Ausfüllhinweise zum Verzeichnis von Verarbeitungstätigkeiten für Verantwortliche gem. Artikel 30 Abs. 1 DSGVO

(Dieser Text basiert auf einem Dokument der Datenschutzkonferenz der Aufsichtsbehörden.)
Für eine Verarbeitung Verantwortliche und Auftragsverarbeiter haben ein Verzeichnis aller Verarbeitungstätigkeiten mit personenbezogenen Daten zu erstellen. Dieses ersetzt die bisher als Verfahrensverzeichnis, Verfahrensbeschreibung oder Dateibeschreibung bekannten Dokumentationspflichten (§ 4g Abs. 2 Satz 1 Bundesdatenschutzgesetz (BDSG) bzw. § 8 DSG NRW).

Zweck des Verzeichnisses

Der Verantwortliche und der Auftragsverarbeiter sollen zum Nachweis der Datenschutzverpflichtungen ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen. Das entspricht auch der sogenannten Rechenschaftspflicht (Artikel 5 Abs. 2 DS-GVO). Es ist also das Ziel zu dokumentieren, dass man sich um Datenschutzfragen gekümmert hat. Die Übersicht ist der Aufsichtsbehörde bei Kontrollen vorzulegen.[1]

Auch Unternehmen oder Organisationen, die mit der Verarbeitung personenbezogenen Daten arbeiten, müssen in Zukunft ein vergleichbares Verzeichnis führen.

- 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 (Art. 12 Abs. 1 DS-GVO)
- zur Schaffung und als Nachweis geeigneter technisch-organisatorischer Maßnahmen (Art. 24 Abs. 1 und Art. 32 DS-GVO)
- zur Prüfung, ob eine Datenschutzfolgenabschätzung erfolgen muss (nach Art. 35 DS-GVO)
- als Basis für die Aufgabenerfüllung des Datenschutzbeauftragten nach Art. 39 DS-GVO

Hierfür können auch über den rechtlich verpflichtenden Rahmen hinaus Daten sinnvollerweise dokumentiert werden.

Verantwortlicher & Datenschutzbeauftragter (Art. 30 Abs. 1 Satz 2, lit. a) DSGVO)

Das Verzeichnis muss die Namen und Kontaktdaten gem. Art. 30 Abs. 1 Satz 2 lit. a) DS-GVO enthalten. Anzugeben sind die postalische, elektronische und telefonische Erreichbarkeit, um zu gewährleisten, dass die Aufsichtsbehörde den Verantwortlichen auf einfachem Wege (und im Eilfall auch über verschiedene Kanäle) erreichen kann. Im Falle einer Änderung muss nicht das komplette Verzeichnis aktualisiert werden; es genügt ein Vermerk oder Austauschblatt.

Name und Kontaktdaten des Verantwortlichen
Hier ist der genaue Name und die Anschrift des Verantwortlichen (Art. 4 Nr. 7 DS-GVO) nötig. (Bsp. Stadt/Gemeinde XX, Landkreis XX, Zweckverband XX, Landesamt für XX).

Name und Kontaktdaten eines oder mehrerer gemeinsam Verantwortlicher
Wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen, so sind sie gemeinsam Verantwortliche (Art. 26 DS-GVO). Diese gemeinsam Verantwortlichen sind anzugeben (postalische, elektronische und telefonische Erreichbarkeit. Eine Auflistung dieser Daten in einer Anlage ist möglich.

Name und Kontaktdaten des Datenschutzbeauftragten (und seiner Stellvertreter)
In diesem Bereich sind die Kontaktdaten des behördlichen Datenschutzbeauftragten (Art. 37 DS-GVO) und seines Stellvertreters anzugeben. Bei Auftragsdatenverarbeitung: Name und Kontaktdaten des Auftragsverarbeiters. Hier sind der Name und die Anschrift des Auftragsverarbeiters (Art. 28 DS-GVO) aufzuführen.

[1] Der Zweck des Verzeichnisses ergibt sich aus dem Erwägungsgrund (EG) 82 zu Art. 30 DS-GVO

GATACA GmbH
Am Riettor 4 | 78048 Villingen-Schwenningen
Tel.: +49 7721 887979-0 | info@gataca.de | www.gataca.de

Zwecke und Grundlagen der Verarbeitung (Art. 30 Abs. 1 Satz 2, lit. b und lit. f DSGVO)

Bezeichnung des Verfahrens und Kurzbezeichnung
Hier ist eine allgemein verständliche Bezeichnung des Verfahrens (z.B. Wohngeldbewilligung, Automatisiertes Liegenschaftskataster, Personalinformationssystem, Schießleistungsnachweis) anzugeben. Der datenschutzrechtliche Verfahrensbegriff ist an logischen Kriterien, wie Funktionalität, Zweckbindung, Verarbeitungslogik, Wirkung von Verknüpfungs- und Zugriffsregeln, orientiert. Die bloße Dokumentation der physischen Datenorganisation (z. B. Datenbankstruktur oder Dateibeschreibung) leistet für das Herbeiführen datenschutzrechtlicher Transparenz keinen geeigneten Beitrag. Die Kurzbezeichnung von max. 8 Stellen soll als Ordnungsmerkmal innerhalb des Verzeichnisses dienen. Die Bezeichnungssystematik wird vom Verantwortlichen nach den jeweiligen Erfordernissen, insbesondere unter Berücksichtigung der Anzahl von Verarbeitungstätigkeiten, selbst festgelegt.

Zwecke, zu deren Erfüllung die Daten verarbeitet werden
Die Zwecke der Verarbeitung für jedes Verfahren sind – aufgegliedert nach Einzelverzeichnissen – zu benennen, z. B.

- Personalaktenführung
- Lohn-, Gehalts- und Bezügeabrechnung
- Arbeitszeiterfassung
- Urlaubsdatei
- Nutzungsprotokollierungen IT / Internet / E-Mail
- Bewerbungsverfahren
- Telefondatenerfassung
- Antragsbearbeitung (Bauanträge, Wohngeldanträge, etc.)
- Rats- und Bürgerinformationssysteme
- Meldewesen (Melderegister)
- Fahrerlaubnisregister und Fahrzeugregister
- Wahlen (Wählerverzeichnis)
- amtsärztliche Untersuchungen
- Erfassung und Überwachung der nichtakademischen Heilberufe
- Projektabrechnung
- Videoüberwachung an Arbeitsplätzen, in Schulen etc.
- Studierendenverwaltung
- Lehrplanung
- Zeugniserstellung
- Finanzbuchhaltung
- Wahlen (Wählerverzeichnis)
- Forschung zum Thema „Forschungsthema“
- Organisation des Praktikums „Praktikum“

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. Werden die Daten für verschiedene Verarbeitungszwecke verwendet, sind diese einzeln aufzuführen. Nicht ausreichend transparent sind Sammelbegriffe wie Personalmanagement, Gemeindeverwaltung, Integrationsverfahren, Vorgangsverwaltung, Recherchesystem oder Controlling.

Angaben zur Verarbeitung

Kategorien betroffener Personen und personenbezogene Daten
Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten. Aufgegliedert z.B. in der Darstellung der betroffenen Kategorie „Beschäftigte“ in die Datenkategorien:

- 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

Bezeichnung der Kategorie von Empfängern (Art. 30 Abs. 1 Satz 2 lit. d DSGVO)

Empfänger im Anwendungsbereich der DSGVO
Zu unterscheiden ist zwischen internen Empfängern, Empfängern außerhalb des Verantwortlichen und Empfängern in Drittländern. Zu erfassen sind hier auch Auftragsverarbeiter. Es empfiehlt sich eine Angabe der Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, einschließlich der Empfänger in Drittländern. Eine Aufgliederung der Empfänger, z. B. für die Lohn- und Gehaltsabrechnung empfiehlt sich wie folgt:

- Banken
- Sozialversicherungsträger
- Finanzämter
- Andere behördeninterne Empfänger (z. B. Personalrat, Fachvorgesetzte)
- ggf. Auftragsverarbeiter

Empfänger innerhalb des Verantwortlichen
Empfänger können auch Teile einer Behörde sein. Dies ist der Fall, sofern ein Zugriff auf die Daten möglich ist (z.B. bei der abgebenden und aufnehmenden Schule desselben Schulträgers). Der Begriff „Empfänger“ umfasst auch „Zugriffsberechtigte“. Die Zugriffsberechtigten sollten, wie bisher ohne namentliche Angabe angegeben werden. Sie müssen aber z.B. über eine Rollen- oder Funktionsbezeichnung eindeutig bestimmbar sein.

Empfänger außerhalb des Verantwortlichen
Hier sind die Datenempfänger außerhalb des Bereichs des Verantwortlichen (sog. Dritte, z.B. andere öffentliche Stellen) anzugeben.

Besondere Daten
Als besondere oder auch sensible Daten sind rechtlich Datenarten eingestuft aus denen sich folgende Informationen hervorgehen:

- rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- genetische und biometrische Daten (zur eindeutigen Identifizierung einer natürlichen Person)
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung

Speicherdauer / Löschfrist

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

- die geltenden handels- und steuerrechtlichen Aufbewahrungspflichten für Finanzdaten (10 Jahre nach Ablauf des Buchungsjahres
- geltende Aufbewahrungs- und Löschfristen für Prüfungsdokumentationen (z.B. Ergebnisse 10 Jahre)
- gesetzlich vorgesehene Löschungsfristen (z.B. LBG)
- vom Verantwortlichen festgelegte Überprüfungs-/Löschungsfristen (Aufbewahrungsrichtlinie)

Ein allgemeiner Verweis auf Aufbewahrungspflichten genügt nicht, vielmehr sind Angaben der sich daraus ableitenden konkreten Fristen erforderlich.

Übermittlungen in Drittländer

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 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.

Technische und organisatorische Maßnahmen

Die allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO erfolgt in einem zentralen Informationssicherheitskonzept. Das ist hier nicht allgemein anzugeben. Konkrete Verweise auf besondere Regelungen in dem Informationssicherheitskonzept können sinnvoll sein. Je nach Schutzbedarf, sollen hier besondere Maßnahmen, die über das übliche Maß hinausgehen dokumentiert werden. Die in Art. 32 Abs. 1 DS-GVO unter anderem genannten Maßnahmenbereiche entsprechen im Wesentlichen dem bisherigen Katalog der technisch-organisatorischen Maßnahmen (TOMs) nach § 9 BDSG und der Anlage hierzu.

Inhalte sind:

- Maßnahmen zur Pseudonymisierung personenbezogener Daten

Hierzu zählen u.a.:

- Trennung von Teilnehmerkontaktdaten und Befragungsdaten
- Verwendung von Feedbackdaten von anderen Daten zu LehrveranstaltungsteilnehmerInnen
- Maßnahmen zur Verschlüsselung personenbezogener Daten (z. B. in stationären und mobilen Speicher- / Verarbeitungsmedien, beim elektronischen Transport).

Hierzu zählen:

- symmetrische Verschlüsselung
- asymmetrische Verschlüsselung mit RSA
- 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

- Maßnahmen zur Gewährleistung der Integrität der Systeme und Dienste, die gewährleisten, dass personenbezogene Daten nicht (unbemerkt) geändert werden können. Hierzu zählen u.a.: Transaktionsbasierte Datenbanken 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.: Backups, Malwareschutz
- 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
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen sollten bereits im allgemeinen Sicherheitskonzept abgedeckt sein.

Datenschutzfolgeabschätzung

Für Verarbeitungen mit hohem Risiko für Betroffene Personen ist eine Datenschutzfolgenabschätzung erforderlich. Hier ist zu dokumentieren, ob eine solche nicht erforderlich ist, oder ob diese stattgefunden hat (mit welchem Ergebnis). Hierzu werden weitere Handlungshinweise erstellt.

Risikoeinschätzung

Die Risikoeinstufung erfolgt nach Schutzklassen, die sich aus
http://www.itsb.ruhr-unibochum. de/intern/klassifikation_von_informationen.pdf ergeben.

Auftragsdatenverarbeitung

In einigen Fällen werden personenbezogene Daten durch beauftragte Partner verarbeitet. Für solche Verarbeitungen ist ein Vertrag zu Datenverarbeitung im Auftrag abzuschließen. Muster dafür können angefragt werden.