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

Jeder Verantwortliche und jeder Auftragsverarbeiter erstellen und führen ein Verzeichnis aller Verarbeitungstätigkeiten mit personenbezogenen Daten.
Dieses ersetzt die bisher als Verfahrensverzeichnis, Verfahrensbeschreibung oder Dateibeschreibung bekannten Dokumentationspflichten (§ 4g Abs. 2 Satz 1 Bundesdatenschutzgesetz (BDSG) bzw. jeweiliges Landesdatenschutzgesetz).

Den Wortlaut der Art. 30 und 32 der EU-Datenschutzgrundverordnung (DS-GVO) finden Sie zusammen mit einem Abkürzungsverzeichnis am Ende des Dokuments.

1. Zweck des Verzeichnisses:

Der Zweck ergibt sich aus dem Erwägungsgrund (EG) 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.

Jeder Verantwortliche und Auftragsverarbeiter ist verpflichtet, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können.

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 solches Verzeichnis zu erstellen und zu führen.
Die Regelung des Art. 30 bezieht sich dabei jeweils auch auf den Vertreter im Sinne von Art. 4 Nr. 17 DS-GVO.

Ausgehend von Mindestanforderungen nach Art. 30 Abs. 1 DS-GVO werden Inhalt und Umfang des Verzeichnisses je nach Art und Größenordnung der Stelle eines Verantwortlichen oder Auftragsverarbeiters zu differenzieren sein.
Hinzu kommt, dass das Verzeichnis über die reine Dokumentation hinaus sinnvollerweise auch eingesetzt bzw. verwendet werden kann:

- 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 geeignete Maßnahme zur Erfüllung der Betroffenenrechte nach Art. 12 Abs. 1 DS-GVO
- zur Schaffung und als Nachweis geeigneter technisch-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

Hierfür sind zwangsläufig zusätzliche Informationen im Verzeichnis nötig, z. B. einzelne Datenfelder, Herkunft bzw. Quelle der Daten, Rechtsgrundlage für die Verarbeitung, verantwortlicher Mitarbeiter, zugriffsberechtigte Personen/Personengruppen etc.

Somit wird das Verzeichnis in der Praxis wegen der Unterschiede bei den eingesetzten Verfahren oft aus einer Reihe von Einzelbeschreibungen bestehen müssen.

2. Vorlage des Verzeichnisses

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

Ziel ist es, dass die Aufsichtsbehörde die Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrollieren kann.

Es entfallen die bisher in § 4d und § 4e BDSG geregelten Meldepflichten an die Aufsichtsbehörde, s. EG 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 EG 82) unverzüglich in deutscher Sprache vorzulegen (Working Paper (WP) 243 der Art. 29-Gruppe (Leitlinien zum Datenschutzbeauftragten nach der DS-GVO, WP 243, Ziff. 2.3)).

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 Mitarbeitern

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-Grupooe (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, so auch die Auffassungen der bisher veröffentlichten Literatur.

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

Das Verzeichnis muss sämtliche der in Art. 30 Abs. 1 S. 2 lit a bis g DS-GVO enumerativ genannten Angaben enthalten. Diese müssen aussagekräftig sein, was auch von der Unternehmensgröße abhängt.

Sinnvoll und empfehlenswert bei einem „erweiterten Verzeichnis“ sind noch folgende Angaben:

- Beschreibung der konkreten Verarbeitungstätigkeiten im Sinne der Definition in Art. 4 Nr. 2 DS-GVO (erheben, speichern, abfragen, offenlegen etc.),
- Nennung der herangezogenen Rechtsgrundlagen (z. B. Art. 6 DS-GVO, Arbeitsvertrag, Betriebsvereinbarung, eine wirksame Einwilligung, spezielle gesetzliche Regelung etc.).

Namen und Kontaktdaten – Art. 30 Abs. 1 S. 2 lit. a

- 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)
  - 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. 2.5).

Bei Behörden und juristischen Personen sind nicht zwingend Daten zu Leitungspersonen gefordert, aus aufsichtsbehördlicher Sicht ist die Angabe des operativ verantwortlichen Ansprechpartners wünschenswert.

Bezüglich der Hauptniederlassung ist diese im Sinne vom Art. 4 Nr. 16 lit. a DS-GVO anzugeben.

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.

Zwecke der Verarbeitung – Art. 30 Abs. 1 S. 2 lit. b

Aufgegliedert in Einzelverzeichnisse wie:

- 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 transparent sein, damit die Aufsichtsbehörde die Angemessenheit der getroffenen Schutzmaßnahmen und die Zulässigkeit der Verarbeitung prüfen kann.

Kategorien betroffener Personen u. personenbez. Daten - Art. 30 Abs. 1 S. 2 lit. c

Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten.

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 f 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

Kategorien von Empfängern – Art. 30 Abs. 1 S. 2 lit. d

Angabe der Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern.

Aufgegliedert z. B.: für die Lohn- und Gehaltsabrechnung:

- Banken
- Sozialversicherungsträger
- Finanzämter
- unternehmensinterne andere Datenempfänger (z.B. Betriebsrat, Fachvorgesetzte)

- 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. ein 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 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.

Übermittlungen in Drittländer – Art. 30 Abs. 1 S. 2 lit. e

Angaben zu 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

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 im Verzeichnis der Verarbeitungstätigkeiten aufnimmt.

Speicherdauer – Art. 30 Abs. 1 S. 2 lit. f

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.

Technische und organisatorische Maßnahmen – Art. 30 Abs. 1 S. 2 lit. g

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

Eine Verarbeitung darf nicht erfolgen, bevor der Verantwortliche seiner Pflicht nach Art. 32 nachgekommen ist. Daher ist davon auszugehen, dass die Dokumentation nicht auf eine konkrete Beschreibung verzichten kann.
Dabei müssen die obligatorischen Angaben des Verzeichnisses einfach nachzuvollziehen sein.

Denkbar sind Verweise auf bestehende Dokumente. Bei größeren Unternehmen genügt ggf. auch ein Verweis auf schon vorhandene Dokumentationen und Sicherheitskonzepte (z.B. Standarddatenschutzmodell (SDM)), ohne dass diese hier in Gänze dargestellt werden.

Die in Art. 32 Abs. 1 DS-GVO unter anderem genannten Maßnahmenbereiche entsprechen im Wesentlichen dem bisherige Katalog der technisch-organisatorischen Maßnahmen (TOMs) nach § 9 BDSG und der Anlage hierzu.

Die Beschreibung der jeweiligen Maßnahme ist konkret auf die Kategorie betroffener Personen bzw. personenbezogener Daten i.S.d. Art. 30 Abs. 1 S. 2 lit. c DS-GVO zu beziehen.

In diesem Zusammenhang wird auch auf eine Verwendung des SDM verwiesen.

Sofern besondere Arten personenbezogener Daten betroffen sind, bedarf es einer sorgfältigen Auswahl der technisch-organisatorischen Maßnahmen.
Nach Art. 32 Abs. 1 DS-GVO sind insbesondere geeignete technische und organisatorische Maßnahmen zu treffen, um Folgendes sicherzustellen:

Maßnahmenbereiche nach Art. 32 Abs. 1 DS-GVO:

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

Begriffsbestimmungen:

- Maßnahmen zur Pseudonymisierung personenbezogener Daten
  Hierzu zählen u.a.:
  - Trennung von Kundenstammdaten und Kundenumsatzdaten
  - Trennung von Patienten-Kontaktdaten und Behandlungsdaten/Befunden etc.
  - Verwendung von Personal-, Kunden-, Patienten-Kennziffern statt Namen

- Maßnahmen zur Verschlüsselung personenbezogener Daten
  (z. B. in stationären und mobilen Speicher-/Verarbeitungsmedien, beim elektronischen Transport).
  Hierzu zählen:
  - symmetrische Verschlüsselung
  - asymmetrische Verschlüsselung

- Maßnahmen zur Gewährleistung der Vertraulichkeit der Systeme und Dienste,
  die einen unautorisierten Zugang oder Zugriff auf personenbezogene Daten verhindern sollen, beim Verantwortlichen selbst oder auf dem Transportweg zu Auftragsverarbeitern oder Dritten.
  Hierzu zählen u.a.:
  - Zutrittskontrolle
  - Zugangskontrolle
  - Zugriffskontrolle
  - Weitergabekontrolle
  - Trennungskontrolle

- Maßnahmen zur Gewährleistung der Integrität der Systeme und Dienste,
  die gewährleisten, dass personenbezogene Daten nicht (unbemerkt) geändert werden können.
  Hierzu zählen u.a.:
  - Eingabekontrolle
  - sowie insbes. organisatorische und technische Absicherung von Berechtigungen, Protokollierungsmaßnahmen, Protokoll-Auswertungen/Revision etc.

- Maßnahmen zur Gewährleistung der Verfügbarkeit der Systeme u. Dienste,
  die sicherstellen, dass personenbezogene Daten dauernd und uneingeschränkt verfügbar und insbesondere vorhanden sind, wenn sie gebraucht werden.
  Hierzu zählen u.a.:
  - Verfügbarkeitskontrolle
  - Auftragskontrolle

- Maßnahmen zur Gewährleistung der Belastbarkeit der Systeme u. Dienste,
  die sicherstellen, dass die Systeme und Dienste so ausgelegt sind, dass auch punktuell hohe Belastungen oder hohe Dauerbelastungen von Verarbeitungen leistbar bleiben.
  - bezieht sich insbes. auf Speicher-, Zugriffs- und Leitungskapazitäten

- Maßnahmen, um nach einem physischen oder technischen Zwischenfall die Verfügbarkeit personenbezogenen Daten und den Zugang zu ihnen rasch wiederherzustellen.
  Hierzu zählen u.a.:
  - Backup-Konzept
  - Redundante Datenspeicherung
  - Cloud-Services
  - Doppelte IT-Infrastruktur
  - Schatten-Rechenzentrum

- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen.
  Hierzu zählen u.a.:
  - Entwicklung eines Sicherheitskonzepts
  - Prüfungen des DSB, der IT-Revision
  - Externe Prüfungen, Audits, Zertifizierungen

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

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.

Namen und Kontaktdaten – Art. 30 Abs. 2 lit. a

Namen und Kontaktdaten

- des Auftragsverarbeiters, ggf. mehrerer i.S.v. Art. 4 Nr. 8 DS-GVO
- ggf. Namen und Kontaktdaten eines Vertreters des Auftragsverarbeiters i.S.v. 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 DS-GVO i.V.m. Art. 27 DS-GVO
- eines etwaigen Datenschutzbeauftragten

Beschreibung der Verarbeitungen – Art. 30 Abs. 2 lit. b

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
- eMail-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

Übermittlungen in Drittländer – Art. 30 Abs. 2 lit. 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 Abs. 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien.

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

Technisch-organisatorische Maßnahmen – Art. 30 Abs. 2 lit. d

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

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

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
EG	Erwägungsgrund (Erläuterungen für die Auslegung der DS-GVO)
WP	Working Paper (Arbeitsunterlagen, Leitlinien zur Klarstellung der einschlägigen Bestimmungen der DS-GVO sowie Orientierungs-hilfe 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

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5
30159 Hannover
Telefon 0511 120-4500
Fax 0511 120-4599
Ihre Ansprechpartner:
E-Mail an poststelle@lfd.niedersachsen.de schreiben

Stand : 30. Juni 2017