Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Standardprozess Datenschutz bei öffentlichen Digitalisierungsvorhaben

Handreichung III

ANLAGE 1 – Grundstruktur Rahmendatenschutzkonzept

Version 1.0

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Standardprozess Datenschutz bei öffentlichen Digitalisierungsvorhaben

Version	1.0
Herausgeberin:	Berliner Beauftragte für Datenschutz und Informationsfreiheit Alt-Moabit 59-61 10555 Berlin Tel.: 030 138 89 0 Fax: 030 215 50 50 mailbox@datenschutz-berlin.de 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
BlnDSG	Berliner Datenschutzgesetz
DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonzept
EDSA	Europäischer Datenschutzausschuss
EG	DSGVO Erwägungsgrund
IKT-S	IKT-Steuerung
ITDZ	IT-Dienstleistungszentrum Berlin
pbD	Personenbezogene Daten
RDSK	Rahmendatenschutzkonzept
Risiko	Risiko für die Rechte und Freiheiten der betroffenen Person
SenV	Senatsverwaltung
Skzl	Senatskanzlei
TOM	Technisch organisatorische Maßnahmen i. S. d. DSGVO (s. v.a. Art. 32 Abs. 1)

Verantwortlicher	Verantwortlicher i.S.d. Art. 4 Nr.7 DSGVO
vuIKT	Verfahrensunabhängige IKT

1 Einführung

- Allgemeine Beschreibung der Funktion des RDSK (s. o. unter 3.)
- Abgrenzung zur Funktion der Datenschutzkonzepte und DSFA (s. o. unter 4. und 5.)

> 🔔 **Wichtig:** Es muss klargestellt werden, dass die datenschutzrechtliche Verantwortlichkeit, im Regelfall, weiterhin bei den die vaIKT/ vuIKT nutzenden Behörden und öffentlichen Stellen verbleibt - diese müssen ein Datenschutzkonzept und ggf. eine DSFA nach → **ANLAGE 2** erstellen. Darin können sie aber maßgeblich auf das RDSK verweisen.

2 Beschreibung des Digitalisierungsvorhabens

- Allgemeine Beschreibung des Digitalisierungsvorhabens.
- Bei **vaIKT (IT-Fachverfahren)**: welche Geschäftsprozesse, Verfahren, Leistungen, Aufgaben der Verwaltung auf welcher **fachgesetzlichen Grundlage** sollen digitalisiert werden.

> 🔔 **Wichtig:** Bei IT-Fachverfahren müssen hier die relevanten gesetzlichen Grundlagen des Verwaltungsrechts genannt werden. Regelmäßig werden z. B. konkrete Verwaltungsaufgaben oder -leistungen digitalisiert, die fachgesetzlich bestimmten Behörden zuständigkeitshalber zugewiesen sind. Diese Aufgabenzuweisung ist zentraler Anknüpfungspunkt für die datenschutzrechtliche Bewertung der Verantwortlichkeit sowie der Rechtmäßigkeit der Verarbeitung pbD (s. → **Handreichung I, 3.2 und 3.4**).

- **vuIKT (z. B. IKT-Basisdiensten)** wird verfahrensunabhängig eingesetzt; hier sollte zumindest beschrieben werden, wie und zu welchen Zwecken die die vuIKT durch die öffentlichen Stellen der Berliner Verwaltung genutzt wird (z. B. alle, nur bestimmte Behörden wie Sozialämter. Gesundheitsämter usw.); hieraus lassen sich Rückschlüsse auf eine etwaige Verarbeitung pbD mittels der vuIKT ziehen.

3 Verarbeitung personenbezogener Daten i. R. d. Digitalisierungsvorhabens

→ Hier fließen die **Ergebnisse der Vorprüfung i. R. d. Projektumfeldanalyse und Machbarkeitsprüfung** (→ PPS 10 und 15) nach → **Handreichung I, 3.1** ein.

→ Auch auf die ggf. bereits i. R. d. Vergabeverfahrens erstellte Kategorisierung der pbD (→ **Handreichung II, 2.1**) kann zurückgegriffen werden.

- Zunächst sollte – soweit möglich – eine allgemeine Kategorisierung der i. R. d. Digitalisierungsvorhabens zu verarbeitenden pbD erfolgen (siehe zu den relevanten Kategorien → Handreichung I, 3.1).
- Sinnvoll ist eine Modellierung der Verarbeitung pbD i. R. d. Digitalisierungsvorhabens anhand der Methodik des **SDM** (**Teil D.2 – Verarbeitungsvorgänge**); insbesondere die darin vorgeschlagene Betrachtung der Verarbeitungstätigkeiten nach ihren Ebenen (s. SDM Teil D.2.3) und Komponenten (s. SDM Teil D.2.5) der Verarbeitung bilden insbesondere für den Bereich der vuIKT eine geeignete Grundlage zur Prüfung von Datenschutzrisiken.

3.1 Allgemeine Kategorisierung der verarbeiteten personenbezogenen Daten

- Siehe allgemein zu den relevanten Kategorien → **Handreichung I, 3.1**).
- Siehe die ggf. bereits i. R. d. Vergabeverfahrens erstellte Kategorisierung der pbD (→ **Handreichung II, 2.1**).

3.2 Modellierung der Verarbeitungsvorgänge

- Die **Modellierung der Verarbeitungstätigkeiten nach SDM, D.2** erfolgt in den folgenden Schritten:
    - Aufbereitung einer Verarbeitungstätigkeit in Vorgänge oder in Phasen eines Datenlebenszyklus (D2.1)
    - Mittel einer Verarbeitung (D2.2)
    - Ebenen einer Verarbeitung oder Verarbeitungstätigkeit (D2.3)
    - Zweck (D2.4)
    - Komponenten einer Verarbeitung oder Verarbeitungstätigkeit (D2.5).
- Sinnvoll erscheint zumindest eine Aufbereitung der Verarbeitungstätigkeiten sowie einer Beschreibung der Ebenen und Komponenten der Verarbeitung i. S. d. SDM, D.2.
- Möglich sind auch **andere Lösungsansätze zur Modellierung der Verarbeitungstätigkeiten**, soweit sie eine vergleichbar tragfähige Grundlage für die Risikoanalyse unter 5. Bilden.
- Nachfolgend werden die Ebenen und Komponenten, die nach SDM D.2, die zur Modellierung einer Verarbeitung herangezogenen werden, unter 3.2.2 und 3.2.3 auszugsweise dargestellt.

3.2.1 Aufbereitung einer Verarbeitungstätigkeit in Vorgänge/ Phasen eines Datenlebenszyklus

- Dies kann z. B. nach **SDM, D.2.1** erfolgen.

3.2.2 Ebenen der Verarbeitung

3.2.2.1 Ebene 1: Fachverfahren/ Geschäftsprozess

Beschreibung SDM, D.2.3: *Auf der Ebene 1 ist eine personenbezogene Verarbeitung im datenschutzrechtlichen Sinne angesiedelt. Diese Verarbeitung findet bspw. im Rahmen eines privatrechtlich agierenden Unternehmens oder einer Behörde, die dem öffentlichen Recht unterliegt, statt, für deren Aktivitäten der Verantwortliche verantwortlich ist. Diese Ebene entspricht dem, was vielfach als ein „Fachverfahren" und „Geschäftsprozess" mit einem bestimmten funktionalen Ablauf der Verarbeitungstätigkeit verstanden wird. Auf dieser Ebene des Verständnisses einer Verarbeitung werden die für eine Verarbeitungstätigkeit erforderlichen personenbezogenen Daten sowie die gesetzlichen Anforderungen bestimmt. Der Verantwortliche definiert entsprechende Rollen, Zuständigkeiten und Berechtigungen an den personenbezogenen Daten und bestimmt die zu verwendenden IT-Systeme und Prozesse. Wesentlich für die datenschutzrechtlich angemessen funktionale Gestaltung dieser Ebene ist die Bestimmung des Zwecks oder der Zwecke der Verarbeitungstätigkeit. Die Zweckbestimmung entfaltet grundsätzlich Bindungswirkung für den Einsatz der Betriebsmittel, die sich in der Ebene 2 und in der Ebene 3 befinden.*

- Bei vuIKT (z.B. Basisdiensten) kann diese Ebene im Regelfall nicht näher beschrieben werden und erfolgt daher in den Datenschutzkonzepten der die vuIKT nutzenden Stellen nach → **ANLAGE 2, 3.1.**
- Bei vaIKT (IT-Fachverfahen) kann hier eine allgemeine Beschreibung der Fachverfahrensebene erfolgen - die genaue Beschreibung der Verarbeitung pbD erfolgt aber ebenfalls in den Datenschutzkonzepten der die vaIKT nutzenden Stellen nach → **ANLAGE 2, 3.1.**

3.2.2.2 Ebene 2: Fachapplikation

Beschreibung SDM, D.2.3: *Auf der Ebene 2 ist die praktische Umsetzung der Verarbeitung und des Zwecks angesiedelt. Diese umfasst zum einen in der Regel die Rolle der Sachbearbeitung sowie die IT-Applikation(en), die sich genauer auch als „Fachapplikation eines Fachverfahrens" bezeichnen lässt. Die Sachbearbeitung und die Fachapplikation müssen die funktionalen und (datenschutz-)rechtlichen Anforderungen, denen die Verarbeitung unterliegt, vollständig erfüllen. Die Fachapplikation muss die Zweckbindung sicherstellen. Die Verarbeitung in der Fachapplikation muss zusätzliche Daten oder zusätzliche Verarbeitungsformen aus der Ebene 1 ausschließen, selbst wenn sie funktional besonders komfortabel sein mögen. Damit soll das Risiko minimiert werden, dass sie die Zweckbindung unterlaufen oder der Zweck überdehnt wird.*

- Beschreibung des Funktionsumfangs der Anwendung.
- Angaben zu Beteiligten an der Fachapplikation (Hersteller, direkter (Support)Dienstleister, Hoster, sonstige Subdienstleister (mit Angabe der Aufgabenwahrnehmung) (siehe hierzu ggf. i. R. d. Vergabeverfahrens bereitgestellte Aufstellung der Subunternehmer, **→Handreichung II, 2.2**).
- Angaben zu Ort und genauem Grund der Dienstleistung.

3.2.2.3 Ebene 3: IT-Infrastruktur

Beschreibung SDM, D.2.3: *Auf der Ebene 3 ist die IT-Infrastruktur angesiedelt, die Funktionen bereitstellt, die eine Fachapplikation der Ebene 2 nutzt. Zu dieser Ebene an „technischen Services" zählen Betriebssysteme, virtuelle Systeme, Datenbanken, Authentifizierungs- und Autorisierungssysteme, Router und Firewalls, Speichersysteme wie SAN oder NAS, CPU- Cluster, sowie die Kommunikationsinfrastruktur einer Organisation wie das Telefon, das LAN oder der Internetzugang. Auch hier gilt, dass diese Systeme innerhalb einer Verarbeitungstätigkeit jeweils so zu gestalten und zu nutzen sind, dass die Zweckbindung erhalten bleibt. Damit die Zweckbindung bzw. Zwecktrennung auf dieser Ebene durchgesetzt werden kann, müssen typischerweise technische und organisatorische Maßnahmen getroffen werden.*

- Welche weiteren IT-Infrastrukturkomponenten sind für das Verfahren erforderlich? (Bsp.: Netzwerke, Proxy, Verzeichnisdienst, Storage)
- Wie hängen sie zusammen und welche Schnittstellen bieten sie jeweils an? (Bsp.: Netzplan mit Datenflüssen und Zugriffswegen)
- Beschreibung der Infrastrukturkomponenten
- Beschreibung der Schnittstellen (technische Bezeichnung, angebundene Software, Grund für Anbindung)

3.2.3 Komponenten der Verarbeitung

Beschreibung SDM, D.2.3: *Aus den Vorgaben der Datenschutz-Grundverordnung ergeben sich unmittelbar die Komponenten Daten, Systeme und Dienste. Bei der konkreten Modellierung von Verarbeitungstätigkeiten mit Personenbezug ist es jedoch notwendig, die folgenden drei Komponenten zu betrachten:*

1. die personenbezogenen Daten,

2. die beteiligten technischen Systeme und Dienste (Hardware, Services, Software und Infrastruktur),

3. die technischen und organisatorischen Prozesse der Verarbeitung von Daten.

4 Verantwortlichkeit & Auftragsverarbeitung

➔ Hier fließen die **Ergebnisse der Vorprüfung i. R. d. Projektumfeldanalyse und Machbarkeitsprüfung** (→ PPS 10 und 15) nach → **Handreichung I, 3.2** ein

- **Siehe zu vuIKT (IKT-Basisdienste n) & vaIKT (IT-Fachverfahren) → Handreichung I, 3.2.1:**

🔔 **Wichtig:** Aus der **Zuständigkeit für die vuIKT** (s. § 21 Abs. 2 und § 24 Abs. 2 S. 1 E-GovG Bln) bzw. **der IT-Fachverfahrensverantwortlichkeit** (§ 20 Abs. 3 S. 1 E-GovG Bln) ergibt sich **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", siehe **→ Handreichung I, 3.2.2**).

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-Basisdienstdienst 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.

➔ Zu den abzuschließenden **Auftragsverarbeitungsverträgen** siehe **→ Handreichung I, 3.3.2**

🔔 **Wichtig**: Die IKT-Steuerung der Berliner Verwaltung hat im Dezember 2022 einen **Muster-Auftragsverarbeitungsvertrag** (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 (siehe: https://b-intern.de/themen/digitalisierung/ikt-vertraege/artikel.1014105.php).

5 Risikoanalyse und Abhilfemaßnahmen/ TOMs

➔ Hier fließen die **Ergebnisse der Vorprüfung i. R. d. Projektumfeldanalyse und Machbarkeitsprüfung** (→ PPS 10 und 15) nach → **Handreichung I, 3.7 und 3.8** ein

- Bei der Entwicklung und Bereitstellung von vaIKT/ vuIKT **verarbeiten die zuständigen Behörden der Hauptverwaltung** im Regelfall **selbst keine pbD** (siehe unter 4.) – die

vertiefte Analyse datenschutzrechtlicher Risiken, die mit der i. R. d. Digitalisierungsvorhabens geplanten Verarbeitung pbD entstehen, erfolgt daher durch die die vaIKT/ vuIKT nutenden Stellen nach → **ANLAGE 2**

- Bereits i. R. d. Entwicklung und Beschaffung von vaIKT/ vuIKT sind mögliche Datenschutzrisiken in den Blick zu nehmen und erforderliche TOMs umzusetzen, da es den die vaIKT/ vuIKT nutzenden öffentlichen Stellen andernfalls nicht vollumfänglich möglich ist, die Erfüllung der Vorgaben des Datenschutzes zu gewährleisten (siehe hierzu v. a. → **Handreichung I, 3.7 und 3.8)**.
- Insbesondere führen die Fachverfahrensverantwortlichen bzw. die IKT-Steuerung die **Beschaffung** der erforderlichen Hard- und Software sowie der Dienstleistungen durch und müssen bereits i. R. d. **Vergabeverfahren** darauf achten, dass die Vorgaben des Datenschutzes beachtet und ihre vollständige Umsetzung später möglich ist (siehe →**Handreichung II**).
- Für die **datenschutzrechtliche Risikoanalyse und -bewertung** i. R. d. Entwicklung und Bereitstellung von vaIKT/ vuIKT sollten die folgenden **Lösungsansätze** verfolgt werden - dabei muss eng mit dem **IT-Dienstleistungszentrum Berlin (ITDZ)** zusammengearbeitet werden, der die vuIKT und zunehmend auch vaIKT in technischer Hinsicht bereitstellt:

5.1 Entsteht voraussichtlich ein hohes Datenschutzrisiko?

- Soweit i. R. d. Entwicklung und Bereitstellung der vuIKT/ vaIKT absehbar ist, welche Kategorien pbD in welchem Umfang mittels dieser verarbeitet werden (siehe oben **unter 3.**) sollte eine geprüft werden, ob bereits absehbar ist, dass hierbei ein hohes Risiko i. S. d. DSGVO entsteht (siehe dazu → **Handreichung I, 3.8.2**).
- Es erfolgt damit eine vorgezogene Prüfung der Regelfälle für hohe Risiken, das sodann durch die verantwortlichen Stellen i. R. d. „Schwellwertanalyse“ i. S. d. Art. 35 DSGVO abschließend zu prüfen ist **(→ ANLAGE 2, 6.)**.
- So kann z. B. bei der Bereitstellung von IKT-Basisdiensten wie der Digitalen Akte Berlin, die durch alle öffentlichen Stellen der Berliner Verwaltung zu nutzen sind, bereits abzusehen sein, dass die Nutzung dieses Basisdiensten in besonderen Behörden, die vor allem besondere Kategorien pbD verarbeiten (siehe hierzu allgemein → **Handreichung, 3.1**), ein hohes Datenschutzrisiko entstehen wird da dort von einer umfangreichen Verarbeitung von pbD i. S. d. Art. 9 Abs. 1 DSGVO erfolgen wird (→ Regelfall des Art. 35 Abs. 3 lit. b DSGVO, siehe dazu → **Handreichung 3.8.2.2**).

→ ist bereits **absehbar**, dass bei Nutzung der vuIKT/ vaIKT durch bestimmte öffentliche Stellen der Berliner Verwaltung höchstwahrscheinlich **ein hohes Risiko** entsteht, so müssen gemeinsam **mit dem ITDZ TOMs für einen hohen Schutzbedarf** geplant und umgesetzt werden

→auch aus Sicht der **Informationssicherheit** erfolgt eine **Schutzbedarfsfeststellung** und die Umsetzung geeigneter TOMs - vor dem Hintergrund gewisser Schnittmenge hinsichtlich der

Gewährleistungsziele zwischen Datenschutz und Informationssicherheit sollte gemeinsam mit dem ITDZ **geprüft und dokumentiert** werden, **welche der aus Sicht der Informationssicherheit umzusetzenden TOMs auch zur Herstellung des aus Sicht des Datenschutzes erforderlichen Schutzniveaus beitragen** (sieh dazu → **Handreichung I, 3.8.5**)

5.2 Abhilfemaßnahmen/ TOMs

- Die konkrete Verarbeitung pbD mittels der vaIKT/ und vuIKT erfolgt durch die nutzenden Behörden, die sodann die konkreten damit verbundenen Risiken zu analysieren und bewerten zu haben (→ANLAGE 2).

5.2.1 Voraussichtlich einfaches/ geringes Risiko

- Bereits i. R. d. Entwicklung der vuIKT können die zuständigen Senatsverwaltungen aber durch **Anwendung der Gewährleistungsziele des SDM (→siehe SDM, C.1)** einen Beitrag zur Umsetzung der Vorgaben des Datenschutzes leisten.
- Grundlage hierfür ist die Modellierung der Verarbeitung pbD unter → 3., die sich insbesondere bei vuIKT im Regelfall auf die 2. Ebene der Fachapplikationen und vor allem der 3. Ebene der IT-Architektur beschränkt.

  → **Anwendung der Gewährleistungsziele** des SDM erfolgt sodann v. a. auf die **2. und 3. Ebene** sowie **die Komponenten** der Verarbeitung (siehe hierzu → **Beispiel Prüfmatrix**).

  → Die **Referenzmaßnahmen des SDM (D.1)** sowie die zusätzlichen **Bausteine des SDM** (https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/) bieten sodann eine Grundlage für die Auswahl und Umsetzung erforderliche TOMs (siehe hierzu → **Beispiel Prüfmatrix**).

5.2.2 Voraussichtlich hohes Risiko

- Entsteht voraussichtlich ein hohes Risiko (siehe unter 5.1) so muss besonders sorgfältig geprüft werden, welche TOMs bereits i. R. d. Entwicklung und Bereitstellung der vaIKT/ vuIKT umgesetzt werden können.
- Dabei kann, soweit wie bereits möglich, auf die **SDM Strategie zur Minderung hoher Risiken (D.3.4)** zurückgegriffen werden (siehe dazu auch →ANLAGE 2, 8.3).
- Ist bereits absehbar, z. B. bei IKT-Basisdiensten wie der Digitalen Akte Berlin, **bei welchen Behörden** voraussichtlich ein **hohes Risiko** aus Sicht des Datenschutzes bei Nutzung der vaIKT/ vuIKT entsteht, so sollten in Zusammenarbeit mit diesen konkret erforderliche TOMs für den hohen Schutzbedarf erörtert werden (→ **Schutzbedarfsfeststellung/ Schutzbedarfsabfrage Datenschutz**).

6 Fortschreibung RDSK/ Datenschutzmanagement

- Das RDSK muss laufend aktualisiert werden, um neue oder sich verändernde Risiken und Aspekte (z. B. im Zusammenhang mit technischen Updates) zu erfassen.
- Siehe zum Datenschutzmanagement z. B. SDM, D.4.

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: 1. Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher, 2. zu ihrer Berufsbildung Beschäftigte, 3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden), 4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte, 5. Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstegesetz oder dem Bundesfreiwilligendienstgesetz leisten, 6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten, 7. Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende, und Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist **(§ 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)[1]	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.[2]
Europäischer Datenschutzausschuss (EDSA)[3]	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 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

[1] Siehe https://www.datenschutzkonferenz-online.de/dsk.html
[2] Siehe allgemein hierzu Gumpp, Stellenwert der Erwägungsgründe in der Methodenlehre des Unionsrechts, ZfPW 2022, 446-476.
[3] Siehe https://www.edpb.europa.eu/edpb_de.

	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.[4]
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. [5]
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.[6]
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 DS-GVO erreicht werden kann.
vaIKT	Der Einsatz der Die „verfahrensabhängige IKT“ (IT-Fachverfahren) wird von den fachlich zuständigen Behörden, in der Regel die fachlich

[4] Siehe Art. 4 Nr. 1 DSGVO

[5] 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).

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

	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).