Blaupause und Handreichung zur Erstellung fachgesetzlicher datenschutzrechtlicher Rechtsgrundlagen (RGL-Generator)

Ausarbeitung durch das Maßnahmencluster Prozessoptimierung und Kompetenzaufbau im Rahmen des Kompetenzteams Datenschutz im Schwerpunktthema Datennutzung des IT-Planungsrates

Kompetenzteam Datenschutz

Version: Version 1.0

Datum: 06.03.2025

# Inhaltsverzeichnis

[Inhaltsverzeichnis 2](#_Toc191022173)

[Einleitung 3](#_Toc191022174)

[Hinweise und Anleitung zum Dokument 5](#_Toc191022175)

[I. Vorab: Verantwortliche 8](#_Toc191022176)

[1 Abs. 1: Verarbeitung personenbezogener Daten 10](#_Toc191022177)

[1.1 Betroffene der Datenverarbeitung 10](#_Toc191022178)

[1.2 Verarbeitete Datenkategorien 12](#_Toc191022179)

[1.3 Zweck der Datenverarbeitung 13](#_Toc191022180)

[1.4 Art der Datenverarbeitung 14](#_Toc191022181)

[2 Abs. 2: Verarbeitung von Daten nach Art. 9 oder Art. 10 DSGVO 16](#_Toc191022182)

[2.1 Betroffene der Datenverarbeitung besonderer Kategorien von Daten 17](#_Toc191022183)

[2.2 Verarbeitete Datenkategorien nach Art. 9 Abs. 1 bzw. Art. 10 DSGVO 18](#_Toc191022184)

[2.3 Zweck der Datenverarbeitung (Art. 9 Abs. 1 bzw. Art. 10 DSGVO-Daten) 23](#_Toc191022185)

[2.4 Art der Datenverarbeitung 23](#_Toc191022186)

[3 Abs. 3: Verarbeitung von Daten, die bei Dritten erhoben werden 26](#_Toc191022187)

[3.1 Betroffene bei Dritterhebung 27](#_Toc191022188)

[3.2 Dritter, bei dem die Daten erhoben werden 28](#_Toc191022189)

[3.3 Zweck der Datenerhebung 28](#_Toc191022190)

[3.4 Erhobene Datenkategorien 29](#_Toc191022191)

[4 Abs. 4: Datenabrufe 30](#_Toc191022192)

[5 Abs. 5: Löschen und Aufbewahrungsfristen 30](#_Toc191022193)

[6 Abs. 6: Technisch organisatorische Maßnahmen 32](#_Toc191022194)

[II. Text der RGL-Blaupause 32](#_Toc191022195)

[7 Kontaktdaten und Mitwirkende 32](#_Toc191022196)

# Einleitung

Diese Vorlage für die Gestaltung von datenschutzrechtlichen Rechtsgrundlagen (RGL-Blaupause) wendet sich vor allem an Referent:innen in Ministerien des Bundes und der Länder, die fachrechtliche Gesetzesentwürfe entwerfen sowie an die Mitarbeiter:innen von Bundes- und Landtagsfraktionen, die für ihre Fraktion Gesetzentwürfe vorbereiten. Angesprochen sind auch Mitarbeiter:innen in Kommunalverwaltungen, die für die Erstellung kommunaler Satzungen zuständig sind, soweit dies in ihrer Regelungshoheit liegt.

Die RGL-Blaupause soll Legist:innen einen knappen und strukturierten Überblick darüber geben, was bei der Formulierung einer datenschutzrechtlichen Rechtsgrundlage zu beachten ist. Damit kann sie zu einer stärkeren Vereinheitlichung nationaler Ermächtigungsgrundlagen für die Verarbeitung personenbezogener Daten in den unterschiedlichen Fachbereichen beitragen. Ein Austausch mit Datenschutzreferent:innen oder eine Rückfrage an die Datenschutz-Aufsichtsbehörde bei komplexen Fragestellungen ist immer angeraten.

**Wann ist eine datenschutzrechtliche Rechtsgrundlage für ein Fachgesetz erforderlich?**

Nach Art. 8 der EU-Grundrechtecharta hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Auf nationaler Ebene ist das Grundrecht auf Datenschutz bereits seit 1983 mit dem Volkszählungsurteil des Bundesverfassungsgerichts als Grundrecht auf informationelle Selbstbestimmung anerkannt und wird aus Art 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 des Grundgesetzes bzw. aus den entsprechenden Bestimmungen der Landesverfassungen hergeleitet.

Seit 25. Mai 2018 gilt die Datenschutzgrundverordnung (DSGVO) in allen Mitgliedstaaten der EU unmittelbar und regelt die Voraussetzungen und Bedingungen für die Verarbeitung personenbezogener Daten. Die DSGVO wird dabei ergänzt durch Bestimmungen des Bundesdatenschutzgesetzes (BDSG) und der Landesdatenschutzgesetze (LDSG).

Kernaussage der DSGVO sowie des BDSG und des jeweiligen LDSG ist, dass jedwede Verarbeitung von personenbezogenen Daten einer Rechtsgrundlage bedarf, soweit eine Einwilligung des Betroffenen nicht in Betracht kommt, was im Bereich der Erfüllung öffentlicher Aufgaben in der Regel der Fall ist. Für die Verarbeitung personenbezogener Daten durch die öffentliche Verwaltung ist dabei vor allem die Bestimmung des Art. 6 Abs. 1 Buchst. e DSGVO relevant, die die Verarbeitung personenbezogener Daten für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, erlaubt, soweit diese erforderlich ist. Für besondere Kategorien personenbezogener Daten, d.h. sensible Daten wie z.B. Gesundheitsdaten oder Daten, aus denen politische Meinungen oder religiöse Überzeugungen hervorgehen, sieht Art. 9 Abs. 2 DSGVO spezielle Anforderungen für eine ausnahmsweise mögliche Verarbeitung vor, die zusätzlich zu einer Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO vorliegen müssen.

Dabei legitimiert Art. 6 Abs. 1 Buchst. e DSGVO nicht bereits für sich allein die Verarbeitung personenbezogener Daten; die Vorschrift dient vielmehr als eine sog. Scharniernorm mit der Folge, dass der eigentliche Erlaubnistatbestand in einer nationalen Rechtsgrundlage, die die Verarbeitung personenbezogener Daten für die konkreten fachlichen Zwecke regelt, gefunden werden muss.

Dabei können u.U. bereits die datenschutzrechtlichen Generalklauseln (vgl. § 3 BDSG und die gleichlautenden landesrechtlichen Normen wie z.B. § 3 des niedersächsischen oder des rheinland-pfälzischen LDSG) in Verbindung mit Art. 6 Abs. 1 Buchst. e DSGVO einzelne Verarbeitungsprozesse nach Maßgabe der Rechtsprechung des Bundesverwaltungsgerichts (BVerwG), Urteil vom 20.03.2024; AZ 6 C 8.22, legitimieren. Demnach können Datenverarbeitungen mit geringer Eingriffsintensität, die zur Erfüllung von Aufgaben im öffentlichen Interesse erforderlich sind, auf die datenschutz-rechtlichen Generalklauseln (sog. Brückennormen) in Verbindung mit den - nicht spezifisch datenschutzrechtlichen - Regelungen des jeweiligen Fachrechts gestützt werden. In dem seitens des BVerwG entschiedenen Fall betraf dies die Erhebung, Speicherung und Verwendung der Postanschrift der eine Auskunft begehrenden Person durch das Bundesinnenministerium zwecks Beantwortung dieser Auskunft.

Sofern diese geringe Eintrittsintensität überschritten ist, bedarf es allerdings der Schaffung fachspezifischer datenschutzrechtlicher Rechtsgrundlagen. Dies dürfte insbesondere in folgenden Fällen erforderlich sein:

- Verarbeitung von Sozialdaten, Beschäftigtendaten, Finanzdaten, Videoüberwachung;

 - im durch Subordination geprägten staatlichen Kernbereich (z.B. Schule, Hochschule);

- klassische Hoheitsbereiche (z.B. Polizei, Verfassungsschutz);

- Verarbeitung besonders schutzwürdiger Daten nach Art. 9 und 10 DSGVO;

- von der Rechtsprechung anerkannte Bereiche (z.B. Statistik, große Datenmengen);

- Datenübermittlungen an Dritte etc.

- Verarbeitung sonstiger Daten, die über Identifikationsdaten wie Name und Adresse hinaus gehen (lt. Urteil BVerwG, 20.03.2024; AZ 6 C 8.22)

Für die Erarbeitung von fachspezifischen datenschutzrechtlichen Rechtsgrundlagen gelten die nachfolgenden Hinweise und Empfehlungen.

Anzumerken ist, dass die Empfehlungen und Hinweise dieses RGL-Generators lediglich einen **allgemeingültigen Rahmen** geben können, um eine fachspezifische datenschutzrechtliche Rechtsgrundlage zu erarbeiten, die als Legitimation zur Verarbeitung personenbezogener Daten bei der Erfüllung einer bestimmten öffentlichen Aufgabe dienen soll. Der RGL-Generator kann es naturgemäß nicht leisten, Antworten auf einzelne fachliche Fragestellungen zu geben oder Hilfestellung hierzu zu leisten. Solche fachlichen Fragestellungen können sich bei oder im Umfeld der Erarbeitung einer bereichsspezifischen datenschutzrechtlichen Rechtsgrundlage stellen und Auswirkungen auf deren Inhalt haben, so etwa die Bewertung der Reichweite von Berufsgeheimnissen, die Regelung sachlicher Zuständigkeiten oder die Pflicht zur Vorlage bestimmter Nachweise oder Dokumente bei öffentlichen Stellen. Diese Fragen im Umfeld oder als Grundlage einer datenschutzrechtlichen Rechtsgrundlage mit zu lösen, ist originäre Fachaufgabe und bleibt daher von dieser Blaupause unberührt.

Dieses Dokument leitet durch die Fragen, deren Klärung zur Erstellung einer Rechtsgrundlage erforderlich ist. Es erläutert auch weitere Konsequenzen, die für die spätere Anwendung im Verwaltungsvollzug relevant sind (Bespiel: der Gesetzgeber liefert die Rechtsgrundlage für die Datenverarbeitung, in der Regel muss trotzdem eine Vereinbarung nach Art. 26 DSGVO geschlossen werden).

Wenn die am Ende jedes Teilkapitels gestellten Fragen beantwortet werden – sollten sie sich am Ende in den Gesetzestext einfügen. Was nach Prüfung des Gesetzestextes nicht benötigt wird, kann selbstverständlich gelöscht oder verändert werden. Wie anhand der Gliederung erkennbar wird, behandelt dieser Generator die Fragen der Verantwortlichkeit, die Verarbeitung nicht-sensibler Daten, die Verarbeitung sensibler Daten, Datenerhebungen bei Dritten und Datenabrufe, sowie das Aufbewahren und Löschen. Innerhalb dessen werden die Betroffenengruppen, die Datenkategorien, der Zweck der Datenverarbeitung und die Verarbeitungstätigkeit an sich abgefragt.

# Hinweise und Anleitung zum Dokument

**Damit diese Datei überhaupt funktionieren kann, muss sie als „docm“ Datei (mit Makros) geöffnet werden.**

**Die folgenden Schritte sind nur notwendig, wenn Sie diese Datei als .docx-Datei erhalten haben, da z.B. sie keine .docm-Dateien per Mail erhalten können.**

**Schritt 0: Ihnen liegt diese Datei als .docx-Datei vor.**

**Schritt 1: Speichern Sie diese Datei als .docm-Datei (also mit „.docm“ am Ende des Dateinamens) an ihrem gewünschten Speicherort ab. Bei „Speichern unter“ ist der Dateityp .docm auszuwählen.**

**Schritt 2: Aktivieren Sie die Entwicklertools** (Datei > Optionen > Menüband anpassen > Ankreuzen bei „Entwicklertools“)

**Schritt 3: Klicken Sie in der obersten Leiste auf „Entwicklertools“.**

**Schritt 4: Es befindet sich ganz links der Knopf für „Visual Basics“. Öffnen Sie dieses mit der linken Maustaste.**

****

**Schritt 5: Öffnen Sie den Bereich für Code mit einem Doppelklick mit der linken Maustaste auf „ThisDocument“**

 ****

**Schritt 6: Fügen Sie folgenden Code in das geöffnete Fenster ein:**

****

**Erklärung des Codes:**

**Wenn ein Inhaltssteuerelement (z.B. ein Kontrollkästchen) verlassen wird und das Tag des Inhaltssteuerelements nicht leer ist, sucht der Code nach einem Lesezeichen mit dem Namen des Tags. Abhängig davon, ob das Kontrollkästchen aktiviert oder deaktiviert ist, wird der Text des Lesezeichens entweder sichtbar oder unsichtbar gemacht. So kann durch ankreuzen Text angezeigt oder versteckt werden, welcher dann im Rechtstext sichtbar gemacht wird.**

**Schritt 7: Speichern Sie den Code ab.**

****

**Schritt 8: Schließen Sie „Visual Basic“.**

**Schritt 9: Nutzen Sie das docm.-Dokument zur Generierung von Rechtstexten.**

**Achtung: Dieses Dokument ist grundsätzlich im schreibgeschützten Modus zu benutzen. Wenn das Dokument im Bearbeitungsmodus benutzt und bearbeitet wird kann es passieren, dass unbeabsichtigt notwendige Textmarken oder Querverweise gelöscht werden, wodurch das Dokument nicht mehr wie vorgesehen genutzt werden kann!**

**Achtung: Textmarken und Querverweise, durch die die Tabellen funktionieren, werden gelöscht, wenn man diese händisch aus den Platzhaltern löscht. Bei der Bearbeitung der Platzhalter ist daher Vorsicht geboten.**

**Weitere Hinweise:**

**Hinweis A:** Nach dem Kopieren der Rechtsgrundlage ist eine erneute Prüfung der Grammatik und Sprache vor der Verwendung des Textes unablässig. Insbesondere bei einer Vielzahl an ausgewählten Kategorien sind Kommata zu ergänzen.

**Hinweis B:** Im geschützten Modus können Felder nur mit einem „Trick“ aktualisiert werden. Die Aktualisierung ist nötig, um die veränderten Felder auf den neusten Stand zu bringen. Dies ist möglich durch folgende Schritte:

1. Gehen Sie oben links auf "Datei".
2. Dann wählen Sie in der linken Leiste "Optionen" an (ggf. unter "Mehr..."), ein Fenster öffnet sich.
3. Im Fenster klicken Sie links auf "Anzeige". Dann setzen Sie im Abschnitt "Druckoptionen" den Haken bei "Felder vor dem Drucken aktualisieren" und bestätigen mit "OK".
4. Sobald Sie nun den Druckdialog über die Tastenkombination [Strg] + [P] öffnen, werden automatisch alle Felder aktualisiert.

**Hinweis C:** Sollten z.B. Datenkategorien ergänzt werden, muss auch das Word Dokument angepasst werden. Dafür ist der Schutzmodus in „Entwicklertools“ aufzuheben.

Um Ergänzungen durchzuführen sind folgende Schritte zu machen:

1. Word „Entwicklertools aktivieren“ (Datei > Optionen > Menüband anpassen > Ankreuzen bei „Entwicklertools“
2. Strg+\* um verborgenen Text sichtbar zu machen
3. Kategorie in die der Tabelle ergänzen
4. Kategorie in dem vorgesehen Platzhalter ergänzen
5. Kategorie im Platzhalter markieren
6. Reiter „Einfügen“ auf Textmarke
7. Kategorie einen Namen (ohne Leerzeichen) geben z.B. Personendaten
8. In Tabelle vor die Kategorie: Entwicklertools > Kontrollkästchensteuerelement (Symbol: Kasten mit blauem Haken)
9. Kontrollkästchensteuerelement markieren und bei „Entwickertools“ auf Eigenschaften
10. Name der Textmarke bei „Tags“ eintragen
11. Ausprobieren, ob es geklappt hat

# Vorab: Verantwortliche

**Wer ist die zuständige Behörde bzw. der Verantwortliche der Datenverarbeitung?**

„**Verantwortlicher**“ der Datenverarbeitung i.S.v. Art. 4 Nr. 7 DSGVO ist die Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Wer für die Erfüllung der Fachaufgabe **zuständig** ist, ist in der Regel die verantwortliche Stelle für die Datenverarbeitung. Um eine Verarbeitung von Daten vorzunehmen muss der/die Verantwortliche, also die zuständige Behörde, klar definiert werden.

**Hinweis**: Jeder, an einer Datenverarbeitung als Verantwortlicher Beteiligte benötigt eine (eigene) Rechtsgrundlage für die Datenverarbeitung, muss also von der zu gestaltenden Regelung erfasst sein.

**Mehrere Beteiligte**:

Es gibt Konstellationen, in denen **mehrere Behörden zusammenwirken** oder ein IT-Dienstleister beauftragt ist. Zunächst muss daher klar sein, welche Stellen an der Datenverarbeitung beteiligt sind und wer als verantwortliche Stelle über die Datenverarbeitung bestimmt.

Sind mehrere Stellen mit der Datenverarbeitung befasst und/oder gemeinsam zuständig, ist die Art der Zusammenarbeit und deren rechtliche Einordnung zu prüfen, ob dies also eine **gemeinsame Verantwortlichkeit** oder eine **Auftragsverarbeitung** darstellt, ggf. eine **Beleihung** vorgenommen/berücksichtigt werden muss oder ob die **Bestimmung einer (ausschließlichen) Verantwortlichkeit** durch Gesetz sinnvoll ist:

* Eine **gemeinsame Verantwortlichkeit** i. S. d. Art. 26 DSGVO liegt vor, wenn mehrere Verantwortliche **gemeinsam** über Zwecke und Mittel der Datenverarbeitung entscheiden (was weit auszulegen ist!), eine Vereinbarung nach Art. 26 DSGVO wird erforderlich.

**Hinweis**: Wenn die Verarbeitung durch mehrere Verantwortliche durchgeführt werden soll, ist es wichtig, dass die zu formulierende Norm für **beide Verantwortliche eine eigene Rechtsgrundlage** enthält und dass die gemeinsame Verantwortlichkeit in der Norm als solche **bezeichnet** wird. Die Rechtsgrundlage regelt das **OB**. Eine solche gemeinsame Verantwortlichkeit hat zur Folge, dass später die verantwortlichen verarbeitenden Behörden eine Vereinbarung nach Art. 26 DSGVO schließen müssen. Die Art.26-Vereinbarung regelt dann das **WIE** der gemeinsamen Verarbeitung.

* Eine **Auftragsverarbeitung** i.S. von Art. 28 DSGVO liegt vor, wenn ein Beteiligter (Auftragnehmer der Auftragsverarbeitung) die personenbezogenen Daten im Auftrag des Verantwortlichen (Auftraggeber der Auftragsverarbeitung) verarbeitet. Es ist für die konkrete Verarbeitung ein Auftragsverarbeitungsvertrag i.S.v. Art. 28 DSGVO abzuschließen, der die Rechte und Pflichten der Beteiligten schriftlich regelt. Die Rechtsgrundlage bezieht sich „nur“ auf den Verantwortlichen (also den Auftraggeber).
* Üben Private hoheitliche Gewalt aus, die ihnen als **Beliehene** übertragen worden ist, gelten auch sie als Behörden und als öffentliche Stellen iSd § 2 BDSG. (Für die Beleihung ist ein förmlicher Rechtsakt notwendig, der auf einer gesetzlichen Grundlage beruht.)
* Es gibt nach Art. 4 Nr. 7 2. HS DSGVO die Möglichkeit, einen Verantwortlichen **gesetzlich zu bestimmen**. Dies ist geeignet für Konstellationen, in denen mehrere Behörden zusammenarbeiten. Hier ist zu beachten, dass der durch die Rechtsgrundlage bestimmte Verantwortliche alle Pflichten aus der DSGVO wahrzunehmen hat. (Angewendet wurde diese Möglichkeit beispielsweise in § 8a Abs. 4 S. 1 OZG.)

**Hinweis:** Bevor Feld des Platzhalters ausgefüllt wird, muss entschieden sein, welche Behörde(n) für die Datenverarbeitung verantwortlich ist/sind. Unter „Zuständige Behörde(n)“ sind **alle Verantwortlichen** anzugeben.

Verortung in der Textvorlage:

**Wer ist als zuständige Behörde Verantwortlicher der Datenverarbeitung?**

Bei gemeinsamer Verantwortung bitte formulieren und einfügen „Behörde A **in gemeinsamer Verantwortung** mit Behörde B“:

**Bitte einfügen: [**Platzhalter (alle) zuständige/n Behörde/n**]**

Verortung in der Textvorlage:

(1) Verarbeitung personenbezogener Daten

Das [*Verarbeiten*] und Anonymisieren von [*Datenkategorien*] der [*Betroffenen*] durch die [Platzhalter (alle) zuständige/n Behörde/n] ist zulässig, soweit dies zur Wahrnehmung der Aufgaben nach [*Zweckbestimmung*] erforderlich ist.

(2) Verarbeitung besonderer Kategorien personenbezogener Daten

Das [*Verarbeiten von Art. 9/Art. 10-Daten*] und Anonymisieren von personenbezogenen Daten nach Artikel 9 Absatz 1 oder Art. 10 der Verordnung (EU) 2016/679, nämlich [*Datenkategorien Art. 9/Art. 10*] der [*Betroffenen Art. 9/Art.10-Daten*] durch die [Platzhalter (alle) zuständige/n Behörde/n] ist zulässig, soweit dies zur Wahrnehmung der Aufgaben [*Zweckbestimmung Art. 9/Art. 10-Daten*] erforderlich ist.

(3) Datenerhebung bei Dritten

[Platzhalter (alle) zuständige/n Behörde/n] erhebt, um [*Zweck Drittdaten*] von [*Betroffenen Drittdaten*], [*Datenkategorie Drittdaten*], bei [*Drittem/n*].

(4) Datenabrufe

Im Geltungsbereich des § 1 EGovG (bzw. des jeweiligen EGovG Land) darf die [Platzhalter (alle) zuständige/n Behörde/n] die erforderlichen Nachweise bei dem zuständigen Register abrufen. § 5 und 5a EGovGE (bzw. EGovG Land) finden Anwendung.

# Abs. 1: Verarbeitung personenbezogener Daten

In jedem Verfahren der Leistungs- oder Eingriffsverwaltung werden personenbezogenen Daten im Sinne von Art. 4 Nr. 1 DSGVO verarbeitet. Die Frage der zuständigen Behörde und damit des datenschutzrechtlichen Verantwortlichen wurde vorab geklärt. In diesem Gliederungspunkt werden die Informationen zu weiteren Parametern abgefragt, die für die Schaffung einer Rechtsgrundlage zur Datenverarbeitung erforderlich sind.

## Betroffene der Datenverarbeitung

Betroffene der Datenverarbeitung sind diejenigen Personen, deren Grundrecht auf informationelle Selbstbestimmung durch die Datenverarbeitung eingeschränkt wird. Sie sind daher zu benennen, um eine (hinreichend) bestimmte Rechtsgrundlage für die Datenverarbeitung zu erhalten.

Betroffen sind diejenigen natürliche Personen, deren personenbezogene Daten verarbeitet werden (Art. 4 Nr. 1 DSGVO). Hier sind alle Betroffenen der Verarbeitungstätigkeiten in möglichst generischer Bezeichnung in Kategorien anzugeben.

Beispielsweise:

* Bürger:innen
* Nutzende
* Administrierende
* Beamt:innen und Tarifbeschäftigte der Verwaltung
* Beschäftigte in Unternehmen
* Leistungsempfänger
* Patienten
* Kinder
* …

**Wer sind die Betroffenen der Datenverarbeitung?**

**Bitte alle Betroffenen einfügen:** [Platzhalter Betroffene]

**Verortung in der Textvorlage:**

(1) Verarbeitung personenbezogener Daten

Das [*Verarbeiten*] und Anonymisieren von [*Datenkategorien*] der [Platzhalter Betroffene] durch die *[(alle) zuständige/n Behörde/n*] ist zulässig, soweit dies zur Wahrnehmung der Aufgaben nach [*Zweckbestimmung*] erforderlich ist.

## Verarbeitete Datenkategorien

Die Rechtsgrundlage muss diejenigen Kategorien von Daten aufführen, die zur Erfüllung der Aufgabe verarbeitet werden müssen, um hinreichend bestimmt zu sein[[1]](#footnote-2). Eine Datenkategorie ist der Oberbegriff, unter den sich verschiedene Daten inhaltlich subsumieren lassen.

Die folgende Tabelle ist nicht abschließend und sollte bei Bedarf ergänzt werden.

|  |  |
| --- | --- |
| Datenkategorie | Beispiel |
| [x]  Identifikationsdaten | Name, Vorname, Geburtsdatum, Geburtsort |
| [x]  Adressdaten | Straße und Hausnummer, Ort |
| [x]  Vertragsstammdaten  | Vertragsbezogene Daten |
| [x]  Daten zu Bank- oder Kreditkartenkonten | Kontonummer, IBAN, BLZ, Kreditkartennummer, Kreditkarteninstitut, Gültigkeitsdauer, Prüfnummer |
| [x]  IT-Nutzungsdaten | IP-Adresse, Loggingdaten, Transaktionsdaten… |
| [x]  Verbindungsdaten | Unterfall der IT-Nutzungsdaten: IP-Adresse, MAC-Adresse ... |
| [x]  Kommunikationsdaten | Telefonnummer, Handynummer, E-Mail-Adresse, … |
| [x]  Patientendaten | Krankenkassen, Versicherungsnummer, Aufnahmedaten, … |
| [x]  Daten über berufliche Qualifikationen | Zeugnisse, dienstliche Beurteilungen, … |
| … | … |

**Welche Datenkategorien müssen verarbeitet werden?**

**Bitte alle einschlägigen Datenkategorien in die Tabelle aufnehmen und ankreuzen:** [Identifikationsdaten, Adressdaten, Vertragsstammdaten, Daten zu Bank- oder Kreditkartenkonten, IT-Nutzungsdaten, Verbindungsdaten, Kommunikationsdaten, Patientendaten, Daten über berufliche Qualifikation, ]

Verortung in der Textvorlage:

(1) Verarbeitung personenbezogener Daten

Das [*Verarbeiten*] und Anonymisieren von [Identifikationsdaten, Adressdaten, Vertragsstammdaten, Daten zu Bank- oder Kreditkartenkonten, IT-Nutzungsdaten, Verbindungsdaten, Kommunikationsdaten, Patientendaten, Daten über berufliche Qualifikation, ] der [*Betroffenen*] durch die *[(alle) zuständige/n Behörde/n*] ist zulässig, soweit dies zur Wahrnehmung der Aufgaben nach [*Zweckbestimmung*] erforderlich ist.

## Zweck der Datenverarbeitung

Eine Datenverarbeitung ist nur rechtmäßig, wenn sie dem festgelegten Zweck entspricht Art. 6 DSGVO. Für den Anwendungsbereich des Art. 6 Abs. 1 Buchst. e DSGVO bedeutet das, dass die Datenverarbeitung für die Erfüllung eines Zwecks erforderlich sein muss, der in der Wahrnehmung der Aufgabe besteht, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

Personenbezogene Daten dürfen nur „für festgelegte, eindeutige und legitime Zwecke erhoben“ werden. Der Zweck der Datenverarbeitung ist die Beschreibung des Zustands, der durch das Mittel der Datenverarbeitung erreicht werden soll. Er ist ein Sollwert, der final und teleologisch das Ziel und den Grund benennt, zu dem der Verantwortliche die Datenverarbeitung durchführt. Der Zweck beantwortet die Frage des „**Wozu**“.

Für die Rechtsgrundlage wird also die möglichst konkrete Beschreibung des Zustands, der erreicht werden soll, benötigt. Beispielsweise: „zur Erfüllung der melderechtlichen Vorgänge“, „zur Prüfung und Bescheidung des Antrags auf …“

* Personalaktenführung
* Stammdatenpflege
* Lohn-/Gehalts- und Bezügeabrechnung
* Arbeitszeiterfassung
* Nutzungsprotokollierung IT / Internet / E-Mail
* Bewerbungsverfahren
* Schülerverwaltung, Unterrichtsplanung, Zeugniserstellung
* Beschaffung / Einkauf sowie Finanzbuchhaltung
* Antragsbearbeitung (Leistungsverwaltung)
* Information der Öffentlichkeit durch Rats- und Bürgerinformationssysteme
* Meldewesen
* Führung eines Fahrerlaubnisregisters und Fahrzeugregisters
* Wahlen (Wählerverzeichnis)
* Amtsärztliche Untersuchungen
* Schwangeren- und Mütterberatung
* Erfassung und Überwachung der nichtakademischen Heilberufe
* **…**

**Zu welchem Zweck werden die personenbezogenen Daten verarbeitet?**

**Bitte hier den Zweck der Datenverarbeitung einfügen:** [Platzhalter Zweckbestimmung]

**Verortung in der Textvorlage:**

(1) Verarbeitung personenbezogener Daten

Das [*Verarbeiten*] und Anonymisieren von [*Datenkategorien*] der [*Betroffenen*] durch die *[(alle) zuständige/n Behörde/n*] ist zulässig, soweit dies zur Wahrnehmung der Aufgaben nach [Platzhalter Zweckbestimmung] erforderlich ist.

## Art der Datenverarbeitung

Die „Verarbeitung“ ist der Oberbegriff nach Art. 4 Nr. 2 DSGVO für jegliche Art der Nutzung von Daten. In einer fachgesetzlichen Rechtsgrundlage ist zu differenzieren, welche Verarbeitungstätigkeit genau vorgenommen werden soll/darf.

|  |  |
| --- | --- |
| Art der Verarbeitung | Definition |
| [x]  erheben | Beschaffen von Daten über eine betroffene Person. Gezielte Verwandlung eines unbekannten Datums in ein Bekanntes. Setzt aktives Handeln des Verantwortlichen voraus. Gilt nicht, wenn der/dem Verantwortlichen eine Information aufgezwungen wird. |
| [x]  erfassen | Technische Formgebung erhobener Daten. Arbeitsvorgang mit dem eine erstmalige Speicherung des bekannten Datums auf einem Datenträger erfolgt. Ermöglicht die weitere technische Verarbeitung. Gilt auch, wenn Datum aufgezwungen wurde. |
| [x]  organisieren | Strukturelle Neuanordnung/systematische Strukturierung der gespeicherten personenbezogenen Daten auf dem Datenträger. Organisation personenbezogener Daten bezeichnet das Ergebnis des Sammelns und Ordnen von Daten. Vereinfacht das Auffinden und Auswerten. |
| [x]  ordnen | Sinnvoll strukturierte Ablage der gespeicherten personenbezogenen Daten auf dem Datenträger, z.B. nach Alphabet. |
| [x]  speichern | Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung. Umfasst nicht nur die erstmalige Speicherung, sondern auch Zwischenspeicherungen auf Datenträger oder das Umspeichern von personenbezogenen Informationen, um diese für eine weitere Verwendung aufzubewahren. Die Aufbewahrung des Speichermediums zählt ebenfalls dazu. Gegenteil von Löschen und Vernichten. |
| [x]  anpassen  | Beispiel für Veränderung. Aktualisierung/Angleichung der personenbezogenen Daten an die reellen Lebensumstände, z.B. Änderung der Wohnanschrift. |
| [x]  verändern | Bearbeitung bzw. inhaltliche Umgestaltung gespeicherter personenbezogener Daten oder ihrer Zuordnung. Es kommt zu einer Änderung des Informationsgehalts. Die Daten können jedoch auch verändert werden, indem sie ergänzt, in einen neuen Zusammenhang gestellt oder für einen anderen Zweck verwendet werden. |
| [x]  auslesen | Bewusste Kenntnisnahme über die auf einem Datenträger befindlichen personenbezogenen Daten/Abrufen von Informationen. Daten werden aus einem Datenträger ausgelesen, um sie einer weiteren Bearbeitung zugänglich zu machen. |
| [x]  abfragen | Gezielte Informationssuche auf einem Datenträger und Kenntnisnahme dieser/Gewinnung von Daten. Zum Beispiel mithilfe der Eingabe eines Suchbegriffs. |
| [x]  abrufen |  |
| [x]  verwenden | Alle Beispiele außer Erheben und Erfassen sind Unterbeispiele von Verwenden. Jeder gezielte Umgang mit personenbezogenen Daten kann als Verwendung der Daten gelten. Sinngemäße Nutzung einer bereits bekannten Information. |
| [x]  offenlegen | Vorgang, der dazu führt, dass Daten für andere zugänglich gemacht werden und sie diese auslesen oder abfragen können. Bekanntgabe gespeicherter Daten an Dritte. |
| [x]  übermitteln,  | Gezielte Weitergabe von Daten an einen oder mehrere Empfänger. |
| [x]  verbreiten  | Ungezielte Weitergabe an unbestimmte Adressaten z.B. Öffentlichkeit. |
| [x]  Bereitstellen durch andere Form | Passive Form der Offenlegung. Bereithaltung der Daten zum potenziellen Gebrauch, z.B. für eine Einsicht. |
| [x]  abgleichen  | Vergleich mehrerer zusammengehöriger bekannter, nicht am selben Ort gespeicherter Daten. Abweichungen oder Übereinstimmungen können festgestellt werden. |
| [x]  verknüpfen | Zuordnung mehrerer zusammengehöriger bekannter, nicht am gleichen Ort gespeicherter Daten. Ziel ist die Entstehung einer neuen Datenstruktur durch Zusammenführung der Daten. (Dient z.B. der Erleichterung der Durchführung von Abfragen.). |
| [x]  einschränken  | Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken (Art. 4 Nr. 3). Entspricht der Sperrung von Daten. |
| [x]  vernichten | Physische Beseitigung der Daten. Vollständige Zerstörung des Datenträgers, sodass keinerlei Information mehr auslesbar ist. |
| [x]  anonymisieren | Die Verarbeitung von Daten in einer Weise, dass die Daten nicht einer bestimmten betroffenen Person zugeordnet werden können. |
| [x]  pseudonymisieren | Die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. |
| [x]  löschen | Entfernung/Unkenntlichmachung einer gespeicherten Information von jedem Datenträger, sodass die Daten keinesfalls mehr ausgelesen bzw. wiederhergestellt werden können. Der Datenträger kann physisch erhalten bleiben. Es erfolgt kein Löschen durch Verschlüsselung oder Anonymisierung der Daten. |
| [ ]  … |  |
|  |  |

**Hinweis**: Die Tabelle sieht vor, dass das Anonymisieren als Verarbeitungstätigkeit enthalten ist. Nach herrschender Meinung der DSK ist das Anonymisieren **kein** Unterfall des Löschens und bedarf einer eigenen Rechtsgrundlage. Damit die Möglichkeit besteht, auf anonymisierte Daten zuzugreifen, sollte daher die Anonymisierung nicht vergessen werden. Natürlich kann der Begriff aus der Textvorlage händisch gelöscht werden.

**Wie werden die erhobenen Daten verarbeitet?**

**Alle Arten der oben bestätigten Verarbeitung in die Tabelle aufnehmen und ankreuzen:** [Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Abrufen, Verwenden, Offenlegen, Übermitteln, Verbreiten, Bereitstellen durch andere Form, Abgleichen, Verknüpfen, Einschränken, Vernichten, Anonymisieren, Pseudonymisieren, Löschen]

**Verortung in der Textvorlage:**

(1) Verarbeitung personenbezogener Daten

Das [Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Abrufen, Verwenden, Offenlegen, Übermitteln, Verbreiten, Bereitstellen durch andere Form, Abgleichen, Verknüpfen, Einschränken, Vernichten, Anonymisieren, Pseudonymisieren, Löschen] von [*Datenkategorien*] der [*Betroffenen*] durch die *[(alle) zuständige/n Behörde/n*] ist zulässig, soweit dies zur Wahrnehmung der Aufgaben nach [*Zweckbestimmung*] erforderlich ist.

# Abs. 2: Verarbeitung von Daten nach Art. 9 oder Art. 10 DSGVO

Für die Verarbeitung besonderer Kategorien von Daten sehen Art. 9 und Art. 10 DSGVO besondere Anforderungen vor. Wenn hierzu keine explizite Einwilligung eingeholt werden soll, muss die Rechtsgrundlage besondere Anforderungen erfüllen. Daher wird hier zwischen personenbezogenen Daten einerseits und personenbezogenen Daten nach Art. 9 oder Art. 10 DSGVO andererseits unterschieden.

**Müssen Daten nach Art. 9 Abs. 1 oder Art. 10 DSGVO (s. dazu unten 2.2) verarbeitet werden?**

Nein 🡪 wenn keine Daten nach Artikel 9 oder Art. 10 DSGVO verarbeitet werden müssen, kann der Absatz 2 im Textvorschlag gelöscht werden.

Ja 🡪 weiter wie folgt

## Betroffene der Datenverarbeitung besonderer Kategorien von Daten

Betroffen sind diejenigen natürliche Personen, deren personenbezogene Daten verarbeitet werden (Art. 4 Nr. 1 DSGVO). Hier sind alle Betroffenen der Verarbeitungstätigkeiten in möglichst generischer Bezeichnung in Kategorien anzugeben. Die Betroffenheit kann sich dabei bereits aus der Betroffenenkategorie ergeben, muss es aber nicht.

Beispielsweise:

* Bürger:innen
* Nutzende
* Gewerkschaftsangehörige
* Parteimitglieder
* Gläubige
* Schwangere
* (schwerbehinderte) Arbeitnehmer:innen
* Leistungsempfänger:innen
* Patienten:innen
* Strafgefangene
* …

**Wer sind die Betroffenen der Datenverarbeitung besonderer Kategorien von Daten?**

**Bitte einfügen alle einschlägigen Kategorien Betroffener:** [Platzhalter Betroffene Art. 9 oder Art. 10]

**Verortung in der Textvorlage:**

(2) Verarbeitung besonderer Kategorien personenbezogener Daten

Das [*Verarbeiten von Art. 9/Art. 10-Daten*] und Anonymisieren von personenbezogenen Daten nach Artikel 9 Absatz 1 oder Art. 10 der Verordnung (EU) 2016/679, nämlich [*Datenkategorien Art. 9/Art. 10*] der [Platzhalter Betroffene Art. 9 oder Art. 10] durch die [*(alle) zuständige/n Behörde/n*] ist zulässig, soweit dies zur Wahrnehmung der Aufgaben [*Zweckbestimmung Art. 9/Art. 10-Daten*] erforderlich ist.

## Verarbeitete Datenkategorien nach Art. 9 Abs. 1 bzw. Art. 10 DSGVO

Art. 9 und Art. 10 DSGVO untersagen die Verarbeitung der dort aufgelisteten Datenkategorien. Diese unterliegen einem Erlaubnisvorbehalt. Die vorliegende Blaupause referiert auf den Erlaubnisvorbehalt nach Art. 9 Abs. 2 Buchst. b und g DSGVO, indem eine Grundlage im Recht eines Mitgliedsstaates geschaffen wird, die die dort aufgelisteten Anforderungen erreicht.

|  |  |
| --- | --- |
| Art 9 Abs. 1 DSGVO |  |
| [x]  Rassische oder ethnische Herkunft | Damit sind solche Informationen gemeint, die Rückschlüsse auf die Zugehörigkeit zu einer „Rasse“ bzw. einer Ethnie erlauben. Dem Gesetzgeber ist dabei die Problematik des Begriffs der Rasse bewusst. Eine Erläuterung findet sich in [Erwägungsgrund 51](https://dsgvo-gesetz.de/erwaegungsgruende/nr-51/).Hierunter fallen beispielsweise die Hautfarbe oder typische, regional begrenzte Sprachen. Nicht erfasst werden aber die Staatsangehörigkeit, und auch nicht allein der Geburtsort. |
| [x]  Politische Meinungen | Darunter fallen Parteimitgliedschaften oder politische Einstellungen. Nicht aber bereits die bloße Teilnahme an einer politischen Veranstaltung. Die berufliche Tätigkeit für eine politische Partei wird nur dann vom Schutzbereich erfasst, wenn ein politischer Bezug besteht. Nicht erfasst wird also beispielsweise die Tätigkeit in einem Parteibüro, wenn es sich dabei um die Arbeit des IT-Administrators handelt, oder um Tätigkeiten im Sekretariat. |
| [x]  Religiöse oder weltanschauliche Überzeugungen | Damit ist die Konfessionszugehörigkeit oder die Mitgliedschaft in einer Sekte gemeint. Nicht dagegen der bloße Austritt aus der Staatskirche oder das Tragen eines Kleidungsstücks, beispielsweise mit satanistischem Motiv. Bei der Verarbeitung von Daten über das Tragen von Kopftüchern, der Kippa oder eines Rosenkranzes kommt es darauf an, wie diese Daten ausgewertet werden sollen.Weltanschauliche Überzeugungen sind die Gesamtheit der persönlichen Wertungen, Vorstellungen und Sichtweisen. Erfasst sind damit ideologische Gesinnungen oder Mitgliedschaften in bestimmten Bünden, beispielsweise den Freimaurern, nicht aber bloße Einstellungen und Merkmale der individuellen Lebensgestaltung wie „Vegetarier“, oder „Pazifist“. |
| [x]  Gewerkschaftszugehörigkeit | Mitglieder einer Gewerkschaft sollen bei der Ausübung ihrer Tätigkeit frei und ohne Angst agieren können, dabei Diskriminierungen zu erfahren. Deshalb ist die Gewerkschaftszugehörigkeit ein sensibles Datum. Die Tätigkeit für eine gewerkschaftsnahe Stiftung ist nur dann erfasst, wenn ein inhaltlicher Zusammenhang zur Gewerkschaftstätigkeit besteht. |
| [x]  Genetische Daten | Eine Definition des Begriffs „genetische Daten“ findet sich in Art. 4 Nr. 13 DSGVO. Genetische Daten sind demnach personenbezogene Daten „zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden. Demnach fallen beispielsweise DNA-Analysen, RNS-Analysen und ähnliche unter Art. 9 DSGVO. Auch gleichwertige Daten, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern, sind erfasst. |
| [x]  Biometrische Daten zur eindeutigen Identifizierung | Biometrische Daten sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Perseon ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten. Darunter fallen beispielsweise der Fingerabdruck (zur Entsperrung des Smartphones), sowie Stimmen- oder Iriserkennungen. Auch Lichtbilder können unter die biometrischen Daten fallen. In [Erwägungsgrund 51](https://dsgvo-gesetz.de/erwaegungsgruende/nr-51/) zu der Datenschutz-Grundverordnung wird zur Verarbeitung von Lichtbildern jedoch einschränkend Stellung genommen. Dort heißt es, dass die Verarbeitung von Lichtbildern nicht grundsätzlich als Verarbeitung besonderer Kategorien von personenbezogenen Daten angesehen werden sollte, da Lichtbilder nur dann von der Definition des Begriffs „biometrische Daten“ erfasst werden, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen.Demnach stellt der Abgleich eines Fotos mit einer Gesichtserkennungssoftware eine Verarbeitung besonderer Kategorien personenbezogener Daten dar, nicht jedoch die Kontrolle eines mit einem Portrait versehenen Mitarbeiterausweises durch bloße Inaugenscheinnahme.Gemeint sind also nur solche biometrischen Daten, die zur eindeutigen Identifizierung einer natürlichen Person verarbeitet werden. Lichtbilder nur dann, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung einer natürlichen Person ermöglichen und eine Auswertungsabsicht besteht. Also nicht bereits das schlichte Passbild eines Brillenträgers oder die Aufnahme eines Fotos mit einem biometriefähigen Endgerät (z.B. Smartphone). |
| [x]  Gesundheitsdaten | Dabei handelt es sich um personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Bei Gesundheitsdaten handelt es sich um Nummern, Symbole oder Kennzeichen, die eine natürliche Person für gesundheitliche Zwecke eindeutig identifizieren können. Auch Informationen über Behinderungen zählen zu den Gesundheitsdaten.Die Vorschrift dient dem individuellen Schutz von Leben und Gesundheit, sowie dem generellen Gesundheitsschutz.Zur medizinischen informationellen Selbstbestimmung gehört, dass der Betroffene darüber entscheiden kann, ob er sich mit Wissen um seine individuellen gesundheitlichen Besonderheiten belasten möchte, weshalb es auch ein Recht auf Nichtwissen gibt.Der Begriff der Gesundheitsdaten ist weit zu verstehen. Aus dem Gesamtzusammenhang können bereits Arztbesuche Angaben über den Gesundheitszustand des Einzelnen vermitteln. Weitere Beispiele sind Daten aus einer Online-Bestellung von Medikamenten, was aber schon infolge des oft gegebenen Auseinanderfallens von Besteller und Patient fragwürdig ist. Der Impfstatus ist ebenfalls Gesundheitsdatum.Beispiele sind weiter:* Befunddaten, z.B. Röntgenbilder, Blutgruppe, Untersuchungsergebnisse,
* Ereignisse, wie z.B. Operationen, Unfälle, Impfungen, Krankheiten, seien sie akut oder chronisch, körperlich oder seelisch, sichtbar oder unsichtbar.
* Daneben auch medizinische Bewertungen, wie z.B. die Einstufung als Schwerbehinderter oder eine Krankschreibung für den Arbeitgeber,
* Die Einnahme von Stoffen mit gesundheitlicher Wirkung, wie z.B. von Alkohol, Drogen oder Medikamenten,
* der kurzfristige oder längerdauernde Aufenthalt in gesundheitsrelevanten Einrichtungen, wie z.B. allgemeinen Krankenhäusern, Aids-, Krebs- oder Kurkliniken, Pflegeheimen, Arzt- oder Heilpraxen, psycho-sozialen Wohngruppen oder Maßregelvollzugsanstalten,
* Bestands-, Verkehrs- wie auch Inhaltsdaten des Telekommunikationsverkehrs zwischen Betroffenen und Gesundheitseinrichtungen wie auch Kommunikationsinhalte generell.

Die Zugehörigkeit zu einer bestimmten Krankenkasse oder Krankenversicherung oder der Umstand einer Beihilfeberechtigung ist kein Gesundheitsdatum. Zudem wird zwischen Gesundheitsdaten und Krankheitsdaten unterschieden. Des Weiteren können auch Sozialdaten nach dem Sozialgesetzbuch zugleich Gesundheits- oder sonstige sensitive Daten sein. Zu denken ist beispielsweise an medizinische Diagnosen, behandelnde (Amts-) Ärzte oder Mutterschaften. Aber auch eine spezifische Form des Versicherungsschutzes, oder die Teilnahme an einem strukturierten Behandlungsprogramm bei chronischen Erkrankungen (Disease Management Programm) stellen Gesundheitsdaten dar und sind damit besonders geschützt. |
| [x]  Daten zum Sexualleben oder sexuellen Orientierung | Diese Kategorie geht auf das Diskriminierungsverbot der Grundrechtecharta zurück. Erfasst sind Informationen über Hetero-, Bi-, oder Homosexualität. Ferner Informationen über eine Geschlechtsumwandlung oder die Zugehörigkeit zu einem anderen, dritten Geschlecht. Ebenso, ob jemand in einer Ehe oder in einer eingetragenen Partnerschaft lebt. Wobei die Angabe, ob jemand verheiratet oder ledig ist, nicht unter diese besondere Kategorie fällt. Weitere Beispiele über Daten zum Sexualleben sind die Kundeneigenschaft in einem Sexshop, der Kauf von Viagra oder Verhütungsmitteln oder der Konsum von erotischen oder pornografischen Medien. |
| [ ]  … |  |

|  |
| --- |
| Art. 10 DSGVO |
| [x]  strafrechtliche Verurteilungen und Straftaten |
| [x]  Sicherungsmaßregeln |
| [ ]  … |

**Welche Datenkategorien nach Art. 9 Abs. 1 bzw. Art. 10 DSGVO müssen verarbeitet werden?**

**Bitte alle erforderlichen Datenkategorien einfügen:** [Platzhalter Datenkategorien Art. 9/Art. 10 Rassische oder ethnische Herkunft, Politische Meinung, Religiöse oder weltanschauliche Überzeugungen, Gewerkschaftsangehörigkeit, Genetische Daten, Biometrische Daten zur eindeutigen Identifizierung, Gesundheitsdaten, Daten zum Sexualleben oder sexuellen Orientierung, strafrechtliche Verurteilungen und Straftaten, Sicherungsmaßregeln, ]

**Verortung in der Textvorlage:**

(2) Verarbeitung besonderer Kategorien personenbezogener Daten

Das [*Verarbeiten von Art. 9/Art. 10-Daten*] und Anonymisieren von personenbezogenen Daten nach Artikel 9 Absatz 1 oder Art. 10 der Verordnung (EU) 2016/679, nämlich [Platzhalter Datenkategorien Art. 9/Art. 10 Rassische oder ethnische Herkunft, Politische Meinung, Religiöse oder weltanschauliche Überzeugungen, Gewerkschaftsangehörigkeit, Genetische Daten, Biometrische Daten zur eindeutigen Identifizierung, Gesundheitsdaten, Daten zum Sexualleben oder sexuellen Orientierung, strafrechtliche Verurteilungen und Straftaten, Sicherungsmaßregeln, ] der [*Betroffenen Art. 9/Art.10-Daten*] durch die [*(alle) zuständige/n Behörde/n*] ist zulässig, soweit dies zur Wahrnehmung der Aufgaben [*Zweckbestimmung Art. 9/Art. 10-Daten*] erforderlich ist.

## Zweck der Datenverarbeitung (Art. 9 Abs. 1 bzw. Art. 10 DSGVO-Daten)

Die Verarbeitung besonderer Kategorien von Daten nach Art. 9 DSGVO unterliegt den besonderen Anforderungen nach Art. 9 Abs. 2 Buchst. g: das nationale Gesetz muss in angemessenem Verhältnis zu dem verfolgten Ziel stehen, den Wesensgehalt des Rechts auf Datenschutz wahren und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsehen, die aus Gründen eines erheblichen öffentlichen Interesses erforderlich sein müssen. Die für diesen Absatz zu formulierende Zweckbestimmung muss daher ein **erhebliches öffentliches Interesse belegen**.

Hier ist also der Zweck der Verarbeitung der Art. 9-Daten anzugeben und zu prüfen, ob die Verarbeitung der Daten zu diesem Zweck dem erheblichen öffentlichen Interesse dient:

**Zu welchem Zweck, werden die besonderen Kategorien von Daten iSv Art.9/10 DSGVO verarbeitet?**

**Bitte einfügen Zweck der Datenverarbeitung der Art. 9/Art. 10-Daten:** [Platzhalter Zweckbestimmung Art. 9/Art. 10-Daten]

**Verortung in der Textvorlage:**

(2) Verarbeitung besonderer Kategorien personenbezogener Daten

Das [*Verarbeiten von Art. 9/Art. 10-Daten*] und Anonymisieren von personenbezogenen Daten nach Artikel 9 Absatz 1 oder Art. 10 der Verordnung (EU) 2016/679, nämlich [*Datenkategorien Art. 9/Art. 10*] der [*Betroffenen Art. 9/Art.10-Daten*] durch die [*(alle) zuständige/n Behörde/n*] ist zulässig, soweit dies zur Wahrnehmung der Aufgaben [Platzhalter Zweckbestimmung Art. 9/Art. 10-Daten] erforderlich ist.

## Art der Datenverarbeitung

Die Auflistung der erforderlichen spezifischen Verarbeitungstätigkeiten unterscheidet sich nicht von der Verarbeitung personenbezogener Daten, die nicht unter Art. 9 DSGVO fallen. Es wird daher auf die Ausführungen oben unter 1.4 verwiesen.

|  |  |
| --- | --- |
| Art der Verarbeitung | Definition |
| [x]  erheben | Beschaffen von Daten über eine betroffene Person. Gezielte Verwandlung eines unbekannten Datums in ein Bekanntes. Setzt aktives Handeln des Verantwortlichen voraus. Gilt nicht, wenn der/dem Verantwortlichen eine Information aufgezwungen wird. |
| [x]  erfassen | Technische Formgebung erhobener Daten. Arbeitsvorgang mit dem eine erstmalige Speicherung des bekannten Datums auf einem Datenträger erfolgt. Ermöglicht die weitere technische Verarbeitung. Gilt auch, wenn Datum aufgezwungen wurde. |
| [x]  organisieren | Strukturelle Neuanordnung/systematische Strukturierung der gespeicherten personenbezogenen Daten auf dem Datenträger. Organisation personenbezogener Daten bezeichnet das Ergebnis des Sammelns und Ordnen von Daten. Vereinfacht das Auffinden und Auswerten. |
| [x]  ordnen | Sinnvoll strukturierte Ablage der gespeicherten personenbezogenen Daten auf dem Datenträger, z.B. nach Alphabet. |
| [ ]  speichern | Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung. Umfasst nicht nur die erstmalige Speicherung, sondern auch Zwischenspeicherungen auf Datenträger oder das Umspeichern von personenbezogenen Informationen, um diese für eine weitere Verwendung aufzubewahren. Die Aufbewahrung des Speichermediums zählt ebenfalls dazu. Gegenteil von Löschen und Vernichten. |
| [ ]  anpassen  | Beispiel für Veränderung. Aktualisierung/Angleichung der personenbezogenen Daten an die reellen Lebensumstände, z.B. Änderung der Wohnanschrift. |
| [ ]  verändern | Bearbeitung bzw. inhaltliche Umgestaltung gespeicherter personenbezogener Daten oder ihrer Zuordnung. Es kommt zu einer Änderung des Informationsgehalts. Sie können jedoch auch verändert werden, indem sie ergänzt, in einen neuen Zusammenhang gestellt oder für einen anderen Zweck verwendet werden. |
| [ ]  auslesen | Bewusste Kenntnisnahme über die auf einem Datenträger befindlichen personenbezogenen Daten/Abrufen von Informationen. Daten werden aus einem Datenträger ausgelesen, um sie einer weiteren Bearbeitung zugänglich zu machen. |
| [ ]  abfragen | Gezielte Informationssuche auf einem Datenträger und Kenntnisnahme dieser/Gewinnung von Daten. Zum Beispiel mithilfe der Eingabe eines Suchbegriffs. |
| [ ]  abrufen |  |
| [ ]  verwenden | Alle Beispiele außer Erheben und Erfassen sind Unterbeispiele von Verwenden. Jeder gezielte Umgang mit personenbezogenen Daten kann als Verwendung der Daten gelten. Sinngemäße Nutzung einer bereits bekannten Information. |
| [ ]  offenlegen  | Vorgang, der dazu führt, dass Daten für andere zugänglich gemacht werden und sie diese auslesen oder abfragen können. Bekanntgabe bekannter gespeicherter Daten an Dritte. |
| [ ]  übermitteln | Gezielte Weitergabe von Daten an einen oder mehrere Empfänger. |
| [ ]  verbreiten | Ungezielte Weitergabe an unbestimmte Adressaten z.B. Öffentlichkeit. |
| [ ]  Bereitstellen durch andere Form | Passive Form der Offenlegung. Bereithaltung der Daten zum potenziellen Gebrauch, z.B. für eine Einsicht. |
| [ ]  abgleichen  | Vergleich mehrerer zusammengehöriger bekannter, nicht am selben Ort gespeicherter Daten. Abweichungen oder Übereinstimmungen können festgestellt werden. |
| [ ]  verknüpfen | Zuordnung mehrerer zusammengehöriger bekannter, nicht am gleichen Ort gespeicherter Daten. Ziel ist die Entstehung einer neuen Datenstruktur durch Zusammenführung der Daten. (Dient z.B. der Erleichterung der Durchführung von Abfragen). |
| [ ]  vernichten | Physische Beseitigung der Daten. Vollständige Zerstörung des Datenträgers, sodass keinerlei Information mehr auslesbar ist. |
| [ ]  einschränken  | Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken (Art. 4 Nr. 3). Entspricht der Sperrung von Daten |
| [x]  anonymisieren | Die Verarbeitung von Daten in einer Weise, dass die Daten nicht einer bestimmten betroffenen Person zugeordnet werden können |
| [ ]  pseudonymisieren | Die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen wer |
| [ ]  löschen | Entfernung/Unkenntlichmachung einer gespeicherten Information von jedem Datenträger, sodass die Daten keinesfalls mehr ausgelesen bzw. wiederhergestellt werden können. Der Datenträger kann physisch erhalten bleiben. Es erfolgt kein Löschen durch Verschlüsselung oder Anonymisierung der Daten. |
| [ ]  … |  |

**Wie müssen diese Datenkategorien verarbeitet werden?**

**Bitte alle Verarbeitungstätigkeiten einfügen:** [ Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Abrufen, Verwenden, Offenlegen, Übermitteln, Verbreiten, Bereitstellen durch andere Form, Abgleichen, Verknüpfen, Einschränken, Vernichten, Anonymisieren, Pseudonymisieren, Löschen]

**Verortung in der Textvorlage:**

(2) Verarbeitung besonderer Kategorien personenbezogener Daten

Das [ Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Abrufen, Verwenden, Offenlegen, Übermitteln, Verbreiten, Bereitstellen durch andere Form, Abgleichen, Verknüpfen, Einschränken, Vernichten, Anonymisieren, Pseudonymisieren, Löschen] von personenbezogenen Daten nach Artikel 9 Absatz 1 oder Art. 10 der Verordnung (EU) 2016/679, nämlich [*Datenkategorien Art. 9/Art. 10*] der [*Betroffenen Art. 9/Art.10-Daten*] durch die [*(alle) zuständige/n Behörde/n*] ist zulässig, soweit dies zur Wahrnehmung der Aufgaben [*Zweckbestimmung Art. 9/Art. 10-Daten*] erforderlich ist.

# Abs. 3: Verarbeitung von Daten, die bei Dritten erhoben werden

Es gibt Konstellationen, da erhebt die Verwaltung Daten von betroffenen Personen nicht direkt bei diesen, sondern bei Dritten.

Eine Datenerhebung bei Dritten liegt zum Beispiel vor, wenn die Daten bei **einer anderen Behörde** abgerufen werden, also dort erhoben werden. Dieser Abruf bedarf einer gesetzlichen Rechtsgrundlage. Bei fachgesetzlich gebotenen Datenabrufen (z.B. Abruf aus Melderegister) benötigt die abrufende Behörde eine Rechtsgrundlage für den Datenabruf. Dies ist insbesondere in der Eingriffsverwaltung geboten.

Der/die Dritte kann auch eine **private Quelle** sein, die gesetzlich verpflichtet ist, Daten zur Verfügung zu stellen: Eine Datenerhebung bei Dritten liegt beispielsweise bei der Mutterschutzmeldung durch einen Arbeitgeber vor: Der Arbeitgeber wird durch das Arbeitsschutzgesetz verpflichtet, die Schwangerschaft einer beschäftigten Arbeitnehmerin bei der Arbeitsschutzbehörde zu melden (dann werden die Daten der betroffenen schwangeren Frau nicht direkt bei ihr, sondern bei/über den Dritten, den Arbeitgeber, erhoben).

Werden Daten von betroffenen Personen verarbeitet und diese Daten werden nicht direkt bei diesen betroffenen Personen erhoben, sondern bei dritten Behörden/Personen, sind die Betroffenen gemäß Art. 14 Abs. 1 DSGVO darüber umfänglich **zu informieren**. Dies würde erheblichen Mehraufwand in Verwaltungsprozessen bedeuten, so dass der Ausnahmeregelung zu dieser Regelung in Art. 14 Abs. 5 Buchst. c DSGVO eine besondere Bedeutung zukommt.

**Art. 14 Abs. 5 DSGVO:**

Wenn die Erlangung oder Offenlegung der Daten durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist, **entfällt die Informationspflicht.**

## Betroffene bei Dritterhebung

Wer sind die Betroffenen der Datenerhebung bei dritten Personen? („Wessen Daten werden erhoben?“)

* Arbeitnehmende
* Eltern von Antragstellenden (z.B. bei BaföG-Beantragung)
* Nachbarinnen und Nachbarn (z.B. in Bauantragsverfahren)
* …

**Wenn Daten verarbeitet werden, die bei Dritten erhoben werden– wessen?**

**Bitte alle Betroffenen einfügen:** [Platzhalter Betroffene Drittdaten]

**Verortung in der Textvorlage:**

(3) Datenerhebung bei Dritten

[*(alle) zuständige/n Behörde/n*] erhebt, um [*Zweck Drittdaten*] von [Platzhalter Betroffene Drittdaten], [*Datenkategorie Drittdaten*], bei [*Drittem/n*].

## Dritter, bei dem die Daten erhoben werden

Hier ist festzulegen, bei welcher dritten Person/Stelle die Daten der Betroffenen erhoben werden dürfen.

* andere Behörden bei Hinzuziehung von Daten/Akten
* Arbeitgebende
* Antragstellende Kinder
* …

**Wer ist die dritte Person/Behörde, bei der die Daten von Betroffenen erhoben werden?**

**Bitte Dritte einfügen:** [Platzhalter Dritte]

**Verortung in der Textvorlage:**

(3) Datenerhebung bei Dritten

[*(alle) zuständige/n Behörde/n*] erhebt, um [*Zweck Drittdaten*] von [*Betroffenen Drittdaten*], [*Datenkategorie Drittdaten*], bei [Platzhalter Dritte].

## Zweck der Datenerhebung

Entsprechend den Ausführungen oben unter 2.3 ist auch hier der Zweck der Datenverarbeitung anzugeben.

**Zu welchem Zweck werden Daten bei dem Dritten erhoben?**

**Bitte Dritte einfügen:** [Platzhalter Zweck Dritte]

**Verortung in der Textvorlage:**

(3) Datenerhebung bei Dritten

[*(alle) zuständige/n Behörde/n*] erhebt, um [Platzhalter Zweck Dritte] von [*Betroffenen Drittdaten*], [*Datenkategorie Drittdaten*], bei [*Drittem/n*].

## Erhobene Datenkategorien

Auch hier müssen die Datenkategorien, die bei dem Dritten erhoben werden müssen, spezifiziert werden.

|  |  |
| --- | --- |
| Datenkategorie | Beispiel |
| [x]  Identifikationsdaten | Name, Vorname, Geburtsdatum, Geburtsort |
| [x]  Adressdaten | Straße und Hausnummer, Ort |
| [x]  Vertragsstammdaten  | Vertragsbezogene Daten |
| [x]  Daten zur Bank- oder Kreditkartenkonten | Kontonummer, IBAN, BLZ, Kreditkartennummer, Kreditkarteninstitut, Gültigkeitsdauer, Prüfnummer |
| [x]  IT-Nutzungsdaten | IP-Adresse, Loggingdaten, Transaktionsdaten… |
| [x]  Verbindungsdaten | Unterkategorie der IT-Nutzungsdaten: IP-Adresse, MAC-Adresse... |
| [x]  Kommunikationsdaten | Telefonnummer, Handynummer, E-Mail-Adresse, … |
| [x]  Patientendaten | Krankenkassen, Versicherungsnummer, Aufnahmedaten, … |
| [ ]  … | Freitextfeld |

**Welche Datenkategorien müssen verarbeitet werden, die bei den Dritten erhoben werden?**

**Bitte Datenkategorien einfügen:** [Identifikationsdaten, Adressdaten, Vertragsstammdaten, Daten zu Bank- oder Kreditkartenkonten, IT-Nutzungsdaten, Verbindungsdaten, Kommunikationsdaten, Patientendaten, ]

**Verortung in der Textvorlage:**

(3) Datenerhebung bei Dritten

[*(alle) zuständige/n Behörde/n*] erhebt, um [*Zweck Drittdaten*] von [*Betroffenen Drittdaten*], [Identifikationsdaten, Adressdaten, Vertragsstammdaten, Daten zu Bank- oder Kreditkartenkonten, IT-Nutzungsdaten, Verbindungsdaten, Kommunikationsdaten, Patientendaten, ], bei [*Drittem/n*].

# Abs. 4: Datenabrufe

§ 5 EGovG sieht vor, dass Nachweise für antragsgebundene Verwaltungsverfahren nach Wahl von Antragstellenden entweder von den Antragstellenden selbst übermittelt werden können, oder beim zuständigen Register abgerufen werden können. Dies gilt im Anwendungsbereich des EGovG für die Verwaltungstätigkeit des Bundes und der Länder in Ausführung von Bundesrecht im Rahmen der Leistungsverwaltung (§ 1 Abs. 1 und Abs. 2 EGovG). Eine gesonderte datenschutzrechtliche Rechtsgrundlage im Anwendungsbereich des § 5 EGovG ist daher nicht erforderlich.

Eine vergleichbare Regelung für Nachweisabrufe unter den Behörden der EU-Mitgliedsstaaten enthält § 5a EGovG in Verbindung mit Art. 14 SDG-VO.

Für die Ausführung von Landesrecht durch die (nach § 1 Abs. 2 EGovG) gleichgestellten Behörden bedarf es einer mit §§ 5 und 5a EGovG vergleichbaren Regelung im Landesrecht. Ferner bedarf es einer mit § 5a Abs. 2 EGovG vergleichbaren Regelung im Landesrecht, wenn eine Landesbehörde Nachweise auf Anfrage an einen anderen EU-Mitgliedsstaat im Rahmen eines Verfahrens übermitteln möchte, welches in Deutschland nach dem Bundesrecht geregelt ist. Auf das jeweilige EGovG des Landes muss je nach Ausgestaltung dieser Rechtsgrundlage verwiesen werden.

**Gibt es eine landesrechtliche Vorschrift zu Datenabrufen auf Veranlassung von Antragstellenden?**

**In welchem Paragraphen wird der Anwendungsbereich des Landesgesetzes definiert?**

**Bitte einfügen:** [Zitierung Anwendungsbereich EGovG Land]

**Wie wird das Gesetz zitiert?**

**Bitte einfügen:** [ § XY EGovG Land]

**Verortung in der Textvorlage:**

(4) Datenabrufe

Im Geltungsbereich des [[Zitierung Anwendungsbereich EGovG Land] darf die [*zuständige/n Behörde/n*] die erforderlichen Nachweise bei dem zuständigen Register abrufen. [§ XY EGovG Land] finden Anwendung.

# Abs. 5: Löschen und Aufbewahrungsfristen

Nach dem Grundsatz der Datenminimierung dürfen Daten nur solange vorgehalten und gespeichert werden, bis der Zweck der Datenverarbeitung (Zweckfortfall) erfüllt ist und sie sind unverzüglich zu löschen, wenn nicht gesetzlichen Aufbewahrungspflichten bestehen.

Für den Entwurf dieser fachgesetzlichen Rechtsgrundlage ist daher zu prüfen, ob aus (diesem) Fachrecht Aufbewahrungspflichten resultieren, die hier klarstellend gesetzlich geregelt werden **können** (z.B. müssen Bauvorlagen einer baulichen Anlage so lange aufbewahrt werden, wie die bauliche Anlage besteht, was im Fachrecht zu regeln ist). Letztlich sind diese antizipierte Festlegungen des Zeitpunkts des Zweckfortfalls.

**Hinweis**: Für die öffentliche Verwaltung besteht eine Aufbewahrungspflicht aus dem Grundsatz der **Nachvollziehbarkeit der Verwaltung**, der sich insbesondere in den Aufbewahrungspflichten von Aktenordnungen und Staatsarchiven niederschlägt. Nicht zu vergessen sind aber auch weitere fachgesetzliche Aufbewahrungspflichten, z.B. bei zahlungsrelevanten Vorgängen nach der AO.

Zu prüfen und einzusetzen ist, welche der zuvor herausgearbeiteten Daten nach Absatz 1 oder Absatz 2 wie lange bzw. bis zu welchem Zeitpunkt aufbewahrt werden müssen, um eine fachgesetzliche Aufbewahrungspflicht festzulegen. Wenn es keine besonderen Aufbewahrungspflichten gibt, ist Satz zwei zu löschen.

**Für welche Daten ist eine spezialgesetzliche Aufbewahrungsfrist festzulegen:** [Platzhalter Verweis auf Abs. 1 oder Abs. 2]

**Wie lange müssen diese aufgehoben werden?** [Platzhalter Aufbewahrungsfrist]

Ggf. gibt es unterschiedliche Fristen für unterschiedliche Datenkategorien, ggf. ist der zweite Satz zu löschen.

**Ist die Löschung vom Eintritt eines bestimmten Ereignisses, z.B. Untergang des Bauwerkes, abhängig:**

[Platzhalter Eintritt Ereignis]

Verortung in der Textvorlage:

(5) Löschung und Aufbewahrungsfristen

Alle Daten sind unverzüglich zu löschen, soweit sie zur Aufgabenerfüllung nicht mehr erforderlich sind.

Die Daten nach [Platzhalter Verweis auf Abs. 1 oder Abs. 2] sind für einen Zeitraum von [Platzhalter Aufbewahrungsfrist] bis … bzw. bis [Platzhalter Eintritt Ereignis] eingetreten ist, je nachdem welcher Zeitpunkt der frühere ist, aufzubewahren. Sie sind sodann unverzüglich zu löschen.

Weitere gesetzliche Aufbewahrungspflichten bleiben unberührt.

# Abs. 6: Technisch organisatorische Maßnahmen

Abs. 6 setzt das Erfordernis aus Art. 9 Abs. 2 Buchst. b, g und i DSGVO um, „geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person“ bzw. „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ vorzusehen sowie das Erfordernis aus Art. 14 Abs. 5 Buchst. c DSGVO „geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person“ vorzusehen.

Er wiederholt beispielhaft („insbesondere“) das, was an technisch-organisatorischen Maßnahmen vor allem in den Art. 24 ff. DSGVO verpflichtend vorgesehen ist, wie es auch § 22 Abs. 2 BDSG tut.

Man kann daher Abs. 6 als Placeboregelung ansehen oder darin gar eine Verletzung des Normwiederholungsverbots erkennen. Abs. 6 hat allerdings **Appellcharakter**, da die darin aufgeführten Maßnahmen sind geeignet, trotz ihrer Duplizität zu DSGVO und BDSG-Regelungen, die verarbeitenden Stellen an ihre Pflicht zu Sicherungsmaßnahmen zu erinnern und die Anwendung im sensitiven Bereich zu erleichtern.

Abs. 6 ist insbesondere einschlägig, wenn Daten nach Abs. 2 (Art. 9 oder 10-Daten i.S.d. DSGVO verarbeitet werden) oder die Daten bei Dritten i.S.v. Abs. 3 erhoben werden.

# Text der RGL-Blaupause

In der Folge ist eine Blaupause für den Text der gesetzlichen Norm, der Rechtsgrundlage für die Datenverarbeitung dargestellt. Die oben eingefügten Elemente müssten hier erscheinen, so dass eine Norm für einen Gesetzestext entsteht. Das, was nicht einschlägig ist, muss gelöscht werden (insbesondere ist zu entscheiden, ob überhaupt die Absätze einschlägig sind und bei Abs. 3, ob eine gebundene Entscheidung vorliegt oder eine Ermessenentscheidung vorliegt).

**(1) Verarbeitung personenbezogener Daten**

Das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Abrufen, Verwenden, Offenlegen, Übermitteln, Verbreiten, Bereitstellen durch andere Form, Abgleichen, Verknüpfen, Einschränken, Vernichten, Anonymisieren, Pseudonymisieren, Löschen von Identifikationsdaten, Adressdaten, Vertragsstammdaten, Daten zu Bank- oder Kreditkartenkonten, IT-Nutzungsdaten, Verbindungsdaten, Kommunikationsdaten, Patientendaten, Daten über berufliche Qualifikation, der Platzhalter Betroffene durch die Platzhalter (alle) zuständige/n Behörde/n ist zulässig, soweit dies zur Wahrnehmung der Aufgaben nach Platzhalter Zweckbestimmung erforderlich ist.

**(2) Verarbeitung besonderer Kategorien personenbezogener Daten**

Das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Abrufen, Verwenden, Offenlegen, Übermitteln, Verbreiten, Bereitstellen durch andere Form, Abgleichen, Verknüpfen, Einschränken, Vernichten, Anonymisieren, Pseudonymisieren, Löschen von personenbezogenen Daten nach Artikel 9 Absatz 1 oder Art. 10 der Verordnung (EU) 2016/679, nämlich Platzhalter Datenkategorien Art. 9/Art. 10 Rassische oder ethnische Herkunft, Politische Meinung, Religiöse oder weltanschauliche Überzeugungen, Gewerkschaftsangehörigkeit, Genetische Daten, Biometrische Daten zur eindeutigen Identifizierung, Gesundheitsdaten, Daten zum Sexualleben oder sexuellen Orientierung, strafrechtliche Verurteilungen und Straftaten, Sicherungsmaßregeln, der Platzhalter Betroffene Art. 9 oder Art. 10 durch die Platzhalter (alle) zuständige/n Behörde/n ist zulässig, soweit dies zur Wahrnehmung der Aufgaben Platzhalter Zweckbestimmung Art. 9/Art. 10-Daten erforderlich ist.

**(3) Datenerhebung bei Dritten**

Platzhalter (alle) zuständige/n Behörde/n erhebt, um Platzhalter Zweck Dritte von Platzhalter Betroffene Drittdaten, Identifikationsdaten, Adressdaten, Vertragsstammdaten, Daten zu Bank- oder Kreditkartenkonten, IT-Nutzungsdaten, Verbindungsdaten, Kommunikationsdaten, Patientendaten, bei Platzhalter Dritte.

**(4) Datenabrufe**

Im Geltungsbereich des [Zitierung Anwendungsbereich EGovG Land darf die Platzhalter (alle) zuständige/n Behörde/n die erforderlichen Nachweise bei dem zuständigen Register abrufen. § XY EGovG Land finden Anwendung.

**(5) Löschung und Aufbewahrungsfristen**

Alle Daten sind unverzüglich zu löschen, soweit sie zur Aufgabenerfüllung nicht mehr erforderlich sind. Die Daten nach Platzhalter Verweis auf Abs. 1 oder Abs. 2 sind für einen Zeitraum von Platzhalter Aufbewahrungsfrist bis … bzw. bis Platzhalter Eintritt Ereignis eingetreten ist, je nachdem welcher Zeitpunkt der frühere ist, aufzubewahren. Sie sind sodann unverzüglich zu löschen. Weitere gesetzliche Aufbewahrungspflichten bleiben unberührt.

**(6) Technisch organisatorische Maßnahmen**

Unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sind angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorzusehen. Dies gilt insbesondere, soweit personenbezogene Daten nach Absatz 2 verarbeitet oder personenbezogene Daten nicht bei der betroffenen Person erhoben werden. Zu den Maßnahmen im Sinne des Satzes 1 können technische und organisatorische Maßnahmen gehören, um sicherzustellen, dass die Verarbeitung im Einklang mit der Verordnung (EU) 2016/679 erfolgt. In Betracht kommen insbesondere folgende Maßnahmen:

1. Verschlüsselung personenbezogener Daten,

2. Pseudonymisierung personenbezogener Daten,

3. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,

4. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen,

5. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,

6. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,

7. Vorschriften und Anweisungen, die die Verarbeitung personenbezogener Daten regeln und

8. Beschränkung des Zugangs zu personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern.

# **Kontaktdaten und Mitwirkende**

Bei Fragen und Anmerkungen kontaktieren Sie bitte das Kompetenzteam Datenschutz:

kompetenzteam.datenschutz@sk.hamburg.de

**Verantwortlich**

Die Erstellung des Dokuments erfolgte im Rahmen des Schwerpunktthemas Datennutzung des IT-Planungsrats im Kompetenzteam Datenschutz unter der Leitung von Dr. Ulrike Klocke und Katja Weber (Senatskanzlei der Freien und Hansestadt Hamburg).

**Mitwirkende**

Mitglieder des Kompetenzteams Datenschutz des IT-Planungsrats

**Stand:** Version 1.0, 21.2.2025

1. In Ausnahmefällen kann es auch Regelungsgegenstände geben, bei denen eine Auflistung der einzelnen zu verarbeitenden Kategorien nicht möglich oder nicht sinnvoll ist, beispielsweise wenn die Norm auf die elektronische Vorbereitung diverser Fachverfahren anwendbar sein soll (siehe beispielsweise § 8a Abs. 1 S. 1 OZG). In diesem Fall genügt zwar die Angabe „personenbezogene Daten“, jedoch muss die Konkretisierung über andere Norminhalte erfolgen. [↑](#footnote-ref-2)