Hinweise zum
Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO

Jeder Verantwortliche und jeder Auftragsverarbeiter erstellen und führen ein Verzeichnis aller Verarbeitungstätigkeiten mit personenbezogenen Daten.

Die bisher als Verfahrensverzeichnis, Verfahrensbeschreibung oder Dateibeschreibung bekannten Dokumentationspflichten (§ 4g Abs. 2 Satz 1 Bundesdatenschutzgesetz (BDSG) bzw. jeweiliges Landesdatenschutzgesetz) werden hinfällig.
Das Verzeichnis von Verarbeitungstätigkeiten dient als wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und hilft dem Verantwortlichen dabei, gemäß Art. 5 Abs. 2 Datenschutzgrundverordnung (DS-GVO) nachzuweisen, dass die Vorgaben aus der DS-GVO eingehalten werden (Rechenschaftspflicht).
Es stellt somit ein wesentliches Element für die Etablierung eines umfassenden Datenschutz- und Informationssicherheits-Managementsystems dar.

Den Wortlaut der Art. 30 und 32 der DS-GVO finden Sie zusammen mit einem Abkürzungsverzeichnis am Ende des Dokuments. Die vollständige Fassung der DS-GVO finden Sie im Internet unter http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679.

1. Zweck des Verzeichnisses:

Der Zweck ergibt sich aus dem Erwägungsgrund (ErwGr.) 82 zu Art. 30 DS-GVO.
Hiernach sollen der Verantwortliche und der Auftragsverarbeiter „zum Nachweis der Einhaltung dieser Verordnung“ ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen.

Dieses Verzeichnis betrifft sämtliche ganz oder teilweise automatisierte Verarbeitungen sowie nichtautomatisierte Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.
Für jede einzelne Verarbeitungstätigkeit ist eine Beschreibung nach Maßgabe des Art. 30 DS-GVO anzufertigen. Als Verarbeitungstätigkeit wird im Allgemeinen ein Geschäftsprozess auf geeignetem Abstraktionsniveau verstanden. Es ist ein strenger Maßstab anzulegen, so dass jeder neue Zweck der Verarbeitung eine eigene Verarbeitungstätigkeit darstellt. Bei einer nur geringen Zweckänderung muss geprüft werden, ob eine bereits bestehende Beschreibung einer Verarbeitungstätigkeit angepasst werden muss oder ob eine vollständig neue Beschreibung anzufertigen ist. Die Summe der Einzelbeiträge ergibt das Verzeichnis von Verarbeitungstätigkeiten.

Mit der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten sind keinesfalls alle von der DS-GVO geforderten Dokumentationspflichten erfüllt. Das Verzeichnis ist nur ein Baustein, um der in Art. 5 Abs. 2 DS-GVO normierten Rechenschaftspflicht zu genügen. So müssen bspw. auch das Vorhandensein von Einwilligungen (Art. 7 Abs. 1 DS-GVO), die Ordnungsmäßigkeit der gesamten Verarbeitung (Art. 24 Abs. 1 DS-GVO) und das Ergebnis von Datenschutz-Folgenabschätzungen (Art. 35 Abs. 7 DS-GVO) durch entsprechende Dokumentationen nachgewiesen werden.

Um Redundanzen zu vermeiden und den Aufwand für die Erstellung und Führung des Verzeichnisses zu reduzieren, können in die einzelnen Beschreibungen Verweise auf bestehende Dokumente aufgenommen werden, insbesondere solche, die im Rahmen des Informationssicherheits-

managements angelegt wurden, ohne dass diese in das Verzeichnis übernommen werden müssen. So wird bspw. ein unternehmens- oder behördenweites Informationssicherheitsrahmenkonzept nur einmal erstellt werden. In verfahrensspezifische Konzepte sind dann nur noch zusätzliche oder abweichende technische und organisatorische Maßnahmen aufzunehmen.

Jeder Verantwortliche und Auftragsverarbeiter ist verpflichtet, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die einzelnen Verarbeitungsvorgänge bzw. –verfahren anhand dieser Verzeichnisse kontrolliert werden können. Sofern auf bestehende Konzepte verwiesen wird, sollten diese der Aufsichtsbehörde ebenfalls auf Anforderung vorgelegt werden.

Die neue Regelung in Art. 30 DS-GVO verpflichtet nicht nur jeden Verantwortlichen im Sinne von Art. 4 Nr. 7 DS-GVO (hierzu zählen sowohl Behörden als auch z. B. Unternehmen, Freiberufler, Vereine), sondern nun auch die Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DS-GVO, ein Verzeichnis von Verarbeitungstätigkeiten, welche sie im Auftrag durchführen, zu erstellen und zu führen. Die Regelung des Art. 30 DS-GVO bezieht sich dabei jeweils auch auf den Vertreter im Sinne von Art. 4 Nr. 17 DS-GVO.

Neben der Umsetzung der Verpflichtung nach Art. 30 DS-GVO kann das Verzeichnis als Grundlage zur Erfüllung weiterer datenschutzrechtlicher Pflichten verwendet werden. Je nach Art und Größenordnung der Stelle eines Verantwortlichen oder Auftragsverarbeiters wird zu differenzieren sein, in welchem Umfang und in welchem Detaillierungsgrad sich die weiteren Dokumentationspflichten in einem Datenschutz- und Informationssicherheitsmanagementsystem widerspiegeln. Vor diesem Hintergrund bietet es sich an, das Verzeichnis sinnvollerweise auch folgendermaßen einzusetzen bzw. zu verwenden:

- für eine Festlegung der Verarbeitungszwecke nach Art. 5 Abs. 1 lit. b DS-GVO
- für Zwecke der Rechenschafts- und Dokumentationspflicht, Art. 5 Abs. 2, Art. 24 DS-GVO
    - als Nachweis der Rechtmäßigkeit der Verarbeitung nach Art. 5 Abs. 1 lit. a DS-GVO,
    - als Nachweis der Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO,
    - als Nachweis der Richtigkeit und Aktualität der Daten nach Art. 5 Abs. 1 lit. d DS-GVO
- als geeignete Maßnahme zur Erfüllung der Betroffenenrechte nach Art. 12 Abs. 1 DS-GVO,
- zur Schaffung und als Nachweis geeigneter technischer und organisatorischer Maßnahmen nach Art. 24 Abs. 1 und Art. 32 DS-GVO,
- zur Prüfung, ob eine Datenschutzfolgenabschätzung nach Art. 35 DS-GVO erfolgen muss,
- als Basis für die Aufgabenerfüllung des Datenschutzbeauftragten nach Art. 39 DS-GVO.

Will der Verantwortliche oder Auftragsverarbeiter sein Verzeichnis für derartige Zwecke verwenden, ist es sinnvoll und zulässig, hierfür zusätzliche Informationen in das Verzeichnis aufzunehmen, z. B. einzelne Datenfelder, Herkunft bzw. Quelle der Daten, Rechtsgrundlage für die Verarbeitung, verantwortliche Mitarbeiter, zugriffsberechtigte Personen/Personengruppen.

2. Vorlage des Verzeichnisses

Der Aufsichtsbehörde müssen die Verzeichnisse der Verarbeitungstätigkeiten auf Anfrage zur Verfügung gestellt werden (Art. 30 Abs. 4 DS-GVO und ErwGr. 82).

Ziel ist es, dass die Aufsichtsbehörde die Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrollieren kann. Sofern die Aufsichtsbehörde ihre Untersuchungen auf bestimmte Verarbeitungstätigkeiten beschränkt, sind nach Maßgabe der Erforderlichkeit und nur die dafür relevanten Abschnitte des Verzeichnisses vorzulegen.

Es entfallen die bisher in § 4d und § 4e BDSG geregelten Meldepflichten an die Aufsichtsbehörde (ErwGr. 89).

Gleichfalls entfällt die bisherige Regelung im BDSG, welche ein allgemeines öffentliches Verfahrensverzeichnis mit einem Einsichtsrecht für jedermann sowie eine detaillierte interne Verarbeitungsübersicht beim Datenschutzbeauftragten vorsah.

3. Form des Verzeichnisses

3.1. Sprache

Die Verzeichnisse sind regelmäßig in deutscher Sprache zu führen, § 23 Abs. 1 und 2 Verwaltungsverfahrensgesetz (VwVfG).

Zumindest muss das Unternehmen in der Lage sein, von der Aufsichtsbehörde angeforderte Verzeichnisse (Art. 30 Abs. 4 DS-GVO und ErwGr. 82) unverzüglich in deutscher Sprache vorzulegen (vgl. Working Paper (WP) 243 der Art. 29-Gruppe (Leitlinien zum Datenschutzbeauftragten nach der DS-GVO, WP 243, Ziff. 2.3 zur sprachlichen Erreichbarkeit des Datenschutzbeauftragten).

3.2. Schriftlich – elektronisch

Die Verzeichnisse sind gemäß Art. 30 Abs. 3 DS-GVO schriftlich zu führen. Dies kann auch in einem elektronischen Format erfolgen.
Die Aufsichtsbehörde kann das Format der Vorlage (schriftlich in Papierform oder elektronisch in Textform) eigenständig festlegen und daher auch bei einem im elektronischen Format geführten Verzeichnis den Ausdruck verlangen (§ 3a VwVfG).
Maßstab sind die Verhältnismäßigkeit und Erforderlichkeit für die jeweils verfolgten aufsichtlichen Zwecke (z. B. nur der erforderliche Teil wird ausgedruckt).

4. Aktualisierung des Verzeichnisses – Änderungshistorie

Um Änderungen der Eintragungen im Verzeichnis nachvollziehen zu können (z. B. wer war wann Verantwortlicher, Datenschutzbeauftragter etc.), sollte eine Dokumentation der Änderungen mit einer Speicherfrist von einem Jahr erfolgen. Dies lässt sich auch aus dem Grundsatz der Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO herleiten.

5. Ausnahmen: Stellen mit weniger als 250 Beschäftigten

Kein Verzeichnis von Verarbeitungstätigkeiten müssen nach Art. 30 Abs. 5 DS-GVO Verantwortliche und Auftragsverarbeiter mit weniger als 250 Mitarbeitern führen, es sei denn, der Verantwortliche bzw. Auftragsverarbeiter führt Verarbeitungen personenbezogener Daten durch, die

- ein Risiko für die Rechte und Freiheiten der betroffenen Personen bergen
  (z. B. Bonitätsscoringverfahren, Betrugspräventionsverfahren) oder
- besondere Datenkategorien gemäß Art. 9 Abs. 1 DS-GVO (Religionsdaten, Gesundheitsdaten, biometrische Daten zur eindeutigen Identifizierung etc.) oder über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DS-GVO betreffen oder
- nicht nur gelegentlich erfolgen
  (alle sonstigen Verarbeitungen, z. B. Lohnabrechnungen, Kundendatenverwaltung, IT-/Internet-/E-Mail-Protokollierung, Schulnoten).

Die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten besteht also bereits dann, wenn mindestens eine der genannten drei Fallgruppen erfüllt ist. Wegen der regelmäßig erfolgenden Lohnabrechnungen werden damit kaum Unternehmen von der Pflicht eines solchen Verzeichnisses generell befreit sein; allenfalls Unternehmen, die diese Tätigkeiten komplett durch

einen Steuerberater erledigen lassen sowie eventuell kleinere Vereine. Zudem liegen bei Lohnabrechnungen oder in der Schülerverwaltung mit der Angabe der Konfessionszugehörigkeit zumeist auch gleich besondere Datenkategorien i. S. d. Art. 9 Abs. 1 DS-GVO vor.

Der Begriff „nicht nur gelegentlich“ ersetzt das „regelmäßig“ des BDSG und kann über die Leitlinien zum Datenschutzbeauftragten nach der DS-GVO der Artikel-29-Gruppe (WP 243) interpretiert werden. Nach Ziff. 2.1.4 liegt der Begriff "regelmäßig" vor, wenn mindestens eine der folgenden Eigenschaften erfüllt ist:

- fortlaufend oder in bestimmten Abständen während eines bestimmten Zeitraums vorkommend,
- immer wieder oder wiederholt zu bestimmten Zeitpunkten auftretend,
- ständig oder regelmäßig stattfindend.

Verarbeitungen, die ein Risiko für die Rechte und Freiheiten der Betroffenen bergen, können z. B. sein:

- Videoüberwachungen,
- Bonitätsscoring- und Betrugspräventionsverfahren,
- Ortung von Mitarbeitern (z. B. mittels GPS),
- Verarbeitungen, bei denen Kommunikationsinhalte betroffen sind.

Fazit: Es ist davon auszugehen, dass die Ausnahmen nur selten greifen werden und vielfach das Erstellen eines Verzeichnisses von Verarbeitungstätigkeiten geboten ist.

6. Inhalt des Verzeichnisses – Verantwortliche, Art. 30 Abs. 1 DS-GVO

Das Verzeichnis muss sämtliche der in Art. 30 Abs. 1 S. 2 lit. a bis g DS-GVO abschließend genannten Angaben enthalten. Diese Angaben müssen die Verarbeitungstätigkeiten des Verantwortlichen aussagekräftig beschreiben. Es ist zu empfehlen, den Namen der jeweiligen Verarbeitungstätigkeit von dem Verarbeitungszweck ausgehend festzulegen (z. B. „Personalaktenführung“/“Stammdaten“, „Lohn-, Gehalts- und Bezügeabrechnung“ usw.).

Nutzt der Verantwortliche das Verzeichnis seiner Verarbeitungstätigkeiten auch dazu, andere Dokumentationspflichten aus der DS-GVO zu erfüllen und seiner Rechenschaftspflicht umfassend zu nachzukommen, sind die bereits im Abschnitt 1 aufgezählten zusätzlichen Angaben sinnvoll und empfehlenswert.

6.1. Namen und Kontaktdaten, Art. 30 Abs. 1 S. 2 lit. a DS-GVO

Anzugeben sind Namen und Kontaktdaten

- des Verantwortlichen i. S. d. Art. 4 Nr. 7 DS-GVO,
- eines ggf. gemeinsam mit ihm Verantwortlichen (Art. 26 DS-GVO),
- eines evtl. Vertreters für in Drittstaaten ansässige Verantwortliche (Art. 4 Nr. 17, Art. 27 DS-GVO) und
- eines etwaigen Datenschutzbeauftragten.

Anzugeben sind die postalische, elektronische und telefonische Erreichbarkeit, um zu gewährleisten, dass die Aufsichtsbehörde den Verantwortlichen auf einfachem Wege (und in Eilfällen auch über verschiedene Kanäle) erreichen kann (s.a. WP 243, Ziff. 2.6).

Bei Behörden und juristischen Personen sind nicht zwingend Daten zu Leitungspersonen gefordert, aus aufsichtsbehördlicher Sicht ist die Angabe des operativ verantwortlichen Ansprechpartners wünschenswert. Dementsprechend sollte ein Eintrag unter „Ansprechpartner“ erfolgen.

Hinsichtlich des Begriffs „Vertreters“ ist die Begriffsbestimmung des Art. 4 Nr. 17 DS-GVO zu beachten, wonach „Vertreter“ nicht nur der inländische Vertreter ist, sondern darüber hinaus eine in der EU niedergelassene natürliche oder juristische Person.

6.2. Zwecke der Verarbeitung, Art. 30 Abs. 1 S. 2 lit. b DS-GVO

Je Beschreibung einer Verarbeitungstätigkeit ist der Verarbeitungszweck zu dokumentieren, z. B.:

- Personalaktenführung/Stammdaten
- Lohn-, Gehalts- und Bezügeabrechnung
- Arbeitszeiterfassung
- Urlaubsdatei
- Nutzungsprotokollierungen IT/Internet/E-Mail
- Bewerbungsverfahren
- Telefondatenerfassung
- Firmenparkplatzverwaltung
- Videoüberwachung an Arbeitsplätzen, in Schulen etc.
- Schülerverwaltung, Unterrichtsplanung, Zeugniserstellung
- Beschaffung/Einkauf sowie Finanzbuchhaltung
- Antragsbearbeitung (Bauanträge, Wohngeldanträge etc.)
- Rats- und Bürgerinformationssysteme
- Meldewesen (Melderegister)
- Fahrerlaubnisregister und Fahrzeugregister
- Wahlen (Wählerverzeichnis)
- amtsärztliche Untersuchungen
- Schwangeren- und Mütterberatung
- Erfassung und Überwachung der nichtakademischen Heilberufe

Für jede Verarbeitung sind vorher die Zwecke festzulegen.

Die Zwecke müssen eindeutig und so aussagekräftig sein, dass die Aufsichtsbehörde die Angemessenheit der getroffenen Schutzmaßnahmen und die Zulässigkeit der Verarbeitung vorläufig einschätzen kann.

6.3. Kategorien betroffener Personen und personenbezogener Daten, Art. 30 Abs. 1 S. 2 lit. c DS-GVO

Zu beschreiben sind die Kategorien betroffener Personen und die Kategorien personenbezogener Daten.
Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO sollte gesondert beschrieben werden (Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person).

Dabei empfiehlt es sich hinsichtlich der einzelnen Kategorien personenbezogener Daten laufende Nummern zu vergeben, die so eine Zuordnung zu den weiteren konkreten Angaben gem. Art. 30 Abs. 1 S. 2 lit. d bis g DS-GVO ermöglichen, z. B. zu konkreten Löschregeln.

Aufgegliedert z. B. in der Darstellung der „Kategorie Beschäftigte“ in die Daten-Kategorien:

- Mitarbeiter-Stammdaten
  mit Adressdaten, Geburtsdatum, Bankverbindung, Steuermerkmale, Lohngruppe, Arbeitszeit, bisherige Tätigkeitsbereiche, Qualifikationen etc.
- Bewerbungen mit Kontaktdaten, Qualifikationsdaten, Tätigkeiten etc.
- Arbeitszeugnisse mit Adressdaten, Leistungsdaten, Beurteilungsdaten etc.
- Abmahnungen mit Adressdaten, Arbeitsverhalten, Leistungsdaten etc.
- Betriebsarztuntersuchungen mit Adressdaten, Gesundheitsdaten etc.
- Stundenplan als Einsatzplan für Lehrkräfte
- Videoüberwachung an Arbeitsplätzen etc.

Aufgegliedert z. B. in der Darstellung der „Kategorie Kundendaten“ in die Kategorien:

- Kunden-Kontaktdaten mit Adressdaten, Ansprechpartnern etc.
- Kundengruppe/-interesse
- Umsatzdaten bisher
- Bonitätsdaten
- Zahlungsdaten usw.
- für Schulen: Fehlzeiten, Schulleistungsnachweise

Aufgegliedert z. B. in der Darstellung „Kategorie Abgeordnetendaten“ in die Kategorien:

- Namen und Kontaktdaten (Adresse, Telefon, E-Mail) von Abgeordneten
- Fraktionszugehörigkeit

6.4. Kategorien von Empfängern, Art. 30 Abs. 1 S. 2 lit. d DS-GVO

Zu beschreiben sind die Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen.

Sie können z. B. für die Lohn- und Gehaltsabrechnung wie folgt aufgegliedert werden:

- Banken
- Sozialversicherungsträger
- Finanzämter
- unternehmensinterne andere Datenempfänger (z. B. Betriebsarzt, Personalrat)
- ggf. Gläubiger bei Lohn-/Gehaltspfändungen
- ggf. Träger der Betriebsrente
- ggf. Auftragsverarbeiter
- ggf. Muttergesellschaft

Empfänger können auch Teile eines Unternehmens oder einer Behörde sein. Dies ist der Fall, sofern ein Zugriff auf die Daten möglich ist (z. B. Zugriff auf Unternehmens- oder Kundendaten bei bundesweit tätigen Banken oder abgebende und aufnehmende Schule bei gleichem Schulträger).

Der Begriff „Datenempfänger“ ist daher zu ergänzen durch „Zugriffsberechtigte“. Die Angaben zu den zugriffsberechtigten Personen sind nach der DS-GVO zwar nicht vorgesehen. Es wird jedoch empfohlen, Angaben zu diesen zu machen.

Die Zugriffsberechtigten sollten, wie bisher, ohne namentliche Angabe angegeben werden.
Sie müssen jedoch z. B. über eine Rollen- oder Funktionsbeschreibung eindeutig bestimmbar sein. Es kann aber, z. B. beim o.g. filialseitigen Zugriff auf die Daten, sinnvoll sein, die Angabe einer Zahl der Zugriffsstellen bzw. Zugriffsberechtigten mit Bezug zum aktuellen Stand (Tagesdatum) anzugeben.

Zu „Drittländern“ sollte in jedem Fall eine Aussage getroffen werden, also auch angegeben werden, wenn eine Übermittlung in Drittländer nicht stattfindet und auch nicht geplant ist.

Eine Übermittlung in Drittländer erfolgt auch, wenn sich dort der Server befindet oder der Mailversand hierüber abgewickelt wird. Ebenso kann eine Übermittlung in Drittländer vorliegen, wenn Supportdienstleistungen aus diesem erbracht werden.

„Offenlegung“ bedeutet, dass sowohl die Empfänger in der Vergangenheit, als auch jene in der Zukunft zu benennen sind.

6.5. Übermittlungen in Drittländer – Art. 30 Abs. 1 S. 2 lit. e DS-GVO

Angaben zu Übermittlungen von personenbezogenen Daten in ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 DS-GVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien

Empfänger in Drittländern und internationale Organisationen sind keine Kategorien und daher konkret zu benennen.

Art. 49 Abs. 6 DS-GVO ist zu beachten, wonach der Verantwortliche die von ihm vorgenommene Beurteilung sowie die angemessenen Garantien im Sinne des Art. 49 Abs. 1 Unterabsatz 2 DS-GVO im Verzeichnis der Verarbeitungstätigkeiten aufnimmt.

6.6. Speicherdauer – Art. 30 Abs. 1 S. 2 lit. f DS-GVO

Angabe der vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien, z. B.

- die geltenden handels- und steuerrechtlichen Aufbewahrungspflichten für Personaldaten, Kundendaten etc.
- geltende Aufbewahrungs- und Löschfristen für Schülerdaten, Prüfungsunterlagen etc.
- gesetzlich vorgesehene Löschungsfristen (z. B. § 14 Bundesmeldegesetz)
- vom Verantwortlichen festgelegte Überprüfungs-/Löschungsfristen

Ein allgemeiner Verweis auf Aufbewahrungspflichten genügt nicht, vielmehr sind präzise Angaben erforderlich.

Referenzdokumente

Es wird empfohlen, weitere Bausteine einer umfassenden Dokumentation der Datenschutzstrategie, wie z. B.

- die Dokumentation interner Verhaltensregeln,
- die Dokumentation einer Risikoanalyse oder allgemeinen Datensicherheitsbeschreibung,
- ein umfassendes Datensicherheits- oder Wiederanlaufkonzept,
- ein Zertifikat oder
- Ergebnisse einer Datenschutz-Folgenabschätzung

am Ende der Dokumentation der Verarbeitungstätigkeit unter „Sonstiges“ als Referenz anzugeben.

Auf Nachfrage können diese Referenzdokumente zusätzlich zum Verzeichnis der Aufsichtsbehörde vorgelegt werden; es ist sinnvoll, zumindest die für das Verständnis und die Bewertung des Verarbeitungsverzeichnisses essentiellen zusätzlichen Dokumente bereits im ersten Schritt freiwillig mitzuliefern. Insofern stellen die zusätzlich aufgeführten Dokumentationen keine Anlagen zum Verzeichnis dar, sondern weitere, darüber hinausgehende Bausteine einer umfassenden Dokumentation der organisationsinternen Datenschutzstrategie, auf welche verwiesen werden und die neben dem Verzeichnis vorgehalten werden können.

Sie dienen zusammen mit dem Verzeichnis der Umsetzung der aus Art. 5 Abs. 2 DS-GVO resultierenden Rechenschaftspflicht. Wird innerhalb des Verzeichnisses auf andere Dokumente, wie z. B. ein anderes Verarbeitungsverzeichnis Bezug genommen, so ist dies an dieser Stelle als Referenzdokument aufzuführen.

Es wird empfohlen, eine solche Dokumentation an zentraler Stelle zu pflegen.

6.7. Technische und organisatorische Maßnahmen Art. 30 Abs. 1 S. 2 lit. g DS-GVO

Trotz der Formulierung „wenn möglich“ stellt die allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO hier den Regelfall dar.
Art. 5 Abs. 2 DS-GVO verpflichtet den Verantwortlichen insbesondere auch zur Dokumentation der technischen und organisatorischen Maßnahmen (Art. 5 Abs. 1 lit. f DS-GVO). Zudem muss der Verantwortliche die Wirksamkeit dieser Maßnahmen regelmäßig überprüfen (Art. 32 Abs. 1 lit. d DS-GVO). Beide Forderungen kann der Verantwortliche nur erfüllen, wenn die technischen und organisatorischen Maßnahmen vollständig beschrieben sind (etwa in einem Sicherheitskonzept).

Eine Verarbeitung darf erst erfolgen, wenn der Verantwortliche seiner Pflicht nach Art. 24 DS-GVO nachgekommen ist. Darunter fallen neben den Verpflichtungen nach Art. 12 und 25 DS-GVO auch diejenigen nach Art. 32 DSGVO zur Bestimmung und Umsetzung geeigneter technischer und organisatorischer Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Das betrifft primär Fragen der Sicherheit der Verarbeitung, schließt somit aber auch Maßnahmen zur Gewährleistung von Betroffenenrechten ein. In das Verzeichnis ist eine allgemeine, einfach nachvollziehbare Beschreibung der für diesen Zweck getroffenen Maßnahmen aufzunehmen.
Die Beschreibung der jeweiligen Maßnahme ist konkret auf die Kategorie betroffener Personen bzw. personenbezogener Daten im Sinne des Art. 30 Abs. 1 S. 2 lit. c DS-GVO zu beziehen, soweit eine entsprechende Differenzierung in ihrer Anwendung erfolgt.

Für die Bestimmung der zu treffenden Maßnahmen wird auf das Standard-Datenschutzmodell, die Leitlinien und Orientierungshilfen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und der Artikel-29-Arbeitsgruppe sowie auf die bestehenden nationalen und internationalen Standards (z. B. BSI-Grundschutz, ISO-Standards) verwiesen. Ist bei der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zu erwarten, hat die Bestimmung der Maßnahmen bereits im Rahmen einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO zu erfolgen.

Eine Verletzung der Sicherheit der Datenverarbeitung ist immer eine Verletzung des Schutzes personenbezogener Daten i. S. v. Art. 4 Nr. 12 DS-GVO.

Nach Art. 32 Abs. 1 DS-GVO sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der mit ihr verbundenen Risiken geeignete technische und organisatorische Maßnahmen zu treffen, um insbesondere Folgendes sicherzustellen:

6.8. Maßnahmenbereiche, die sich aus Art. 32 Abs. 1 DS-GVO ergeben:

- Pseudonymisierung personenbezogener Daten
- Verschlüsselung personenbezogener Daten
- Gewährleistung der Integrität und Vertraulichkeit der Systeme und Dienste
- Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste
- Wiederherstellung der Verfügbarkeit personenbezogener Daten und des Zugangs zu ihnen nach einem physischen oder technischen Zwischenfall
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen

Nachfolgend werden den einzelnen Bereichen typische, bewährte technische und organisatorische Maßnahmen zugeordnet. Die Auflistung ist nicht vollständig oder abschließend. In Abhängigkeit von den konkreten Verarbeitungstätigkeiten können weitere oder andere Maßnahmen geeignet und angemessen sein. Auch ist die Zuordnung einzelner Maßnahmen zu einem bestimmten Maßnahmenbereich nicht in jedem Fall eindeutig.

- Maßnahmen zur Pseudonymisierung personenbezogener Daten

  Hierzu zählen u. a.:

  - Festlegung der durch Pseudonymisierung zu ersetzenden identifizierenden Daten
  - Definition der Pseudonymisierungsregel, ggf. anknüpfend an Personal-, Kunden- oder Patienten-Kennziffern
  - Autorisierung: Festlegung der Personen, die zur Verwaltung der Pseudonymisierungsverfahren, zur Durchführung der Pseudonymisierung und ggf. der Depseudonymisierung berechtigt sind
  - Festlegung der zulässigen Anlässe für Pseudonymisierungs- und Depseudonymisierungsvorgänge
  - zufällige Erzeugung der Zuordnungstabellen oder der in eine algorithmische Pseudonymisierung eingehenden geheimen Parameter
  - Schutz der Zuordnungstabellen bzw. geheimen Parameter sowohl gegen unautorisierten Zugriff als auch gegen unautorisierte Nutzung
  - Trennung der zu pseudonymisierenden Daten in die zu ersetzenden identifizierenden und die weiteren Angaben

- Maßnahmen zur Verschlüsselung personenbezogener Daten

  (z. B. in stationären und mobilen Speicher-/Verarbeitungsmedien, beim elektronischen Transport)

  Schlüssel können flüchtig (z. B. für die Dauer eines Kommunikationsvorgangs) oder statisch (mittel- oder langfristig) für den Schutz personenbezogener Daten eingesetzt werden.

  Es sind Festlegungen zu treffen (z. B. im Rahmen eines Kryptokonzepts) u. a. zur Auswahl geeigneter kryptografischer Verfahren und Produkte, zur Organisation ihres Einsatzes, zu Maßnahmen bei der Entdeckung von Schwächen in Verschlüsselungsverfahren oder -produkten (Um- oder Überverschlüsselung) sowie zu Schlüssellängen. Voraussetzung für effektive Verschlüsselung ist ein adäquates Schlüsselmanagement, das u. a. folgende Aspekte betrifft:

  - zufällige Erzeugung der Schlüssel
  - Autorisierung von Personen zur Verwaltung und zur Nutzung von Schlüsseln bzw. ihre Zuweisung zu Geräten, in denen sie eingesetzt werden
  - zuverlässige Schlüsselverteilung, Verknüpfung von Schlüsseln mit Identitäten von natürlichen Personen oder informationstechnischen Geräten, ggf. Einbringen in speziell gesicherte Speichermedien (z. B. Chipkarten)
  - Schutz der Schlüssel vor nicht autorisiertem Zugriff oder Nutzung
  - regelmäßiger oder situationsbezogener Schlüsselwechsel, ggf. eine Schlüsselarchivierung, stets sorgfältige Schlüssellöschung nach Ablauf des Lebenszyklusses
  - Verwaltung des Lebenszyklus der Schlüssel von Erzeugung und Verteilung über Nutzung bis zu ihrer Archivierung und Löschung

- Maßnahmen zur Gewährleistung der Integrität und Vertraulichkeit der Systeme und Dienste

  Die folgenden Maßnahmen sollen eine spezifikationsgerechte Verarbeitung sichern und nicht autorisierte bzw. unberechtigte Verarbeitung sowie unbeabsichtigte Änderung, Verlust oder Schädigung personenbezogener Daten ausschließen; beim Verantwortlichen selbst oder auf

dem Transportweg zu Auftragsverarbeitern oder Dritten.
Hierzu zählen u. a.:

- Formulierung von verbindlichen Sicherheitsleitlinien
- Definition der Verantwortlichkeiten für das Informationssicherheitsmanagement
- Inventarisierung der zu verarbeitenden personenbezogenen Daten
- Inventarisierung der Informationstechnik
- Erarbeitung eines Sicherheitskonzepts, ggf. unter Durchführung einer Risikoanalyse
- Personalsicherheit: Überprüfung und Verpflichtung des Personals, Sensibilisierung und Training, Aufgabentrennung
- Spezifikation der Sicherheitsanforderungen an Informationssysteme und deren Konfiguration, Prüfung ihrer Einhaltung
- Schutz vor unberechtigtem physischem Zugang, einschließlich Schutz von Mobilgeräten
- Erarbeitung eines Rollen- und Rechtekonzepts
- Maßnahmen zur Autorisierung von Personen für den Zugriff auf personenbezogene Daten und die Steuerung der Verarbeitung
- Zugriffskontrolle und sicherer Umgang mit Speichermedien, einschließlich der Maßnahmen zur zuverlässigen Authentisierung von Personen gegenüber der Informationstechnik, zur Sicherung der Revisionsfähigkeit der Eingabe und der Änderung von personenbezogenen Daten sowie ggf. der Nutzung und des Zugriffs auf diese und zur Revision dieser Prozesse
- Maßnahmen der Betriebssicherheit, insbesondere zur Spezifikation der Bedienabläufe, zur Änderungssteuerung, zum Schutz vor Malware, zum Umgang mit technischen Schwachstellen, zur kontrollierten Installation und Konfiguration neuer Software, sowie zur Ereignisüberwachung und -protokollierung, einschließlich der regelmäßigen und anlassbezogenen Auswertung dieser Protokolle
- Maßnahmen, die (berechtigte oder unberechtigte) Veränderung gespeicherter oder übertragener Daten nachträglich feststellbar machen (z. B. Signaturverfahren, Hashverfahren)
- Maßnahmen zur Kommunikationssicherheit: Netzwerksicherheitsmanagement, insbesondere zur Kontrolle und Einschränkung des Datenverkehrs (Firewalls, Application Layer Gateways), Einrichtung von Sicherheitszonen, Authentisierung von Geräten gegeneinander
- sichere Gestaltung von Informationsübertragungen, einschließlich des Abschlusses von Vereinbarungen mit regelmäßigen Übermittlern und Empfängern personenbezogener Daten und der Authentisierung der Kommunikationspartner
- Sicherung und Überprüfung der Authentizität der übermittelten Daten
- sichere Einbeziehung von externen Diensten
- Management von Informationssicherheitsvorfällen
- Aufrechterhaltung der Informationssicherheit bei ungeplanten Systemzuständen
- Durchführung von internen oder externen Sicherheitsaudits
- logische oder physikalische Trennung der Datenverarbeitung z. B. nach verantwortlichen Stellen, den verfolgten Verarbeitungszwecken und nach Gruppen betroffener Personen
- sicheres, rückstandsfreies Löschen von Daten bzw. Vernichten von Datenträgern nach Ablauf der Aufbewahrungsfristen, Festlegungen zu Löschverfahren und zur Beauftragung von Dienstleistern

- Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste

  Die folgenden Maßnahmen sollen sicherstellen, dass personenbezogene Daten dauernd und uneingeschränkt verfügbar und insbesondere vorhanden sind, wenn sie gebraucht werden.
  Hierzu zählen u. a.:

  - Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß eines getesteten Konzepts

- Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage z. B. DDOS, höhere Gewalt)
- Dokumentation von Syntax und Semantik der gespeicherten Daten
- Redundanz von Hard- und Software sowie Infrastruktur
- Umsetzung von Reparaturstrategien und Ausweichprozessen
- Vertretungsregelungen für abwesende Mitarbeiter

- Maßnahmen, um nach einem physischen oder technischen Zwischenfall (Notfall) die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen rasch wiederherzustellen

  Eine besondere Ausprägung der Gewährleistung von Verfügbarkeit ist hinsichtlich möglicher Notfälle (siehe dazu auch BSI Standard 100-4) erforderlich. Hierzu sind u. a. folgende Maßnahmen erforderlich:
  - Erstellung und Umsetzung eines Notfallkonzepts
  - Erarbeitung eines Notfallhandbuches
  - Integration des Notfallmanagements in Geschäftsprozesse
  - Durchführung von Notfallübungen
  - Erprobung von Wiederanlaufszenarien

- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen

  Hierzu zählen u. a.:
  - regelmäßige Revision des Sicherheitskonzepts
  - Information über neu auftretende Schwachstellen und andere Risikofaktoren, ggf. Überarbeitung der Risikoanalyse und -bewertung
  - Prüfungen des Datenschutzbeauftragten und der IT-Revision auf Einhaltung der festgelegten Prozesse und Vorgaben zur Konfiguration und Bedienung der IT-Systeme
  - externe Prüfungen, Audits, Zertifizierungen

6.9. Weitere Maßnahmenbereiche, die sich aus der DS-GVO ergeben und deren Darstellung im Verzeichnis empfohlen wird:

Die Formulierung in Art. 32 Abs. 1 DS-GVO „diese Maßnahmen schließen unter anderem Folgendes ein“ verdeutlicht, dass die dort vorgenommene Aufzählung nicht abschließend ist. Die Sicherheit der Verarbeitung ist u. a. auch Voraussetzung dafür, dass Daten nur für den Zweck verarbeitet und ausgewertet werden können, für den sie erhoben werden (Zweckbindung), dass Betroffene, Verantwortliche und Kontrollinstanzen u. a. erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden (Transparenz) und dass den Betroffenen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt werden (Intervenierbarkeit). Entsprechend sind auch die Maßnahmenbereiche zu berücksichtigen, die vorrangig der Minimierung der Eingriffsintensität in die Grundrechte Betroffener dienen.

- Maßnahmen zur Gewährleistung der Zweckbindung personenbezogener Daten (Nichtverkettung) – Art. 5 Abs. 1 lit. b) DS-GVO:
  - Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten
  - programmtechnische Unterlassung bzw. Schließung von Schnittstellen in Verfahren und Verfahrenskomponenten
  - regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung
  - Trennung nach Organisations-/Abteilungsgrenzen
  - Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentisierungsverfahrens
  - Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle

- Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten
- geregelte Zweckänderungsverfahren

- Maßnahmen zur Gewährleistung der Transparenz für Betroffene, Verantwortliche und Kontrollinstanzen – Art. 5 Abs. 1 lit. a) DS-GVO:
  - Dokumentation von Verfahren insbesondere mit den Bestandteilen Geschäftsprozesse, Datenbestände, Datenflüsse, dafür genutzte IT-Systeme, Betriebsabläufe, Verfahrensbeschreibungen, Zusammenspiel mit anderen Verfahren
  - Dokumentation von Tests, der Freigabe und ggf. der Vorabkontrolle von neuen oder geänderten Verfahren
  - Dokumentation der Verträge mit den internen Mitarbeitern, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen
  - Dokumentation von Einwilligungen und Widersprüchen
  - Protokollierung von Zugriffen und Änderungen
  - Nachweis der Quellen von Daten (Authentizität)
  - Versionierung
  - Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts
  - Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept

- Maßnahmen zur Gewährleistung der Betroffenenrechte – Art. 13 ff. DS-GVO (Intervenierbarkeit):
  - differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten
  - Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen
  - dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen am Verfahren sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes
  - Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem
  - Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen
  - Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte
  - Einrichtung eines Single Point of Contact (SPoC) für Betroffene
  - operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten

7. Inhalt des Verzeichnisses – Auftragsverarbeiter, Art. 30 Abs. 2 DS-GVO

Jeder Auftragsverarbeiter und ggf. sein Vertreter im Sinne von Art. 4 Nr. 17 DS-GVO führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitungen.

Das Verzeichnis enthält sämtliche der in Art. 30 Abs. 2 lit a bis d DS-GVO enumerativ genannten Angaben und bildet so ein Auftragskataster mit Angabe der Auftraggeber und der Subunternehmer.

Dabei muss ein Subunternehmer nur seine direkten Auftraggeber nennen und nicht die dahinter stehende weitere Kette bis zu den Verantwortlichen zurück.

Hinsichtlich der Erläuterungen und Begriffsbestimmungen wird auf die Ausführungen zu Kapitel 1 bis 6 verwiesen.

7.1. Namen und Kontaktdaten – Art. 30 Abs. 2 lit. a DS-GVO

Namen und Kontaktdaten

- des Auftragsverarbeiters, ggf. mehrerer im Sinne von Art. 4 Nr. 8 DS-GVO
- ggf. Namen und Kontaktdaten eines Vertreters des Auftragsverarbeiters im Sinne von Art. 4 Nr. 17 DS-GVO i.V.m. Art. 27 DS-GVO
- jedes Verantwortlichen i.S.v. Art. 4 Nr. 7 DS-GVO, in dessen Auftrag der Auftragsverarbeiter tätig ist
- ggf. Namen und Kontaktdaten eines Vertreters des Verantwortlichen im Sinne von Art. 4 Nr. 17 i.V.m. Art. 27 DS-GVO
- eines etwaigen Datenschutzbeauftragten

7.2. Beschreibung der Verarbeitungen – Art. 30 Abs. 2 lit. b DS-GVO

Beschreibung der Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden.

Das Auftragskataster ist nach den einzelnen Aufträgen zu differenzieren, z. B.:

- Lohn- und Gehaltsabrechnung
- Finanzbuchhaltung
- E-Mail-Datenbank
- Übernahme der betrieblichen/behördlichen Telefonanlage
- Werbeadressenverarbeitung
- Einscannen von betrieblichen/behördlichen Schriftstücken
- Support-/Wartungsservice
- Rechnerservice mit Support und Datensicherung, bei denen allein der Auftraggeber den Zweck und die Verarbeitungen festlegt
- Archivierung von Datenbeständen
- Löschung sowie Entsorgung von Datenträgern
- Lernplattform
- Datenverarbeitung in einem externen Rechenzentrum

7.3. Übermittlungen in Drittländer – Art. 30 Abs. 2 lit. c DS-GVO

Angaben zu Übermittlungen von personenbezogenen Daten in ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Abs. 1 Unterabsatz 2 DS-GVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien

- Darstellung wie bei Art. 30 Abs. 1 lit. e DS-GVO
- mit Angabe der konkreten Datenempfänger im Drittland

7.4. Technisch-organisatorische Maßnahmen – Art. 30 Abs. 2 lit. d) DS-GVO

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO

Hinsichtlich der Erläuterungen und Begriffsbestimmungen wird auf die Ausführungen zu Art. 30 Abs. 1 S. 2 lit. g DS-GVO verwiesen, s. Ziff.6.7 bis 6.9.

8. Rechtsfolgen bei Verstoß – Art. 83 Abs. 4 lit. a DS-GVO

Verstöße durch

- fehlende oder nicht vollständige Führung eines Verzeichnisses aller Verarbeitungstätigkeiten oder
- Nichtvorlegen des Verzeichnisses nach Aufforderung durch die Aufsichtsbehörde

werden mit Geldbußen von bis zu 10.000.000 € oder im Fall eines Unternehmens von bis zu 2% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

9. Rechtsgrundlagen

Artikel 30 – Verzeichnis von Verarbeitungstätigkeiten

(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen.
Dieses Verzeichnis enthält sämtliche folgenden Angaben:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
b) die Zwecke der Verarbeitung;
c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

(2) Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:

a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung

geeigneter Garantien;
d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

(3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

(4) Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

(5) Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt.

Artikel 32 – Sicherheit der Verarbeitung

(1) 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 treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

10. Abkürzungsverzeichnis:

DS-GVO	Datenschutz-Grundverordnung
VwVfG	Verwaltungsverfahrensgesetz
ErwGr.	Erwägungsgrund (Erläuterungen für die Auslegung der DS-GVO)
WP	Working Paper (Arbeitsunterlagen, Leitlinien zur Klarstellung der einschlägigen Bestimmungen der DS-GVO sowie Orientierungshilfe bei deren Auslegung)
Verantwortlicher	ersetzt den bisherigen Begriff der verantwortlichen Stelle Definition in Art. 4 Nr. 7 DS-GVO
Auftragsverarbeiter	ersetzt den bisherigen Begriff des Auftragnehmers Definition in Art. 4 Nr. 8 DS-GVO

Stand: Februar 2018