Abs. 3 DSGVO), 3. Dokumentation der Art der Verarbeitung (Art. 28 Abs. 3, Art. 28 Abs. 3 lit. a DSGVO), 4. ggf. rechtliche Grundlagen der Verarbeitung (Art. 28 Abs. 3 lit. a DSGVO), 5. Verpflichtung des Auftragsverarbeiters, Daten nur auf dokumentierte Weisung - auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation - zu verarbeiten (Art. 28 Abs. 3 lit. a DSGVO) 6. Zweck der Verarbeitung (Art. 28 Abs. 3 DSGVO), 7. Art der verarbeiteten personenbezogenen Daten (Art. 28 Abs. 3 DSGVO),

	8. Kategorien der betroffenen Personen (Art. 28 Abs. 3 DSGVO), 9. Pflichten und Rechte der Verantwortlichen (Art. 28 Abs. 3 DSGVO), 10. Verpflichtung der befugten Mitarbeiter des Auftragsverarbeiters zur Vertraulichkeit und Verschwiegenheit bzw. Verweis auf eine eventuell bestehende gesetzliche Verschwiegenheitspflicht (Art. 28 Abs. 3 lit. b DSGVO), 11. Ergreifung aller Maßnahmen zur Sicherheit der Verarbeitung nach Art. 32 DSGVO (Art. 28 Abs. 3 lit. c DSGVO), 12. Festlegung, dass der Auftragsverarbeiter keine weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch nimmt (Art. 28 Abs. 2 DSGVO) und das der Auftragsverarbeiter die Bedingungen gem. Art. 28 Abs. 2 und 4 DSGVO für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält (Art. 28 Abs. 3 lit. d DSGVO),Unterstützung des Verantwortlichen bei der Bearbeitung von Anträgen betroffener Personen (Art. 28 Abs. 3 lit. e DSGVO), 13. Unterstützung des Verantwortlichen bei der Erfüllung der Pflichten nach Art. 32 bis 36 durch den Auftragsverarbeiter (Art. 28 Abs. 3 lit. f DSGVO, detailliertere Anforderungen dazu in den nachfolgenden Kriterien), 14. Löschung bzw. Rückgabe der PBD nach Abschluss der Erbringung der Verarbeitungsleistungen (Art. 28 Abs. 3 lit. g DSGVO), 15. Bereitstellung der Informationen zum Nachweis der Erfüllung der hier genannten Verpflichtungen (Art. 28 Abs. 3 lit. h DSGVO), 16. Ermöglichen und Unterstützen von Prüfungen zum Nachweis der Erfüllung der hier genannten Verpflichtungen (Art. 28 Abs. 3 lit. h DSGVO), 17. Informationspflicht des Auftragsverarbeiters gegenüber dem Verantwortlichen über das Bestehen einer widerrechtlichen Anweisung (Art. 28 Abs. 3 Satz 3 DSGVO). Die jeweilige operative Durchführung der Auftragsverarbeitung muss beschrieben sein. Der Auftragsverarbeiter hat ein revisionssicheres Auftragsmanagement implementiert, hierzu gehören insbesondere 1. Dokumentation der Abläufe der Auftragsverarbeitung einschließlich der Tätigkeiten von weiteren Auftragsverarbeitern, 2. Beschreibung von Rollen und Schnittstellen, 3. Sicherstellung, dass erst nach Abschluss des Auftragsverarbeitungsvertrages mit der Auftragsverarbeitung begonnen wird, 4. Protokollierung von Änderungen der Auftragsverarbeitung. Der Vertrag oder das andere Rechtsinstrument nach dem Unionsrecht oder dem deutschen Recht ist gem. Art. 28 Abs. 9 DSGVO schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann. Der Auftragsverarbeiter hat Prozesse zur Auswahl und Überprüfung der Unterauftragsverarbeiter implementiert. Diesbezüglich gelten die Anforderungen von **DS07.07.** Die zur Verarbeitung der personenbezogenen Daten befugten Personen beim Auftragsverarbeiter und bei den Unterauftragsverarbeitern müssen zur Vertraulichkeit verpflichtet sein oder einer gesetzlichen Verschwiegenheitspflicht unterliegen.

	Der Vertrag oder das andere Rechtsinstrument nach dem Unionsrecht oder dem deutschen Recht ist gem. Art. 28 Abs. 9 DSGVO schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann. Der Vertrag oder das andere Rechtsinstrument muss für den Auftragsverarbeiter in Bezug auf den Verantwortlichen verbindlich sein, d. h. er muss dem Auftragsverarbeiter Verpflichtungen auferlegen, die nach dem Unionsrecht oder dem Recht der Mitgliedstaaten verbindlich sind. Zudem müssen darin die Pflichten des Verantwortlichen niedergelegt werden. Es sind Prozesse implementiert, die sicherstellen, dass eine Datenverarbeitung erst erfolgt, wenn der jeweilige Auftragsverarbeitungsvertrag wirksam abgeschlossen wurde. Hierfür ist mindestens geregelt: • Dokumentation wie Auftragsvergabe erfolgt (Beschaffungswege/ -prozess) • Richtlinien für die Beauftragung von Dienstleistern (z. B. Einkaufspolicy) • Festlegung wann Datenschutzbeauftragte einzubeziehen ist • Vorhandensein von Muster-Auftragsverarbeitungsverträgen • Festlegung von Zuständigkeiten bzgl. der Überprüfung, ob ein Auftragsverarbeitungsvertrag geschlossen werden muss • Festlegung von Zuständigkeiten bzgl. der Prüfung von Auftragsverarbeitungsverträgen • Festlegung von Zuständigkeiten für den Abschluss des Auftragsverarbeitungsvertrages (Unterschriftenregelung) • Dokumentation des Abschlusses des Auftragsverarbeitungsvertrages • Dokumentation des Auftragsverarbeitungsvertrages gemäß etablierten Dokumentenmanagement Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. Art. 28 Abs. 3 lit. a, Art. 29

DS07.10	**A) Verantwortlicher** Die Auftragsverarbeitung erfolgt stets auf **Weisung des Verantwortlichen** – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation. Das Verfahren für die Weisungserteilung sind zwischen Verantwortliche und Auftragsverarbeiter festzulegen. Mündliche Weisungen werden schriftlich (z. B. per E-Mail) nachgefasst. Weisungsbefugte Personen des Anwenders und befugte Empfänger beim Auftragsverarbeiter sind definiert. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen. **B) Auftragsverarbeiter** Die Auftragsverarbeitung durch den Auftragsverarbeiter, die ihm unterstellten Personen und weiteren Auftragsverarbeiter erfolgt stets auf **Weisung des Verantwortlichen** – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation. Mündliche Weisungen werden schriftlich nachgefasst. Erteilte Weisungen werden dokumentiert und archiviert. Weisungsbefugte Personen des Anwenders und befugte Empfänger beim Auftragsverarbeiter sind

	definiert. Es sind Prozesse implementiert, die eine Überprüfung der Weisungen auf Datenschutzkonformität sicherstellen (Festlegung von Zuständigkeiten bzgl. der Prüfung von Weisungen, Kommunikationswege, Festlegung wann Datenschutzbeauftragte einzubeziehen ist). Wenn die Weisungen des Verantwortlichen keine Übermittlung oder Offenlegung an Drittländer zulassen, darf der Auftragsverarbeiter weder einen Unterauftragsverarbeiter in einem Drittland mit der Verarbeitung beauftragen, noch darf er die Daten in einer seiner Abteilungen außerhalb der EU verarbeiten lassen. Der Auftragsverarbeiter muss den Verantwortlichen unverzüglich informieren, wenn er der Ansicht ist, dass eine Weisung des Verantwortlichen gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder Deutschlands verstößt. Der Auftragsverarbeiter muss den Verantwortlichen umgehend informieren, wenn eine Weisung möglicherweise gegen das Datenschutzrecht verstößt. Die Zuständigkeiten und Kommunikationswege hierfür sind zu dokumentieren. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

[DSGVO] Art. 30

DS07.11	**A) Verantwortlicher** Der Verantwortliche erstellt gem. Art. 30 Abs. 1 DSGVO ein Verzeichnis von Verarbeitungstätigkeiten mit folgenden Inhalten: 1. Name und Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten, 2. Vorgesehene Zwecke der Verarbeitung (Art. 30 Abs. 1 lit. b DSGVO), 3. Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 lit. c DSGVO), 4. Beschreibung der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DSGVO), 5. Kategorien von Empfängern, denen mit Hilfe des IVS PBD offengelegt werden können (Art. 30 Abs. 1 lit. d DSGVO), 6. ggf. 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 Art. 49 Abs. 1 Unterabsatz 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien, 7. im IVS vorgesehene Löschfristen für die PBD (Art. 30 Abs. 1 lit. f DSGVO), 8. ggf. allgemeine Beschreibung spezieller technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO, die im Zusammenhang mit dem Einsatz des IVS erforderlich sind. 9. Im Kontext der Rechenschaftspflicht sind die jeweiligen Rechtsgrundlagen im VVT aufgeführt. Das Verzeichnis von Verarbeitungstätigkeiten ist regelmäßig auf Vollständigkeit sowie Aktualität zu prüfen und bei Änderungen an den Verarbeitungstätigkeiten anzupassen. Zuständigkeiten für die regelmäßige

	Überprüfung und Anpassung des Verzeichnisses von Verarbeitungstätigkeiten sind festzulegen. Änderungen am Verzeichnis von Verarbeitungstätigkeiten müssen dokumentiert und mindestens ein Jahr gespeichert werden (Änderungshistorie). Eine Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten besteht gem. Art. 30 Abs. 5 DSGVO nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn, die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 DSGVO bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO. Sofern der Verantwortliche aufgrund des Ausnahmetatbestandes des Art. 30 Abs. 5 DSGVO kein Verzeichnis von Verarbeitungstätigkeiten führt, ist zu dokumentieren, dass tatsächlich keine der Gegenausnahmen vorliegt. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen. Im Falle einer gemeinsamen Verantwortung führt jeder der Verantwortlichen ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO. Hierbei ist anzugeben, ob die jeweilige Verarbeitungstätigkeit in gemeinsamer oder alleiniger Verantwortung erfolgt. **B) Auftragsverarbeiter** Der Auftragsverarbeiter erstellt gem. Art. 30 Abs. 2 DSGVO ein Verzeichnis von Verarbeitungstätigkeiten mit folgenden Inhalten: 1. Name und Kontaktdaten des Auftragsverarbeiters sowie jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist und eines etwaigen Datenschutzbeauftragten (Art. 30 Abs. 2 lit. a DSGVO), 2. Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden (Art. 30 Abs. 2 lit. b DSGVO), 3. ggf. 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 Art. 49 Abs. 1 Unterabsatz 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien (Art. 30 Abs. 2 lit. c DSGVO), 4. ggf. allgemeine Beschreibung spezieller technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO, die im Zusammenhang mit dem Einsatz des IVS erforderlich sind (Art. 30 Abs. 2 lit. d DSGVO). Das Verzeichnis von Verarbeitungstätigkeiten ist regelmäßig auf Vollständigkeit sowie Aktualität zu prüfen und bei Änderungen an den Verarbeitungstätigkeiten anzupassen. Zuständigkeiten für die regelmäßige Überprüfung des Verzeichnisses von Verarbeitungstätigkeiten sind festzulegen. Änderungen am Verzeichnis von Verarbeitungstätigkeiten müssen dokumentiert und mindestens ein Jahr gespeichert werden (Änderungshistorie). Eine Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten besteht gem. Art. 30 Abs. 5 DSGVO nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn, die

	von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 DSGVO bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO. Sofern der Auftragsverarbeiter aufgrund des Ausnahmetatbestandes des Art. 30 Abs. 5 DSGVO kein Verzeichnis von Verarbeitungstätigkeiten führt, ist zu dokumentieren, dass tatsächlich keine der Gegenausnahmen vorliegt. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

DS08 Sicherheit der Verarbeitung

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen müssen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (vgl. Art. 32 Abs. 1 DSGVO). Bei der Beurteilung des Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugtem Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Im vorliegenden Kapitel werden die technischen und organisatorischen Maßnahmen betrachtet, welche durch den Verantwortlichen und dem Auftragsverarbeiter umgesetzt werden müssen. Sofern durch den Verantwortlichen Auftragsverarbeiter eingesetzt werden, ist zu prüfen, ob diese Auftragsverarbeiter angemessene technische und organisatorische Maßnahmen implementiert haben.

Sofern durch den Auftragsverarbeiter weitere Unterauftragsverarbeiter eingesetzt werden, ist zu prüfen, ob auch für diese Unterauftragsverarbeiter angemessene technische und organisatorische Maßnahmen vertraglich vereinbart wurden.

Im Hinblick auf die Beurteilung, ob geeignete technische und organisatorische Maßnahmen getroffen wurden, ist zu berücksichtigen, welche Risiken für die Rechte und Freiheiten für die Betroffenen im Hinblick auf die Datenverarbeitungen im Kontext des IVS bestehen. Hierbei ist zu evaluieren, ob die Verarbeitungsvorgänge ein Risiko oder ein hohes Risiko für die Betroffenen bergen. Die Anforderungen, welche an eine Risikoanalyse gestellt werden, sind unten aufgeführt. Auf Basis der ermittelten Risiken für die Rechte und Freiheiten der natürlichen Personen ist anschließend eine Schutzbedarfsfeststellung (normal oder hoch) vorzunehmen. Abgeleitet aus der Schutzbedarfsfeststellung sind die unten aufgeführten Standardanforderungen (Schutzbedarfsfeststellung normal) oder zusätzlich zu den Standardanforderungen die Anforderungen bei erhöhtem Schutzbedarf (Schutzbedarfsfeststellung hoch) umzusetzen.

Bei der Beurteilung der Angemessenheit der implementierten technischen und organisatorischen Maßnahmen ist zu berücksichtigen, ob diese dem aktuellen Stand der Technik entsprechen. Bei der Beurteilung des Stands der Technik orientieren sich die Evaluatoren insbesondere an der Handreichung zum Stand der Technik, Bundesverband der IT-Sicherheit (jeweils aktuelle Version), Veröffentlichungen der Datenschutz-Aufsichtsbehörden, Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) (z. B. Technische Richtlinien, IT-Grundschutz-Kompendium), Veröffentlichungen der Europäischen Agentur für Netz- und Informationssicherheit (ENISA).

Die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DSGVO kann herangezogen werden, um nachzuweisen, dass geeignete technische und organisatorische Maßnahmen getroffen wurden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Weiterhin können anerkannte internationale Zertifizierungen (z. B. DIN EN ISO / IEC 27000-Reihe, BSI C5 etc.) als Nachweis herangezogen werden. In diesem Zusammenhang ist zu evaluieren, ob die genehmigten Verhaltensregeln bzw. die anerkannte internationale Zertifizierung auf den Evaluierungsgegenstand Anwendung finden.

[DSGVO] Art. 32 Abs. 1 lit. d

DS08.01	**Verantwortlicher und Auftragsverarbeiter** Das Sicherheitsniveau des Evaluierungsgegenstands und die Wirksamkeit der implementierten technischen Maßnahmen muss durch die Durchführung eines Penetrationstests (Pentest) nachgewiesen und in einem Prüfbericht dokumentiert werden. Der Penetrationstest kann im Kontext der Evaluierung durchgeführt werden oder durch Dritte erbracht werden (Third-Party-Pentest). Sofern ein Third-Party-Pentest eingereicht wird, sind die folgenden Anforderungen zu

	erfüllen. • Der Pentest muss von einer nach DIN EN ISO/IEC 17025 zugelassenen Konformitätsbewertungsstelle durchgeführt worden sein. • Der Pentest muss sich auf die exakte Version des Evaluierungsgegenstandes beziehen. • Aus dem Prüfbericht muss der Scope des Pentest bzw. die betrachteten Komponenten eindeutig hervorgehen. Alle Komponenten/Funktionen des Evaluierungsgegenstandes müssen überprüft worden sein. • Aus dem Prüfbericht muss hervorgehen wie getestet wurde (manuell/automatisiert). Voll automatisierte Tests sind nicht zulässig. • Die verwendeten Testkonten-/rollen müssen dokumentiert sein. • Es muss klar erkennbar sein, welche Prüf- bzw. Angriffsverfahren zum Einsatz kamen, so dass erkennbar ist, dass mindestens alle Risiken des OWASP Top 10 Katalogs geprüft wurden bzw. Bestandteil der Tests gewesen sind / berücksichtigt wurden. Um die umgesetzten Sicherheitsmaßnahmen des Evaluierungsgegenstandes hinsichtlich Wirksamkeit und Vollständigkeit zu bewerten und Risiken zu identifizieren sind im Kontext der Pentests mindestens folgende Prüfungen durchzuführen: a) Port- und Schwachstellenscans Im Rahmen von Port- und Schwachstellenscans und somit Tests auf Netzwerkebene, sind die relevanten Systeme des Evaluierungsgegenstands auf die ermittelten erreichbaren Dienste sowie IT-Schwachstellen hin zu überprüfen. Dabei sind insbesondere folgende Schritte bzw. Scans durchzuführen: • Ermittlung aller (von außen / aus dem Internet) erreichbaren Netzwerkdienste mittels automatisierter Portscans (Protokolle TCP und UDP) der Zielsysteme, • SSL/TLS-Scan (bei entsprechend verfügbaren Diensten) zur Ermittlung der eingesetzten SSL/TLS-Version und -Konfiguration, • Automatisierte Schwachstellenscans gegen die identifizierten Netzwerkdienste. Die Ergebnisse werden anschließend bewertet und verifiziert um False-Positive Schwachstellen/Sachverhalte zu ermitteln. Darüber hinaus werden öffentlich verfügbare Quellen (z. B. CVE Datenbanken) genutzt, um Informationen über potenzielle Schwachstellen des Untersuchungsgegenstands bzw. der verwendeten Dienste/Software (z. B. eines Webservers) zu ermitteln. b) Konfigurationsanalysen von Systemen und Komponenten Im Rahmen von Konfigurationsanalysen erfolgt eine manuelle Untersuchung auf System- bzw. Anwendungsebene. Die Konfigurationsanalyse erfolgt gemäß White-Box-Ansatz. Ein (administrativer) Zugriff auf das zu untersuchende Systeme wird somit vorausgesetzt. Die Konfigurationsanalysen werden zusammen mit dem Verantwortlichen bzw. Auftragsverarbeiter durchgeführt. Hierbei ist der uneingeschränkte Zugriff auf die Systeme und Komponenten notwendig. Im Rahmen der Konfigurationsanalysen müssen sicherheitsrelevante und ggf. funktionale Konfigurationseinstellungen eingesehen werden. Dabei werden im Wesentlichen technische Maßnahmen zur Systemhärtung,

	Patchmanagement, Routing, Protokollierung, Monitoring und ggf. Cluster- und Virtualisierungslösungen untersucht. c) Penetrationstest auf Anwendungsebene Im Rahmen des Penetrationstests auf Anwendungsebene sind die ausgewählten Anwendungen (z. B. mobile Apps, Webanwendungen) zu überprüfen. Der Penetrationstest muss als Kombination aus automatisierten und manuellen Tests durchgeführt werden. Ausschließlich vollautomatisierte Tests sind nicht zulässig. Im Rahmen der automatisierten Tests wird gegen die relevanten Systeme des Evaluierungsgegenstandes (z. B. der Webserver) die Prüfhandlungen gem. a) Port- und Schwachstellenscans angewendet, um Überprüfungen auf der Netzwerkebene durchzuführen. Im Rahmen der manuellen Tests wird im Wesentlichen das Tool Burp Suite Professionals genutzt. Die Vorgehensweise orientiert an • das Durchführungskonzept für Penetrationstests vom Bundesamt für Sicherheit in der Informationstechnik. Darüber hinaus werden, je nach Evaluierungsgegenstand • die „Open Web Application Security Project (OWASP) Top 10 Web Application Security Risks“, • die „OWASP Top 10 API Security Risks“ und/oder • die „OWASP Mobile Top 10 Security Risks“ in der jeweils aktuellen Version berücksichtigt bzw. Prüfungen auf diese Risiken durchgeführt. Die zugehörigen Tests sind im OWASP Application Security Verification Standard (ASVS) bzw. OWASP Mobile Application Security Verification Standard (MASVS) beschrieben. Der Fokus des Pentests liegt somit, je nach Anwendbarkeit, auf nachfolgenden Bereichen: • Injection / Ein- und Ausgabevalidierung • Authentifizierung (Session Management) • Zugriffskontrolle (Autorisierung) / Mandantentrennung • Datensicherheit / Verlust der Vertraulichkeit sensibler Daten • Sicherheitsrelevante Fehlkonfiguration / Mangelnde Härtung • Anwendungslogik • Herausgabe sicherheitsrelevanter Informationen / Information Disclosure Abhängig von den spezifischen Eigenschaften des jeweiligen Untersuchungsgegenstands werden ggf. Besonderheiten oder weitere Schwerpunktthemen berücksichtigt. Alle Ergebnisse des Penetrationstests werden in Form eines Abschlussberichtes in deutscher Sprache (alternativ englisch) zur Verfügung gestellt. Dazu werden die Ergebnisse der Prüfung analysiert, bewertet und untereinander priorisiert. Schwachstellen, welche mit einem Risikograd „Mittel“ oder höher eingestuft werden, sind zertifizierungsverhindernd und müssen für eine erfolgreiche Zertifizierung behoben werden. Die Risikoanalyse wird nach dem anerkannten Standard BSI-Standard 200-3 durchgeführt. Zu jeder Schwachstelle wird eine Risikokategorie definiert, mit der die Kritikalität der jeweiligen Schwachstelle beschrieben wird. Das Gesamtrisiko setzt

	sich dabei aus den Auswirkungen (Impact), sowie der Eintrittshäufigkeit (Likelihood) zusammen. Bei der Einschätzung der Risikograde ist zu berücksichtigen, dass die Angabe eines Risikograds immer subjektiv erfolgt. Nicht bekannte Details oder unterschiedliche Interpretation der Sicherheitsanforderungen können zu einer anderen als der in diesem Bericht abgegebenen Bewertung führen. Für identifizierte Schwachstellen ist ein Risikomaßnahmenplan zu erstellen, welcher mindestens folgendes beinhaltet: • Technische und organisatorische Abhilfemaßnahmen • Priorität der Risikobehandlung • Zuständigkeiten für die Umsetzung • Fristen für die Umsetzung der Abhilfemaßnahmen • Dokumentation wann Maßnahme umgesetzt wurde • Stand (Datum) des Risikomaßnahmenplans Die Historie des Risikomaßnahmenplans ist mindestens ein Jahr aufzubewahren. Sofern seitens des Verantwortlichen bzw. Auftragsverarbeiters Schwachstellen behoben werden, die im Rahmen des initialen Penetrationstests identifiziert wurden, muss mittels Re-Test nachgewiesen werden, dass diese behoben wurden. Zudem muss dokumentiert werden, wie diese behoben wurden. Die Ergebnisse des Penetrationstests müssen in den etablierten Risikomanagementprozess (vgl. die Anforderungen in **DS08.02**) einbezogen werden. Im Hinblick auf die Überwachung der Wirksamkeit der technischen und organisatorischen Maßnahmen sind ergänzend zu dem verpflichtenden Nachweis des Penetrationstests weiterhin regelmäßig Penetrationstests durchzuführen. Hierfür muss eine entsprechende Planung vorhanden sein, die insbesondere vorsieht: • Häufigkeit der Penetrationstests • Art des Penetrationstests (intern oder extern) • Umfang der Penetrationstests • Zuständigkeiten für Durchführung der Penetrationstest • Prozesse bzgl. des Umgangs mit Feststellungen aus der Untersuchung inklusive Erstellung Risikomaßnahmenplan (inhaltliche Anforderungen siehe vorstehend) Im Hinblick auf die Bestimmung der Häufigkeit der Penetrationstest gilt folgender Maßstab: Sofern im Rahmen der systematischen Analyse möglicher Risiken für den Schutz der personenbezogenen Daten, die sich aus deren Verarbeitung mit dem IVS ergeben, die Schutzbedarfsfeststellung zu dem Ergebnis „hoch“ kommt (vgl. **DS08.02**) sind Penetrationstests mindestens jährlich oder anlassbezogen (z. B. bei sicherheitsrelevanten Änderungen an der IT-Infrastruktur, bekannte Sicherheitsvorfälle oder erhöhtes Risiko durch Bedrohungslage) durchzuführen. Bei einem normalen Schutzbedarf sind Penetrationstest aller zwei Jahre oder anlassbezogen durchzuführen (z. B. bei sicherheitsrelevanten Änderungen an der IT-Infrastruktur, bekannte Sicherheitsvorfälle oder erhöhtes Risiko durch Bedrohungslage).

[DSGVO] Art. 32 Abs. 1, 2

DS08.02	**Verantwortlicher und Auftragsverarbeiter** Den im Zusammenhang mit dem Betrieb des IVS vorgesehenen technischen und organisatorischen Maßnahmen liegt eine systematische **Analyse möglicher Risiken** für den Schutz der personenbezogenen Daten, die sich aus deren Verarbeitung mit dem IVS ergeben, zu Grunde. Die Prozesse der Risikoermittlung, Risikobewertung und Risikobehandlung müssen in einem systematischen Verfahren dokumentiert sein, das regelmäßig durchgeführt wird und sich an standardisierten Vorgehensweisen zum Risikomanagement ([BSI-200-3], [ISO 31000], [ISO/IEC 27005], [ISO 14971]) orientiert. Das Risikomanagement muss folgende Anforderungen erfüllen: 1. Die Prozesse zum Risikomanagement müssen regelmäßig (mindestens jährlich) durchlaufen werden und bei Bedarf, insbesondere bei Änderungen von Risiken angepasst werden. Die Verantwortlichen für das Risikomanagement müssen die Risikobewertung und Risikobehandlung inklusive der Akzeptanz der Restrisiken freigeben. 2. Risikoidentifikation: Es müssen relevante Risikoquellen systematisch identifiziert werden. Hierbei ist zu bestimmen, welche Ereignisse (Ursachen) zu einem bestimmten Ereignis führen können und durch welche Umstände oder Handlungen diese eintreten können. Die Risikoszenarien müssen so konkret wie möglich gefasst werden. Es ist bei der Risikoidentifikation der gesamte Verarbeitungszyklus zu berücksichtigen. 3. Risikoanalyse: Bei der Risikoanalyse müssen für jedes identifizierte Risiko folgende Parameter bestimmt werden: • Art der Verarbeitung einschließlich Kategorien der personenbezogenen Daten • Umfang der Verarbeitung: Hierbei ist die Menge der personenbezogenen Daten und die Anzahl der betroffenen Personen, deren Daten verarbeitet werden, zu berücksichtigen. • Umstände der Verarbeitung: Hierbei sind insbesondere die an der Verarbeitung Beteiligten sowie der Ort und die Dauer einer Verarbeitung, die Quelle der Daten und die Art der Erhebung zu berücksichtigen • Zweck der Verarbeitung: Hierbei bedarf eines eindeutig festgelegten Zwecks. 4. Risikobewertung und Risikobehandlung: Für die Risikobewertung müssen die möglichen Risikoniveaus (Kombination aus Eintrittswahrscheinlichkeit und Schadensausmaß) in einer Risikomatrix definiert werden. Für die Risikobehandlung müssen angemessene Risikoakzeptanzkriterien definiert werden. Bei der Auswahl von risikomitigierenden Maßnahmen muss sich am IT-Grundschutz-Kompendium des BSI, Umsetzungshinweise der ISO/IEC 27002, und Maßnahmenkatalog des Standarddatenschutzmodells orientiert werden. Für jedes analysierte Risiko müssen folgende Parameter bestimmt werden: • Eintrittswahrscheinlichkeit, • Schadensausmaß (hinsichtlich der Betroffenenrechte) • Risikoniveau entsprechend der festgelegten Risikomatrix • Schutzbedarfsfeststellung (normal oder hoch)

	• Risikoeigentümer • Geplante risikominimierende Maßnahmen • Restrisiko nach Umsetzung der risikominimierenden Maßnahmen • Datenschutz-Folgenabschätzung Ergibt sich in der Schutzbedarfsfeststellung ein hoher Schutzbedarf, so müssen zusätzlich zu den technischen und organisatorischen Standardanforderungen aus den Kapiteln **DS08.01, DS08.03 bis DS08.05** die Anforderungen für den hohen Schutzbedarf erfüllt werden. Im Rahmen des etablierten Risikomanagements sind auch die Ergebnisse von durchgeführten Penetrationstests (Risikoidentifikation, Risikoanalyse, Risikobewertung und Risikobehandlung) zu berücksichtigen, vgl.**DS08.01.** Im Kontext der Risikoanalyse ist zu evaluieren, ob eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO durchzuführen ist, vgl. die Anforderungen in **DS10**. Die implementierten technischen und organisatorischen Maßnahmen sind in einem **Datensicherheitskonzept** zu dokumentieren. Das Datensicherheitskonzept muss zumindest Regelungen treffen zu: • Rollen und Zuständigkeiten • Anwendungsbereich • Maßnahmen zur Gewährleistung der Vertraulichkeit (Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Trennungskontrolle, Pseudonymisierung, Verschlüsselung) • Maßnahmen zur Gewährleistung der Integrität (Weitergabekontrolle, Eingabekontrolle) • Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit • Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung • Überprüfung und Aktualisierung des Datensicherheitskonzeptes Das Datensicherheitskonzept ist regelmäßig auf Aktualität zu prüfen (mindestens jährlich oder bei Veränderungen) und weiterzuentwickeln. **Ergänzend für Auftragsverarbeiter** Sofern der Verantwortliche für die Umsetzung einzelner technischer und organisatorischer Maßnahmen verantwortlich ist, muss der Auftragsverarbeiter den Verantwortlichen hierüber informieren. Hierfür muss eine entsprechende Dokumentation vorhanden sein.

[DSGVO] Art. 25 Abs. 1, 2, [DSGVO] Art. 32 Abs. 1 lit. a, b

DS08.03	**Verantwortlicher und Auftragsverarbeiter** Der Verantwortliche und Auftragsverarbeiter treffen unter Berücksichtigung des Stands der Technik geeignete technische und organisatorische Maßnahmen zur Sicherstellung der Vertraulichkeit der verarbeiteten PBD. Zudem ist dafür Sorge zu tragen, dass auch eingesetzte Auftragsverarbeiter bzw. Unterauftragsverarbeiter diese Maßnahmen umgesetzt haben. Die nachfolgenden Standardanforderungen an die Vertraulichkeit der verarbeiteten PBD müssen umgesetzt werden. Ergibt sich in der Schutzbedarfsfeststellung ein hoher Schutzbedarf, so müssen zusätzlich zu Standardanforderungen die Anforderungen für den hohen Schutzbedarf erfüllt werden.

1. Zutrittskontrollmaßnahmen

Der Verantwortliche und Auftragsverarbeiter müssen Zutrittskontrollmechanismen etabliert haben, die sicherstellen, dass der Zutritt zu Gebäuden und Räumlichkeiten wie auch der Zugang zum IVS für Unbefugte ausgeschlossen ist.

Standardanforderungen:

1. Sicherheitskonzept:
   a. Ein Konzept zu Zutrittsregelungen und zur physischen Zugangskontrolle (Perimeterschutz) von Büros, Räumen und Einrichtungen muss dokumentiert und umgesetzt werden.
   b. Es müssen Sicherheitsbereiche mit physische Zutrittskontrollen festgelegt werden.
2. Bauliche Sicherheitsmaßnahmen:
   a. Es müssen Maßnahmen zum Brandschutz (Feuer-, Rauchmelder, Brandmeldeanlage, Löschanlage, etc.) getroffen werden.
   b. Kabel, die Strom oder Daten transportieren, müssen vor Abhören, Störung oder Beschädigung geschützt werden.
3. Schlüsselverwaltung und Zutrittsmittel:
   a. Es muss eine dokumentierte Regelung zur physischen Schlüsselverwaltung vorliegen.
   b. Die Ausgabe und der Entzug von Zutrittsmitteln wie Chipkarten und Schlüsseln müssen dokumentiert werden.
   c. Zutrittsmittel, die kompromittiert oder verloren sind, müssen ausgewechselt bzw. gesperrt werden.
4. Umgang mit Besuchern und externen Dienstleistern:
   a. Es muss eine Regelung zum Umgang mit Besuchern geben. In gesicherten Bereichen muss es eine ständige Begleitung der Besucher durch eine befugte Person geben.
   b. Es müssen Regelungen für externe Dienstleister, wie Verschwiegenheitserklärung und persönliche Begleitung, getroffen werden.
5. Überprüfung und Aktualisierung von Zutrittsberechtigungen:
   a. Zutrittsberechtigungen müssen regelmäßig auf Aktualität und Angemessenheit überprüft und bei Bedarf aktualisiert werden.
   b. Bei längeren Abwesenheiten müssen Zutrittsberechtigungen vorübergehend gesperrt werden.
   c. Es muss eine Multi-Faktor-Authentifizierung für den Zutritt zu Datenverarbeitungsanlagen geben.
6. Protokollierung:
   a. Es muss eine Protokollierung des physischen Zutritts zu Räumlichkeiten in gesicherten Bereichen oder mit Datenverarbeitungsanlagen geben.

Anforderungen für den hohen Schutzbedarf:

7. Bauliche Sicherheitsmaßnahmen:
   a. Maßnahmen wie Umzäunung, Videoüberwachung, einbruchsichere Türen und Fenster sind erforderlich. Die Ausgestaltung dieser Maßnahmen muss das Risiko für die Rechte und Freiheiten der Betroffenen berücksichtigen.
8. Protokollierung:
   a. Jeder unbefugte Zutritt und jeder Zutrittsversuch muss protokolliert werden und nachträglich feststellbar sein.

2. Zugangskontrolle sowie Identitäts- und Berechtigungsmanagement

Der Verantwortliche und Auftragsverarbeiter müssen ein Identitäts- und Berechtigungsmanagement etabliert haben, welches sicherstellt, dass Unbefugte keine Berechtigungen auf das IVS haben. Die Prozesse und Maßnahmen zum Identitäts- und Berechtigungsmanagement müssen sich an dem Stand der Technik ([BSI IT-Grundschutz-Kompendium ORP.4 Identitäts- und Berechtigungsmanagement], [ISO 27002 Ziffer 5.15 - 5.18]) orientieren.

Standardanforderungen:

1. Berechtigungskonzept:
   a. Das Berechtigungskonzept muss alle Zugänge und Zugriffe auf Dienste und Systeme dokumentieren, die personenbezogene Daten verarbeiten.
   b. Jeder Zugang und Zugriff auf Dienste und Systeme, die personenbezogene Daten verarbeiten, muss einer Berechtigungsprüfung durchlaufen haben und eindeutig identifizierbar sein.
   c. Der Verantwortliche/Auftragsverarbeiter muss Verfahren zur Vergabe, Prüfung, Durchsetzung und Löschung von Berechtigungen für Zutritte, Zugänge und Zugriffe in einem Berechtigungskonzept dokumentieren.
   d. Die Vergabe und Änderung von Berechtigungen muss auf Basis des Prinzips der geringsten Berechtigungen („Least Privilege Prinzip“) und wie es für die Aufgabenwahrnehmung erforderlich ist („Need to know Prinzip“) erfolgen.
   e. Der Verantwortliche/Auftragsverarbeiter muss Rollen und Berechtigungen definieren und dokumentieren.
   f. Die Aufgaben und Funktionen von Administrationsrollen und Benutzerrollen müssen klar getrennt werden.
   g. Zuständigkeiten für die Verfahren zur Vergabe, Prüfung, Durchsetzung und Löschung von Berechtigungen müssen festgelegt werden.
   h. Änderungen an Berechtigungen für den Zugang und Zugriff auf Dienste und Systeme, die personenbezogene Daten verarbeiten, müssen durch Vorgesetzte oder verantwortliche Personen freigegeben werden.
   i. Die Vergabe, Prüfung und Durchsetzung und Löschung von Rechten und Berechtigungen müssen dokumentiert werden.
   j. Das Berechtigungsmanagement muss Zugänge und Zugriffe zu relevanten Systemen von Beschäftigten von Auftragsverarbeitern miteinschließen.
2. Verwaltung von Zugängen und Berechtigungen:
   a. Das Speichern, Bearbeiten, Löschen und den Zugriff auf Berechtigungen und die damit verbundenen Zugriffsberechtigungen müssen über Administrator-Konten bzw. Benutzerkonten mit erhöhten Rechten erfolgen.
   b. Alle Benutzer und Benutzergruppen werden ausschließlich über separate administrative Rollen eingerichtet und gelöscht.

c. Nicht benötigte Benutzerkonten, wie beispielsweise eingerichtete Gastkonten oder Standard-Administratorkonten müssen gesperrt oder gelöscht werden.
d. Gruppenbenutzerkonten sollten vermieden werden.
e. Bei Nutzung von Gruppenbenutzerkonten muss es eine datenschutzkonforme Protokollierung der dazugehörigen Nutzeraktivitäten geben.
f. Bei personellen Veränderungen müssen, die nicht mehr benötigten Benutzerkonten und Berechtigungen entfernt werden.

3. Umgang mit physischen Daten:
   a. Für physische Akten und Daten müssen sichere Schließsysteme samt dokumentierter Schlüsselverwaltung eingesetzt werden.
4. Überprüfung und Aktualisierung von Zugängen und Berechtigungen:
   a. Inaktive Benutzerkonten müssen identifiziert und gesperrt oder gelöscht werden.
   b. Der Verantwortliche/Auftragsverarbeiter muss die Erforderlichkeit der Berechtigungen für den Zutritt zu Räumen und Anlagen, Zugang und Zugriff auf das IVS und Sicherungskopien in regelmäßigen Abständen auf Aktualität und Angemessenheit überprüfen und bei Bedarf aktualisieren.
5. Maschine-zu-Maschine-Kommunikation:
   a. Maschine-zu-Maschine-Kommunikation muss bei relevanten Datenverarbeitungsvorgängen über gegenseitige Authentifizierungs-Mechanismen abgesichert werden.
   b. Der Kommunikationskanal zwischen dem authentifizierten Server und dem Client muss entsprechend den Anforderungen im Kryptokonzept verschlüsselt werden.

Anforderungen für den hohen Schutzbedarf:

6. Protokollierung:
   a. Jede Änderung und Löschung an Berechtigungen für den Zugang und Zugriff auf Dienste und Systeme, die personenbezogene Daten verarbeiten, muss protokolliert werden und nachträglich feststellbar sein.
   b. Der Verantwortliche/Auftragsverarbeiter ergreift Maßnahmen zur aktiven Erkennung von unbefugten Änderungen und Angriffen auf Berechtigungssysteme und vergebene Berechtigungen.
   c. Die Anmeldevorgänge und Tätigkeiten auf administrativen IT-Systemen sind zu protokollieren.
   d. Administratoren dürfen nicht die Möglichkeiten haben, Protokolldateien über ihre eigenen Tätigkeiten mit ihren Administratorkonten zu ändern oder zu löschen.
7. Vertrauliche Datenverarbeitungen:
   a. Für Administrationstätigkeiten muss das Mehraugenprinzip zur Anwendung kommen. Bei Datenverarbeitungsanlagen darf ein einzelner Administrator allein keinen Zugriff auf die im Server verarbeiteten Daten erlangen.

3. Zugriffskontrollmaßnahmen

Der Verantwortliche und Auftragsverarbeiter müssen Zugriffskontrollmechanismen etabliert haben, die sicherstellen, dass der Zugriff auf das IVS und personenbezogene Daten für Unbefugte ausgeschlossen ist.

Standardanforderungen:

1. Allgemeine Anforderungen:
   a. Netzwerke müssen segmentiert werden, sodass der Zugriff auf das IVS, relevante Systeme und personenbezogene Daten für Unbefugte erschwert wird.
   b. Verfahren zur Sperrung von Daten bei Verdacht auf unbefugten Zugriff müssen implementiert werden.
2. Protokollierung und Überwachung:
   a. Alle Zugriffe auf personenbezogene Daten müssen protokolliert werden.
   b. Der Zugriff auf Datensicherungen muss auf berechtigte Personen begrenzt sein.
   c. Der Zugriffsschutz für persönliche Daten auf mobilen Geräten muss auch bei Verlust oder Diebstahl gewährleistet werden.
   d. Der Verantwortliche/Auftragsverarbeiter muss Schutzmaßnahmen vor bekannten Angriffsszenarien in Bezug auf Zugriffsverletzungen ergreifen.
3. Fernzugriffe:
   a. Fernzugriffe auf das IVS oder personenbezogene Daten über das Internet oder andere unsichere Netze müssen die Nutzung eines virtuellen privaten Netzwerks (VPN) und Maßnahmen zur Verschlüsselung der Datenströme gemäß Kryptokonzept vorsehen.
   b. Eine Liste von Nutzern bzw. Nutzerkategorien mit Fernzugriff muss erstellt werden.

Anforderungen für den hohen Schutzbedarf:

4. Protokollierung:
   a. Jeder unbefugte Zugriff und jeder Zugriffsversuch muss protokolliert werden und nachträglich feststellbar sein.

4. Authentisierung und Authentifizierung

Standardanforderungen:

1. Authentifizierungskonzept:
   a. Der Verantwortliche/Auftragsverarbeiter muss ein Authentifizierungskonzept erstellen, in dem für jedes relevante IT-System und jede relevante Anwendung definiert ist, welche Anforderungen an die Authentifizierung gestellt werden.
2. Passwortrichtlinie:
   a. Der Verantwortliche und Auftragsverarbeiter müssen den Gebrauch von Authentifizierungsmitteln (Passwörter, etc.) verbindlich regeln.
   b. Die Passwortrichtline muss festlegen, welche Nutzer und nutzergruppen für den Zugriff auf das IVS einer Multifaktor-Authentifizierung unterliegen.

	c. Eine Multifaktor-Authentifizierung muss für Nutzer mit Administratorkonten, Nutzer mit Zugriff auf sensible Daten gemäß DSGVO, und Nutzer mit Fernzugriff über ein virtuelles privates Netzwerk eingesetzt werden. d. Es muss ein Verfahren zur Zuweisung von Passwörtern dokumentiert werden. e. Es müssen Mindestanforderungen an die Komplexität von Passwörtern unter Berücksichtigung des Stands der Technik festgelegt werden. f. Es muss ein Verfahren zur Zurücksetzung und Sperrung von Passwörtern implementiert werden. g. Es müssen Regelungen zum Umgang mit Passwörtern dokumentiert werden. h. Mitarbeiter müssen in den Umgang mit Authentifizierungsverfahren und -mechanismen eingewiesen werden. i. Die Beschäftigten müssen bezüglich des Umgangs mit Authentisierungsmitteln, wie Passwörtern sensibilisiert werden. Dies gilt insbesondere für die Unzulässigkeit der Weitergabe, Unzulässigkeit der Mehrfachverwendung, Unzuverlässigkeit der Dokumentation des Passwortes auf einem Zettel. 3. <u>Verwaltung von Passwörtern:</u> a. Standardpasswörter müssen beim erstmaligen Login oder nach erfolgter Zurücksetzung des Passwortes geändert werden. b. Bei Administratorkonten müssen Passwörter regelmäßig erneuert werden. 4. <u>Passwortkomplexität:</u> a. Die Passwortkomplexität bei ausschließlicher Passwortauthentifizierung muss die Entropie des Passworts mindestens 80 Bit betragen (beispielsweise 12 Zeichen mit Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen). b. Die Passwortkomplexität bei Passwortauthentifizierung mit Zugangsbeschränkungen muss die Entropie des Passworts mindestens 50 Bit betragen (beispielsweise 8 Zeichen mit allen Zeichenkategorien). c. Die Passwortkomplexität bei Passwortauthentifizierung mit Besitzfaktor und Zugangssperrung nach Fehlversuchen muss die Entropie des Passworts mindestens 13 Bit betragen. 5. <u>Technische Maßnahmen bei Systemen:</u> a. Von den Systemen dürfen keine spezifischen Hinweise bei erfolglosen Anmeldeversuchen erfolgen. b. Starke Passwörter gemäß Stand der Technik müssen technisch erzwungen werden. c. Es müssen Maßnahmen zur Erkennung der Kompromittierung von Passwörtern implementiert werden. d. Um Brute-Force-Angriffen auf Passwörter vorzubeugen muss:

1. es eine Verzögerung des Zugriffs auf den Account nach mehreren Fehlversuchen geben, deren Dauer exponentiell mit der Anzahl der Versuche innerhalb eines bestimmten Zeitraums ansteigt; oder
2. einen Mechanismus, der eine maximale Anzahl an zulässigen Versuchen innerhalb eines bestimmten Zeitraums festlegt, mit maximal 10 Versuchen pro Stunde; oder
3. eine Sperrung des Benutzeraccounts nach einer Anzahl von höchstens 10 aufeinanderfolgenden fehlgeschlagenen Authentifizierungen, mit einem Freigabemechanismus.

e. Systeme müssen fehlgeschlagene Authentifizierungsversuche protokollieren.

6. Schutz von Authentifizierungsfaktoren:
   a. Das Versenden und die Speicherung von Passwörtern im Klartext muss unterbunden werden.
   b. Passwörter müssen unter Anwendung von kryptografischen Hashfunktionen gespeichert werden.

Anforderungen für den hohen Schutzbedarf:

-

5. Kryptographie

Standardanforderungen:

1. Kryptokonzept
   a. Es muss ein Kryptokonzept vorhanden sein, das für Einsatz von Verschlüsselung zu verwendende Verschlüsselungsalgorithmen, Einsatzdauer des kryptografischen Verfahrens und dazu gehörige Schlüssellängen dokumentiert.
   b. Verschlüsselung sollte bereits bei niedrigem Risiko als Schutzmaßnahme eingesetzt werden.
   c. Eingesetzte Verschlüsselungsverfahren und Schlüssellängen müssen dem Stand der Technik entsprechen [BSI-TR-02102-01, -02, -03, -04].
   d. Bei den eingesetzte Verschlüsselungsverfahren dürfen keine Sicherheitslücken bekannt sein.
   e. Es müssen Maßnahmen zur Schlüsselverwaltung dokumentiert und implementiert werden.
   f. Die technische Entwicklung im Bereich der Verschlüsselung muss laufend verfolgt werden.
   g. Der Verantwortliche prüft das Kryptokonzept regelmäßig und aktualisiert es bei Bedarf.
2. Schlüsselverwaltung
   a. Es müssen Regeln für Erstellung, Erneuerung, Austausch, Vernichtung und Speicherung von Schlüsseln festgelegt werden.
   b. Kryptografische Schlüssel sollten mit geeigneten Schlüsselgeneratoren und in einer sicheren Umgebung erzeugt werden.

c. In Hard- oder Software mit kryptografischen Funktionen müssen voreingestellte Schlüssel (ausgenommen öffentliche Zertifikate) ersetzt werden
d. Geheime Schlüssel müssen sicher gespeichert und vor unberechtigten Zugriff geschützt werden.
e. Langlebige kryptografische Schlüssel müssen offline, außerhalb der eingesetzten IT-Systeme, aufbewahrt werden.
f. Eine Vorgehensweise sollte für den Fall festgelegt werden, dass ein privater Schlüssel offengelegt wird.

3. Transportverschlüsselung
   a. Bei Datenübertragungsvorgängen muss eine Transportverschlüsselung nach dem Stand der Technik eingesetzt werden.
   b. Die Verarbeitung von verschlüsselten Daten muss ermöglicht werden, soweit technisch möglich.
4. Verschlüsselung gespeicherter Daten
   a. Anmeldedaten zur Nutzung von Systemen und Diensten müssen verschlüsselt gespeichert werden.
   b. Personenbezogene Daten müssen verschlüsselt gespeichert werden.
5. . Dokumentation
   a. Die Implementierung der Verschlüsselungsverfahren muss dokumentiert werden.

Anforderungen für den hohen Schutzbedarf:

6. Kryptokonzept
   a. Das Unternehmen muss mindestens jährlich überprüfen, ob die eingesetzten kryptografischen Verfahren und die zugehörigen Parameter sicher sind und keine bekannten Schwachstellen aufweisen.
   b. Es muss eine Verfahrensweise festgelegt werden, wie ein autorisierter physischer Zugriff auf Hardware mit kryptografischen Funktionen erfolgen kann, z.B. für Wartungszwecke.
7. Schlüsselverwaltung
   a. Hard- und Software mit kryptografischen Funktionen und Schlüsseln muss auf Manipulationsversuche hin überwacht werden und jeder entsprechende Versuch muss nachträglich festgestellt werden können.
   b. Die Konfiguration der kryptografischen Hardware sollte regelmäßig überprüft werden.
8. Test der Verschlüsselungsverfahren
   a. Die Eignung der Verschlüsselungsverfahren muss fortlaufend geprüft und getestet werden.

6. Trennungskontrolle

Standardanforderungen:

1. Allgemeine Anforderungen:
   a. Der Verantwortliche/ Auftragsverarbeiter verarbeitet die Daten des System-Kunden logisch oder physisch getrennt von den Datenbeständen anderer System-Kunden.
   b. Der Verantwortliche ermöglicht dem System-Kunden, die Datenverarbeitung nach verschiedenen Verarbeitungszwecken zu trennen.

c. Der Verantwortliche/ Auftragsverarbeiter muss Verletzungen der Datentrennung verhindern, die durch technische oder organisatorische Fehler, einschließlich Bedienfehlern, oder fahrlässiger Handlungen von Mitarbeitenden oder Nutzer verursacht werden.
d. Der Verantwortliche/ Auftragsverarbeiter muss vorsätzliche Verstöße gegen das Trennungsgebot erkennen können.
e. Bei Entwicklungen muss es eine Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen geben.
f. Bei IT-Systemen muss es eine Trennung der Testumgebung von der Produktivumgebung geben.

2. Mandantentrennung:
   a. Es muss ein Mandantentrennungskonzept erstellt und umgesetzt werden.
   b. Das Mandantentrennungskonzept muss sicherstellen, dass Daten und Verarbeitungskontexte verschiedener Nutzer sicher getrennt werden.
   c. Es muss zwischen mandantenabhängigen und mandantenübergreifenden Daten unterschieden werden.
   d. Die benötigten Mechanismen zur Mandantentrennung müssen auch durch Dienstleister im Falle von relevanten Datenverarbeitungen umgesetzt werden.

Anforderungen für den hohen Schutzbedarf:

1. Erweiterte Schutzmaßnahmen:
   a. Der Verantwortliche/Auftragsverarbeiter muss Maßnahmen vor bekannten Angriffsszenarien gegen das Trennungsgebot ergreifen.
   b. Verschlüsselung von Datenspeicherungen von unterschiedlichen Kunden müssen mit (Kunden-) individuellen Schlüsseln erfolgen.

7. Pseudonymisierung

Der Einsatz von Pseudonymisierung muss sich an dem Stand der Technik ([EDPB Guidelines[5]], [ISO 27002]) orientieren.

Standardanforderungen:

Allgemeine Anforderungen:

a. Der Einsatz von Pseudonymisierung oder Anonymisierung muss in Abhängigkeit der Schutzbedarfsfeststellung und der Verwendung der Daten erfolgen.
b. Der Verantwortliche muss Maßnahmen ergreifen, dass pseudonymisierte oder anonymisierte Daten nicht unbefugt mit anderen Informationen abgeglichen werden, um Personen zu identifizieren.

1. Getrennte Verarbeitung:
   a. Pseudonymisierte Daten und Zusatzinformationen, die eine Re-Identifizierung ermöglichen, müssen getrennt verarbeitet werden.
   b. Bei der Pseudonymisierung von personenbezogenen Klartextdaten durch kryptographische Verfahren, muss der Verantwortliche oder Auftragsverarbeiter sicherstellen, dass

[5] https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf

der kryptographische Schlüssel zur Wiederherstellung des Personenbezugs gesondert aufbewahrt wird.

c. Die gesonderte Aufbewahrung von Schlüsseln kann auf logischer Ebene (z. B. durch Berechtigungskonzepte), aber auch auf physischer Ebene (z. B. durch dedizierte Datenverarbeitungsanlagen) oder organisatorischer Ebene (z. B. durch einen Datentreuhänder) erfolgen.

Anforderungen für den hohen Schutzbedarf:

-

<u>Ergänzend für Auftragsverarbeiter</u>

Auftragsverarbeiter müssen gem. Art. 28 Abs. 3 lit. c DSGVO sicherstellen, dass alle gem. Art. 32 DSGVO erforderlichen Maßnahmen ergriffen werden und die Vorgaben für die Datensicherheit gemäß der mit dem Verantwortlichen getroffenen Vereinbarung umgesetzt werden. Hierfür muss die Vereinbarung zwischen den Verantwortlichen und dem Auftragsverarbeiter Informationen zu folgenden Punkten enthalten:

- Die zu ergreifenden technischen und organisatorischen Maßnahmen
- Verpflichtung des Auftragsverarbeiters, wesentliche Änderungen an den technischen und organisatorischen Maßnahmen mit dem Verantwortlichen (schriftlich oder elektronisch) abzustimmen und mindestens für die Dauer der Vereinbarung aufzubewahren
- Regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen

Der Verantwortliche muss dem Auftragsverarbeiter eine Beschreibung der Verarbeitungstätigkeiten und der Sicherheitsziele (auf Grundlage der Risikobeurteilung des Verantwortlichen) zur Verfügung stellen und die vom Auftragsverarbeiter vorgeschlagenen technischen und organisatorischen Maßnahmen genehmigen.

Die Informationen über die beim Auftragsverarbeiter implementierten technischen und organisatorischen Maßnahmen müssen so detailliert sein, dass der Verantwortliche die Angemessenheit der Maßnahmen gem. Art. 32 Abs. 1 DSGVO prüfen kann.

Der Auftragsverarbeiter muss Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen implementiert haben. Die implementierten Verfahren treffen mindestens Festlegungen zu:

- Den Zuständigkeiten bzgl. der regelmäßigen Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen.
- zeitlichen Zyklen bzgl. der regelmäßigen Überprüfung der technischen und organisatorischen Maßnahmen (mindestens aller zwei Jahre). Zudem ist festzulegen, wann anlasslose Kontrollen durchzuführen sind, z. B. bei technischen Änderungen wie Software-Updates oder Bekanntwerden neuer Angriffsmethoden.
- der Art und Weise der Überprüfung.
- Vornahme der Überprüfung der beim jeweiligen Verantwortlichen konkret eingesetzten technischen und organisatorischen Maßnahmen
- Vornahme eines Abgleichs mit den Sicherheitszielen und des damit korrespondierenden Schutzniveaus. Bewertung, ob die technischen und organisatorischen Maßnahmen das Schutzniveau sicherstellen. Hierbei sind auch Anpassungen an den Sicherheitszielen aufgrund von

	Änderungen an den Umständen und Rahmenbedingungen der Verarbeitung selbst, etwaige Aktualisierungen oder bekannt gewordene Sicherheitslücken zu berücksichtigen und es ist zu evaluieren, ob weitere Risiken hinzugetreten sind, die eine Anpassung der Maßnahmen erfordern. ▪ Vornahme der Evaluierung der Effektivität der technischen und organisatorischen Maßnahmen, z. B. durch Penetrationstests. ▪ Die durchgeführten Überprüfungen sind zu dokumentieren. Soweit die beim Auftragsverarbeiter getroffenen Maßnahmen den Anforderungen des Verantwortlichen nicht genügen, ist der Verantwortliche unverzüglich hierüber (schriftlich, auch elektronisch) zu benachrichtigen. Hierfür sind entsprechende Prozesse inklusive Zuständigkeiten und Kommunikationswege festgelegt.

[DSGVO] Art. 25 Abs. 1, 2, [DSGVO] Art. 32 Abs. 1 lit. b, c

DS08.04	**Verantwortlicher und Auftragsverarbeiter** Im Zusammenhang mit dem Betrieb des IVS treffen Verantwortlicher und Auftragsverarbeiter unter Berücksichtigung des Stands der Technik technische und organisatorische Maßnahmen zur Sicherstellung der **Verfügbarkeit** der verarbeiteten PBD. Die Prozesse und Maßnahmen müssen sich an standardisierten Vorgehensweisen zum Continuity Management und dem Stand der Technik ([BSI-200-4], [BSI IT-Grundschutz-Kompendium], [ISO 22301]) orientieren. Folgende Standardanforderungen an die Verfügbarkeit der verarbeiteten PBD müssen umgesetzt werden. **Standardanforderungen:** 1. Datensicherungsstrategie und -konzept: a. Es muss ein Datensicherungskonzept geben, dass die regelmäßige Datensicherung von relevanten Systemen, Konfigurationen, Datenstrukturen und Transaktionshistorien, sowie die Anforderungen an die Aufbewahrung und den physischen und logischen Schutz beschreibt. b. Das Datenschutzkonzept muss eine Übersicht geben, welche IT-Systeme und welche darauf befindlichen Daten durch welche Datensicherung gesichert werden. c. Die Reihenfolge der Wiederherstellung der IT-Systeme und Anwendungen muss festgelegt werden. d. Das Datensicherungskonzept muss die regelmäßige Überprüfung der Wiederherstellbarkeit von Sicherungskopien beschreiben. 2. Datensicherungspläne: a. Es müssen Datensicherungspläne von relevanten IT-Systemen oder Gruppen von IT-Systemen erstellt werden. b. In den Sicherungsplänen müssen folgende Aspekte festgelegt werden: 1. den zu sichernden Datenbestand, 2. Anforderungen an das Datensicherungsarchiv, 3. Vertraulichkeitsbedarf der Daten, 4. Einsatz von Verschlüsselungstechniken, 5. die Anzahl der Datensicherungen, 6. benötigtes Speichervolumen,

	7. die Art der Datensicherung, 8. Häufigkeit und Zeitpunkt der Datensicherung, 9. das Speichermedium, 10. Prüfung des Datenbestandes und des zu verwendenden Speichermediums auf Schadsoftware 11. vorherige sichere Löschung der Datenträger vor Wiederverwendung, 12. den Speicher-Ort (physisch, logisch) der Datensicherung, 13. die eingesetzte Hardware und Software für die Datensicherung, 14. Zuständigkeit für die Datensicherung, 15. Transport- und Aufbewahrungsmodalitäten, 16. Dokumentation der erstellten Sicherungen (Datum, Art der Durchführung der Sicherung sowie gewählte Parameter, Beschriftung der Datenträger) c. Die Datensicherungspläne müssen Aufbewahrungs- und Löschfristen der Daten berücksichtigen. d. Es muss eine Benutzerdokumentation für die Durchführung der Datensicherung und die Wiederherstellung der Daten aus der Datensicherung geben. 3. <u>Rahmenbedingungen für die Datensicherung:</u> a. Für die Datensicherung müssen ausreichende Hardware-Ressourcen vorhanden sein. b. Datensicherungen dürfen nicht dauerhaft mit dem IT-Netz verbunden sein, sondern nur während der Zeit des Datensicherungs-Vorgangs bzw. der Wiederherstellung. c. Die Mitarbeitenden müssen über ihre Aufgaben bei der Datensicherung informiert und ggfs. geschult sein. 4. <u>Sichere Aufbewahrung:</u> a. Datenträger müssen räumlich getrennt vom gesicherten IT-System aufbewahrt werden. b. Klimatische Bedingungen für die langfristige Aufbewahrung von Datenträgern müssen gewährleistet sein. c. Der Zugang und Zugriff auf Datenträger mit Datensicherungen darf nur befugten Personen möglich sein. d. IT-Systeme, die für die Datensicherung eingesetzt werden, dürfen einen schreibenden Zugriff auf die Speichermedien für die Datensicherung nur für autorisierte Datensicherungen oder autorisierte Administrationstätigkeiten gestatten. e. Gebäude bzw. Räumlichkeiten mit relevanten Systemen für die Datenverarbeitung müssen mit angemessenen Schutzmaßnahmen gegen elementare Bedrohungen, wie beispielsweise Feuer, Wasser, Blitz, elektromagnetische Felder ausgestattet sein. f. Die Verfügbarkeit der Daten bzw. des IVS muss bei kurzfristigen Stromausfällen sichergestellt werden. 5. <u>Cloud-Datensicherungen:</u> a. Es muss einen Vertrag mit dem Diensteanbieter geben, der den Ort der Datenspeicherung, Vereinbarungen zur Dienstgüte (SLA), technische und organisatorische Maßnahmen festlegt. b. Es muss geeignete Authentisierungsmethoden nach dem Stand der Technik geben.

	c. Die Verschlüsselung der Daten auf dem Transportweg und auf dem Online-Speicher muss nach dem Stand der Technik erfolgen. 6. Funktionstests und Überprüfung der Wiederherstellbarkeit: a. Es müssen regelmäßige Tests der Datensicherungen durchgeführt werden. b. Bei den Tests der Datensicherungen muss sichergestellt werden, dass die Datensicherung vollständig ist und die Daten nach Wiederherstellung benutzbar sind. c. Im Bedarfsfall muss ein schneller Zugang bzw. Zugriff auf die Datensicherungen gewährleistet sein. **Anforderungen für den hohen Schutzbedarf:** 7. Datensicherungsstrategie und -konzept: a. Das Datensicherungskonzept muss Wiederanlauf- und Wiederherstellungszeiten definieren. 8. Datensicherungspläne: a. Die Durchführung von Datensicherungen muss nach der 3-2-1-Regel oder einem adäquaten Prinzip erfolgen: 3 Datenspeicherungen, 2 verschiedene Backupmedien (auch „Offline“ wie Bandsicherungen) und 1 davon an einem externen Standort. 9. Sichere Aufbewahrung: a. Datenträger müssen räumlich getrennt vom gesicherten IT-System, in einem anderen Brandabschnitt, aufbewahrt werden. 10. Verschlüsselung: a. Es muss sichergestellt werden, dass sich die verschlüsselten Daten auch nach längerer Zeit wieder einspielen lassen. b. Verwendete kryptografische Schlüssel müssen mit einer getrennten Datensicherung geschützt werden. 11. Funktionstests und Überprüfung der Wiederherstellbarkeit: a. Bei den regelmäßigen Tests der Datensicherungen muss geprüft werden, ob die definierten Zeiten für den Wiederanlauf und die Wiederherstellung gemäß Datensicherungskonzept eingehalten werden. 12. Redundanzen: a. Es müssen Redundanzen für das IVS vorhanden sein, um einen möglichst unterbrechungsfreien Zugriff auf das IVS und personenbezogene Daten sicherzustellen. 13. Beschaffung von Datensicherungssystemen: a. Bevor ein Datensicherungssystem beschafft wird, muss der IT-Betrieb eine Anforderungsliste erstellen, nach der die am Markt erhältlichen Produkte bewertet werden. Die angeschafften Datensicherungssysteme müssen die Anforderungen des Datensicherungskonzepts des Unternehmens erfüllen.

[DSGVO] Art. 25 Abs. 1, 2, [DSGVO] Art. 32 Abs. 1 lit. b, c

DS08.05	**Verantwortlicher und Auftragsverarbeiter** Im Zusammenhang mit dem Betrieb des IVS treffen Verantwortlicher und Auftragsverarbeiter unter Berücksichtigung des Stands der Technik

	technische und organisatorische Maßnahmen zur Sicherstellung der **Integrität** der verarbeiteten PBD. Die nachfolgenden Standardanforderungen an die Integrität der verarbeiteten PBD müssen umgesetzt werden. Ergibt sich in der Schutzbedarfsfeststellung ein hoher Schutzbedarf, so müssen zusätzlich zu Standardanforderungen die Anforderungen für den hohen Schutzbedarf erfüllt werden. **Standardanforderungen:** 1. <u>Allgemeine Anforderung:</u> a. Es muss ein dokumentierter Prozess zur Auswahl und Umsetzung technischer und organisatorischer Maßnahmen vorhanden sein, der die Integrität der Datenverarbeitung gewährleistet (Festlegung von Zuständigkeiten, Kriterien für die Auswahl der technischen und organisatorischen Maßnahmen, Dokumentation der technischen und organisatorischen Maßnahmen). b. Der Verantwortliche/ Auftragsverarbeiter muss Verfahren dokumentieren und implementieren, sobald Verletzungen der Integrität verarbeiteter Daten erkannt oder begründet vermutet werden. c. Diese Verfahren müssen eine Sperrung oder Löschung von Daten beinhalten, für die keine Einhaltung des Schutzbedarfs auseichende Integrität festgestellt werden kann. d. Es müssen Mechanismen zur Verhinderung bzw. zur Aufdeckung unbefugter oder unbeabsichtigter Modifikationen gespeicherter oder übertragener Daten eingerichtet werden. e. Es müssen Mechanismen zur Sicherstellung der Aktualität von Daten eingerichtet werden. f. Es müssen Mechanismen zur Sicherstellung der Datenkonsistenz eingerichtet werden. g. Es muss der Schutz der Integrität, der hinsichtlich der PBD zum Einsatz kommenden Algorithmen sichergestellt werden. h. Der Verantwortliche/ Auftragsverarbeiter muss den Transport von Datenträgern schützen, sodass personenbezogene Daten beim Transport der Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. 2. <u>Protokollierung (Logging):</u> a. Der Verantwortliche/ Auftragsverarbeiter muss Eingaben, Veränderungen und Löschungen personenbezogener Daten protokollieren. Hierbei ist außerdem zu protokollieren wer Änderungen vorgenommen hat und wann dies erfolgt ist. b. Es muss dokumentiert sein, wie, wo (welches IT-System) und was protokolliert wird. Art und Umfang der Protokollierung müssen sich am Schutzbedarf orientieren. c. Der Verantwortliche/ Auftragsverarbeiter muss bei Protokollierungen die Grundsätze der Erforderlichkeit, Zweckbindung, Datenminimierung und Speicherbegrenzung beachten. Bei der Bestimmung der Speicherdauer sind der verfolgte Zweck sowie das bestehende Risiko zu berücksichtigen. Die jeweilige Speicherdauer ist zu dokumentieren und darzulegen warum diese als erforderlich erachtet wird (z.

B. im Verzeichnis von Verarbeitungstätigkeiten). Nach Ablauf der Speicherfrist müssen die Protokolldaten gelöscht werden. Das Verfahren zur Löschung muss dokumentiert sein. Bei der Protokollierung von Löschvorgängen für Protokolldaten dürfen keine personenbezogenen Daten in den Inhalten des Lösch-Protokolls enthalten sein. Stattdessen sind gegebenenfalls Hinweise auf Aktenzeichen oder Dateinamen aufzunehmen.

d. Die Protokollierung muss so ausgestaltet sein, dass eine Auswertung dieser ermöglicht wird.
e. Die Protokollierung muss so gestaltet werden, dass die Nachvollziehbarkeit von Eingaben, Veränderungen und Löschungen auch bei technischen oder organisatorischen Fehlern, einschließlich Bedienfehlern von Nutzern oder Mitarbeitenden gewahrt bleibt.
f. Protokolldaten müssen sicher aufbewahrt werden, d. h. es muss sichergestellt sein, dass ein ändernder Zugriff nicht möglich ist, es muss sichergestellt sein, dass nur berechtigte Personen Zugriff haben
g. Die Protokollierungsdaten sind regelmäßig zu überprüfen, z. B. durch den Informationssicherheitsbeauftragten.
h. Zugriffe auf Protokolldaten sind zu dokumentieren.
i. Administrative Tätigkeiten sind zu protokollieren.

3. <u>Datensicherung und Malware-Schutz:</u>
   a. Der Verantwortliche/ Auftragsverarbeiter muss Verfahren zur Analyse und Überprüfung von Protokollen einrichten, um Anomalien und Vorfälle effektiv erkennen und in der Folge einen Alarm auslösen zu können.
   b. Der Verantwortliche/ Auftragsverarbeiter muss sicherstellen, dass die Integrität personenbezogener Daten auch in Datensicherungen sichergestellt ist.
   c. Der Verantwortliche/ Auftragsverarbeiter muss sicherstellen, dass bei der Wiederherstellung von Daten keine Änderungen oder Manipulationen an den Daten vorgenommen wurden.
4. <u>Einsatz kryptographischer Verfahren:</u>
   a. Für den Transport von Daten und Remote-Zugriff auf Daten müssen entsprechend der Schutzbedarfsfeststellung Verschlüsselungsverfahren eingesetzt werden.
   b. Für die Verschlüsselung müssen Verschlüsselungsverfahren gemäß Stand der Technik [BSI-TR-02102-01, -02, -03, -04] genutzt werden.

Anforderungen für den hohen Schutzbedarf:

5. <u>Einsatz kryptographischer Verfahren:</u>
   a. Ergibt sich gemäß der Schutzbedarfsfeststellung ein hoher Schutzbedarf der PBD, müssen die Daten verschlüsselt werden.
   b. Um die Integrität gesicherter Daten zu gewährleisten, müssen alle Datensicherungen verschlüsselt werden.
6. <u>Manipulationsschutz und Schutz vor Schadsoftware:</u>
   a. Der Verantwortliche/ Auftragsverarbeiter ergreift Maßnahmen zur aktiven Erkennung von Manipulationen an Protokollierungsinstanzen und -dateien und Abwehr von Angriffen, und stellt jedes unbefugte Lesen, Kopieren, Verändern

	oder Entfernen von Daten und auch jeden entsprechenden Versuch nachträglich fest.

[DSGVO] Art. 32 Abs. 1 lit. d

DS08.06	**Verantwortlicher und Auftragsverarbeiter** Der Verantwortliche sowie der Auftragsverarbeiter unterhalten **Verfahren zur regelmäßigen Überprüfung**, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen unter Beachtung der Weiterentwicklung des Standes der Technik und der Anforderungen des Datenschutzes. Hierbei sind insbesondere nachzuweisen: ▪ Regelmäßige Durchführung interner Audits/Überprüfungen im Bereich Datenschutz und IT-Sicherheit. Hierfür muss ein Prüfplan vorhanden sein. Der insbesondere Regelungen trifft zu: o Zuständigkeiten für die Überprüfung o Art der Überprüfung o Umfang der Überprüfung o Zeitplan für die Überprüfung Die Überprüfungen müssen dokumentiert sein. ▪ anlassbezogene Kontrollen, z. B. wenn technische Änderungen wie Software-Updates vorgenommen oder neue Angriffsmethoden bekannt werden. ▪ Prozesse bzgl. der Überprüfung und Aktualisierung des Datensicherheitskonzeptes unter Berücksichtigung geänderter Sicherheitsanforderungen und der Berücksichtigung etwaiger Änderungen an der Risikobewertung (vgl. **DS08.01** and **DS08.02**) ▪ Kontakt zu Behörden und Interessenverbänden, um stets über aktuelle Bedrohungslagen und Gegenmaßnahmen informiert zu sein und diese zeitnah und angemessen berücksichtigen zu können o Es sind Prozesse (Zuständigkeiten, Kommunikationswege) etabliert, um diese Informationen an die relevanten Mitarbeiter zu kommunizieren ▪ Überprüfung aktualisierter Software und IT-Verfahren nach einem Prüfplan (vgl. **DS09.07**) ▪ ggf. Vorhandensein Zertifizierungen im Bereich der IT-Sicherheit Durchführung von Angriffsszenarien in angemessenen Abständen (bspw. Penetrationstests, vgl. **DS08.01**)

[DSGVO] Art. 32

DS08.07	**Verantwortlicher und Auftragsverarbeiter** Beim Betrieb des IVS sind **Zuständigkeiten für die Sicherheit der Verarbeitung** (z. B. IT-Sicherheitsbeauftragter, Datenschutzbeauftragter) festgelegt.

DS09 Datenschutz-Management

[DSGVO] Art. 33, Art. 28 Abs. 3 Satz 2 lit. f DSGVO

DS09.01	**A) Verantwortlicher** Im Falle der **Verletzung des Schutzes personenbezogener Daten** meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, vgl. Art. 33 Abs. 1 Satz 1 DSGVO. Im Hinblick auf die Handhabung von Verletzungen des Schutzes personenbezogener Daten sind Prozesse mit klaren Vorgehensweisen, Vorgaben bzgl. der Risikobewertung (Zuständigkeiten und Vorgehen) und Zuständigkeiten zur Meldung gegenüber der Aufsichtsbehörde vorhanden. Hierzu zählen: 1. Dokumentation der Datenschutzverletzungen, ihrer Auswirkungen und der getroffenen Abhilfemaßnahmen, 2. Zuständigkeiten bzgl. der Bewertung des Risikos der Verletzung des Schutzes personenbezogener für die Rechte und Freiheiten natürlicher Personen 3. Prozesse und Methoden zur Risikobewertung der Verletzung des Schutzes personenbezogener Daten 4. Zuständigkeiten bzgl. der Beurteilung, ob eine Pflicht zur Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde besteht 5. Zuständigkeiten und Abläufe für die Meldung an die zuständige Aufsichtsbehörde unter Berücksichtigung der einzuhaltenden 72-Stunden-Frist, sofern eine Meldepflicht besteht. Der Verantwortliche verfügt über Prozesse im Umgang mit **Informationssicherheitsvorfällen** und berücksichtigt bei der Ursachenermittlung im Zuge einer Verletzung PBD, ob diese Verletzung auf einen Sicherheitsvorfall zurückzuführen ist. Vom Prozess im Umgang mit Informationssicherheitsvorfällen sollten zumindest folgende Aspekte durch den Verantwortlichen berücksichtigt werden: 1. Es stehen Mechanismen sowie eine Kontaktstelle bereit, die Mitarbeitern eine Meldung von Vorfällen, Verstößen oder Schwachstellen über etablierte Kanäle ermöglichen. Rollen für den Umgang mit Informationssicherheitsvorfällen sind definiert und an relevante Stellen kommuniziert. Es muss sichergestellt werden, dass speziell geschultes Personal für die Bearbeitung von Informationssicherheitsvorfällen zuständig ist und Zugang zu einer entsprechenden Prozessdokumentation erhält. 2. Definition sowie Einstufung von Informationssicherheitsvorfällen ○ Es erfolgt eine effektive Kategorisierung und Priorisierung von Informationssicherheitsereignissen. Nach dieser Kategorisierung sollte jedes Informationssicherheitsereignis anhand eines festgelegten Schemas von zuständigem Personal beurteilt werden können. Die Beurteilung sollte dokumentiert werden. 3. Sicherstellung, dass auf Informationssicherheitsvorfälle reagiert wird und eine Bewertung derselben erfolgt. Folgende Punkte sollten

	Berücksichtigung finden: ○ Eingrenzung der Ausbreitung des Vorfalls auf weitere Systeme ○ Beweismaterialsammlung, die im Zusammenhang mit dem Informationssicherheitsvorfall stehen ○ Identifizierung und Behebung von Schwachstellen ○ Berücksichtigung von ggf. vorhandenen Business-Continuity-Plänen ○ Durchführung von (forensischen) Informationssicherheitsanalysen 4. Die Untersuchung der gewonnenen Erkenntnisse aus der vorhergehenden Bewertung der Ereignisse sollten in einer Optimierung der Prozesse für das Management von Vorfällen münden und bei der Risikoanalyse berücksichtigt werden. 5. Neuen bzw. wiederkehrenden Vorfällen sollte durch Schaffung von Überwachungsprozessen vorgebeugt werden. Hierzu kann eine kontinuierliche Protokollierung und Überwachung von sicherheitsrelevanten Aktivitäten bzw. Auffälligkeiten innerhalb der Netzwerke, Systeme und Anwendungen dienen. **B) Auftragsverarbeiter** Es besteht eine vertragliche Verpflichtung zur Unterstützung des Verantwortlichen bei einer Meldung über Datenschutzverletzungen. Der Auftragsverarbeiter hat Prozesse implementiert und dokumentiert, die sicherstellen, dass Datenschutzverletzungen zeitnah erkannt und untersucht werden (Festlegung von Meldewegen, Festlegung von Zuständigkeiten bzgl. der Handhabung von Datenschutzverletzungen inklusive Umsetzung von Abhilfemaßnahmen, Dokumentation der Datenschutzverletzung). Außerdem hat der Auftragsverarbeiter Prozesse implementiert und dokumentiert, die eine unverzügliche Information des Verantwortlichen über die Datenschutzverletzung gewährleisten, vgl. Art. 33 Abs. 2 DSGVO (Festlegung von Zuständigkeiten und Kommunikationswegen, Festlegung, welche Informationen dem Verantwortlichen mitgeteilt werden). Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen bei der Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, vgl. Art. 28 Abs. 3 Satz 2 lit. f DSGVO. Der Auftragsverarbeiter verfügt ferner über einen Prozess, der den Umgang mit Informationssicherheitsvorfällen regelt (Festlegung von Meldewegen, Festlegung von Zuständigkeiten bzgl. der Handhabung von Informationssicherheitsvorfällen inklusive Umsetzung von Abhilfemaßnahmen, Dokumentation des Informationssicherheitsvorfalls). Dabei ergreift der Auftragsverarbeiter technische Maßnahmen, die Sicherheitsvorfälle effektiv erkennen und eine Alarmierung auslösen können. Der Prozess sieht eine Meldung über einen Sicherheitsvorfall an Verantwortliche vor (Festlegung von Zuständigkeiten und Kommunikationswegen, Festlegung, welche Informationen dem Verantwortlichen mitgeteilt werden). Der Auftragsverarbeiter stellt sicher, dass auf Informationssicherheitsvorfälle reagiert wird und eine Analyse derselben erfolgt. Die Ergebnisse der Analyse sind dem Verantwortlichen bereitzustellen.

[DSGVO] Art. 34, Art. 28 Abs. 3 Satz 2 lit. f DSGVO

DS09.02	**A) Verantwortlicher** Es ist ein Prozess vorhanden, der, sofern die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat, eine unverzügliche Benachrichtigung der Betroffenen hierüber gewährleistet. Hierbei sind Prozesse (Festlegung von Zuständigkeiten und Kommunikationswegen bzgl. der Benachrichtigung der Betroffenen) und Methoden zur Risikobewertung der Verletzung des Schutzes personenbezogener Daten implementiert, vgl. DS09.01. Es ist sichergestellt, dass die Information in klarer und einfacher Sprache über die Art der Verletzung PBD erfolgt. Die Information enthält mindestens folgende Angaben: 1. Namen und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen, 2. Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes PBD, 3. Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes PBD und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen. Die Benachrichtigung der Betroffenen ist nicht erforderlich, wenn eine der folgenden Bedingungen vorliegt (vgl. Art. 34 Abs. 3 DSGVO): 1. Der Verantwortliche hat vorbeugende Sicherheitsvorkehrungen getroffen, die im Vorfeld der Datenpanne auf die betroffenen pbD angewendet worden sind und eine unbefugte Kenntnisnahme der Daten verhindern (z. B. durch angemessene Verschlüsselung); 2. Das zunächst angenommene hohe Risiko besteht aufgrund der nachträglichen Maßnahmen des Verantwortlichen nicht mehr, wenn nach menschlichem Ermessen bei normalem Gang der Dinge nicht damit zu rechnen ist, dass die stattgefundene Sicherheitsverletzung entweder noch eintritt oder immer noch eine Schadensauswirkung besteht; 3. Eine individuelle Adressierung der Betroffenen ruft einen Aufwand hervor, der im Verhältnis zu den verbundenen Kosten unangemessenen ist. Die Benachrichtigungspflicht des Verantwortlichen erstreckt sich in diesem Fall auf eine öffentliche Bekanntmachung oder eine sachlich vergleichbare Maßnahme. **B) Auftragsverarbeiter** Es besteht eine vertragliche Verpflichtung zur Unterstützung des Verantwortlichen bei einer Benachrichtigung des Betroffenen über die Verletzung des Schutzes seiner PBD. Entsprechende Prozesse zur Unterstützung des Verantwortlichen bei der Benachrichtigung des Betroffenen sind implementiert und dokumentiert (Festlegung von Zuständigkeiten und Kommunikationswegen). Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen bei der Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, vgl. Art. 28 Abs. 3 Satz 2 lit. f DSGVO.

[DSGVO] Art. 37, [BDSG] § 38

DS09.03	**Verantwortlicher und Auftragsverarbeiter** Sofern nach Art. 37 Abs. 1 DSGVO ein Datenschutzbeauftragter zu benennen ist, wurde diese Benennung vorgenommen. Ergänzend zu Art. 37 Abs. 1 lit. b und c DSGVO ist nach § 38 Abs. 1 BDSG ein Datenschutzbeauftragter zu benennen, soweit beim Verantwortlichen oder Auftragsverarbeiter, a) in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind oder b) wenn der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vornehmen, die einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO unterliegen (unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen) oder sie geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeiten (unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen). • Als Datenschutzbeauftragte dürfen nur Personen mit entsprechender Fachkunde auf dem Gebiet des Datenschutzrechts und mit der Fähigkeit zur Erfüllung der in Art. 39 genannten Aufgaben (Art. 37 Abs. 5 DSGVO) benannt werden. • Die Kontaktdaten des Datenschutzbeauftragten sind durch den Verantwortlichen oder Auftragsverarbeiter zu veröffentlichen (Art. 37 Abs. 7 DSGVO). • Es ist sicherzustellen, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird (Art. 38 Abs. 1 DSGVO). • Der Datenschutzbeauftragte darf bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung seiner Aufgaben erhalten (Art. 38 Abs. 3 S. 1 DSGVO). • Dem Datenschutzbeauftragen werden die für seine Aufgabenerfüllung notwendigen Ressourcen zur Verfügung gestellt (Art. 38 Abs. 3 S. 1 DSGVO). • Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene (Art. 38 Abs. 3 S. 3 DSGVO). • Der Datenschutzbeauftragte besitzt Zugang zu allen erforderlichen Dokumentationen im Zusammenhang mit dem Datenschutz, der Datensicherheit bzw. Informationstechnik. • Es ist sichergestellt, dass sofern der Datenschutzbeauftragte weitere Aufgaben in der Organisation erfüllt, er sich nicht in einem Interessenskonflikt befindet. • Es gibt eine Dokumentation zu den Aufgaben des Datenschutzbeauftragten. • Die Dokumentation enthält insbesondere die in Art. 39 DSGVO aufgeführten Aufgabenbereiche. • Der Datenschutzbeauftragte wurde der zuständigen Aufsichtsbehörde gemeldet.

[DSGVO] Art. 24, Art. 38 Abs. 1 lit. d

DS09.04	**Verantwortlicher** Es ist ein kontinuierlicher Verbesserungsprozess vorhanden. • Die implementierten Datenschutzprozesse sowie die Einhaltung der gesetzlichen Anforderungen werden hierbei in Anlehnung an den PDCA-Zyklus („Plan-Do-Check-Act“) im Rahmen regelmäßiger (mindestens jährlich) Qualitäts- und Evaluationsprüfungen überprüft. In diesem Zusammenhang werden die Wirksamkeit der technischen und organisatorischen Maßnahmen evaluiert und Abweichungen sowie Verbesserungspotenzial identifiziert. • Es ist ein Prüfplan inklusive Prüfmethodik aufzustellen. • Es sind Kennzahlen (z. B. einzelne KPIs) bzw. Bewertungsmaßstäbe für die Evaluierung festzulegen, die eine Bewertung der Wirksamkeit der implementierten Prozesse und eine Identifikation von Verbesserungspotenzialen ermöglichen. • Managementreview des Datenschutzmanagementsystems. • Die Qualitätsprüfung wird dokumentiert. Es ist eine Person benannt, die Prüfkriterien für Evaluationsprüfungen definiert und aktualisiert. • Es ist ein Zeitfenster vorgesehen, innerhalb dessen vorgeschlagene Maßnahmen umzusetzen sind. • Es ist eine bestimmte Person benannt, in deren Zuständigkeitsbereich die Qualitäts- und Evaluationsprüfungen fallen. • Die Geschäftsführung wird über die Ergebnisse der Qualitäts- und Evaluationsprüfungen in Kenntnis gesetzt.

DS09.05	**Verantwortlicher und Auftragsverarbeiter** Es ist ein Datenschutzkonzept (bzw. Datenschutz-Richtlinie) vorhanden, das eine zusammenfassende Dokumentation aller datenschutzrelevanten Aspekte und Prozesse des Unternehmens darstellt. Das Datenschutzkonzept (bzw. die Datenschutz-Richtlinie) wird regelmäßig aktualisiert (mindestens jährlich oder wenn Änderungen notwendig sind) und trifft mindestens Festlegungen zu: • Ziel und Geltungsbereich des Datenschutzkonzeptes bzw. der Datenschutz-Richtlinie • Übergreifende Datenschutzpolitik inklusive Datenschutzziele des Unternehmens • Relevante rechtliche Rahmenbedingungen • Zuständigkeiten und Datenschutzorganisation • Informationen zum Datenschutzbeauftragten • Referenzierung auf die Grundsätze der Verarbeitung personenbezogener Daten nach Art. 5 DSGVO • Erläuterungen zum Schutzbedarf und Verfahren, um den Schutzbedarf zu bestimmen inklusive Risikoanalyse • Sicherstellung der Betroffenenrechte • Handhabung von Verletzungen des Schutzes personenbezogener Daten • Übersicht der technischen und organisatorischen Maßnahmen • Führung des Verzeichnisses von Verarbeitungstätigkeiten • Einsatz von Auftragsverarbeitern

	• Datenschutz-Folgenabschätzungen • Datenschutz-Schulungen • Verpflichtung der Mitarbeiter zur Wahrung der Vertraulichkeit und des Datenschutzes • Prozesse zur regelmäßigen Kontrolle und Überprüfung der Datenschutzorganisation • Löschung von Daten • Sanktionen für Verstöße gegen das Datenschutzkonzept bzw. die Datenschutz-Richtlinie • Mitgeltende Unterlagen • Die Mitarbeiter sind regelmäßig (mindestens jährlich und zu Beginn der Tätigkeit) über das Datenschutzkonzept (bzw. die Datenschutz-Richtlinie) zu informieren und es sind ausreichende Betriebsmittel für die Umsetzung des Datenschutzkonzepts (bzw. die Datenschutz-Richtlinie) vorhanden. Die Auswahl ausreichender Betriebsmittel berücksichtigt Personalkapazitäten sowie die Unternehmensgröße. • Die Mitarbeiter müssen jederzeit Zugriff auf das Datenschutzkonzept (bzw. die Datenschutz-Richtlinie) haben. • Es sind bestimmte Personen für die regelmäßige Prüfung auf Aktualität und Aktualisierung des Datenschutzkonzepts (bzw. der Datenschutzrichtlinie) beauftragt. • Dem Datenschutzkonzept (bzw. der Datenschutz-Richtlinie) ist eine Änderungshistorie zu entnehmen. • Ein Turnus für die Prüfung auf Aktualität ist dokumentiert (mindestens jährlich).

DS09.06	**Verantwortlicher und Auftragsverarbeiter** Es sind Prozesse vorhanden, die die Einhaltung der datenschutzrechtlichen Anforderungen im laufenden Betrieb aufrechterhalten und regelmäßig überprüfen. Zudem sind Prozesse zur regelmäßigen Anpassung, vor allem bei Änderungen im Datenschutzrecht oder in den IT-Verfahren, implementiert. Die implementierten Prozesse berücksichtigen mindestens folgende Anforderungen: • Es finden regelmäßig Überprüfungen (anlassbezogen als auch regelmäßig) im Datenschutzkontext statt. • Für regelmäßige Überprüfungen sind entsprechende Prüfpläne vorhanden. • Es sind Zuständigkeiten für die Durchführung von Überprüfungen im Datenschutzkontext festgelegt. • Die Überprüfung wird dokumentiert. • Es ist eine Person benannt, die Prüfkriterien für Überprüfungen im Datenschutzkontext definiert und aktualisiert. • Es ist ein Zeitfenster vorgesehen, innerhalb dessen vorgeschlagene Maßnahmen umzusetzen sind. • Es sind Prozesse implementiert, die eine frühzeitige und ordnungsgemäße Einbindung des Datenschutzbeauftragten und weiterer relevanter Stellen (z. B. Informations-/IT-Sicherheitsbeauftragter) bei Änderungen in den IT-Verfahren sicherstellen (Festlegung von Zuständigkeiten, Festlegung wie und wann der Datenschutzbeauftragte einzubeziehen ist, Festlegung, welche Informationen dem Datenschutzbeauftragten zur Verfügung gestellt werden). • Zuständigkeiten im Hinblick auf die Vornahme etwaiger Anpassungen bei Änderungen im Datenschutzrecht oder in den IT-Verfahren (z. B. Anpassung Verzeichnis von Verarbeitungstätigkeiten, Anpassung Datenschutzinformationen sowie sonstiger Dokumente im Datenschutzkontext) sind festgelegt.

DS09.07	**Verantwortlicher und Auftragsverarbeiter** Es werden neue bzw. aktualisierte Software und IT-Verfahren nach einem Testplan überprüft. Hierfür muss ein Testplan vorhanden sein, der mindestens folgendes festlegt: • Rollen und Zuständigkeiten • Durchzuführende Testarten, Testfälle und die zu erwartenden Ergebnisse • Freigabekriterien • Vorgehensweise für Situationen, wenn eine Freigabe abgelehnt wird • Zeitplan für die Durchführung der Tests inklusive Durchführungsfrist • Erforderliche Ressourcen für die Durchführung der Tests (einschließlich Hardware, Software, Personal) • Prüfkriterien zur Bewertung der Qualität und Vollständigkeit der Tests Der Datenschutzbeauftragte wird vor den Software-Tests mit Daten, die Personenbezug haben könnten, informiert und vor der Freigabe von IT-Verfahren, die personenbezogene Daten verarbeiten, wird eine datenschutzrechtliche Prüfung durchgeführt.

DS09.08	**Verantwortlicher und Auftragsverarbeiter** Es werden regelmäßig Datenschutz-Schulungen für die Mitarbeiter durchgeführt. • Es ist eine bestimmte Person mit der Durchführung von Schulungen beauftragt. • Es sind Schulungsunterlagen vorhanden. • Die Schulungsunterlagen werden regelmäßig an die aktuelle Gesetzgebung im Datenschutz angepasst. • Die Schulung ist für die Mitarbeiter verpflichtend. • Die Mitarbeiter werden in Bezug auf die technischen und organisatorischen Maßnahmen geschult. • Die Teilnahme an Datenschutzschulungen wird dokumentiert.

DS10 Datenschutz Folgenabschätzung und vorherige Konsultation

[DSGVO] Art. 35

DS10.01	**A) Verantwortlicher** Sofern eine Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung (DSFA) besteht, so wird diese vom Verantwortlichen durchgeführt. Im Rahmen einer Schwellwertanalyse ist dabei zunächst zu evaluieren, ob die Durchführung einer DSFA erforderlich ist. In diesem Zusammenhang ist zu ermitteln, ob eine Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zu Folge hat, vgl. Art. 35 Abs. 1 DSGVO. Dabei ist folgendes Prüfschema umzusetzen: a) Prüfung, ob für die Verarbeitung gemäß der Liste der Aufsichtsbehörden nach Art. 35 Abs. 4 DSGVO für den (nicht-) öffentlichen Bereich eine DSFA zu erstellen ist. b) Gemäß Art. 35 Abs. 4 DSGVO sind die Aufsichtsbehörden zur Erstellung einer Muss-Liste (Blacklist) von Verarbeitungsvorgängen, für die aufgrund eines voraussichtlich hohen Risikos für die Rechte und Freiheiten natürlicher Personen eine DSFA durchzuführen ist, verpflichtet. Sofern ein Verarbeitungsvorgang in der Liste aufgeführt ist, so ist für diesen Verarbeitungsvorgang eine DSFA zu erstellen. Maßgeblich hierbei sind die Veröffentlichungen der DSK, vgl. Prüfhinweis. Sofern die Verarbeitung nicht auf der Liste der Aufsichtsbehörden genannt ist, ist zu prüfen, ob für die Verarbeitung nach Art. 35 Abs. 3 DSGVO eine DSFA durchzuführen ist. Demnach ist insbesondere in folgenden Fällen eine DSFA durchzuführen ▪ Es handelt sich um eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen. ▪ Es handelt sich um eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO. c) Handelt es sich bei dem Verarbeitungsvorgang auch nicht um einen Fall des Art. 35 Abs. 3 DSGVO, dann ist zu prüfen, ob dennoch ein hohes Risiko nach Art. 35 Abs. 1 DSGVO vorliegt. Bei der Prüfung, ob die Verarbeitung wahrscheinlich ein hohes Risiko mit sich bringt, ist den Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“ angenommen am 4. April 2017, zuletzt überarbeitet und angenommen am 4. Oktober 2017 (WP 248 Rev. 01) der Datenschutzgruppe nach Artikel 29 zu folgen. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

	Durchführung der DSFA Die DSFA enthält gem. Art. 35 Abs. 7 DSGVO mindestens nachfolgende Mindestangaben. Dabei ist den Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“ angenommen am 4. April 2017 zuletzt überarbeitet und angenommen am 4. Oktober 2017, der Datenschutzgruppe nach Artikel 29 zu folgen. 1. systematische Beschreibung der geplanten Verarbeitungsvorgänge und ihrer Zwecke mit folgendem Mindestinhalt: ▪ funktionelle Beschreibung der Verarbeitungsvorgänge (z. B. Prozesse, IT-Systeme, Datenflüsse, Produkte, Schnittstellen, Systemgrenzen) ▪ die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sind zu berücksichtigen (ErwG 90 DSGVO) (z. B. eingesetzte Technik, wie Cloud-Dienst, On-Premise-Lösung, Menge der PBD, Anzahl der Datensätze, Anzahl der involvierten Parteien und Dienstleister, Umstände der Verarbeitung (automatisiert, papiergebunden, offen oder verdeckt, pseudonymisierte Daten oder Daten im Klartext) ▪ Kategorien der PBD ▪ Kategorien der betroffenen Personen ▪ Speicherdauer der PBD ▪ Kategorien von Empfängern inkl. Angaben zu möglichen Drittstaatentransfers ▪ Wirtschaftsgüter, auf die sich personenbezogene Daten stützen, wurden ermittelt (Hardware, Software, Netzwerke, Personen, Papiere oder Übertragungsmedien für Papiere) ▪ Berücksichtigung der Einhaltung genehmigter Verhaltensregeln gem. Art. 40 (Art. 35 Abs. 8 DSGVO) ▪ Konkrete Zwecke der einzelnen Datenverarbeitungsvorgänge inklusive der Rechtsgrundlagen für die Datenverarbeitung 2. ggf. Darstellung der im Zusammenhang mit der Verarbeitung verfolgten berechtigten Interessen des Verantwortlichen, ▪ Ggf. Darstellung der verfolgten berechtigten Interessen, sofern die Datenverarbeitung auf Art. 6 Abs. 1 lit. f DSGVO gestützt wird 3. Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung vor dem Hintergrund ihrer Zwecke mit folgendem Mindestinhalt: ▪ Maßnahmen zur Einhaltung der DSGVO bestimmt (Art. 35 Abs. 7 lit d DSGVO und ErwG 90 DSGVO), wobei Folgendes berücksichtigt wurde: a) Maßnahmen im Sinne der Verhältnismäßigkeit und Notwendigkeit der Verarbeitung, und zwar auf folgender Grundlage: o eindeutige und legitime Zwecke (Art. 5 Abs. 1 lit. b DSGVO) für die Verarbeitung wurden festgelegt o Rechtmäßigkeit der Verarbeitung anhand der jeweiligen Rechtsgrundlage (Art. 6 DSGVO) ist gegeben o Verarbeitungsvorgänge sind dem Zweck angemessen und erheblich sowie auf das notwendige Maß beschränkt (Art. 5 Abs. 1 lit. c DSGVO) o Begrenzte Speicherfrist (Art. 5 Abs. 1 lit. e DSGVO)

	b) Maßnahmen im Sinne der Rechte der betroffenen Personen: ○ Informationspflicht gegenüber den betroffenen Personen (Art. 12, 13 und 14 DSGVO) werden erfüllt ○ Betroffene Personen können ihre Rechte aus Art. 15-21 DSGVO ungehindert ausüben ○ Verhältnis zu Auftragsverarbeitern (Art. 28 DSGVO) ist geklärt ○ Garantien in Bezug auf die internationale Übermittlung von Daten (Kapitel V der DSGVO) werden eingehalten ○ Ggf. Vorherige Konsultation nach Art. 36 DSGVO ist erfolgt 4. Bewertung der Risiken nach Ursache, Art, Besonderheit und Schwere für die betroffenen Personen, hierbei sind mindestens zu berücksichtigen: ○ Identifikation von Risikoquellen (ErwG 90 DSGVO) ○ Potenzielle Bedrohungen und Auswirkungen auf die Rechte und Freiheiten von betroffenen Personen inklusive der zu erwartenden Ereignisse wurden ermittelt (z. B. unrechtmäßiger Zugriff, unerwünschte Änderung oder Verschwinden von Daten) ○ Bedrohungen, die einen unrechtmäßigen Datenzugriff, eine unerwünschte Änderung und das Verschwinden von Daten nach sich ziehen, wurden ermittelt ○ Bewertung der Eintrittswahrscheinlichkeit und Schwere der Risiken (ErwG 90 DSGVO) 5. Ermittlung von Abhilfemaßnahmen zur Bewältigung der Risiken (Art. 35 Abs. 7 lit. d DSGVO und ErwG 90 DSGVO). ○ Nach Identifizierung der Risiken sind Abhilfemaßnahmen zur Bewältigung dieser zu ergreifen (Maßnahmen können technischer, organisatorischer oder rechtlicher Natur sein) ○ Pro identifiziertem Risiko muss mindestens eine entsprechende Abhilfemaßnahme getroffen werden ○ Sofern die geplanten Abhilfemaßnahmen nicht ausreichend sind, die Restrisiken zu minimieren oder keine Abhilfemaßnahmen definiert werden können, sodass die Restrisiken weiterhin hoch sind, muss der Verantwortliche die Aufsichtsbehörde nach Art. 36 DSGVO konsultieren. Es ist eine DSFA-Methodik zu wählen, bei der die Kriterien gem. Anhang 2 der Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“ angenommen am 4. April 2017 zuletzt überarbeitet und angenommen am 4. Oktober 2017, der Datenschutzgruppe nach Artikel 29, erfüllt sind. Eine Verfahrensanweisung bzgl. der Durchführung einer DSFA einschließlich der erforderlichen Risikobewertung ist vorhanden. Diese regelt mindestens: ▪ Zuständigkeiten für die Durchführung der DSFA ▪ Festlegung des Ablaufs der DSFA ▪ Festlegung, welche Informationen von der jeweiligen Fachabteilung, für die DSFA zur Verfügung gestellt werden müssen (z. B. durch Musterformulare)

	▪ Sicherstellung, dass die DSFA zum frühestmöglichen Zeitpunkt bereits in der Entwicklungsphase der Verarbeitungstätigkeiten begonnen wird. Hierfür sind entsprechende Kommunikationswege festzulegen. ▪ Reglung bzgl. der Einholung des Rates des Datenschutzbeauftragten (wann und wie) ▪ Regelungen bzgl. der Berücksichtigung der Einholung des Rates unabhängiger Spezialisten (z. B. Anwälte, IT-Experten, Sicherheitsexperten) bei Bedarf ▪ Festlegung der DSFA-Methodik inklusive Dokumentation des erforderlichen Mindestinhalts ▪ Regelung bzgl. der Einholung des Standpunktes der betroffenen Personen oder ihrer Vertreter ▪ Die Rollen und Zuständigkeiten der Auftragsverarbeiter müssen vertraglich festgehalten werden. Die DSFA muss mit Unterstützung des Auftragsverarbeiters unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen durchgeführt werden (Art. 28 Abs. 3 lit. f DSGVO). ▪ Prozesse für die Konsultation der Aufsichtsbehörde, vgl. **DS10.04** ▪ Festlegung wie Dokumentation der DSFA erfolgen soll ▪ Festlegungen inklusive Zuständigkeiten bzgl. der Überprüfung der DSFA sowie der darin bewerteten Verarbeitung in regelmäßigen Abständen bzw. spätestens, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbunden Risikos Änderungen eingetreten sind, vgl. **DS10.03.** <u>Konsultation Betroffener</u> Gemäß Art. 35 Abs. 9 DSGVO ist gegebenenfalls der Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung ein. Es sind Zuständigkeiten für die Einholung des Standpunktes der betroffenen Personen oder ihrer Vertreter festzulegen. Die Einholung des Standpunktes kann in Abhängigkeit des jeweiligen Kontextes auf verschiedenen Wegen erfolgen, dies ist für den jeweiligen Sachverhalt gesondert zu beurteilen. Den betroffenen Personen oder ihrer Vertreter sind hinreichende Informationen über die beabsichtigte Verarbeitung zur Verfügung zu stellen, sodass sich diese sachgerecht einbringen können. Hierbei sind insbesondere folgende Informationen zur Verfügung zu stellen, wobei die zur Verfügungstellung von Informationen nur insoweit erfolgen muss, dass gewerbliche oder öffentliche Interessen nicht beeinträchtigt werden: ▪ systematische Beschreibung der geplanten Verarbeitungsvorgänge und ihrer Zwecke, ▪ ggf. Darstellung der im Zusammenhang mit der Verarbeitung verfolgten berechtigten Interessen des Verantwortlichen, ▪ Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung vor dem Hintergrund ihrer Zwecke, ▪ Bewertung der Risiken für die betroffenen Personen, ▪ Abhilfemaßnahmen zur Bewältigung der Risiken. Sofern die endgültige Entscheidung des Verantwortlichen vom Standpunkt der betroffenen Personen abweicht, müssen die Gründe für das weitere Verfahren dokumentiert werden. Sofern auf die Einholung des Standpunktes der betroffenen Personen

	verzichtet wird, muss der Verantwortliche dokumentieren, warum er eine solche Einholung nicht für angemessen hält. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt, unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen, den Verantwortlichen bei der Durchführung der DSFA (Art. 28 Abs. 3 lit. f DSGVO). Hierfür sind, insbesondere wenn die genaue Wirkungsweise, Risiken und Schutzmaßnahmen des IVS dem Verantwortlichen nicht bekannt sind, die notwendigen Angaben in einer standardmäßigen Aufstellung bereitzuhalten bzw. ist selbst eine DSFA durchzuführen und jeweils dem Verantwortlichen zur Verfügung zu stellen.

[DSGVO] Art. 35 Abs. 2

DS10.02	**A) Verantwortlicher** Bei der Durchführung der Datenschutz-Folgenabschätzung für den IVS wurde der Rat des Datenschutzbeauftragten eingeholt, sofern einer benannt wurde. Sofern der Rat des Datenschutzbeauftragten nicht befolgt wird, ist dies zusammen mit den maßgeblichen Gründen hierfür zu dokumentieren. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt, unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen, den Verantwortlichen bei der Durchführung der DSFA (Art. 28 Abs. 3 lit. f DSGVO). Hierfür sind, insbesondere wenn die genaue Wirkungsweise, Risiken und Schutzmaßnahmen des IVS dem Verantwortlichen nicht bekannt sind, die notwendigen Angaben in einer standardmäßigen Aufstellung bereitzuhalten.

[DSGVO] Art. 35 Abs. 11

DS10.03	**A) Verantwortlicher** Das IVS wird nach der ersten Datenschutz-Folgenabschätzung regelmäßig anlassunabhängig (mindestens jährlich) bzw. anlassbezogen, z. B. bei einer Risikoänderung, sofern die Möglichkeit besteht, dass vormals festgelegte Abhilfemaßnahmen nicht eingehalten werden oder sich die rechtlichen bzw. tatsächliche Rahmenbedingungen der Verarbeitung geändert haben, überprüft, um sicherzustellen, dass eine Verarbeitung tatsächlich nach den festgestellten Vorgaben vollzogen wird Eine solche Überprüfung findet insbesondere bei einer Änderung der mit der Verarbeitung verbundenen Risiken statt. Die Frist für die regelmäßige anlassunabhängige Überprüfung ist zu dokumentieren. **B) Auftragsverarbeiter** Sofern eine standardmäßige Aufstellung der relevanten Informationen erstellt wird, überprüft der Auftragsverarbeiter regelmäßig, ob die Verarbeitung tatsächlich nach den festgestellten Vorgaben erfolgt. Eine solche Überprüfung findet insbesondere bei einer Änderung der mit der

	Verarbeitung verbundenen Risiken statt. Soweit erforderlich, ist die standardmäßige Aufstellung der relevanten Informationen anzupassen und die aktualisierte Variante den Verantwortlichen zur Verfügung zu stellen.

[DSGVO] Art. 36

DS10.04	**A) Verantwortlicher** Entsteht mit dem Einsatz des IVS ein hohes Risiko für die Rechte und Freiheiten der Betroffenen und trifft der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos, so konsultiert der Verantwortliche vor der Verarbeitung die Aufsichtsbehörde. Der Verantwortliche stellt folgende Informationen zur Verfügung: 1. Zuständigkeit der Verantwortlichen und beteiligten Auftragsverarbeiter, 2. Zwecke der Verarbeitung, 3. Mittel der Verarbeitung, 4. Maßnahmen und Garantien zum Schutze der Betroffenen, 5. Gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten, 6. die Datenschutz-Folgenabschätzung. Es ist eine Person festzulegen, die für die Abwicklung der Konsultation mit der Aufsichtsbehörde verantwortlich ist. **B) Auftragsverarbeiter** Der Auftragsverarbeiter unterstützt, unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen, den Verantwortlichen bei der vorherigen Konsultation der Aufsichtsbehörde (Art. 28 Abs. 3 lit. f DSGVO). Hierzu hält er notwendige Angaben bereit, die der Verantwortliche benötigt, um die Aufsichtsbehörde entsprechend Art. 36 Abs. 3 DSGVO zu informieren.

DS11 Verhaltensregeln und Zertifizierung

[DSGVO] Art. 40, 41

DS11.01	**Verantwortlicher und Auftragsverarbeiter** Sofern relevant werden Verhaltensregeln nach Art. 40 DSGVO beachtet und deren Einhaltung ist dokumentiert.

DS12 Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen

Schritt 1: Ermittlung von Datentransfers

[DSGVO] Art. 45 ff.

DS12.01	**Verantwortlicher und Auftragsverarbeiter** Es ist festzustellen und zu dokumentieren, ob und welche personenbezogenen Daten im Kontext des Evaluierungsgegenstandes (vgl. 1.6) an welche Empfänger und an welches Drittland oder internationale Organisation übermittelt werden. Hierbei sind auch Weiterübermittlungen durch Unterauftragsverarbeiter anzugeben. Die Übermittlung der personenbezogenen Daten muss angemessen, erheblich sowie auf das für die Zwecke ihrer Übermittlung notwendige Maß beschränkt sein. Hierbei sind die entsprechenden Länder, in denen eine Verarbeitung von personenbezogenen Daten, auch im Auftrag, erfolgt, aufzuführen. Hierbei sind auch alle etwaigen Weiterübermittlungen oder extraterritoriale Zugriffe, z. B. aufgrund einer Geschäftstätigkeit im Drittland zu berücksichtigen. Das Ergebnis hinsichtlich der extraterritorialen Anwendbarkeit des Drittlands-Rechts und einer ggf. darüberhinausgehenden praktischen extraterritorialen Anwendung ist zu dokumentieren. Der Anbieter muss eine Bewertung (z. B. Transfer Impact Assessment) vorlegen, ob der Auftragsverarbeiter und/oder die verarbeiteten Daten unter eine drittstaatliche Norm oder Praxis fallen, die nach EU-Recht unzulässige Verarbeitungen personenbezogener Daten verlangen kann. Hierbei sind sämtliche Umstände des Einzelfalls zu berücksichtigen und nachfolgende Punkte zu evaluieren. a) Es sind alle diejenigen Rechtsvorschriften genau zu prüfen, in denen die Voraussetzungen hinsichtlich einer extraterritorialen Anwendbarkeit des Drittlands-Rechts und einer ggf. darüberhinausgehenden praktischen extraterritorialen Anwendung. b) Bei einer extraterritorialen Anwendbarkeit und/oder Anwendung: Das Ergebnis c) Das Risiko, dass die Drittlands-Muttergesellschaft eines EWR-Tochterunternehmens dieses anweisen könnte, personenbezogene Daten in ein Drittland zu übermitteln. d) Es ist zu evaluieren, ob der Auftragsverarbeitungsvertrag nach europäischen Maßstäben unzulässige Verarbeitungen auf der Grundlage von Drittlands-Recht erlaubt e) etwaige Zusicherungen der Drittlands-Muttergesellschaft und des EWR-Unternehmens zum Umgang mit kollidierenden Anforderungen des Rechts eines Drittstaates und der EU f) eine Bewertung der Rechtslage und -praxis des Drittlands, ob derartige Zusicherungen auch tatsächlich eingehalten werden können g) eine Bewertung aller weiteren Aspekte, ob derartige Zusicherungen auch tatsächlich eingehalten werden h) etwaige in der Vergangenheit festgestellte Datenschutzverstöße

	i) die Schwere und Wahrscheinlichkeit einer Sanktionierung von Zuwiderhandlungen nach EU-Recht und dem Recht des Drittlands j) der Ausschluss unzulässiger Übermittlungen durch geeignete technische und organisatorische Maßnahmen. Sofern ein Dienstleister mit Niederlassung in der EU, aber mit einer Muttergesellschaft in den USA bzw. in anderen Ländern, in denen kein angemessenes Datenschutzniveau besteht, eingesetzt wird, und die Speicherung und Verarbeitung sämtlicher Daten durch den Dienstleister in einem Rechenzentrum innerhalb der EU erfolgt, müssen die personenbezogenen Daten nach dem Stand der Technik im Sinne von Art. 25 und 32 DSGVO verschlüsselt gespeichert sein und ausgetauscht werden und die Schlüssel vom Verantwortlichen in der EU selbst verwaltet oder gespeichert werden (beispielsweise Customer-Managed Encryption Keys, CMEK,). Anstelle des Verantwortlichen kann auch ein Treuhänder die Verwaltung der Schlüssel übernehmen, sofern die Verwaltung des Schlüssels in der EU/EWR oder in einem Drittland erfolgt, für das ein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt. Ergänzend muss der jeweilige Dienstleister zusichern, dass kein Datentransfer und auch keine Datenverarbeitungen außerhalb der Europäischen Union durchgeführt werden. Sowohl Verantwortliche als auch dessen relevante Dienstleister müssen bestätigen, dass im Fall von Herausgabeverlangen von Behörden keine Daten zur Verfügung gestellt und auch nicht an das Mutterunternehmen herausgegeben werden. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

Schritt 2: Dokumentation der eingesetzten Übermittlungsinstrumente

[DSGVO] Art. 45 ff.

DS12.02	**Verantwortlicher und Auftragsverarbeiter** Sofern eine Datenübermittlung an ein Drittland erfolgt, ist diese Übermittlung nur zulässig, wenn eine der nachfolgenden Bedingungen erfüllt ist: 1. Das Bestehen eines Angemessenheitsbeschlusses (Art. 45 DSGVO), 2. Das Bestehen von geeigneten Garantien (Art. 46 DSGVO), 3. Das Vorliegen von Ausnahmen für bestimmte Fälle (Art. 49 DSGVO). Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

Schritt 3: Wirksamkeit der Übermittlungsinstrumente nach Art. 46 DSGVO

[DSGVO] Art. 46

DS12.03	**Verantwortlicher und Auftragsverarbeiter** Folgende geeignete Garantien können bestehen: 1. ein rechtlich bindendes und durchsetzbares Dokument zwischen den Behörden oder öffentlichen Stellen (Art. 46 Abs. 2 lit. a DSGVO), 2. das Bestehen von verbindlichen internen Datenschutzvorschriften (Art. 47 DSGVO), 3. von der EU-Kommission erlassene Standarddatenschutzklauseln nach Art. 93 Abs. 2 DSGVO (Art. 46 Abs. 2 lit. c DSGVO), 4. von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. d DSGVO),

	5. genehmigte Verhaltensregeln gemäß Art. 40 DSGVO zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland (Art. 46 Abs. 2 lit. e DSGVO), 6. ein genehmigter Zertifizierungsmechanismus gemäß Art. 42 DSGVO zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland (Art. 46 Abs. 2 lit. f DSGVO). Bei der Beurteilung der Wirksamkeit der Übermittlungsinstrumente nach Art. 46 DSGVO ist den Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Version 2.0, angenommen am 18. Juni 2021 sowie den Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, angenommen am 10. November 2020, des EDSA zu folgen. Die einzelnen Evaluierungsanforderungen ergeben sich dabei aus dem nachfolgenden Prüfhinweis. Sofern beabsichtigt ist, zusätzliche Maßnahmen zu verwenden, die die Standarddatenschutzklauseln ergänzen, bedarf er für die Aufnahme von Klauseln oder zusätzlichen Garantien solcher Art keiner Genehmigung der zuständigen Aufsichtsbehörde, sofern die betreffenden zusätzlichen Maßnahmen weder unmittelbar noch mittelbar mit den Standarddatenschutzklauseln in Konflikt stehen und sofern sie hinreichende Gewähr dafür bieten, dass das durch die DSGVO verbürgte Schutzniveau nicht beeinträchtigt wird (vgl. **DS12.04**). Datenexporteur und -importeur müssen sicherstellen und nachweisen können, dass die zusätzlichen Klauseln nicht auf eine Weise ausgelegt werden können, die die in den Standarddatenschutzklauseln niedergelegten Rechte und Verpflichtungen einschränkt oder das Datenschutzniveau in sonstiger Weise reduziert. Wenn der Datenexporteur beabsichtigt, die eigentlichen Standarddatenschutzklauseln zu ändern, oder wenn die hinzugefügten ergänzenden Maßnahmen mit den Standarddatenschutzklauseln unmittelbar oder mittelbar in Konflikt stehen, kann nicht mehr angenommen werden, dass sich der Datenexporteur auf die Standarddatenschutzklauseln stützt; der Datenexporteur muss sodann gemäß Art. 46 Abs. 3 lit. a DSGVO die Genehmigung der zuständigen Aufsichtsbehörde einholen. Es ist eine Person festzulegen, die für die Abwicklung der Konsultation mit der Aufsichtsbehörde verantwortlich ist.

[DSGVO] Art. 46 f. DSGVO

DS12.04	**Verantwortlicher und Auftragsverarbeiter** Sofern keines der in Art. 46 DSGVO dargelegten Übermittlungsinstrumente effektiv ist, also keines der Übermittlungsinstrumente sicherstellt, dass das durch die DSGVO garantierte Schutzniveau durch die Übermittlung in der Praxis nicht untergraben wird (vgl. DS12.03), sind zusätzliche Maßnahmen als Ergänzung der Garantien nach Art. 46 DSGVO zu ergreifen. Diese können vertraglicher, technischer oder organisatorischer Natur sein. Vertragliche und organisatorische Maßnahmen sind in der Regel nicht ausreichend, sondern ergänzende technische Maßnahmen sind zwingend umzusetzen. Im Hinblick auf die Auswahl effektiver zusätzlicher Maßnahmen ist den Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten Version 2.0, angenommen am 18. Juni 2021, des EDSA zu folgen. Eine Auflistung einzelner Szenarien und diesbezüglicher Anforderungen an technische, organisatorische und vertragliche Maßnahmen erfolgt im Prüfhinweis. Die entsprechende Umsetzung muss dargelegt werden. Als Bewertungsmaßstab bzgl. getroffener Maßnahmen zur Ergänzung von Übermittlungstools ist den Empfehlungen zu den Anwendungsfällen in den Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, angenommen am 18. Juni 2021, des EDSA zu folgen (vgl. Prüfhinweis). Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

Schritt 5: Neubewertung in angemessenen Abständen

[DSGVO] Art. 46

DS12.05	**Verantwortlicher und Auftragsverarbeiter** Der Verantwortliche sowie der Auftragsverarbeiter muss die Lage in dem Drittland, in das er personenbezogene Daten übermittelt hat, fortlaufend – soweit angemessen in Zusammenarbeit mit dem Dienstleister – auf Entwicklungen hin überwachen, die für seine ursprüngliche Beurteilung des Schutzniveaus und die von ihm getroffenen Entscheidungen bezüglich seiner Übermittlungen relevant sein könnten. Hierfür sind entsprechende Prozesse zu implementieren, die zumindest regeln: • Zuständigkeiten bzgl. der Evaluation des angemessenen Datenschutzniveaus • Festlegung der Häufigkeit der Evaluierung (mindestens jährlich bzw. anlassbezogen) • Festlegung der Art und Weise der Evaluation (vgl. Anforderungen bzgl. der Beurteilung des Schutzniveaus in DS12.02) • Ggf. Einbeziehung des Dienstleisters (z. B. Befragung mittels Musterdokument) • Aussetzung bzw. Beendigung des Datentransfers, wenn die Verpflichtungen, die mit dem Übermittlungsinstrument gem. Art. 46 DSGVO einhergehen verletzt werden • Dokumentation des Evaluierungsergebnisses Sofern festgestellt wird, dass die Verpflichtungen gem. Art. 46 DSGVO

	verletzt werden, deren Erfüllung unmöglich ist oder wenn die zusätzlichen Maßnahmen in dem betreffenden Drittland nicht mehr wirksam sind, müssen die Übermittlungen umgehend ausgesetzt oder beendet werden. Hierfür sind entsprechende Zuständigkeiten und Kommunikationswege festzulegen.

Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung, Art. 48 DSGVO

[DSGVO] Art. 48 DSGVO

DS12.06	**<u>Verantwortlicher und Auftragsverarbeiter</u>** Jegliches Urteil eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird, dürfen unbeschadet anderer Gründe für die Übermittlung gemäß Kapitel V DSGVO jedenfalls nur dann anerkannt oder vollstreckbar werden, wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder Deutschland gestützt sind. Nach Art. 48 DSGVO sind behördliche oder gerichtliche Entscheidungen von Drittländern als solche keine berechtigenden Grundlagen für die Übermittlung von Daten an ein Drittland. Es sind Prozesse zu implementieren und zu dokumentieren, wie mit behördlichen oder gerichtlichen Entscheidungen von Drittländern bzgl. der Übermittlung und Offenlegung von personenbezogenen Daten umgegangen wird. Die Prozesse müssen insbesondere berücksichtigen: • Prüfung, ob sich das Ersuchen auf ein Urteil oder eine Entscheidung eines Gerichts oder einer Verwaltungsbehörde bezieht • Prüfung, ob sich das Urteil oder die Entscheidung auf ein anwendbares internationales Übereinkommen stützt • Prüfung, ob das internationale Abkommen eine Rechtsgrundlage gem. Art. 6 Abs. 1 lit. c oder lit. e DSGVO für die Übermittlung von Daten bietet. • Prüfung, ob das internationale Abkommen die geeigneten Garantien gem. Art. 46 Abs. 2 lit. a DSGVO und den Leitlinien 2 2/2020 zu Artikel 46 Absatz 2 Buchstabe a und Absatz 3 Buchstabe b der Verordnung (EU) 2016/679 für die Übermittlung personenbezogener Daten zwischen Behörden und öffentlichen Stellen im EWR und Behörden und öffentlichen Stellen außerhalb des EWR, Version 2.0, angenommen am 15. Dezember 2020, enthält

Bestehen von Ausnahmen für bestimmte Fälle gem. Art. 49 DSGVO

[DSGVO] Art. 49

DS12.07	**Verantwortlicher und Auftragsverarbeiter** Falls weder Art. 45 Abs. 3 DSGVO einschlägig ist noch geeignete Garantien nach Art.46 DSGVO, einschließlich verbindlicher interner Datenschutzvorschriften bestehen, ist eine Übermittlung von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation nur unter einer der folgenden Bedingungen zulässig: a) Die betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde (Art. 49 Abs. 1 lit. a DSGVO) b) Die Datenübermittlung ist für die Erfüllung eines Vertrages zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung vorvertraglicher Maßnahmen auf Antrag der betroffenen Person erforderlich (Art. 49 Abs. 1 lit. b DSGVO) c) Die Datenübermittlung ist für den Abschluss oder die Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich (Art. 49 Abs. 1 lit. c DSGVO) d) Die Datenübermittlung erfolgt aus wichtigen Gründen des öffentlichen Interesses (Art. 49 Abs. 1 lit. d DSGVO) e) Die Datenübermittlung erfolgt zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 49 Abs. 1 lit. e DSGVO) f) Die Datenübermittlung erfolgt zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben (Art. 49 Abs. 1 lit. f DSGVO). g) Die Datenübermittlung erfolgt aus einem Register, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist, sofern ein berechtigtes Interesse nachgewiesen werden kann (Art. 49 Abs. 1 lit. g DSGVO). Art. 49 DSGVO stellt eine Ausnahmeregelung dar. Die Ausnahmetatbestände des Art. 49 DSGVO sind somit restriktiv auszulegen und anzuwenden. Hierbei ist den Leitlinien 2/2018 zu den Ausnahmen nach Art. 49 der Verordnung 2016/679, angenommen am 25. Mai 2018, zu folgen und dezidiert zu prüfen, ob die beabsichtigte Übermittlung tatsächlich die Tatbestandsvoraussetzungen erfüllt, die für die einzelnen Ausnahmen gelten. Die einzelnen Tatbestandsvoraussetzungen der Ausnahmetatbestände nach Art. 49 DSGVO sind im Prüfhinweis dargestellt und der Datenexporteur muss die tatsächliche Erfüllung der aufgeführten Tatbestandsvoraussetzungen dezidiert darlegen. Zu beachten ist, dass die Anwendung der Ausnahmetatbestände nicht zur „Regel“ werden darf, sondern auf bestimmte Situationen beschränkt ist. Die Spezifikation der einzelnen Anforderungen ist dem Prüfhinweis zu entnehmen.

3. Begriffsdefinitionen

Die im vorliegenden Dokument verwendeten unbestimmten Rechtsbegriffe orientieren sich an deren semantischer Bedeutung im Kontext der DSGVO und anderer normativer Dokumente. Für ein einheitliches Verständnis und Anwendung dieser Rechtsbegriffe findet sich nachfolgend eine spezifische Definition. Die einzelnen Begriffsdefinitionen orientieren sich hierbei an den der Beschreibung im Standard-Datenschutzmodell [SDM][6] sowie an Veröffentlichungen der Datenschutz-Aufsichtsbehörden, der Rechtsprechung sowie der juristischen Literatur

Eine gesonderte Erläuterung von Rechtsbegriffen, die bereits in der DSGVO definiert sind, erfolgt nicht.

Begriff	Beschreibung
Angemessenheit / **Erheblichkeit** / auf das **notwendige Maß Beschränktheit der Daten** (vgl. **DS02.06**)	**Angemessen** sind Daten, die einen konkreten inhaltlichen Bezug zum Verarbeitungszweck aufweisen. **Erheblich** sind Daten, deren Verarbeitung einen Beitrag zur Zweckerreichung leisten. Dieses Merkmal entspricht der Geeignetheit bei der Verhältnismäßigkeitsprüfung. **Auf das notwendige Maß beschränkt** sind nur die Daten, die zur Erreichung des Zwecks erforderlich sind, ohne deren Verarbeitung der Verarbeitungszweck also nicht erreicht werden kann. vgl. [SDM] B1.3
Anonymisieren	Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können, vgl. ErwG 26 DSGVO
Einsatzkonzeption	Jeder Evaluierungsgegenstand besteht aus Verarbeitungsprozessen, die eine Zielfunktion verfolgen. Der Anwendungsbereich von zu zertifizierenden Verarbeitungen wird vom Antragsteller bestimmt.
Datenminimierung	Datenminimierung erfasst die grundlegende datenschutzrechtliche Anforderung, die Verarbeitung personenbezogener Daten auf das dem Zweck angemessene, erhebliche und notwendige Maß zu beschränken. [SDM] C1.1
datenschutzfreundliche Voreinstellungen	Der Verantwortliche muss geeignete technische und organisatorische Maßnahmen treffen, die sicherstellen, dass durch Voreinstellungen nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Hierzu ist nicht nur die Menge der verarbeiteten Daten zu minimieren, sondern auch der Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. vgl. [SDM] B1.17
Endeinrichtung	Eine Endeinrichtung ist jede direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtung zum Aussenden, Verarbeiten oder Empfangen von Nachrichten; sowohl bei direkten als auch bei indirekten Anschlüssen kann die Verbindung über Draht, optische Faser oder elektromagnetisch hergestellt

[6] Standarddatenschutzmodell, s. Abschnitt 1.5 ("Verweise auf Gesetze, Vorschriften und Normen").

	werden; bei einem indirekten Anschluss ist zwischen der Endeinrichtung und der Schnittstelle des öffentlichen Netzes ein Gerät geschaltet.
Endnutzer	Endnutzer ist jede natürliche oder juristische Person, die einen öffentlichen Telekommunikationsdienst in Anspruch nimmt, ohne dabei selbst ein öffentliches Telekommunikationsnetz oder einen öffentlich zugänglichen Telekommunikationsdienst bereitzustellen.
Freiwilligkeit	Die Freiwilligkeit der Einwilligung ist gegeben, wenn die betroffene Person eine echte und freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile (d. h., dass nicht das Risiko einer Täuschung, Einschüchterung, Nötigung, sonstige beträchtliche nachteilige Folgen (z. B. Zusatzkosten) besteht) zu erleiden, sollte sie die Einwilligung nicht erteilen. In Fällen, in denen Zwang oder Druck ausgeübt wird oder keine Möglichkeit zur Ausübung des freien Willens besteht, ist eine Einwilligung nicht frei.
Handeln im Auftrag	Der Auftragsverarbeiter bzw. Unterauftragsverarbeiter dient dem Interesse eines anderen.
Integrität	Integrität bezeichnet einerseits die Anforderung, dass informationstechnische Prozesse und Systeme die Spezifikationen kontinuierlich einhalten, die zur Ausübung ihrer zweckbestimmten Funktionen für sie festgelegt wurden (B1.6 Integrität). Integrität bezeichnet andererseits die Eigenschaft, dass die zu verarbeitenden Daten unversehrt (B1.6 Integrität), vollständig, richtig und aktuell (B1.4 Richtigkeit) bleiben. Abweichungen von diesen Eigenschaften müssen ausgeschlossen werden oder zumindest feststellbar sein (B1.23 Angemessene Überwachung der Verarbeitung), damit sie berücksichtigt und korrigiert werden können (B1.22 Behebung und Abmilderung von Datenschutzverletzungen). vgl. [SDM] B1.6, C1.3
Lebenswichtiges Interesse	Unter einem lebenswichtigen Interesse ist ein existenzielles Interesse im Bereich des Gesundheitsschutzes zu verstehen, wobei dies nicht gleichzusetzen ist mit „lebensnotwendig“.
Löschen	Löschen ist das Unkenntlichmachen gespeicherter personenbezogener Daten.
Richtigkeit der Daten	Die von einer Verarbeitung betroffenen personenbezogenen Daten müssen sachlich richtig und erforderlichenfalls auf dem neusten Stand sein. Um diese Anforderung sicherzustellen, sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtig werden. vgl. [SDM] B1.4
Risiko	Ein Risiko im Sinne der DSGVO ist das Bestehen einer Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden darstellt

	oder zu einem Schaden für natürliche Personen führen kann. Es hat zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten. (vgl. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Kurzpapier Nr. 18, S. 1)
Speicherbegrenzung	Personenbezogene Daten dürfen nur so lange in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. B1.5 "Speicherbegrenzung"
Treu und Glauben	Eine Verarbeitung von personenbezogenen Daten nach Treu und Glauben bedeutet, die Gewährleistung einer „fairen“ Datenverarbeitung. Diese ist gegeben, wenn durch den Verantwortlichen und den Auftragsverarbeiter keine unzulässige Rechtsausübung zum Nachteil der betroffenen Person erfolgt. Ferner fordert der Grundsatz von Treu und Glauben bzw. einer „fairen“ Datenverarbeitung, dass die vernünftigen Erwartungen der betroffenen Person berücksichtigt werden müssen. Im Hinblick auf die vernünftigen Erwartungen ist zu evaluieren, was die betroffene Person unter Berücksichtigung des Erhebungskontextes erwarten würde, wofür ihre Daten verarbeitet werden. Ein wichtiger Aspekt ist hierbei die Art der Beziehung zwischen dem Verantwortlichen und der betroffenen Person, unter Berücksichtigung dessen, was in dem gegebenen Kontext und in der gegebenen (geschäftlichen oder sonstigen) Beziehung üblich und allgemein zu erwarten ist. Hierbei gilt: je unerwarteter oder überraschender die Verarbeitung ist, desto eher ist davon auszugehen, dass sie über die vernünftigen Erwartungen des Betroffenen hinausgeht.
Transparenz	Betroffene als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen müssen in einem unterschiedlichen Maße erkennen können, welche Daten wann und für welchen Zweck bei einer Verarbeitungstätigkeit erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt. [SDM] B1.1, C1.6.
Verfügbarkeit	Verfügbarkeit bezeichnet die Anforderung, dass der Zugriff auf personenbezogene Daten und ihre Verarbeitung unverzüglich möglich ist und sie ordnungsgemäß im vorgesehenen Prozess verwendet werden können. Dazu müssen sie im Zugriff von Berechtigten liegen und die vorgesehenen Methoden zu deren Verarbeitung müssen auf sie angewendet werden können. Die Verfügbarkeit umfasst die konkrete Auffindbarkeit von Daten z. B. durch Datenmanagement-Systeme, strukturierte Datenbanken und Suchfunktionen und die Fähigkeit der verwendeten technischen Systeme, Daten auch für Menschen angemessen. vgl. [SDM] B1.18, C1.2
Vertraulichkeit	Vertraulichkeit bezeichnet die Anforderung, dass keine unbefugte Person personenbezogene Daten zur Kenntnis nehmen oder nutzen kann. Unbefugte sind nicht nur Dritte außerhalb der verantwortlichen

Stelle, sondern auch Beschäftigte von technischen Dienstleistern, die zur Erbringung der Dienstleistung keinen Zugriff zu personenbezogenen Daten benötigen, oder Personen in Organisationseinheiten, die keinerlei inhaltlichen Bezug zu einer Verarbeitungstätigkeit oder zu der jeweiligen betroffenen Person haben. vgl. [SDM] B1.7, C1.4

Wesentliche Mittel

Wesentliche Mittel der Verarbeitung sind solche, die in engen Zusammenhang mit dem Zweck und dem Umfang der Verarbeitung stehen, insbesondere die Bestimmung über die Art der personenbezogenen Daten („welche Daten werden verarbeitet“), die Dauer der Verarbeitung („wie lange werden sie verarbeitet“), die Kategorien von Empfängern („wer hat Zugang zu ihnen“) und die Kategorien betroffener Personen („wessen personenbezogene Daten werden verarbeitet“).

Wiederherstellbarkeit

Wiederherstellbarkeit ist die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, vgl. [SDM] B1.20.

Zweckbindung

Die Verpflichtung, Daten nur für den Zweck zu verarbeiten, zu dem sie erhoben wurden, ist insbesondere den einzelnen Verarbeitungsbefugnissen zu entnehmen, die die Geschäftszwecke, die Forschungszwecke etc. zum Maßstab machen und findet über den Zweckbindungsgrundsatz aus Art. 5 Abs. 1 lit. c DSGVO Eingang in die Grundverordnung.
Eine darauffolgende Verarbeitung für weitere Zwecke muss mit dem ursprünglichen Zweck kompatibel sein und die Umstände der Verarbeitung berücksichtigen (Art. 6 Abs. 4 DSGVO). Über eine Weiterverarbeitung über den ursprünglichen Zweck hinaus, sind die betroffenen Personen ggfs. zu informieren, die von ihrem unter Umständen bestehenden Widerspruchsrecht Gebrauch machen können.
vgl. [SDM] B1.2

Impressum

Kriterienkatalog
für Prüfungen der Konformität einer
Datenverarbeitung zur Europäischen Datenschutz-Grundverordnung

Katalogkürzel:	**DSGVO**
Ausgabe:	2
Version:	2.16
Stand:	27.01.2026
Herausgeber:	TÜVNORD TÜV NORD CERT GmbH Zertifizierungsstelle Am TÜV 1 45307 Essen, Germany
Redaktion:	**TÜV NORD CERT GmbH**
Freigabe:	03.02.2026
gültig bis:	auf Widerruf