Ausfüllhinweise zum Verzeichnis von Verarbeitungstätigkeiten für Verantwortliche Gemäß Artikel 30 DS-GVO

(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.

Neben diesem formalen Zweck ist das Verzeichnis ebenfalls nützlich:

- 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.

[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

Inhalte zur Dokumentation einer einzelnen Verarbeitungstätigkeit

Grundangaben

Es wird ein Kennungsmuster vorgegeben, der eine Verarbeitungstätigkeit eindeutig referenziert. Ein sprechender Kurzname soll als Bezeichnung angegeben werden (1.8.).

Die **Änderungshistorie** ist nachvollziehbar zu dokumentieren, dazu sind Vorversionen aufzubewahren.

Ansprechpartner und die verantwortliche Einrichtung sind in diesem Bereich zu dokumentieren.

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

Beispiele für Zwecke sind:

- Personalaktenführung / Stammdaten (§ 84 LBG NRW)
- Lohn-, Gehalts- und Bezügeabrechnung (§ 84 LBG NRW)
- Projektabrechnung
- Arbeitszeiterfassung
- Bewerbungsverfahren
- Videoüberwachung an Arbeitsplätzen, in Schulen etc.
- Studierendenverwaltung
- Lehrplanung
- Zeugniserstellung
- Finanzbuchhaltung
- Antragsbearbeitung „Prüfungsfreistellungen“
- Wahlen (Wählerverzeichnis)
- Forschung zum Thema „Forschungsthema“
- Organisation des Praktikums „Praktikum“

Für jede Verarbeitung sind vorher die Zwecke festzulegen, um den Grundsatz der Zweckbindung prüfen zu können. Die Angabe einer Rechtsgrundlage, die die Verarbeitung erlaubt sollte dabei angegeben werden.

Angaben zur Verarbeitung

Kategorien betroffener Personen u. personenbez. 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

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

Aufgegliedert z. B. in der Darstellung der betroffenen Kategorie „Beschäftigte“ in die Datenkategorien:

- Adressdaten für das Anschreiben zur Forschungsteilnahme
- Fragebogendaten
- Soziodemografische Angaben
- Einstellungen zum Thema …
- Testdaten zur Beurteilung der Eignung …

Aufgegliedert z. B. in der Darstellung der Kategorie„Studierende“ in die Datenkategorien:

- Kontaktdaten
- Prüfungsdaten (Studiengänge, Anmeldungen, Ergebnis, etc.)

Die Auflistungen sind Beispiele. Gemachte Angaben müssen alle Datenkategorien umfassen, die verarbeitet werden. Verarbeitung umfasst dabei jeglichen Umgang mit personenbezogenen Daten incl. der bloßen Speicherung.

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

Sollten derartige Daten enthalten sein, so ist das in Spalte 2.4. anzugeben.

Kategorien von Empfängern

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:

- Andere Behörden
- Banken
- Sozialversicherungsträger
- unternehmensinterne andere Datenempfänger (z.B. Betriebsrat, Fachvorgesetzte)
- ggf. Gläubiger bei Lohn-/Gehaltspfändungen
- ggf. Auftragsverarbeiter

Empfänger können auch Teile der Hochschule sein. Dies ist der Fall, sofern ein Zugriff auf die Daten möglich ist. Der Begriff „Datenempfänger“ ist daher zu ergänzen durch „Zugriffsberechtigte“. Solche internen Empfänger werden in Spalte 2.5 erfasst. Die Zugriffsberechtigten sollten ohne namentliche Angabe angegeben werden. Sie müssen jedoch z.B. über eine

Rollen- oder Funktionsbeschreibung eindeutig bestimmbar sein.

Zu Übermittlungen in „Drittländer“ sollte in jedem Fall eine Aussage getroffen werden, also auch angegeben werden, wenn eine Übermittlung in Drittländer nicht stattfindet und auch nicht geplant ist. Drittländer sind Länder, die nicht zur EU gehören.

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.

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 bisherige 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 mit VeraCrypt oder ZIP
- 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

Weitere Angaben

Außerbetriebnahme

Bei einigen Verarbeitungstätigkeiten ist der zeitliche Ablauf klar definiert (gefördertes Forschungsprojekt von bis). In solchen Fällen kann hier eine Außerbetriebnahme dokumentiert werden.

Datenschutzfolgenabschätzung

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.

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