Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Standardprozess Datenschutz bei öffentlichen Digitalisierungsvorhaben

**Handreichung I**

# Datenschutz in der Zielvision, Projektumfeldanalyse und Machbarkeitsprüfung

Version 1.0

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

**Standardprozess Datenschutz bei öffentlichen Digitalisierungsvorhaben**

| | |
|---|---|
| **Version** | 1.0 |
| **Herausgeberin**: | Berliner Beauftragte für Datenschutz<br>und Informationsfreiheit<br>Alt-Moabit 59-61<br>10555 Berlin<br>Tel.: 030 138 89 0<br>Fax: 030 215 50 50<br>mailbox@datenschutz-berlin.de<br>www.datenschutz-berlin.de |
| **Redaktion:** | mailbox@datenschutz-berlin.de |

# Inhaltsverzeichnis

## Abkürzungsverzeichnis

| **Abkürzung** | **Vollständige Bezeichnung** |
|---|---|
| BGH | Bundesgerichtshof |
| BlnDSG | Berliner Datenschutzgesetz |
| BSI | Bundesamt für Informationssicherheit |
| DSGVO | Datenschutz-Grundverordnung |
| DSK | Datenschutzkonferenz |
| EDSA | Europäischer Datenschutzausschuss |
| EG | Erwägungsgrund (der DSGVO) |
| E-GovG Bln | E-Government-Gesetz Berlin |
| EuGH | Europäischer Gerichtshof |
| IKT | Informations- und Kommunikationstechnik |
| IKT-S | IKT-Steuerung |
| ITDZ | IT-Dienstleistungszentrum Berlin |
| pbD | Personenbezogene Daten |
| PPS | Projektmanagementprozessschritte |
| RDSK | Rahmendatenschutzkonzept |
| Risiko | Risiko für die Rechte und Freiheiten der betroffenen Person |
| Rspr | Rechtsprechung |
| SDM | Standard-Datenschutzmodell |
| SenV | Senatsverwaltung |
| SGB | Sozialgesetzbuch |
| Skzl | Senatskanzlei |
| vaIKT | Verfahrensabhängige IKT (IT-Fachverfahren) |
| vuIKT | Verfahrensunabhängige IKT |

# 1 Einführung/ Sinn und Zweck des Dokumentes

Diese Handreichung wird insbesondere durch das in → **PPS 7 („Projektteam zusammenstellen")** festgelegte Mitglied des Projektteams genutzt, das für die Umsetzung der Datenschutzanforderungen zuständig ist. Soweit erforderlich, muss Datenschutzexpertise hinzugezogen werden. Hierzu wird im Regelfall zunächst der behDSB beratend einbezogen. Ein vollumfängliches Outsourcing der Erfüllung der Vorgaben des Datenschutzes an externe Beratungsunternehmen ist nicht zielführend und muss sich auf klar umrissene Aufträge wie z. B. die Beantwortung konkreter Fragestellungen beschränken.

Diese Handreichung unterstützt die Umsetzung der Vorgaben des **Standardprozess Datenschutz bei öffentlichen Digitalisierungsvorhaben** zu → **PPS 2 „Zielvision"**, → **PPS 10 „Projektumfeldanalyse" und → PPS 15 „Machbarkeitsprüfung".** Bereits in der Definitionsphase des Projektes muss das Projektteam **grundsätzliche Fragen und mögliche Risiken aus Sicht des Datenschutzes** in den Blick nehmen, so dass diese auch bereits in einem ggf. durchzuführenden Vergabeverfahren berücksichtigt werden können (siehe hierzu → **Handreichung II**). Andernfalls können sich **Risiken für die Projektumsetzung** ergeben, wie etwa die Gefahr der späteren Untersagung einer unrechtmäßigen Verarbeitung pbD durch die zuständige Aufsichtsbehörde.

Geeignete Anknüpfungspunkte bieten sich hierfür in Zielvision, Projektumfeldanalyse und Machbarkeitsprüfung insbesondere dadurch, dass Betroffene i. S. d. Datenschutzes ausdrücklich als Stakeholder des Projektes definiert und die Einhaltung datenschutzrechtlicher Anforderungen als sachliche und soziale Umfeldfaktoren einbezogen werden (siehe hierzu 2. und 3.).

Die Ergebnisse dieser Vorabprüfung aus Sicht des Datenschutzes kann sodann als Grundlage der i. R. d. Planungs- und Durchführungsphase (→ PPS 24 „**Chancen- und Risikomanagement**"; →PPS 25 „**Stakeholdermanagement**") vorzunehmenden vertieften Risikoanalyse nach den Vorgaben der DSGVO (**siehe →Handreichung III**).

Die Handreichungen des Standardprozess Datenschutz unterscheiden öffentliche Digitalisierungsvorhaben insbesondere in zwei Konstellationen:

- Die Hauptverwaltung (IT-fachverfahrensverantwortliche Behörde oder IKT-Steuerung/ Senatskanzlei) entwickeln ein IT-Fachverfahren (vaIKT) / einen Basisdienst (vuIKT) und stellen dies der Berliner Verwaltung zur Nutzung zur Verfügung.
- Eine öffentliche Stelle führt ein IT-Fachverfahren (vaIKT) / einen Basisdienst (vuIKT) ein oder ein allgemeines Digitalisierungsvorhaben durch.

## 2 Datenschutz in der Zielvision

Die datenschutzkonforme Umsetzung der Projekte wird als eine der **Anforderungen** definiert, die die Zielvision konkretisieren.

Als **Stakeholder** des Projektes werden insbesondere auch „betroffene Personen“ im Sinne des Datenschutzes (s. Art. 4 Nr. 1 DSGVO) definiert, d. h. Menschen, deren personenbezogene Daten im Zusammenhang mit dem Projekt verarbeitet werden sollen. Hierzu erfolgt eine erste grobe Analyse, ob und inwieweit im Rahmen der Verwirklichung der Zielvision bzw. der Umsetzung des Projekts personenbezogene Daten verarbeitet werden. Ggf. kann bereits der behDSB beratend hinzugezogen werden.

Die Auswirkungen auf Stakeholder in diesem Sinne sind auch im gemäß PMH, Anlage 9 bei IKT-Projekten zu erstellenden **Fach- und Realisierungskonzept** zu berücksichtigen **(→ PPS 9).**

Eine detaillierte Prüfung erfolgt sodann auf dieser Grundlage in **→ PPS 10 „Projektumfeldanalyse“** und **→ PPS 15 „Machbarkeitsprüfung“**.

## 3 Datenschutz in Projektumfeldanalyse und Machbarkeitsprüfung

Die Anforderungen des Datenschutzes müssen i. R. d. Projektumfeldanalyse sowohl in Form **sachlicher** als auch **sozialer Umfeldfaktoren** berücksichtigt werden. Als sachliche Umfeldfaktoren sind auch die gesetzlichen und technischen Rahmenbedingungen des Projektes, und damit aus Sicht des Datenschutzes v. a. die **DSGVO** und weitere **Datenschutzgesetze**, in den Blick zu nehmen. Soziale Umfeldfaktoren sind hinsichtlich der Stakeholder zu analysieren, zu denen auch **betroffene Personen i. S. d. Datenschutzes** gehören (s. unter 2.1)

Im Rahmen der **Machbarkeitsprüfung** muss sodann festgestellt werden, ob sich aus diesen Datenschutz-Umfeldfaktoren **Hindernisse für die Projektumsetzung** ergeben. Dabei ist zunächst sorgfältig zu prüfen, ob der Lösungsansatz des Projektes tatsächlich mit einer Verarbeitung pbD verbunden ist (siehe dazu unter 3.1) und welche öffentliche Stelle diesbezüglich als Verantwortliche i. S. d. Datenschutzes einzustufen ist (siehe unter 3.2).

Darüber hinaus erfolgt eine erste Prüfung **möglicher Datenschutzrisiken**, die regelmäßig im Zusammenhang mit öffentlichen Digitalisierungsvorhaben auftreten (siehe 3.3 bis 3.8). Als Grundlage kann hierfür das bei IKT-Projekten gemäß PMH, Anlage 9 zu erstellende **Fach- und Realisierungskonzept** (**→ PPS 9**) dienen. Dieses muss u. a. eine Definition der Geschäftsprozesse, die den Einsatz der IKT beschreiben, eine Benennung der Akteure/Stakeholder, die in den Einsatz der IKT eingebunden bzw. davon betroffen sind, eine Beschreibung der konkreten Rollen der in den Einsatz der IKT eingebundenen Akteure/ Stakeholder; eine Benennung der einzuführenden IKT-

Komponenten, der Schnittstellen zu anderer IKT des Landes Berlin sowie der Anforderungen an die Sicherheit der einzuführenden IKT enthalten.

In der Planungs- und Durchführungsphase des Projekts wird i. R. d. → **PPS 24 „Chancen- und Risikomanagement“** und → **PPS 25 „Stakeholdermanagement“** sodann eine förmliche Risikoanalyse nach den Vorgaben der DSGVO durchgeführt (→ **Handreichung III**).

Sind Hindernisse aus Sicht des Datenschutzes festzustellen, so hat der im Projekt in den Blick genommene Lösungsansatz keine Aussicht auf Erfolg. Das Projektteam muss für diesen Fall frühzeitig im Projekt einen neuen Lösungsansatz entwickeln.

## 3.1 Werden i. R. d. Projektumsetzung personenbezogene Daten verarbeitet?

Zentraler Ausgangspunkt ist die Frage, inwieweit personenbezogene Daten i. R. d. geplanten Projektes verarbeitet werden. Ist sicher festzustellen, dass das Digitalisierungsvorgaben nicht zu einer Verarbeitung pbD führt, so kommen die DSGVO und weitere Vorschriften zum Datenschutz **nicht** zur Anwendung.

Vorab muss jedoch eine genaue Prüfung durchgeführt werden, da oft nicht unmittelbar erkennbar ist, dass letztlich pbD verarbeitet werden. Als Grundlage dient bei Digitalisierungsvorhaben die als IKT-Projekte i. S. d. PHM einzuordnen sind, das **Fach- und Realisierungskonzept (→ PPS 9).** Eine erste Orientierung können ggf. bereits bestehende **Verarbeitungsverzeichnisse i. S. d. Art. 30 DSGVO** bieten.

### 3.1.1 Typische Konstellationen

Einige Projekte der Verwaltungsdigitalisierung sind typischerweise mit der Verarbeitung pbD verbunden, z. B.:

- **Digitalisierung von Verfahren der Leistungsverwaltung**

Hier werden regelmäßig pbD der antragsstellenden Bürger:innen verarbeitet (v. a. bei vaIKT/ IT-Fachverfahren).

- **Digitalisierung von Verwaltungsverfahren, Geschäftsprozessen**

Auch außerhalb der Leistungsverwaltung werden oft zumindest die pbD der Beschäftigten verarbeitet (Beschäftigtendaten).

### 3.1.2 Prüfung

In allen sonstigen Fällen sollte genau geprüft werden, ob i. R. d. Projektes pbD verarbeitet werden. Ausgangspunkt ist dabei stets die Definition des Art. 4 Nr. 1 und 2 DSGVO. Die nachfolgenden Hinweise sollen dem Projektteam ermöglichen, Regelfälle richtig einzuordnen und Sonderfälle zumindest zu erkennen, so dass bei Bedarf datenschutzrechtliche Beratung eingeholt werden kann (behDSB, ggf. BlnBDI).

**Definition „personenbezogene Daten“:**

*„[A]lle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“* ***(Art. 4 Nr. 1 DSGVO)****.*

Eine Person ist „**identifiziert**“, wenn sich die Identität der Person unmittelbar aus der Information ergibt (**Beispiel**: Information beinhaltet Identifikationsmerkmal, z. B. Name, Anschrift und Geburtsdatum der Person oder die Information erlaubt nach Inhalt und Kontext eine eindeutige Identifikation, ohne dass auf weitere Informationen zurückgegriffen werden muss).

**Praxisbeispiel**: Bei den typischen pbD, die i. R. v. öffentlichen Digitalisierungsvorhaben verarbeitet werden, handelt es sich um Antragsdaten (Name, Geburtsdatum, Adresse, usw.), die sich auf identifizierte Personen beziehen.

Eine Person wird **identifizierbar**, wenn sich der Bezug zu einer Person zwar nicht unmittelbar aus der Information ergibt, aber durch Verknüpfung mit weiteren Informationen hergestellt werden kann.

Art. 4 Nr. 1 DSGVO definiert eine Person dann als identifizierbar, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Nach EG[1] 26 zur DSGVO sind bei der Frage, ob eine Person identifizierbar ist, alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren.

[1] Siehe zu Funktion der EG das Glossar.

Die Frage, inwieweit auch das Wissen und die Mittel anderer Personen zur Identifizierung von Personen zu berücksichtigen sind, ist umstritten. Die Problematik betrifft die Frage, ob es bei der Herstellbarkeit des Personenbezugs auf den jeweils Verantwortlichen ankommt (relativer Personenbezug) oder ob es ausreicht, dass irgendeine andere Person einen Personenbezug herstellen kann (absoluter Personenbezug).

**Anonyme Informationen** liegen nur dann vor, wenn diese sich (von vornherein) nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten (nachträglich) in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.

🔔 **Wichtig:** In der Praxis wird eine **Anonymisierung** häufig mit einer **Pseudonymisierung** verwechselt. Bei pseudonymen Daten besteht – im Unterschied zu anonymen Daten – eine Zuordnungsregel, welche den unter einem Pseudonym erfassten Daten ein Identifikationsmerkmal einer Person zuweist (siehe auch Art. 4 Nr. 5 DSGVO). Das bedeutet, dass der Personenbezug der Informationen, anders als bei einer Anonymisierung, wieder hergestellt werden kann. Bei einer bloßen Pseudonymisierung bleiben die DSGVO und Datenschutzgesetze vollumfänglich anwendbar. Es handelt sich dabei lediglich um eine technisch-organisatorische Maßnahme der Datensicherheit (siehe auch Art. 32 Abs. 1 lit. a DSGVO).

**→ Sollen i. R. e. Projekts lediglich anonymisierte Daten verarbeitet werden, so sollte bei der Projektumfeldanalyse Datenschutzexpertise hinzugezogen werden (behDSB, ggf. BlnBDI).**

***Definition „Verarbeitung“:***

*„[J]eden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“ (**Art. 4 Nr. 2 DSGVO**).*

Aufgrund der sehr breiten Definition dürfte im Regelfall eine Verarbeitung im Sinne der DSGVO vorliegen, wenn pbD i. R. d. Digitalisierungsvorhabens betroffen sind.

#### *3.1.2.1 Besondere Kategorien personenbezogener Daten*

Besonders wichtig sind die verschiedenen Kategorien pbD, die die DSGVO unterscheidet. In Abgrenzung zu „einfachen" pbD enthält vor allem Art. 9 Abs. 1 DSGVO einen abschließenden Katalog sog. besonderer Kategorien pbD. Diese werden auch häufig als „sensible" oder „besonders sensible" pbD bezeichnet.

**Definition „besondere Kategorien personenbezogener Daten":**

*„[...] [P]ersonenbezogene [...] Daten, aus denen die **rassische** und **ethnische Herkunft, politische Meinungen, religiöse** oder **weltanschauliche Überzeugungen** oder die **Gewerkschaftszugehörigkeit** hervorgehen, sowie die Verarbeitung von **genetischen Daten, biometrischen Daten** zur eindeutigen Identifizierung einer natürlichen Person, **Gesundheitsdaten** oder **Daten zum Sexualleben** oder der **sexuellen Orientierung** einer natürlichen Person ist untersagt" (**Art. 9 Abs. 1 DSGVO**).*

Darüber hinaus sind zu unterscheiden:

**Definition „personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten":**

*„[...] [P]ersonenbezogene [...] Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln aufgrund von Artikel 6 Absatz 1 darf nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist. [...]" (**Art. 10 DSGVO**).*

#### *3.1.2.2 Besonders geschützte personenbezogene Daten*

Darüber hinaus unterliegen pbD in einigen Bereichen der Verwaltung einem besonderen Schutz, der sich nicht unmittelbar aus der DSGVO, sondern aus dem entsprechenden Fachrecht ergibt:

**Definition „Sozialdaten":**

Sozialdaten sind personenbezogene Daten, die von einer in § 35 des SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden (s. **§ 67 Abs. 2 S. 1 SGB X**). Die in **§ 35 des SGB I** genannten Stellen sind die „**Leistungsträger**", d. h. die in den §§ 18 bis 29 SGB I genannten Körperschaften, Anstalten und Behörden (Leistungsträger), die für die Sozialleistungen zuständigen sind (s. **§ 12 S. 1 SGB I**).

**Praxistipp zum Vorgehen**: Es sollte i. R. d. Projektumfeldanalyse zunächst festgestellt werden, ob ein Regelfall (s. o.) vorliegt. Anschließend sollte die nachfolgende Liste konkreter Beispiele und Beispielsfälle durchlaufen werden. Sofern anschließend noch Zweifel bestehen, ob mit Blick auf die o. g. Erläuterungen eine Identifizierbarkeit vorliegt, sollte Datenschutzexpertise hinzugezogen werden (behDSB, ggf. BlnBDI).

### 3.1.3 Beispiele und Beispielsfälle[2]

- pbD können sich nur auf **natürliche Personen** beziehen (im Wortlaut der DSGVO: „betroffene Personen").
- Informationen zu **juristischen Personen, Gruppen** oder **Personenmehrheiten** sind grundsätzlich keine pbD (s. auch EG 14) – außer es liegt ein Fall vor, in dem die Information auf ein identifiziertes oder identifizierbares Mitglied „durchschlagen" (**Beispiel**: Angabe zur finanziellen Situation einer Personengesellschaft oder einer „Ein-Mann-GmbH").
- Informationen zu **Verstorbenen** fallen nicht unter den Schutz der DSGVO (es gibt aber **Sonderregelungen**, die zu beachten sind: § 35 Abs. 5 SGB I; § 203 Abs. 4 S. 2 Nr. 3 StGB und § 2a Abs. 5 Nr. 1 AO); in manchen Fällen können Daten eines Verstorbenen einen Bezug zu einer lebenden Person haben und insoweit einen Personenbezug aufweisen (Beispiel: Die Information, der Verstorbene habe an einer Erbkrankheit gelitten, kann im Verhältnis zu seinem lebenden Nachkommen einen Personenbezug aufweisen, sofern die Information nahelegt, dass auch dieser von der Erbkrankheit betroffen ist).
- Ob Daten, die sich auf ein noch **ungeborenes Kind** beziehen, einen Personenbezug aufweisen können, wird von der DSGVO nicht eindeutig beantwortet und ist umstritten (→ behDSB einbeziehen); Information kann zumindest pbD der Mutter enthalten.
- **Sachdaten** sind keine pbD; Sachdaten können aber aufgrund individualisierender Identifikationsmerkmale, des Detaillierungsgrads oder der Einzigartigkeit der Sache einen Bezug zu einer Person aufweisen (**Beispiel**: Die Information, dass unter der Telefonnummer X zu einer konkreten Uhrzeit ein Anruf getätigt wurde – durch die Angabe der Telefonnummer als eine einem konkreten Anschlussinhaber und damit einer natürlichen Person zugeordneten Kennziffer bezieht sich die Information nicht nur auf eine Sache (Telefonanschluss), sondern auch auf eine natürliche Person).
- **Aggregierte und statistische Daten** sind in der Regel keine pbD, sofern sie sich nicht auf eine hinreichend große Personengruppe beziehen (Beispiel: Information, dass der Krankenstand der Mitarbeiter des Unternehmens A um X % zugenommen hat, ist kein pbD, wenn das Unternehmen eine Vielzahl von Mitarbeitern beschäftigt; anders ggf. bei geringer Belegschaft; Einzelfallabwägung).

[2] Vgl. für die genannten Beispiele und Beispielsfälle die Kommentierung von Klar/Kühling, in: Kühling/Buchner, DSGVO BDSG, 4. Auflage 2024, Art. 4 Nr. 1/ Rn. 4-7; 12-16, 31-39.

- **Konkrete Beispielsfälle:**
  - **Kennziffern** (z. B. eine Sozialversicherungsnummer) oder **E-Mail-Adressen** sind pbD, soweit sie „sprechend" sind, d.h. eindeutige Identifizierungsmerkmale (wie Namen etc.) enthalten.
  - **Lichtbilder** von Personen sind i. d. R. pbD (s. EG 51 DSGVO); bei Verarbeitung mit entsprechenden technischen Mitteln, kommt auch eine Qualifikation als biometrische Daten i. S. v. Art. 4 Nr. 14 DSGVO in Betracht.
  - Durch **Videoüberwachung** gewonnene Aufnahmen sind pbD, wenn die erfassten Personen erkennbar sind.
  - **Dynamische IP-Adressen** sind nach der Rspr. für den Internetzugangsanbieter und für den Webseitenbetreiber pbD, soweit Letzterem rechtliche Mittel zustehen, Daten, die eine Identifikation ermöglichen, vom Internetzugangsanbieter herauszuverlangen.
  - **Cookies** können dann pbD sein, wenn der Nutzer bei dem den Cookie ablegenden Anbieter Identifikationsmerkmale (z. B. seine IP-Adresse) hinterlässt.
  - **Visualisierungen des öffentlichen Raums** wie Gebäudeansichten (z. B. im Rahmen von Google Street View) oder **Satelliten- und Luftbildaufnahmen** können einen Personenbezug aufweisen, wenn sie mit einer Adresse versehen bzw. georeferenziert sind. Bei Satelliten- und Luftbildaufnahmen kommt es zudem auf den Detaillierungsgrad, d. h. auf die Bodenauflösung der Abbildungen an.
  - **Grundstücksinformationen/ Informationen aus Liegenschaftskatastern**, die z. B. für Projekte wie Solardachflächenkataster, Wärmekataster oder Starkregengefahrenkarten/ Starkregenhinweiskarten genutzt werden sollen) können pbD darstellen, wenn ein Bezug zu den jeweiligen Eigentümer:innen oder Erbbauberechtigten hergestellt werden kann.
  - Auch **Antworten eines Kandidaten in einer schriftlichen Prüfung** sowie Anmerkungen des Prüfers können nach der Rspr. des EuGH einen Personenbezug aufweisen.[3]
  - Nach Rspr. des BGH sollen auch **Schreiben einer Person an einen Dritten** sowie **Korrespondenz** zwischen dem Dritten und einem weiteren Empfänger über diese Person ihrem gesamten Inhalt nach als pbD anzusehen sein[4]; dasselbe soll für **interne Vermerke** gelten.[5]

[3] Siehe EuGH 20.12.2017 – C-434/16, ECLI:EU:C:2017:994 – Nowak; BVerwG 30.11.2022 – 6 C 10.21).
[4] Siehe BGH 15.6.2021 – VI ZR 576/19, NJW 2021, 2726.
[5] Siehe BGH 15.6.2021 – VI ZR 576/19, NJW 2021, 2726; siehe dazu aber auch EuG 26.4.2023 – T-557/20, ECLI:EU:T:2023:219 = ZD 2023, 399 Rn. 69 ff.

🔔 **Wichtig:** Es ist abschließend eine **Kategorisierung der pbD** vorzunehmen, die i. R. d. geplanten Projekts zu verarbeiten sind. Diese Kategorisierung der pbD sollte sich dabei an den Kategorien der DSGVO orientieren (s. o.) und vor allem ausweisen, ob und in welchem Rahmen besondere Kategorien pbD i. S. v. Art. 9 Abs. 1 DSGVO verarbeitet werden. Zudem sollten den pbD ihr Erhebungszweck, die Rechtsgrundlage (siehe unter 3.4) sowie die Speicherdauer zugewiesen werden. Diese Kategorisierung ist auch zwingender Bestandteil der Leistungsbeschreibung eines möglichen **Vergabeverfahrens** (siehe 5.1).[6]

## 3.2 Wer trägt die datenschutzrechtliche Verantwortung?

Stellt das Projektteam fest, dass der favorisierte Lösungsansatz des Projektes auf eine Verarbeitung pbD hinausläuft, muss festgestellt werden, welche Stelle die Verantwortliche i. S. d. Art. 4 Nr. 7 DSGVO für diese Verarbeitung ist. Zusätzlich muss geprüft werden, welche Stellen als Auftragsverarbeiter i. S. d. Art. 4 Nr. 8 DSGVO wirken.

Projekte der Verwaltungsdigitalisierung binden regelmäßig eine Vielzahl von Behörden und öffentlicher Stellen verschiedenster Hierarchieebenen ein. Die Bewertung der datenschutzrechtlichen Verantwortung und die Anwendung der einschlägigen Normen der DSGVO stellt dabei oft eine Herausforderung dar. Vor diesem Hintergrund sind insbesondere die nachfolgenden Bewertungen zu typischen Konstellationen zu beachten.

### 3.2.1 Typische Konstellationen

🔔 **Wichtig: IKT-Basisdienste & IT-Fachverfahren**

Die zentrale Entwicklung und Bereitstellung der vuIKT/ vaIKT (siehe Glossar), d. h. insbesondere der IKT-Basisdienste und IT-Fachverfahren, liegt im Regelfall in der Zuständigkeit der Hauptverwaltung (§§ 20 Abs. 3; 21 Abs. 2 E-GovG Bln). Aus der **Zuständigkeit für die vuIKT** bzw. **aus der IT-Fachverfahrensverantwortlichkeit ergibt sich** jedoch **nicht automatisch die datenschutzrechtliche Verantwortlichkeit.**

Im Regelfall sind nur diejenigen **öffentlichen Stellen, die die vuIKT/ vaIKT nutzen** und mittels dieser pbD zur Erfüllung ihrer Aufgaben verarbeiten, als **Verantwortliche** i. S. d. Art. 4 Nr. 7 DSGVO einzuordnen („mittelbare gesetzliche Zuweisung“, s. 3.2.2).

[6] Vgl dazu auch V-Model XT, C.1.10.3 – „Anforderungen Datenschutz“.

Die die vuIKT/ vaIKT bereitstellende Behörden der Hauptverwaltung sind regelmäßig **keine** datenschutzrechtlich Verantwortlichen, außer diese verarbeiten selbst pbD im konkreten Zusammenhang mit der Bereitstellung der vuIKT/ vaIKT. Hiervon zu unterscheiden ist die Konstellation, dass die Behörden der Hauptverwaltung die vuIKT/ vaIKT auch selber nutzen (z. B. den IKT-Basisdienst Digitale Akte Berlin).

Das **IT-Dienstleistungszentrum (ITDZ)** stellt insbesondere die vuIKT in technischer Sicht bereit (vgl. § 24 Abs. 2 S. 1 E-GovG Bln) und wird hinsichtlich der damit verbundenen Verarbeitung pbD als **Auftragsverarbeiter** i. S. d. Art. 4 Nr. 8, Art. 28 DSGVO tätig. Auch andere IT-Dienstleister, die v. a. i. R. d. vaIKT in Anspruch genommen werden, sind im Regelfall Auftragsverarbeiter.

**Wichtig: Hersteller/ Produzenten**

Regelmäßig muss i. R. v. Digitalisierungsvorhaben Hard- und Software beschafft werden (s. generell dazu → **Handreichung II**)., mit der pbD verarbeitet werden. Die Hersteller/ Produzenten solcher Hard- und Software sind grundsätzlich weder Verantwortliche noch sonstige Adressaten der Pflichten der DSGVO, sofern sich ihre Rolle auf den reinen Verkauf oder die Vermietung der Produkte beschränkt.[7] Verarbeiten die Hersteller/ Produzenten darüber hinaus auch pbD z. B. bei Software as a Service (Saas) oder Cloud-Lösungen, so ist genau zu prüfen. Im Regelfall dürften die Hersteller/ Produzenten sodann als **Auftragsverarbeiter** einzustufen sein.

**Wichtig: Abschluss der Auftragsverarbeitungsverträge**

Das ITDZ und andere Auftragsverarbeiter verarbeiten i. R. v. vuIKT/ vaIKT pbD für die datenschutzrechtlich verantwortlichen Stellen. Sie verarbeiten damit pbD im Auftrag der die vuIKT/ vaIKT nutzenden Stellen. Die regelmäßig abzuschließenden Auftragsverarbeitungsverträge (AVV) i. S. d. Art. 28 Abs. 2 DSGVO sind damit grundsätzlich zwischen den nutzenden Stellen und dem ITDZ abzuschließen. Im Einzelfall sind hier gesonderte Lösungsansätze zu verfolgen, die mit behDSB und ggf. BlnBDI abgestimmt werden müssen.

**Beachte**: Es liegt ein **Muster-AVV der Berliner Verwaltung** vor, der auf der Grundlage der Standardvertragsklauseln der EU-Kommission erstellt wurde (siehe: https://b-intern.de/themen/digitalisierung/ikt-vertraege/artikel.1014105.php).

[7] Die Pflichten aus Art. 25 DSGVO zu Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen sollen Hersteller und Produzenten laut EG 78 nur „ermutigen".

### 3.2.2 Prüfung

Liegt keine typische Konstellation vor, muss eine Einzelfallprüfung auf Grundlage der Definition der DSGVO erfolgen:

> ***Definition „Verantwortlicher“:***
>
> *„D]ie natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden“ (**Art. 4 Nr. 7 DSGVO**).*

Eine detaillierte Auslegungshilfe bieten die **EDSA Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO**, Version 2.0 v. 7. Juli 2021 („EDSA Leitlinien 07/2020“).[8]

Danach umfasst die Definition des Begriffs „Verantwortlicher“ fünf Hauptkomponenten:

**(1) „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle“**
**(2) „entscheidet“**
**(3) „allein oder gemeinsam mit anderen“**
**(4) „Zwecke und Mittel“**
**(5) „der Verarbeitung von personenbezogenen Daten“**

**(1)** Mögliche Adressaten sind „**die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle**“ – damit gibt es grundsätzlich keine Beschränkung hinsichtlich der Art der Stelle, die als Verantwortlicher auftreten kann (jede Form von Organisationen, Personenmehrheiten oder auch Einzelpersonen).

- In der Praxis soll **i. d. R. die Organisation** als solche und **nicht eine natürliche Person** innerhalb der Organisation (wie z. B. einzelne Behördenmitarbeiter:innen) als Verantwortliche im Sinne der DSGVO fungieren.[9]
- In Ausnahmefällen kann eine Verarbeitung einzelnen Mitarbeitenden zugerechnet werden, wenn diese eindeutig außerhalb Ihres Aufgaben- und Zuständigkeitsbereichs handeln und ausreichend angewiesen und geschult wurden (sog. **Exzess** – muss im Einzelfall genau geprüft werden; behDSB und ggf. BlnBDI hinzuziehen).[10]

[8] Alle Leitlinien des EDSA können abgerufen werden auf: https://www.datenschutz-berlin.de/infothek/leitlinien-des-edsa/.
[9] Siehe EDSA Leitlinien 07/2020, Rn. 17.
[10] Siehe EDSA Leitlinien 07/2020, Rn. 19.

**(2)** die Verantwortliche **„entscheidet“** über die Zwecke und Mittel der Verarbeitung – sie muss also Einfluss auf die Verarbeitung im Wege der Ausübung von Entscheidungsbefugnissen haben

- diese Verantwortlichkeit kann gesetzlich festgelegt sein oder sich aus einer Analyse des Sachverhalts und der Umstände des Falls ergeben.

🔔 **Wichtig**: Im **öffentlichen Bereich** ist die Verantwortlichkeit regelmäßig **gesetzlich festgelegt**. Hierfür gibt es zwei Konstellationen:

→ Es kann gem. Art. 4 Nr. 7, 2. HS DSGVO eine **unmittelbare gesetzliche Zuweisung** der Verantwortlichkeit durch die Mitgliedstaaten erfolgen (vgl. z. B. § 8a Abs. 4 Onlinezugangsgesetz); siehe näheres EDSA Leitlinien 07/2020, Rn. 22 f.

→ Der Regelfall ist laut EDSA jedoch eine **„mittelbare“ gesetzliche Festlegung** der Verantwortlichkeit durch Zuweisung einer Aufgabe per Rechtsvorschrift (EDSA Leitlinien 07/2020, Rn. 24); hieraus ergibt sich, dass i. d. R. diejenige Behörde oder öffentliche Stelle, der bestimmte Aufgaben zugewiesen sind, hinsichtlich der dafür erforderlichen Verarbeitung pbD auch die Verantwortung i. S. d. Art. 4 Nr. 7 DSGVO trägt.

**(3)** die Verantwortliche entscheidet **„allein oder gemeinsam mit anderen“**; es kann auch mehrere Verantwortliche geben:

→ **„gemeinsame Verantwortung“** (i. S. d. **Art. 26 DSGVO**)

- Eine gemeinsame Verantwortung liegt vor, wenn eine **gemeinsame Beteiligung an der Festlegung der Zwecke und Mittel** vorliegt; d.h., dass mehr als eine Stelle entscheidenden Einfluss darauf hat, ob und wie die Verarbeitung erfolgt.
- Der EuGH hat in einigen Grundsatzentscheidungen ein durchaus weites Verständnis der gemeinsamen Verantwortung vertreten, so dass in der Praxis sehr verschiedene Fälle darunterfallen können.[11]

[11] Siehe EDSA Leitlinien 07/2020, Rn. 54 ff.

🔔 **Wichtig**: Im öffentlichen Bereich wird die Verantwortlichkeit regelmäßig, zumindest mittelbar, gesetzlich festgelegt (s. o.). Im Regelfall muss damit **auch eine gemeinsame Verantwortung**, zumindest mittelbar, **gesetzlich festgelegt** sein. Wenn mehrere an einem digitalisierten Verwaltungsverfahren beteiligte öffentliche Stelle als gemeinsame Verantwortliche für die damit verbundene Verarbeitung pbD gelten sollen, müssen auch die in diesem Verwaltungsverfahrens zu erfüllenden Verwaltungsaufgaben allen diesen Stellen gesetzlich zugewiesen sein. Insbesondere i. R. d. Bereitstellung von **vuIKT/ vaIKT** ist dies regelmäßig nicht der Fall, so dass hier im Regelfall **keine gemeinsame Verantwortung** vorliegt (s. (1)).

**(4)** Verantwortlich im Sinne des Datenschutzes ist die natürliche oder juristische Person, die über **„Zwecke und Mittel“** der Verarbeitung pbD entscheidet (siehe vertiefend EDSA Leitlinien 07/2020, Rn. 32 ff.)

- PbD dürften grundsätzlich nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (Art. 5 Abs. 1 lit. b DSGVO, **Grundsatz der Zweckbindung**).
- Im **öffentlichen Bereich** ist der Zweck der Verarbeitung regelmäßig durch die gesetzliche Beschreibung und Zuweisung v. a. einer konkreten Aufgabe festgelegt – die Adressatin dieser Zuweisung ist im Regelfall die Verantwortliche i. S. d. Art. 4 Nr. 7 DSGVO (siehe hierzu auch oben zur mittelbaren gesetzlichen Zuweisung der Verantwortlichkeit).

**(5) „der Verarbeitung von personenbezogenen Daten“**

- Die vom Verantwortlichen festgelegten Zwecke und Mittel müssen sich auf die „Verarbeitung von personenbezogenen Daten“ beziehen.
- die DSGVO definiert die Verarbeitung personenbezogener Daten als *„jede[n] Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten*“ (Art. 4 Abs. 2 DSGVO).
- Folglich kann der Begriff eines Verantwortlichen entweder mit einem einzigen Verarbeitungsvorgang oder mit einer Reihe von Vorgängen verknüpft werden.
- In der Praxis kann dies bedeuten, dass sich die Kontrolle durch eine bestimmte Organisation auf die gesamte fragliche Verarbeitung erstrecken, sich aber auch auf einen bestimmten Verarbeitungsschritt beschränken kann (siehe vertiefend EDSA Leitlinien 07/2020, Rn. 42 ff.).

## 3.3 Wer ist Auftragsverarbeiter, wer schließt die Auftragsverarbeitungsverträge?

Öffentliche Stellen setzen bei Digitalisierungsvorhaben, die mit einer Verarbeitung pbD verbunden sind, fast immer Auftragsverarbeiter ein. Vergleichbar zur Bestimmung der Verantwortlichkeit (→ siehe 3.2) bereitet auch die Bewertung, welche der beteiligten Stellen als Auftragsverarbeiter einzustufen sind, in der Praxis Schwierigkeiten. Insbesondere im Bereich der vaIKT und vuIKT ist dabei auch oft unklar, welche Stellen Auftragsverarbeitungsverträge miteinander abschließen müssen.

### 3.3.1 Abgrenzung Verantwortliche, Auftragsverarbeiter

Auftragsverarbeiter sind gem. **Art. 4 Nr. 8 DSGVO** natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten. Der EDSA erläutert, dass es sich bei einem Auftragsverarbeiter damit um eine **von der Verantwortlichen getrennte Stelle** handelt. Die Verantwortliche beschließt also, die Verarbeitungstätigkeiten ganz oder teilweise an eine **externe Organisation zu delegieren**.[12]

Die Verarbeitung pbD „im Auftrag" bedeutet dabei **im Interesse** und nach den **Weisungen** des Verantwortlichen, zumindest in Bezug auf den Zweck der Verarbeitung und die wesentlichen Elemente der Mittel (s. zum Verarbeitungsbegriff, oben unter **→ 3.1.2., S. 10**).[13]

In der Praxis sollen Auftragsverarbeiter aber regelmäßig über einen gewissen Handlungsspielraum verfügen und können einige Entscheidungen, insbesondere über „nicht wesentliche Mittel" der Verarbeitung, wie etwa die Wahl einer bestimmten Hard- oder Software oder detaillierte Sicherheitsmaßnahmen, treffen.[14]

Die **Rechtmäßigkeit der Verarbeitung** pbD durch den Auftragsverarbeiter i. S. d. Art. 6 Abs. 1 bzw. Art. 9 Abs. 2 DSGVO (→ siehe 3.4.3) leitet sich aus der Tätigkeit des Verantwortlichen ab. Der Auftragsverarbeiter ist insoweit Empfänger i. S. v. Art. 4 Nr. 9 DSGVO, nicht aber Dritter i. S. d. Art. 4 Nr. 10 DSGVO.

Ein Auftragsverarbeiter, darf die pbD **nicht zu eigenen Zwecken** verarbeiten. Bestimmt er über Zwecke und Mittel der Verarbeitung pbD, ist er als Verantwortlicher einzustufen (siehe hierzu ausdrücklich Art. 28 Abs. 10 DSGVO). Er haftet sodann vollumfänglich nach der DSGVO.

[12] Siehe EDSA Leitlinien 07/2020, Rn. 76
[13] Siehe EDSA Leitlinien 07/2020, Rn. 78.
[14] Siehe EDSA Leitlinien 07/2020, Rn. 37, 40.

### 3.3.2 Wirksamer Auftragsverarbeitungsvertrag

Art. 28 Abs. 3 DSGVO gibt vor, dass die Verarbeitung durch einen Auftragsverarbeiter auf der Grundlage eines **Vertrags** oder eines **anderen Rechtsinstruments** erfolgen muss. Andere Rechtsinstrumente könnten insbesondere im öffentlichen Bereich in Form von Verordnungen, Richtlinien oder formellen Gesetzen von Bedeutung sein. In der Praxis wird hiervon, soweit ersichtlich, bisher nur in Form ergänzender Regelungen Gebrauch gemacht (s. etwa § 80 Abs. 3 SGB X, § 1 Abs. 1 S. 2 AZRG). Andere Rechtsinstrumente müssten alle Vorgaben des Art. 28 Abs. 3 DSGVO enthalten.

🔔 **Hinweis:** Die IKT-Steuerung der Berliner Verwaltung hat im Dezember 2022 einen **Muster-Auftragsverarbeitungsvertrag** (siehe: https://b-intern.de/themen/digitalisierung/ikt-vertraege/artikel.1014105.php) (Muster-AVV) veröffentlicht, auf den i. R. v. Digitalisierungsvorhaben zurückgegriffen werden kann. Der Muster-AVV beruht dabei auf Standardvertragsklauseln der EU-Kommission und ist mit dem ITDZ und der BlnBDI abgestimmt.

### 3.3.3 Eignung des Auftragsverarbeiters

Gem. **Art. 28 Abs. 1 DSGVO** – dürfen Verantwortliche nur mit Auftragsverarbeitern zusammenarbeiten, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit der DSGVO erfolgt. **EG 81 DSGVO** betont darüber hinaus, dass Auftragsverarbeiters insbesondere über das erforderliche Fachwissen, die Zuverlässigkeit und Ressourcen verfügen müssen.

🔔 **Wichtig**: Ein Auftragsverarbeiter darf sich nicht vorbehalten, z. B. im Auftragsverarbeitungsvertrag (siehe dazu 3.3.2), die pbD auch **zu eigenen Zwecken**, beispielsweise zur Produktverbesserung oder Produktentwicklung, zu verarbeiten. Verarbeitet der Auftragsverarbeiter die pbD zu eigenen Zwecken ist er als Verantwortlicher einzustufen und benötigt eigene gesetzliche Befugnisse, die die Verarbeitung personenbezogener Daten erlauben (Art. 28 Abs. 10 DSGVO). Dies wird in der Praxis im öffentlichen Bereich jedoch nur selten der Fall sein.

Die Verantwortliche muss i. R. d. Art. 28 Abs. 1 DSGVO insbesondere auch sicherstellen, dass bei Inanspruchnahme von Anbietern außerhalb der EU die Vorgaben der DSGVO zur **Drittlandsübermittlung (Art. 44 ff DSGVO)** erfüllt werden (siehe dazu **4.3**).

Die Verantwortliche muss insbesondere hinsichtlich dieser Aspekte und der weiteren Vorgaben der DSGVO auch sicherstellen, dass der Auftragsverarbeiter nur **geeignete Unter-Auftragsverarbeiter** einbezieht (sieh hierzu auch Art. 28 Abs. 2, Abs. 3 lit. d und Abs. 4 DSGVO).

Hinsichtlich der Beauftragung von Anbietern in den Vereinigten Staaten von Amerika ist mittlerweile das **„EU-U.S. Data Privacy Framework“**[15] in Kraft getreten und kann unter den o. g. Voraussetzungen als Grundlage der Einbeziehung eines in den USA ansässigen Unternehmens als Auftragsverarbeiter dienen.

> **Wichtig:** Auch bei Beauftragung eines in der EU ansässigen Unternehmens als Auftragsverarbeiterin können die Art. 44 ff DSGVO einschlägig sein, sofern das Unternehmen eine **Tochter eines in einem Drittland ansässigen Konzerns** ist und so den Rechtsvorschriften eines Drittlands unterliegt.[16]

## 3.4 Ist die Verarbeitung personenbezogener Daten rechtmäßig?

Kommt die Prüfung nach Abschnitt 3.1 zu dem Ergebnis, dass mit dem geplanten Projektansatz eine Verarbeitung pbD verbunden ist, so muss sorgfältig geprüft werden, ob diese Verarbeitung rechtmäßig i. S. d. DSGVO wäre.

### 3.4.1 Prüfung

Eine Verarbeitung pbD ist dann rechtmäßig, wenn sich die Verantwortliche dabei auf eine Rechtsgrundlage i. S. d. **Art. 6 Abs. 1 DSGVO** stützen kann. Das bedeutet, dass die Verarbeitung pbD grundsätzlich untersagt ist, es sei denn es liegt einer der in Art. 6 Abs. 1 lit. a bis f DSGVO aufgeführten sog. Erlaubnistatbestände vor.

**Art. 6 Abs. 1 DSGVO enthält sechs Erlaubnistatbestände:**

Art. 6 Abs. 1 lit. a - **Einwilligung**

Art. 6 Abs. 1 lit. b - Erfüllung eines **Vertrags**

Art. 6 Abs. 1 lit. c - Erfüllung einer **rechtlichen Verpflichtung**

Art. 6 Abs. 1 lit. d - **lebenswichtige Interessen** der betroffenen Person

Art. 6 Abs. 1 lit. e - **Aufgabe im öffentlichen Interesse/ Ausübung öffentlicher Gewalt**

Art. 6 Abs. 1 lit. f – **berechtigte Interessen**

[15] Der Angemessenheitsbeschluss kann abgerufen werden unter: https://www.datenschutz-berlin.de/themen/unternehmen/internationaler-datenverkehr/.

[16] S. EDSA Leitlinien 5/2021 über das Zusammenspiel zwischen der Anwendung des Artikels 3 und der Bestimmungen über internationale Übermittlungen nach Kapitel V DSGVO, Version 2.0 v. 14. Februar 2023, Rn. 24; DSK Beschluss „Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten“ v. 31. Januar 2023.

🔔 **Wichtig:** Für öffentliche Stellen sind einige dieser Erlaubnistatbestände **nicht** oder **nur eingeschränkt anwendbar**:

➔ **Art. 6 Abs. 1 lit a DSGVO - Einwilligungen gegenüber öffentlichen Stellen**

Einwilligung müssen gem. **Art 4 Nr. 11 DSGVO** vor allem **freiwillig** erteilt werden. Laut **EG 43 S. 1 DSGVO** sollen Einwilligungen in dem besonderen Fall, dass zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern.

Hat eine betroffene Person gegenüber einer Behörde keine andere Wahl, als in die Verarbeitung ihrer pbD einzuwilligen – z. B. weil sie nur dann und nur von dieser zuständigen Behörde eine Verwaltungsleistung erhalten kann, so liegt keine ausreichende Freiwilligkeit der Einwilligung vor. Die Einwilligung ist damit unwirksam.

➔ **Art. 6 Abs. 1 lit. f DSGVO – berechtigtes Interesse bei öffentlichen Stellen**

Der Erlaubnistatbestand des Art. 6 Abs. 1 lit. f DSGVO **gilt nicht für** die von **Behörden** in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung pbD. Dies ergibt sich ausdrücklich aus **Art. 6 Abs. 1 S. 2 DSGVO**.

🔔 **Wichtig:** Besondere Bedeutung bei der Verarbeitung pbD durch öffentliche Stellen haben die Erlaubnistatbestände der **Art. 6 Abs. 1 lit. c und e DSGVO**. Danach ist die Verarbeitung dann rechtmäßig, wenn sie:

- *„zur Erfüllung einer rechtlichen Verpflichtung erforderlich [ist], der der Verantwortliche unterliegt“* (**Art. 6 Abs. 1 lit. c DSGVO**);
- *„für die Wahrnehmung einer Aufgabe erforderlich [ist], die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde“* (**Art. 6 Abs. 1 lit. e DSGVO**).

Auf Grundlage **der Öffnungsklausel in Art. 6 Abs. 3 S. 1 DSGVO** können die Rechtsgrundlagen nach diesen Normen auch im „Recht der Mitgliedstaaten“ festgelegt werden. Das bedeutet, dass hier vorrangig die besonderen **Datenschutzvorschriften des deutschen Rechts** zur Anwendung kommen (siehe dazu 3.4.4).

Diese Datenschutzvorschriften sind regelmäßig in den jeweiligen **Fachgesetzen des Bundes oder der Länder** für den jeweiligen Verwaltungsbereich geregelt. Im Berliner Landesrecht sind zudem in einigen Bereichen gesonderte Datenverarbeitungsvorschriften geschaffen worden.

Demnach muss bei der Einführung eines IT-Fachverfahrens zunächst die Datenverarbeitungsvorschriften des jeweiligen Fachrechts in den Blick genommen werden (z. B. des Sozialrechts, des Schulrechts oder des Polizeirechts).

### 3.4.2 Was bedeutet „Erforderlichkeit“?

Auf der Grundlage von § 6 Abs. 1 lit e, Abs. 3 DSGVO sind die in der obigen Übersicht genannten Rechtsgrundlagen regelmäßig so formuliert, dass die Verarbeitung der pbD für die Erfüllung der Aufgabe, die der Verantwortlichen übertragen wurde, „**erforderlich**“ sein muss.

Erforderlichkeit soll immer dann vorliegen, wenn die öffentliche Stelle aus einer **ex-ante Sicht** ihre jeweilige **Aufgabe ohne die Verarbeitung der pbD nicht, nicht vollständig oder nicht in rechtmäßiger oder zumutbarer Weise erfüllen kann**. Dabei muss beachtet werden, dass der mit der Verarbeitung pbD verbundene Eingriff in das Grundrecht auf Datenschutz und informationelle Selbstbestimmung auf das „**absolut Notwendige**“ beschränkt bleiben muss.

### 3.4.3 Rechtmäßigkeit der Verarbeitung durch Auftragsverarbeiter

Die Rechtmäßigkeit der Verarbeitung pbD durch den Auftragsverarbeiter i. S. d. Art. 6 Abs. 1 bzw. Art. 9 Abs. 2 DSGVO (→ siehe 3.3) leitet sich aus der Tätigkeit des Verantwortlichen ab. Der Auftragsverarbeiter darf lediglich in dem Rahmen, den die Verantwortliche vorgegeben hat, pbD verarbeiten.

🔔 **Wichtig**: Auftragsverarbeiter benötigen keine eigene Rechtsgrundlage für die Datenverarbeitung, da diese vollständig in der Verantwortung der beauftragenden Verantwortlichen liegt, die zu der Verarbeitung gesetzlich befugt sein muss. Besteht i. R. e. geplanten Digitalisierungsvorhabens für eine Verarbeitung pbD durch eine beteiligte interne oder externe Stelle **keine Rechtsgrundlage**, so kann diese nicht einfach dadurch **„geschaffen“ werden**, dass die Verarbeitung als Auftragsverarbeitung deklariert wird. Die Regelung über die Auftragsverarbeitung stellt keine Rechtsgrundlage für die Datenverarbeitung als solche dar.

### 3.4.4 Übersicht wichtiger Rechtsgrundlagen

Die nachfolgende Übersicht benennt einige der wichtigsten Datenschutzvorschriften der Fachgesetze des Bundes und des Landes Berlin:

| **Bundesnormen** |
|---|
| ➔ §§ 67 ff SGB X |
| ➔ §§ 86 ff AufenthG |
| ➔ §§ 7, 8 AsylG |
| ➔ §§ 61 ff. SGB VIII (Jugendhilfe) |
| ➔ §§ 2 Abs. 4, 3 ff BMG |
| ➔ § 21 iVm §§ 16, 17, 18 Passgesetz |
| ➔ §§ 14 ff. Personalausweisgesetz |
| ➔ § 24 Berliner Betriebegesetz |
| ➔ § 11 ff GWO |
| ➔ §§ 29b ff. AO |
| ➔ § 26 BDSG (siehe Landesnormen → § 18 BlnDSG) |

| **Landesnormen** |
|---|
| ➔ §§ 64 ff SchulG/ SchulDatVO |
| ➔ §§ 4a ff GDG |
| ➔ §§ 17, 18 ASOG |
| ➔ § 4a BezVG |
| ➔ §§ 24 ff KrankenhausG |
| ➔ § 6 ff. HochschulG |
| ➔ §§ 2 ff. KultDatenG |
| ➔ §§ 84, 85, 87 LandesbeamtenG |

| |
|---|
| ➔ §§ 1 ff. Stadtplanungsdatenverarbeitungsges |
| ➔ §§ 3 Abs. 1, 5 , 7 ArchGB |
| ➔ §§ 18, 55 Berliner Architekten- und Baukammergesetz |
| ➔ § 18 BlnDSG i. V. m. §§ 26 BDSG |

Neben diesen besonderen Datenschutzvorschriften existieren **allgemeine Datenverarbeitungsvorschriften** in den Bundes- und Landesdatenschutzgesetzen, die als Auffangklauseln dienen sollen. Im BlnDSG ist eine solche Generalklausel in § 3 geregelt (wichtig: § 3 BDSG ist daneben für die öffentlichen Stellen der Berliner Verwaltung nicht anwendbar).

**➔ § 3 BlnDSG:**

*„Außerhalb des Anwendungsbereichs der Richtlinie (EU) 2016/680 ist die nicht in besonderen Rechtsvorschriften geregelte Verarbeitung personenbezogener Daten zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist und*
*1. schutzwürdige Belange der betroffenen Personen wegen der Kategorien der personenbezogenen Daten, wegen der Zwecke der Verarbeitung, wegen der Dauer der Verarbeitung oder wegen ihrer Offenkundigkeit nicht entgegenstehen oder*
*2. Bundesrecht vollzogen wird und dieses die Verarbeitung personenbezogener Daten nicht abschließend regelt.“*

🔔 **Wichtig**: Die Generalklausel des **§ 3 BlnDSG** kann **nur in Ausnahmefällen** herangezogen werden, wenn **keine besonderen Rechtsvorschriften** zur Verarbeitung pbD dem Fachrecht existieren (siehe Tabelle oben). Zudem dürfen keine **schutzwürdigen Belange der betroffenen Personen**, insbesondere wegen der Kategorien der personenbezogenen Daten entgegenstehen. Aufgrund der Unbestimmtheit des § 3 BlnDSG können auf dieser Grundlage **keine besonderen Kategorien pbD i. S. d. Art. 9 Abs. 1 DSGVO** verarbeitet werden.

➔ **Informationsverarbeitungsgesetz (IVG)** – neben § 3 BlnDSG existiert weiterhin das IVG, das hinsichtlich seines Anwendungsbereichs teilweise nicht trennscharf von § 3 BlnDSG abgegrenzt werden kann.

## 3.5 Kann eine Rechtsgrundlage geschaffen werden?

Sofern die Prüfung unter **3.3** zu dem Ergebnis gelangt, dass **keine Rechtsgrundlage** für die i. R. d. Projektes geplante Verarbeitung pbD vorliegt, so sollte frühestmöglich geprüft werden, ob im Wege eines **Gesetzgebungsverfahrens** eine solche Rechtsgrundlage geschaffen werden kann.

Dazu müssen die folgenden Prüfungspunkte durchlaufen werden:

### 3.5.1 Keine besondere Rechtsvorschrift im Fachrecht?

Bereits i. R. d. Prüfung nach 6.1 muss zunächst festgestellt werden, dass nicht bereits eine spezielle Regelung zur Verarbeitung pbD im einschlägigen Fachrecht geschaffen worden ist. Dabei können auch Bundesnormen für die Berliner Landesverwaltung einschlägig sein, sofern diese Bundesgesetze vollziehen (siehe Übersicht unter 6.1.2).

Eine Legitimation der Verarbeitung pbD durch Einwilligungen ist im Regelfall keine zielführende Lösung. Zum einen können sich öffentliche Stellen nur bedingt auf Einwilligungen i. S. d. Art. 6 Abs. 1 lit. a, Art. 4 Nr. 11 DSGVO für die Verarbeitung pbD berufen (siehe 3.4.1). darüber hinaus sind das Einholen und Verwalten von Einwilligungen mit deutlich höherem Aufwand verbunden. Zudem sind Einwilligungen jeder Zeit widerrufbar (s. Art. 7 Abs. 3 S. 1 DSGVO).

### 3.5.2 Hat das Land Berlin die Gesetzgebungskompetenz?

Das Land Berlin hat eine Gesetzgebungskompetenz zum Datenschutz nur dort, wo der Bund weder von seiner ausschließlichen noch konkurrierenden Gesetzgebungskompetenz i. S. d. Art. 73 und 74 GG Gebrauch gemacht hat.

**Beispiel: Sozialgesetzbuch**

Für den Bereich des Sozialrechts fällt dem Bund die konkurrierende Gesetzgebungskompetenz gem. Art. 74 Abs. 1 Nr. 7 GG („Öffentliche Fürsorge“) zu.

Von dieser Gesetzgebungskompetenz hat der Bund u. a. auch durch das Sozialgesetzbuch Gebrauch gemacht. Das Land Berlin kann vor diesem Hintergrund auch nicht die v. a. in den §§ 67 ff. SGB X enthaltenen Regelungen zum Sozialdatenschutz ändern oder ergänzen.

Für Digitalisierungsvorhaben der Berliner Verwaltung, die auch den Bereich des Sozialrechts betreffen, können vor diesem Hintergrund **keine** neuen Rechtsgrundlagen geschaffen werden.

**Beispiel: Schule/ Hochschule**

Hinsichtlich dieses Bereiches besteht keine ausschließliche oder konkurrierende Gesetzgebungskompetenz i. S. d. Art. 73 und 74 GG. Gemäß Art. 70 Abs. 1 GG fällt die Gesetzgebungskompetenz damit den Ländern zu.

Für Digitalisierungsvorhaben im Schul- und Bildungsbereich **können** damit grundsätzlich unter den o. g. Voraussetzungen Rechtsgrundlagen für die Verarbeitung pbD geschaffen werden.

### 3.5.3 Sind die Vorgaben des Art. 6 Abs. 3 DSGVO erfüllt?

Die genauen Vorgaben zum Erlass einer Datenschutzvorschrift im nationalen Recht ergeben sich aus Art. 6 Abs. 3 DSGVO. Die konkrete Kompetenznorm ist dabei in Art. 6 Abs. 3 S. 3 DSGVO enthalten. Nähere Erläuterungen hierzu finden sich in auch in EG 45 DSGVO.

**(1) „Recht der Mitgliedstaaten“**

Der Begriff „Recht der Mitgliedstaaten“ in Art. 6 Abs. 3 S. 1 DSGVO ist weit auszulegen und muss **nicht nur Parlamentsgesetze** umfassen (s. EG 41 S. 1). Bund oder Länder können damit i. R. ihrer Gesetzgebungskompetenz auch in anderen Gesetzen im materiellen Sinn wie z. B. **Rechtsverordnungen**, **Tarifverträgen** oder **kommunalen Satzungen** Rechtsgrundlagen für die Verarbeitung pbD schaffen. Diese müssen jedoch klar und präzise sein und ihre Anwendung sollte für die Rechtsunterworfenen vorhersehbar sein (vgl. EG 41 S. 2 DSGVO). Diesen Anforderungen genügen reine Verwaltungsvorschriften nicht.

**„Zweck der Verarbeitung in der Rechtsgrundlage festgelegt“**

Art. 6 Abs. 3 S. 2 DSGVO schreibt vor, dass der Zweck der Verarbeitung in der Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gem. Art. 6 Abs. 1 lit. e DSGVO für die Erfüllung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

**(2) Spezifische und spezifischere Bestimmungen**

Gem. Art. 6 Abs. 3 S. 3 DSGVO kann die Rechtsgrundlage spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften der DSGVO enthalten, die sodann beispielhaft aufgeführt werden (u. a. Bestimmungen über allgemeine Bedingungen für die Rechtmäßigkeit der Verarbeitung, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen, welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen).

Art. 6 Abs. 2 DSGVO stellt ergänzend klar, dass die Mitgliedstaaten i. R. von Art. 6 Abs. 1 lit c. und e DSGVO „spezifischere Bestimmungen [...] zur Anpassung der Anwendung der DSGVO beibehalten oder einführen dürfen.

**(3) Grenzen der Rechtsetzungsbefugnis**

Grundsätzlich dürfen die nach Art. 6 Abs. 3 DSGVO erlassenen spezifischeren Vorschriften das Schutzniveau der DSGVO nicht unterschreiten, außer es sind konkrete Ausnahmetatbestände, wie v. a. in Art. 23 DSGVO, formuliert.

## 3.6 Rechtmäßige Datenübermittlung in ein Drittland?

Typischerweise stellt sich auch in öffentlichen Digitalisierungsvorhaben die Frage, inwieweit Angebote von Unternehmen einbezogen werden können, die ihren Sitz nicht innerhalb der EU haben. Sollen diese pbD verarbeiten, beispielsweise i. R. e. Auftragsverarbeitung (siehe dazu 3.3)., so sind die Voraussetzungen gem. **Art. 44 ff DSGVO** zu beachten.

Gem. Art. 44 ff DSGVO dürfen pbD nur dann an sog. **„Drittländer“**, d. h. Länder außerhalb der EU oder des Europäischen Wirtschaftsraums (EWR) (s. EDSA Guidelines 05/2021, Version 2.0, Rn. 22 ff), übermittelt werden, wenn ein besonderer Erlaubnisgrund der Art. 44 ff DSGVO vorliegt.[17]

Besondere Bedeutung kommt dabei **Art. 45 DSGVO** zu, auf dessen Grundlage die EU-Kommission beschließen kann, dass ein bestimmtes Drittland ein angemessenes Schutzniveau bietet (sog. **Angemessenheitsbeschluss**). Die EU-Kommission hat eine **Liste der Angemessenheitsbeschlüsse**[18] veröffentlicht.

[17] Siehe https://www.datenschutz-berlin.de/themen/unternehmen/internationaler-datenverkehr
[18] Siehe https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

🔔 **Wichtig:** Die Europäische Kommission hat am 10. Juli 2023 einen Angemessenheitsbeschluss gem. Art. 45 DSGVO für das **„EU-U.S. Data Privacy Framework“** angenommen. Auf dieser Grundlage können nun Datenübermittlungen an zertifizierte Organisationen in den USA erfolgen, z. B. als Auftragsverarbeitung. Hier muss aber **genau geprüft** werden:

**(1)** Ist die geplante Verarbeitung pbD (in der EU) **rechtmäßig** (siehe unter **3.4**)?

**(2)** Ist das **Unternehmen/ die Organisation** unter dem „EU-U.S. Data Privacy Framework“ **freiwillig zertifiziert** (siehe hierzu die öffentliche **Liste**[19] des US-Handelsministeriums)?

→ **Achtung**: Die Zertifizierung nach dem Privacy Framework unterscheidet in „hr data“ (Beschäftigtendaten) und „non hr data“. Sollen auch **Beschäftigtendaten** übermittelt werden so muss auch eine entsprechende **Zertifizierung für „hr data“** vorliegen.

Sofern **kein Angemessenheitsbeschluss** i. S. d. Art. 45 DGSVO für ein Drittland vorliegt, in das pbD übermittelt werden sollen, sind die weiteren Möglichkeiten zu prüfen, siehe hierzu die Hinweise aus der Website der BlnBDI.[20]

## 3.7 Können die Betroffenenrechte umgesetzt werden?

Ein weiteres typisches Datenschutzrisiko ist, dass nach der Umsetzung von Projekten, die mit der Verarbeitung von pbD verbunden sind, die **Betroffenenrechte der DSGVO** nicht oder nicht rechtzeitig umgesetzt werden können. Das bedeutet, dass z. B. ein Auskunftsbegehren nach Art. 15 DSGVO nicht rechtzeitig erfüllt oder ein Antrag auf Löschung der pbD nach Art. 17 DSGVO nicht umgesetzt werden kann.

In der Praxis wird oft übersehen, dass auch die **Verfahrensvorgaben** für die Ausübung der Betroffenenrechte aus **Art. 12 DSGVO** zu erfüllen sind.

🔔 **Wichtig:** Die Erfüllung der Datenschutzvorhaben zu den Betroffenenrechten nach den Art. 12 ff DSGVO sind **allgemeine Datenschutzvorgaben**, die nicht erst im Zusammenhang mit Digitalisierungsvorhaben zu erfüllen sind. Jede öffentliche Stelle, die pbD verarbeitet, muss gewährleisten, dass sie die Art. 12 ff DSGVO jederzeit und vollumfänglich erfüllen kann. Jede Behörde bzw. öffentliche Stelle sollte vor diesem Hintergrund ein allgemeines **Betroffenenrechtekonzept** erstellen, da in vielen öffentlichen Bereichen auch wichtige Ausnahmen greifen. Digitalisierungsprojekte sind sodann nur noch darauf zu überprüfen, ob neue Risiken für die Umsetzung der Betroffenenrechte entstehen, die nicht bereits durch das Betroffenenrechtekonzept beseitigt werden.

[19] Siehe: https://www.dataprivacyframework.gov/s/participant-search

[20] Siehe: https://www.datenschutz-berlin.de/themen/unternehmen/internationaler-datenverkehr/#c1814

### 3.7.1 Übersicht Betroffenenrechte der DSGVO

| | |
|---|---|
| Art. 13 | Informationspflicht (Erhebung bei der betroffenen Person) |
| Art. 14 | Informationspflicht (Erhebung nicht bei der betroffenen Person) |
| Art. 15 | Auskunftsrecht |
| Art. 16 | Recht auf Berichtigung |
| Art. 17 | Recht auf Löschung |
| Art. 18 | Recht auf Einschränkung der Verarbeitung |
| Art. 21 | Widerspruchsrecht |

### 3.7.2 Typische Risiken für die Umsetzung von Betroffenenrechten

Nachfolgend sind einige allgemeine und typische Risiken, im Zusammenhang mit Digitalisierungsvorhaben genannt.

#### *3.7.2.1 Unklarheiten zur Verantwortlichkeit*

Bei öffentlichen Digitalisierungsvorhaben ergeben sich oft bereits daraus Risiken für die Betroffenenrechte, weil unklar ist, welche der beteiligten Stellen die **datenschutzrechtliche Verantwortung** trägt und damit auch für die Erfüllung der Betroffenenrechte zu sorgen hat.

Eine klare Bestimmung der Verantwortlichen ist daher notwendig (siehe dazu → **3.2**).

Im Fall einer **gemeinsamen Verantwortung** i. S. d. Art. 26 DSGOV muss u. a. auch die Umsetzung der Betroffenenrechte in der nach Art. 26 Abs. 1 S. 2 DSGVO zu erstellender Vereinbarung genau geregelt werden.

#### *3.7.2.2 Umsetzbarkeit des Rechts auf Löschung, Art. 17 DSGVO*

Führt ein verfolgter Projektansatz dazu, dass pbD verarbeitet werden, so muss sichergestellt sein, dass die pbD auch stets wieder gelöscht werden können. Das gilt insbesondere bei der Nutzung von neueren Technologien, wie z. B. der Blockchain-/ Distributed-Ledger-Technologie.

Betroffene Personen können gegenüber der verantwortlichen öffentlichen Stelle gemäß Art. 17 Abs. 1 DSGVO ein Recht auf Löschung ihrer pbD geltend machen. Das bedeutet, dass die Verantwortliche auch gegenüber möglichen Auftragsverarbeitern sicherstellen muss, dass diese Löschung der pbd v. a. auch technisch möglich ist.

🔔 **Wichtig:** Betroffene Personen haben gem. Art. 17 Abs. 1 lit. a DSGVO vor allem dann ein **Recht auf Löschung ihrer pbD,** wenn diese für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, **nicht mehr notwendig sind.** Öffentliche Stellen müssen damit gerade bei Digitalisierungsvorhaben sicherstellen, dass pbD dann auch gelöscht werden können.

Betroffenen Personen steht, sofern eine Verarbeitung ausnahmsweise auf eine Einwilligung gestützt wird, auch bei **Widerruf ihrer Einwilligungen** i. S. d. Art. 6 Abs. 1 lit. a DSGVO ein Recht auf Löschung zu (Art. 17 Abs. 1 lit. b DSGVO); soweit eine Verarbeitung also auf diese Rechtsgrundlage gestützt werden soll, muss besonders auf die Umsetzbarkeit des Rechts auf Löschung geachtet werden.

🔔 **Wichtig:** Insbesondere die Erfüllung des Rechts auf Löschung aus Art. 17 DSGVO ist eine allgemeine Vorgabe des Datenschutzes, mit der sich jede öffentliche Stelle, die pbD verarbeitet, beschäftigen muss. Sinnvoll erscheint die Erstellung eines allgemeinen **Löschkonzeptes** (ggf. als Teil des Betroffenenrechtekonzepts, s. o.). Digitalisierungsvorhaben führen regelmäßig zu zusätzlichen Risiken für das Recht auf Löschung. Allgemeine **Ausnahmetatbestände** (s. hierzu v.a. Art. 17 Abs. 3 DSGVO; § 83 SGB X; § 24 BlnDSG), die für viele Behörden in der Praxis sehr wichtig sind, sollten aber in einem allgemeinen Konzept niedergelegt sein.

#### *3.7.2.3 Fristgerechte Antragsbearbeitung (Art. 12 Abs. 3 DSGVO)*

In der Praxis vieler Behörden treten Datenschutzverletzungen oftmals in Verbindung mit Art. 12 DSGVO auf, insbesondere weil die **Frist aus Art. 12 Abs. 3 S. 1 DSGVO** nicht eingehalten wird.

Digitalisierungsvorhaben, die auf die Verarbeitung pbD hinauslaufen, müssen von Anfang an so geplant werden, dass möglichst schon durch technische Funktionen gewährleistet werden kann, dass der Anspruch betroffener Personen nach Art. 15 bis 21 DSGVO erfüllt werden kann.

#### *3.7.2.4 Unterstützungspflicht (Art. 12 Abs. 2 S. 1) & Unentgeltlichkeit (Art. 12 Abs. 5 S. 1 DSGVO)*

Digitalisierungsvorhaben müssen von Anfang an so geplant und IT-Systeme so entwickelt werden (siehe hierzu auch Art. 24 DSGVO), dass die Wahrnehmung der Betroffenenrechte nicht erschwert wird. Der Verantwortliche muss den Betroffenen die Ausübung ihrer Rechte sogar ausdrücklich erleichtern. Diese Vorgabe der DSGVO muss auch i. R. d. Vergabe und bei der Inanspruchnahme von Dienstleistern und Auftragsverarbeitern berücksichtig werden.

Projekte der Verwaltungsdigitalisierung dürfen nicht dazu führen, dass für die Ausübung der Betroffenenrechte der DSGVO Kosten entstehen. Dies muss i. R. d. Vergabe und bei der Inanspruchnahme von Dienstleistern und Auftragsverarbeitern berücksichtig werden.

#### *3.7.2.5 Betroffenenrechte in Systementwicklung und Systembetrieb*

IT-Systeme müssen i. R. v. Digitalisierungsvorhaben so entwickelt und später betrieben werden können, dass die Betroffenenrechte i. S. d. Art. 12 ff. DSGVO, insbesondere unter Berücksichtigung der o. g. Aspekte, umgesetzt werden können (siehe hierzu auch Art. 24 DSGVO „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung“).

Entsprechend müssen diese Aspekte auch im Rahmen der Beschaffung und Vergabe berücksichtigt werden (siehe dazu → **Handreichung II**).

## 3.8 Kann die Sicherheit der Verarbeitung gewährleistet werden?

Schließlich muss in Digitalisierungsvorgaben, die mit einer Verarbeitung pbD verbunden sind, die **Sicherheit dieser Verarbeitung** gewährleistet werden. Die DSGVO definiert eine Verletzung des Schutzes pbD als Verletzung der Sicherheit, die „ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“ (**Art. 4 Nr. 12 DSGVO**).

Konkret verpflichten die Vorgaben des **technischen Datenschutzes** die Verantwortlichen und Auftragsverarbeiter, durch geeignete technische und organisatorische Maßnahmen (TOMs) sicherzustellen und den Nachweis dafür zu erbringen, dass eine Verarbeitung pbD gemäß der DSGVO erfolgt (**Art. 24 DSGVO**). Diese Vorgabe wird insbesondere durch **Art. 32 DSGVO** konkretisiert, der Verantwortliche und den Auftragsverarbeiter dazu verpflichtet, geeignete TOMs zur Gewährleistung eines angemessenen Schutzniveaus umzusetzen. Ergänzend richten sich die Vorgaben des **Art. 25 DSGVO** zu Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen auf den Zeitpunkt der Wahl der Mittel der Verarbeitung.

Die Beurteilung, welche TOMs konkret ergriffen werden müssen, knüpft an das **Risiko für die Rechte und Freiheiten der Betroffenen** an, das bei der Verarbeitung der pbD entsteht. Hinsichtlich dieses Risikos muss ein angemessenes Schutzniveau gewährleistet werden.

Die Umsetzung dieser Normen durch Bestimmung des Risikos einer Verarbeitung pbD stellt aufgrund der komplexen rechtlichen Vorgaben und des erforderlichen technischen Sachverstands in der Praxis eine Herausforderung für die Verwaltung dar. Zusätzlich sind in der Frühphase von Digitalisierungsvorhaben häufig noch viele insbesondere technische Umsetzungsfragen offen, so dass auch die näheren Umstände der Verarbeitung nach o. g. Normen ausdrücklich in die Auswahl der geeigneten TOMs einfließen muss. Gleichzeitig können aber besondere Anforderungen an die Sicherheit der Verarbeitung, die zu spät Berücksichtigung in der Projektplanung und -umsetzung finden, ein späteres Umsetzungshindernis für das gesamte Projekt darstellen.

Vor diesem Hintergrund empfiehlt es sich hinsichtlich der i. R. e. Digitalisierungsprojekt geplanten Verarbeitung pbD schon bei der Projektumfeldanalyse und Machbarkeitsprüfung bereits eine überschlagende Risikoprüfung vorzunehmen, die sich an den nachfolgenden Prüffragen orientieren kann. Regelmäßig kann dabei zumindest bereits festgestellt werden, ob höchstwahrscheinlich ein hohes Datenschutzrisiko entsteht.

### 3.8.1 Was ist ein Risiko i. S. d. Datenschutzes?

Es ist sinnvoll zunächst ein Grundverständnis dafür zu entwickeln, was ein Risiko i. S. d. Datenschutzes ist.

**Definition Risiko**: Ein Risiko im Sinne der DSGVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann. Es hat zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.[21]

Gemäß EG 75 DSGVO zählen zu den möglichen Schäden physische, materielle und immaterielle Schäden. Ungerechtfertigte Beeinträchtigungen der Rechte und Freiheiten von natürlichen Personen (Grundrechtsverletzungen) sind unter die immateriellen Schäden zu fassen.[22]

Risiken i. S. d. DSGVO beziehen sich auf den weiten Begriff der „Rechte und Freiheiten natürlicher Personen“, sind also ausdrücklich nicht nur auf direkte Verletzungen des Grundrechts auf

[21] Siehe DSK Kurzpapier Nr. 18, S. 1.: https://www.datenschutz-berlin.de/infothek/publikationen-der-dsk/kurzpapiere/
[22] Ebenda.

Schutz der pbD bzw. der informationellen Selbstbestimmung i. S. d. Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 2 GG begrenzt.

**Rechte und Freiheiten natürlicher Personen:** Dieser zentrale Begriff der DSGVO bezieht sich auf die Grundrechte und Grundfreiheiten nach der Grundrechtecharta (GrCh) der EU und der Europäischen Menschenrechtskonvention, insbesondere auf das Grundrecht auf Schutz der pbD gem. Art. 8 GrCh. Umfasst sind aber auch alle Grundrechte, die durch das Datenschutzrecht zumindest mittelbar geschützt werden.[23]

Die DSGVO verwendet die Unterscheidungen **„Risiko"** und **„hohes Risiko"** (z. B. **EG 76 DSGVO**) und nutzt an anderer Stelle die Formulierung „voraussichtlich nicht zu einem Risiko" führend (Art. 27 Abs. 2 lit. a und Art. 33 Abs. 1 DSGVO). Da es vollständig risikolose Verarbeitungen nicht geben kann, wird die Formulierung „nicht zu einem Risiko" von ihrem Sinn und Zweck ausgehend als „nur zu einem geringen Risiko" führend verstanden.

🔔 **Wichtig:** Auch nach Auslegung der Datenschutzaufsichtsbehörden geht die DSGVO von **drei Risikoabstufungen** aus:[24]
**→„geringes Risiko"**
**→„Risiko"**
**→„hohes Risiko"**

Im Unterschied zum allgemeinen Risikomanagement und auch zum Risikomanagement in der Informationssicherheit verpflichten die o. g. Normen der DSGVO die Verantwortlichen dazu, die im Zusammenhang mit der Verarbeitung pbD entstehenden Risiken mit geeigneten und angemessenen TOMs auf ein angemessenes Schutzniveau zu reduzieren. Es ist nach der DSGVO nicht zulässig, hierauf zu verzichten oder die aus der Verarbeitung pbD resultierenden Risiken einfach in Kauf zu nehmen.[25]

🔔 **Wichtig** Die aus dem Bereich der Informationssicherheit bekannten Instrumente der **Risikoakzeptanz** oder des **Risikotransfers** stehen im datenschutzrechtlichen Kontext dem Verantwortlichen **nicht zur Verfügung**.[26]

[23] Ebenda.
[24] Ebenda.
[25] Vgl. SDM, D 3.1, S. 50. Das SDM ist abrufbar unter: https://www.datenschutzzentrum.de/sdm/.
[26] Ebenda.

### 3.8.2 Entsteht bei der geplanten Verarbeitung pbD ein hohes Risiko?

Es empfiehlt sich, bereits i. R. d. Projektumfeldanalyse bzw. Machbarkeitsprüfung mögliche hohe Risiken i. S. d. Datenschutzes in den Blick zu nehmen. Dabei sollten zunächst geprüft werden, ob eines oder mehrere der folgenden bereits festgelegten **Regelbeispiele für hohe Datenschutzrisiken** einschlägig sind, so dass eine komplexe datenschutzrechtliche Prüfung zunächst entbehrlich ist.

#### *3.8.2.1 Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DSGVO („Blacklist" der BlnBDI)*

Entstehen bei einer Verarbeitung pbD hohe Risiken i. S. d. Datenschutzes, so ist gem. Art. 35 DSGVO eine Datenschutzfolgenabschätzung (DSFA) durchzuführen (siehe → **Handreichung III**, Anlage 2). Gemäß Art. 35 Abs. 4 DSGVO kann die **zuständige Aufsichtsbehörde** eine **Liste von Verarbeitungsvorgängen** veröffentlichen, für die eine **DSFA** durchzuführen ist.

Wird im Zusammenhang mit einem Digitalisierungsvorhaben festgestellt, dass dabei pbD verarbeitet werden, so ist frühestmöglich zu prüfen, ob diese Verarbeitung einen der nachgenannten Regelfälle der **„Blacklist" der BlnBDI**[27] enthält:

| **Maßgebliche Definition** |
|---|
| Die umfangreiche Verarbeitung von Daten, die dem *Sozial-*, einem *Berufs-* oder *besonderen Amtsgeheimnis* unterliegen, auch wenn es sich nicht um Daten gemäß Art. 9 Abs. 1 und 10 DS-GVO handelt |
| Die Verarbeitung von Daten gemäß Art. 9 Abs. 1 und 10 DS-GVO und von anderen Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen, soweit sie<br>- durch verschiedene Stellen unter gemeinsamer Verantwortung gemäß Art. 26 DS-GVO erfolgt,<br>- die Übermittlung derartiger Daten auf automatisierten Abruf seitens einer anderen Stelle involviert oder<br>- einem anderen Zweck als demjenigen dient, zu dem die Daten erhoben wurden |
| Die Verarbeitung von Daten gemäß Art. 9 Abs. 1 und 10 DS-GVO und von anderen Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen, durch Auftragsverarbeiter, denen von einem Gericht oder einer Verwaltungsbehörde eines Drittlands die Pflicht auferlegt werden kann, diese Daten entgegen Art. 48 DS-GVO zu exportieren oder offenzulegen |

[27] Siehe https://www.datenschutz-berlin.de/themen/unternehmen/datenschutz-folgenabschaetzung/

| |
|---|
| Die Datenverarbeitung der Personenstands- und Melderegister sowie anderer Stellen, die Daten aus diesen Registern in großem Umfang, Meldedaten mit Sperrvermerken gemäß § 51 Abs. 1 und 5 Bundesmeldegesetz oder Personenstandsdaten gemäß § 63 Personenstandsgesetz verarbeiten |
| Die umfangreiche Verarbeitung von Daten über Kinder |
| Die umfangreiche Verarbeitung von Daten über den Aufenthaltsort von Personen |
| Die Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Weiterverarbeitung der so zusammengeführten Daten, sofern<br>- die Zusammenführung oder Weiterverarbeitung in großem Umfang vorgenommen werden,<br>- für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den Betroffenen erhoben wurden,<br>- die Anwendung von Algorithmen einschließen, die für die Betroffenen nicht nachvollziehbar sind, und<br>- der Erzeugung von Datengrundlagen dienen, die dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den betroffenen Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen können |
| Die Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Weiterverarbeitung der so zusammengeführten Daten, sofern<br>- die Zusammenführung oder Weiterverarbeitung in großem Umfang vorgenommen werden,<br>- für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den Betroffenen erhoben wurden,<br>- die Anwendung von Algorithmen einschließen, die für die Betroffenen nicht nachvollziehbar sind, und<br>- der Entdeckung vorher unbekannter Zusammenhänge zwischen den Daten für nicht im<br>- Vorhinein bestimmte Zwecke dienen |
| Die Erfassung und Veröffentlichung von Daten, die zur Bewertung des Verhaltens und anderer persönlicher Aspekte von Personen dienen und von Dritten dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den bewerteten Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen |

| |
|---|
| Die Verarbeitung von umfangreichen Angaben über das Verhalten von *Beschäftigten*, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben, oder diese in andere Weise erheblich beeinträchtigen |
| Die Verarbeitung von Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO - auch wenn sie nicht als „umfangreich“ im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist - sofern die Daten dazu verwendet werden, die Leistungsfähigkeit von *Beschäftigten* zu bestimmen |
| Der Einsatz von *künstlicher Intelligenz* zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der Betroffenen |
| Die mobile und für die Betroffenen intransparente *optoelektronische Erfassung* öffentlicher Bereiche |
| Die Nutzung von Sensoren eines *Mobilfunkgeräts* im Besitz der Betroffenen oder von Funksignalen, die von solchen Geräten versandt werden, zur *Bestimmung des Aufenthaltsorts* oder der Bewegung von Personen über einen substantiellen Zeitraum und nachfolgende zentralisierte Verarbeitung der resultierenden Angaben |
| Die umfangreiche Erhebung personenbezogener Daten über Schnittstellen *persönlicher elektronischer Geräte*, die nicht gegen ein unbefugtes Auslesen geschützt sind, soweit diese Erhebung für die Betroffenen nicht erkennbar ist |
| Die automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung der Persönlichkeit der Betroffenen |

#### *3.8.2.2 Regelfälle des Art. 35 Abs. 3 DSGVO*

Darüber hinaus muss geprüft werden, ob bereits absehbar ist, dass die geplante Verarbeitung pbD einen der folgenden Regelfälle des **Art. 35 Abs. 3 DSGVO** erfüllt:

a. systematische und umfassende **Bewertung persönlicher Aspekte** natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich **Profiling** gründet und die ihrerseits als Grundlage für **Entscheidungen** dient, die **Rechtswirkung** gegenüber natürlichen Personen **entfalten** oder diese in ähnlich erheblicher Weise beeinträchtigen;

b. **umfangreiche** Verarbeitung **besonderer Kategorien von personenbezogenen Daten** gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

c. systematische **umfangreiche Überwachung öffentlich zugänglicher Bereiche**.

🔔 **Wichtig:** In der Praxis muss insbesondere der Fall des **Art. 35 Abs. 3 lit b DSGVO** beachtet werden. Zwar wird hier nicht genau beziffert, was eine **„umfangreiche"** Verarbeitung von pbD i. S. d. Art. 9 Abs. 1 DSGVO ist.[28] Einige Behörden verarbeiten aber bereits aufgrund ihres jeweiligen Aufgabenbereichs pbD i. S. d. Art. 9 Abs. 1 DSGVO in großem Umfang, wie **z. B. Sozial-, Gesundheits- und Jugendämter**. Sind solche Behörden in ein Digitalisierungsvorhaben, insbesondere im Bereich der vuIKT, einbezogen (z. B. die Einführung der E-Akte) so kann davon auszugehen sein, dass eine umfangreiche Verarbeitung pbD i. S. d. Art. 9 Abs. 1 DSGVO zu bejahen ist.

Auch Art. 35 Abs. 3 lit c DSGVO kann für öffentliche Digitalisierungsvorhaben relevant sein. Mit der hier erwähnten Überwachung öffentlich zugänglicher Bereiche ist die in der DSGVO nicht spezifisch geregelte **Audio- und Videoüberwachung** gemeint.[29] Die im Erwägungsgrund genannte optoelektronische Erfassung öffentlicher Bereiche ist speziell in der „Blacklist" der BlnBDI erwähnt (siehe unter 3.8.2.1).

Unter **„Profiling"** i. S. d. Art. 35 Abs. 3 lit. a DSGVO versteht die DSGVO: jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen (**Art. 4 Nr. 4 DSGVO**).

#### *3.8.2.3 Liste des EDSA, Working Paper 248*

Schließlich kann geprüft werden, ob die geplante Verarbeitungstätigkeit Kriterien erfüllt, die der EDSA in seiner **Auflistung zu Verarbeitungsvorgängen mit „voraussichtlich hohem Risiko"** im **Working Paper 248 rev. 01** aufführt.[30] Liegen mindestens zwei dieser Kriterien vor, soll ein in den meisten Fällen ein voraussichtlich hohes Risiko bestehen:

1. Bewerten oder Einstufen (Scoring) („Evaluation or scoring")
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung („Automated-decicion making with legal or similar significant effect")
3. Systematische Überwachung („Systematic monitoring")

[28] EG 91, S. 1 deutet darauf hin, dass neben der Menge der verarbeiteten Daten insbesondere auf die Anzahl der betroffenen Personen sowie auf die geographische Reichweite relevant sind.
[29] EG 91 S. 3 spricht technikneutral von einer Überwachung „mittels optoelektronischer Vorrichtungen".
[30] Siehe EDSA, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" v. 4. April 2017; siehe auch den Verweis im SDM, D 3.2.2, S. 53. Alle Leitlinien des EDSA können abgerufen werden auf: https://www.datenschutz-berlin.de/infothek/leitlinien-des-edsa/

4. Vertrauliche Daten oder höchst persönliche Daten („Sensitive data or data of a highly personal nature“)
5. Datenverarbeitung in großem Umfang („Data processed in a large scale“)
6. Abgleichen oder Zusammenführen von Datensätzen („Matching or combining datasets“)
7. Daten zu schutzbedürftigen Betroffenen (Data concerning vulnerable data subjects“)
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen („Innovative use or applying new technological or organisational solutions“)
9. Betroffene werden an der Ausübung ihres Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrages gehindert („When the processing in itself prevents data subjects from exercising a right or using a service or a contract“)

Diese allgemein gehaltenen Kriterien werden weitestgehend durch speziellere Fallkonstellationen in der „Blacklist“ der BlnBDI und den Regelbeispielen des Art. 35 Abs. 3 DSGVO aufgegriffen.

### 3.8.3 Voraussichtlicher Schutzbedarf

Auf Grundlage der Risikoprognose muss der voraussichtliche Schutzbedarf der Betroffenen und die dazu umzusetzenden TOMs bestimmt werden. Das SDM[31] bestimmt für die verschiedenen Risikostufen den folgenden Schutzbedarf:

- ➔ kein oder geringes Risiko der Verarbeitung = normaler Schutzbedarf für von der Verarbeitung betroffene Personen
- ➔ normales Risiko der Verarbeitung = normaler Schutzbedarf für von der Verarbeitung betroffene Personen
- ➔ hohes Risiko der Verarbeitung = hoher Schutzbedarf für von der Verarbeitung betroffene Personen

Wird i. R. d. Projektumfeldanalyse und Machbarkeitsprüfung festgestellt, dass - vorbehaltlich einer eingehenden Risikoanalyse in der Planungs- und Durchführungsphase (siehe ➔ **PPS 24 und 25, Handreichung III**) - voraussichtlich:

- ➔ kein hohes Risiko entsteht, so sind lediglich TOMs für einen **normalen Schutzbedarf** zu planen;
- ➔ ein hohes Risiko entsteht, so müssen TOMs für **einen hohen Schutzbedarf** geplant werden.

[31] Abrufbar unter: https://www.datenschutzzentrum.de/sdm/.

### 3.8.4 Auswahl der TOMs

Für einen **normalen Schutzbedarf** empfiehlt sich, auf die „generischen Maßnahmen“ des SDM zurückzugreifen.[32]

Für einen **hohen Schutzbedarf** ergibt sich aus dem SDM eine standardisierte Strategie zur wirksamen Minderung der Risiken.[33] Für die Definitions- und Planungsphase bietet sich hier aber bereits eine vertieftere Beschäftigung mit den möglicherweise zu ergreifenden TOMs an.

🔔 **Wichtig:** Entsteht bei einem Digitalisierungsvorhaben voraussichtlich ein **hohes Risiko** durch die damit verbundene Verarbeitung pbD, z. B. beim Einsatz neuer Technologien wie KI (siehe dazu BlnBDI „Blacklist“), so sind **TOMs für einen hohen Schutzbedarf** umzusetzen. Dies kann, u. a., zu höheren Kosten führen und muss der Projekt- und Behördenleitung zur Kenntnis gebracht werden. Können die erforderlichen TOM i. R. d. Durchführungsphase des Projekts nicht umgesetzt werden, so verstößt die damit verbundene Verarbeitung pbD gegen die DSGVO. Das Projekt kann dann u. U. nicht umgesetzt werden.

### 3.8.5 Datenschutz und Informationssicherheit

Neben den spezifischen Datenschutzrisiken sind im Zusammenhang mit Digitalisierungsvorhaben auch die Risiken der Informationssicherheit zu betrachten. Im Regelfall richtet sich diese Betrachtung nach der IT-Grundschutz-Methodik des BSI und erfolgt ebenfalls in Form einer Schutzbedarfsfeststellung.[34] Ziel der Schutzbedarfsfeststellung aus Sicht der Informationssicherheit ist dabei die Ermittlung des für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik angemessenen Schutzes und der entsprechend erforderlichen TOMs.[35]

Wesentliche Aspekte von Grundschutz-Maßnahmen sind auch Voraussetzungen für einen wirksamen Datenschutz, wie z. B. die Herstellung eines geordneten Betriebs, die Sicherstellung der Verfügbarkeit und Integrität der Daten, Systeme und Dienste sowie die Verhinderung eines unbefugten Zugriffs auf Geschäfts-, Produktions- und Personendaten, also die Sicherstellung der Vertraulichkeit.[36] Auch methodisch ist Datenschutz in die Risikoanalyse aus Sicht der Informationssicherheit einzubeziehen, indem insbesondere i. R. d. Schutzbedarfsfeststellung auch das typische

[32] Siehe SDM, D1.
[33] Siehe SDM D.3.4., S. 56.
[34] Siehe BSI-Standard 200-1 (Managementsysteme für Informationssicherheit [ISMS]), 200-2 (IT-Grundschutz-Methodik) und 200-3 (Risikomanagement) sowie das IT-Grundschutz-Kompendium.
[35] Vgl. BSI-Standard 200-2 (IT-Grundschutz-Methodik), 7.5 und 8.2.
[36] Siehe dazu SDM, D 3.2.2, S. 53.

Schadensszenarium „Beeinträchtigung des informationellen Selbstbestimmungsrechts“ zu berücksichtigen ist.[37]

Vor diesem Hintergrund können TOMs, die i. R. e. Digitalisierungsvorhabens bereits aus Sicht der Informationssicherheit bzw. des IT-Grundschutzes erforderlich sind, auch zur Gewährleistung eines angemessenen Datenschutzes relevant sein. Mögliche „Synergien“ zwischen Datenschutz und Informationssicherheit sollten frühestmöglich i. R. d. Projektplanung in den Blick genommen werden.

Die **Risikoanalyse aus Sicht der Informationssicherheit erledigt** dabei jedoch **nicht** die Betrachtung der **Datenschutzrisiken**. So ist der Schutzbereich des Datenschutzes gegenüber der Informationssicherheit deutlich breiter gefasst und ergänzt die Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit von Informationen) um weitere Grundwerte, die z. B. nach der Methodik des SDM in Form der Schutzziele Datenminimierung, Intervenierbarkeit (als technische Gestaltung von Verfahren zur Ausübung der Betroffenenrechte), Transparenz und Nichtverkettung (als Sicherung der Zweckbindung) beschrieben werden.[38] Auch die IT-Grundschutz-Methodik empfiehlt ausdrücklich, in entsprechenden Anwendungsfällen die Betrachtung der Grundwerte um die zusätzlichen Schutzziele des SDM zu ergänzen.[39]

Schließlich ist bei TOMs, die aus Sicht der Informationssicherheit umgesetzt werden, stets darauf zu achten, dass diese ihrerseits datenschutzkonform eingerichtet sind (z. B. Videoüberwachung zur Objektsicherung, Cloud-Lösungen zum Malwareschutz oder Protokollierung). Hierbei müssen etwaige Konflikte zwischen den Anforderungen des Datenschutzes und der Informationssicherheit aufgelöst werden.[40]

🔔 **Wichtig** Die aus Sicht der **Informationssicherheit** umzusetzenden **TOMs** können auch für den **Datenschutz relevant** sein und sollten i. R. d. Projektplanung darauf hin überprüft werden. Dabei ist stets darauf zu achten, dass auch die TOMs für die Informationssicherheit datenschutzkonform umzusetzen sind. Durch die **Bewertung der Risiken aus Sicht der Informationssicherheit** werden die **Datenschutz-Risiken** aber **nicht** bereits mitgeprüft.

[37] Siehe BSI-Standard 200-2 - IT-Grundschutz-Methodik, 8.2, S. 104.
[38] Siehe hierzu SDM, V. 3.1, S. 10, das ausdrücklich an die Grundwerte der Informationssicherheit anknüpft.
[39] Siehe BSI-Standard 200-2 - IT-Grundschutz-Methodik, 2.5, S. 14.
[40] Ebenda

# Glossar

| | |
|---|---|
| **Auftragsverarbeiter** | Auftragsverarbeiter sind natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten (**Art. 4 Nr. 8 DSGVO)** |
| **Beschäftigtendaten** | Personenbezogene Daten von Beschäftigten; Beschäftigte sind:<br>1. Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher,<br>2. zu ihrer Berufsbildung Beschäftigte,<br>3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),<br>4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,<br>5. Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstegesetz oder dem Bundesfreiwilligendienstgesetz leisten,<br>6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,<br>7. Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende,<br>und<br>Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist<br>**(§ 26 Abs. 8 BDSG)** |
| **Besondere Kategorien personenbezogener Daten („sensible Daten“)** | Personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur |

| | |
|---|---|
| | eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. (**Art. 9 Abs. 1 DSGVO**) |
| **Betroffene Person** | Die identifizierte oder identifizierbare natürliche Person, auf die sich die Informationen i. S. d. **Art. 4 Nr. 1 DSGVO**, d. h. die personenbezogenen Daten, beziehen |
| **Datenschutzkonferenz (DSK)**[41] | Die Datenschutzkonferenz ist das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder. Sie hat die Aufgabe, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Dies geschieht namentlich durch Entschließungen, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen. |
| **Erwägungsgründe (EG)** | Erwägungsgründe sind gem. Art. 296 Abs. 2 AEUV unabdingbarer Bestandteil von allen Richtlinien und Verordnungen der EU. Sie sind dabei jedoch nicht Bestandteil des verfügenden Teils dieser Rechtsakte, der in Form von Artikeln formuliert ist. Erwägungsgründe sind damit nicht rechtsverbindlich, nehmen aber eine herausragende Rolle bei der Auslegung der Richtlinien und vor allem Verordnungen ein.[42] |
| **Europäischer Datenschutzausschuss (EDSA)**[43] | Der Europäische Datenschutzausschuss ist ein unabhängiges europäisches Gremium. Es ist die Dachorganisation, die die nationalen Datenschutzbehörden der Länder des Europäischen Wirtschaftsraums sowie den Europäischen Datenschutzbeauftragten (EDPS) zusammenbringt. Der EDSA stellt sicher, dass die DSGVO und die Strafverfolgungsrichtlinie einheitlich angewandt werden |

[41] Siehe https://www.datenschutzkonferenz-online.de/dsk.html

[42] Siehe allgemein hierzu Gumpp, Stellenwert der Erwägungsgründe in der Methodenlehre des Unionsrechts, ZfPW 2022, 446-476.

[43] Siehe https://www.edpb.europa.eu/edpb_de

| | |
|---|---|
| | und die Zusammenarbeit, auch bei der Durchsetzung, gewährleistet wird. Der EDSA fasst verbindliche Entscheidungen über grenzüberschreitende Fälle, in denen kein Konsens erzielt wird. |
| **IKT-Steuerung** | Der Einsatz der Informations- und Kommunikationstechnik (IKT) in der Berliner Verwaltung wird zentral durch die nach den §§ 20 ff E-GovG Bln gesteuert. Teil der IKT-Steuerung ist die IKT-Staatssekretärin (Chief Digital Officer, CDO) die bei der für die Grundsatzangelegenheiten der IKT zuständigen Senatsverwaltung (z. Zt. Senatskanzlei) angesiedelt ist. |
| **Personenbezogene Daten** | Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.[44] |
| **Rechte und Freiheiten natürlicher Personen** | Dieser zentrale Begriff der DSGVO bezieht sich auf die Grundrechte und Grundfreiheiten nach der Grundrechtecharta (GrCh) der EU und der Europäischen Menschenrechtskonvention, insbesondere auf das Grundrecht auf Schutz der pbD gem. Art. 8 GrCh. Umfasst sind aber auch alle Grundrechte, die durch das Datenschutzrecht zumindest mittelbar geschützt werden. [45] |
| **Risiko** | Ein Risiko im Sinne der DSGVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten |

[44] Siehe Art. 4 Nr. 1 DSGVO

[45] Siehe Datenschutzkonferenz Kurzpapier Nr. 18 - Risiko für die Rechte und Freiheiten natürlicher Personen (DSK Kurzpapier Nr. 18), S. 1 (abrufbar unter https://www.datenschutzkonferenz-online.de/kurzpapiere.html).

| | |
|---|---|
| | natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann. Es hat zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.[46] |
| **Sozialdaten** | Sozialdaten sind personenbezogene Daten, die von einer in § 35 des SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden (s. **§ 67 Abs. 2 S. 1 SGB X**). Die in § 35 des SGB I genannten Stellen sind die „Leistungsträger", d. h. die in den §§ 18 bis 29 SGB I genannten Körperschaften, Anstalten und Behörden (Leistungsträger), die für die Sozialleistungen zuständigen sind (s. **§ 12 S. 1 SGB I**). |
| **Standard-Datenschutzmodell** | Als „Standard-Datenschutzmodell" (SDM) bezeichnen die deutschen Datenschutzaufsichtsbehörden eine Methode, mit der für den Bereich des operativen Datenschutzes sichergestellt ist, dass eine einheitliche Datenschutz-Beratungs- und Prüfpraxis in Bezug insbesondere zur Bestimmung von technisch-organisatorischen Maßnahmen der DSGVO erreicht werden kann. |
| **vaIKT** | Der Einsatz der Die „verfahrensabhängige IKT" (IT-Fachverfahren) wird von den fachlich zuständigen Behörden, in der Regel die fachlich zuständigen Senatsverwaltungen, verantwortet (§ 20 Abs. 3 S. 1 E-GovG Bln). |
| **Verantwortlicher** | Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (**Art. 4 Nr. 7 DSGVO**). |
| **vuIKT** | Die „verfahrensunabhängige vuIKT" (v. a. IKT-Basisdienste) liegt in der Zuständigkeit der IKT-Steuerung (§ 21 Abs. 2 E-GovG Bln). Als vuIKT stellt die IKT-Steuerung insbesondere IKT-Basisdienste wie die Digitale Akte Berlin bereit (z. B. § 10 Abs. 1, § 12 Abs. 2 E-GovG Bln). |

[46] DSK Kurzpapier Nr. 18 unter Bezug auf DSGVO EG 75 und 94 S. 2.