Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Standardprozess Datenschutz bei öffentlichen Digitalisierungsvorhaben

Handreichung III

ANLAGE 2 - Grundstruktur Datenschutzkonzept und Datenschutzfolgenabschätzung

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 Datenschutzkonzeptes (s. o. unter 4.).
- bei Nutzung vaIKT/ vuIKT: Verweis auf vorliegendes RDSK in aktuellster Version und Fundstelle.
- Verweis auf bereits existierende Dokumente mit Datenschutzbezug (z. B. Löschkonzept, Verarbeitungsverzeichnis i. S. d. Art. 30 DSGVO).

🔔 **Wichtig:** Regelmäßig bestehen bereits weitere Konzepte mit Datenschutzbezug (z.B. Löschkonzept, Verarbeitungsverzeichnis etc.). Es reicht nicht aus, lediglich auf diese zu verweisen; vielmehr müssen die für das Datenschutzkonzept/ die DSFA relevanten Teile aus diesen Konzepten an den richtigen Stellen in das Datenschutzkonzept aufgenommen werden (z. B. Inhalte des Löschkonzepts bei der Umsetzung der Betroffenenrecht, speziell des Rechts auf Löschung aus Art. 17 DSGVO).

2 Beschreibung des Digitalisierungsvorhabens

- Allgemeine Beschreibung des Digitalisierungsvorhabens.
- Bei **Einführung vaIKT (IT-Fachverfahren)**: Welche Geschäftsprozesse, Verfahren, Leistungen, Aufgaben der Verwaltung werden digitalisiert? Auf welcher fachrechtlichen Grundlage beruhen die zu digitalisierenden Geschäftsprozesse, Verfahren, Leistungen, Aufgaben? (→Verweis auf das **RDSK**, → **Handreichung III, ANLAGE 1, 2.**)
- **Bei Einführung vuIKT (z. B. IKT-Basisdienst)**: Welche Geschäftsprozesse, Verfahren, Leistungen, Aufgaben der Verwaltungen werden mittels der vuIKT umgesetzt? (Dies wird nicht bereits im RDSK beschrieben.)

🔔 **Wichtig:** Es müssen hier die relevanten verwaltungsrechtlichen Grundlagen der fortan digital umgesetzten Verwaltungsverfahren,- aufgaben, -leistungen oder Geschäftsprozesse beschrieben werden. Dieses Fachrecht ist regelmäßig Anknüpfungspunkt für die datenschutzrechtliche Bewertung v. a. der Verantwortlichkeit sowie der Rechtmäßigkeit der Verarbeitung pbD (→ **Handreichung I, 3.2 und 3.4**).

3 Verarbeitung personenbezogener Daten i. R. d. Digitalisierungsvorhabens

➔ Hier fließen die **Ergebnisse der Projektumfeldanalyse und Machbarkeitsprüfung** (→ PPS 10 und 15) ein, d. h. die Prüfung nach **→ Handreichung I, 3.1.**
➔ Auch die ggf. bereits i. R. d. Vergabeverfahrens erstellte Kategorisierung der pbD (**→ Handreichung II, 2.1**) .
➔ Relevant können daneben auch bereits erstellte **Verarbeitungsverzeichnisse** i. S. d. Art. 30 DSGVO sein.

- Zunächst sollte eine allgemeine Kategorisierung der i. R. d. Digitalisierungsvorhabens zu verarbeitenden pbD erfolgen (siehe zu den relevanten Kategorien **→ Handreichung I, 3.1**).
- Sinnvoll ist darüber hinaus bereits eine Modellierung der Verarbeitung pbD anhand der Verarbeitungsebenen des SDM (Anknüpfungspunkt zur Struktur ggf. vorliegender RDSK, siehe → ANLAGE 1, 3.).

➔ 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

- Nach SDM, D.2:
  - 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

3.2.1 Aufbereitung der Verarbeitungstätigkeit in Vorgänge/ Phasen eines Datenlebenszyklus

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.*

🔔 **Wichtig:** Insbesondere bei der Einführung/ Nutzung von vuIKT (z. B. IKT Basisdienst) und vaIKT (IT-Fachverfahren) muss die Verarbeitung auf dieser Ebene für den konkreten Einsatz bei der verantwortlichen Behörde präzise beschrieben werden; insoweit kann nicht auf das RDSK verwiesen werden.

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.*

🔔 **Wichtig:** Bei der Einführung/ Nutzung von vuIKT sollte hier maßgeblich auf das nach **ANLAGE 1** zu erstellende **RDSK** verwiesen werden (es muss stets geprüft werden, ob die erforderlichen Informationen tatsächlich bereits im RDSK enthalten sind oder es einer Konkretisierung bedarf.

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.*

🔔 **Wichtig:** Bei der Einführung/ Nutzung von vuIKT sollte hier maßgeblich auf das nach **ANLAGE 1** zu erstellende **RDSK** verwiesen werden (es muss stets geprüft werden, ob die erforderlichen Informationen tatsächlich bereits im RDSK enthalten sind.

3.2.3 Komponenten der Verarbeitung

🔔**Wichtig:** Bei der Einführung/ Nutzung von vuIKT sollte hier maßgeblich auf das nach **ANLAGE 1** zu erstellende **RDSK** verwiesen werden (es muss stets geprüft werden, ob die erforderlichen Informationen tatsächlich bereits im RDSK enthalten sind).

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.

5 Rechtmäßigkeit/ Rechtsgrundlagen der Verarbeitung

➔ Hier fließen die **Ergebnisse der Vorprüfung i. R. d. Projektumfeldanalyse und Machbarkeitsprüfung** (→ PPS 10 und 15) nach → **Handreichung I, 3.4 - 3.6** ein

6 Risikoprüfung („Schwellwertanalyse")

➔ Hier fließen die **Ergebnisse der Vorprüfung i. R. d. Projektumfeldanalyse und Machbarkeitsprüfung** (→ PPS 10 und 15) nach → **Handreichung I, 3.8.2** ein

➔ Nach dieser Vorprüfung erfolgt hier eine **abschließende Prüfung**, ob ein **hohes Risiko** i. S. d. Art. 35 DSGVO durch die i. R. d. Digitalisierung geplante Verarbeitung pbD entsteht und damit eine **DSFA** durchzuführen ist

➔ Siehe allgemein zum Risikobegriff → **Handreichung I, 3.8.1**

6.1 Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DSGVO („Blacklist“ der BlnBDI)

Siehe → Handreichung I, 3.8.2.1

6.2 Regelfälle des Art. 35 Abs. 3 DSGVO

Siehe → Handreichung I, 3.8.2.2

6.3 Liste des EDSA, Working Paper 248

Siehe → Handreichung I, 3.8.2.3

- Erfüllt ein Verarbeitungsvorgang zwei oder der Kriterien des Working Paper 248, so soll im Regelfall ein hohes Risiko i. S. d. Art. 35 DSGVO vorliegen und eine DSFA durchzuführen sein; im Einzelfall soll aber auch die Erfüllung nur eines der genannten Kriterien zu einem hohen Risiko führen können.

6.4 Ergebnis der Risikoprüfung

Ergebnis: geringes/ einfaches Risiko → Fortfahren mit der Risikobewertung unter 7.

Ergebnis: hohes Risiko → Fortfahren mit der DSFA nach 8.

7 Bewertung einfaches/ geringes Risiko

➔ Siehe allgemein zum Risikobegriff → **Handreichung I, 3.8.1**

- Auch bei einfachen/ geringen Risiken müssen Verantwortliche und Auftragsverarbeiter ein angemessenes Schutzniveau durch entsprechende TOMs gewährleisten (s. insbesondere Art. 32 DSGVO).
- Eine Bewertung einfacher/ geringer Risiken sowie Identifikation geeigneter TOMs lassen sich z. B. anhand einer Prüfung der Referenzmaßnahmen des SDM (D.1) durchführen

(**siehe → Risikomatrix**); siehe ferner auch die zusätzlichen Bausteine des SDM (https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/).

8 Bewertung hohes Risiko (Datenschutzfolgenabschätzung)

→ Siehe zur DSFA insbesondere das **DSK Kurzpapier Nr. 5 „Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO“** (abrufbar unter: https://www.datenschutzkonferenz-online.de/kurzpapiere.html)

8.1 Modellierung der Risikoquellen

*Die Quellen des Risikos für die Rechte und Freiheiten natürlicher Personen müssen identifiziert werden. Insbesondere ist zu bestimmen, welche Personen motiviert sein könnten, die Verarbeitungsvorgänge und die hierin verarbeiteten Daten in unrechtmäßiger Weise zu nutzen, und welches ihre Beweggründe und möglichen Ziele sein können. Anhand dessen können die damit zusammenhängenden Eintrittswahrscheinlichkeiten ermittelt werden (**DSK Kurzpapier Nr. 5, S. 3**).*

8.2 Risikobeurteilung

*Aufbauend auf den vorherigen Schritten wird bestimmt, ob in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Potenzielle Schäden können physischer, materieller oder immaterieller Art sein. Ihre Schwere sowie die jeweilige Eintrittswahrscheinlichkeit sind dabei zu berücksichtigen (ErwGr. 75 f.) (**DSK Kurzpapier Nr. 5, S. 3**).*

8.3 Auswahl geeigneter Abhilfemaßnahmen

*Die ermittelten Risiken müssen durch geeignete Abhilfemaßnahmen (insbesondere durch TOMs) eingedämmt werden. Eine Auswahl sowie Planung der Umsetzung der Maßnahmen findet statt. Dabei wird den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen. Verbleibende Restrisiken werden ermittelt und dokumentiert (**DSK Kurzpapier Nr. 5, S. 3**).*

SDM Strategie zur Minderung hoher Risiken (D.3.4):

Im Fall eines hohen Risikos wird die folgende standardisierte Strategie zur wirksamen Minderung der Risiken empfohlen:

1. Es sind die Maßnahmen des Referenzmaßnahmen-Katalogs umzusetzen, die bei normalem Ausgangsrisiko einer Verarbeitung bzw. normalem Schutzbedarf einer Person zu ergreifen sind.

2. Zusätzliche Maßnahmen aus dem Referenzmaßnahmen-Katalog sind umzusetzen.

3. Zusätzlich sind individuelle Maßnahmen auszuwählen. Ein Beispiel für eine individuelle Maßnahme könnte darin bestehen, bestimmte Vorgänge einer Verarbeitungstätigkeit nur auf Antrag bzw. nach einer Prüfung freizugeben und diese Tätigkeit dann im Betrieb zu überwachen, so dass bei Abweichungen ein Abbruch oder die Korrekturmaßnahme ausgelöst wird.

4. Die Wirkung einer Maßnahme kann erhöht wird, indem Skalierungsmöglichkeiten genutzt werden. Ein Beispiel hierfür ist die Erhöhung der Länge eingesetzter kryptografischer Schlüssel. Ein anderes Beispiel wäre die Sicherung von Protokolldaten, durch den Betrieb eines dedizierten Protokollservers für die Verarbeitung von Protokolldaten, der an zentraler Stelle sämtliche Protokolldaten speichert und sie dem Zugriff von den Produktionsmaschinen aus und durch deren Administratoren entzieht.

5. Auf alle schon getroffenen Maßnahmen sind ihrerseits technische und organisatorische Maßnahmen anzuwenden, um die Wirksamkeit, die Zuverlässigkeit, die Robustheit, die Belastbarkeit und die Evaluierbarkeit der Maßnahmen zu verbessern und ihre Rechtmäßigkeit sicherzustellen.

Das folgende Beispiel verdeutlicht die Strategie der Selbstanwendung der Maßnahmen auf sich selbst. Transparenz bedeutet, dass eine Verarbeitungstätigkeit anhand von Soll-Ist-Bilanzen prüfbar sein muss. Prüfbarkeit im Nachhinein bedeutet, dass Protokolldaten erzeugt, gespeichert und verarbeitet werden müssen. Die Protokolldaten müssen dann durch zusätzliche Maßnahmen revisionsfest gespeichert und deren Vertraulichkeit gewährleistet sein, indem sie signiert und verschlüsselt übertragen und gespeichert werden.

8.4 Erstellung DSFA-Bericht (ggf. Zwischenbericht)

*Der DSFA-Bericht enthält gem. Art. 35 Abs. 7 DS-GVO jedenfalls die systematische Beschreibung der geplanten Verarbeitungsvorgänge und ihrer Zwecke, die Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung, die Beschreibung und Beurteilung der Risiken sowie der Abhilfemaßnahmen zur Risikoeindämmung. Der Bericht ist um eine Darstellung der Restrisiken samt Entscheidung über den Umgang mit diesen zu ergänzen. Er kann sich dabei an den hier dargestellten Phasen orientieren. Der DSFA-Bericht dient ferner als Baustein einer umfassenden Dokumentation zur Umsetzung der in Art. 5 Abs. 2 DS-GVO normierten Rechenschaftspflicht. Es ist zu prüfen, inwieweit Teile des DSFA-Berichts im Sinne einer erhöhten Transparenz für die betroffenen Personen veröffentlicht werden sollen. (**DSK Kurzpapier Nr. 5, S. 4**).*

- → Die für den DSFA-Bericht geforderte **„systematische Beschreibung der geplanten Verarbeitungsvorgänge und ihrer Zwecke“**, **„Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung“** sowie die **„Beschreibung und Beurteilung der Risiken“** dürfte bereits i. R. d. des Datenschutzkonzeptes (zumindest unter **Punkt 3. und 6.**) erstellt worden sein; hierauf kann für den DSFA-Bericht zurückgegriffen bzw. verwiesen werden.
- → Es ist dringend zu empfehlen, dass bereits vor dem abschließenden DSFA-Bericht, wenn die wichtigsten zu ergreifenden TOMs absehbar sind, der Team- und Behördenleitung einen **DSFA-Zwischenbericht** vorzulegen damit diese Informationen bereits in die weitere Projektumsetzung einbezogen werden können.

8.5 Umsetzung der Abhilfemaßnahmen

*Bevor die geplante Datenverarbeitung eingesetzt wird, müssen die für die Eindämmung des Risikos geeigneten Abhilfemaßnahmen (insbesondere TOMs) umgesetzt sein. Vorher darf die Verarbeitung personenbezogener Daten nicht stattfinden. Sofern sich bei der Umsetzung herausstellt, dass geplante Maßnahmen nicht (wirksam) realisiert werden können, müssen andere geeignete Maßnahmen ausgewählt, die Restrisikobewertung angepasst oder die Verarbeitungsvorgänge insgesamt angepasst werden, so dass sie den Anforderungen der DS-GVO genügen (**DSK Kurzpapier Nr. 5, S. 4**).*

8.6 Test und der Abhilfemaßnahmen (inkl. Dokumentation)

*Nachdem Abhilfemaßnahmen umgesetzt wurden, müssen sie auf ihre Wirksamkeit getestet werden. Möglicherweise zeigt sich bei der Umsetzung der Maßnahmen, dass weitere Risiken bestehen, die ebenfalls zu behandeln sind (**DSK Kurzpapier Nr. 5, S. 4**).*

8.7 Freigabe der Verarbeitungstätigkeit

*Im Anschluss und mit Vorliegen der vollständigen Dokumentation können die Verarbeitungsvorgänge formal durch den Verantwortlichen freigegeben werden (**DSK Kurzpapier Nr. 5, S. 4**).*

🔔 **Wichtig:** Erst wenn die erforderlichen TOMs, die ein angemessenes Schutzniveau hinsichtlich der hohen Risiken gewähren, tatsächlich umgesetzt sind, darf die Verarbeitung pbD i. R. d. Digitalisierungsvorhabens aufgenommen werden. Das gilt insbesondere auch für die **Test- und Pilotierungsphase** des Projekts.

9 Bewertung hohes Restrisiko (Art. 36 DSGVO)

*Ergibt eine DSFA, dass trotz technischer und organisatorischer Maßnahmen zur Risikoeindämmung weiterhin ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht (Restrisiko), muss nach Art. 36 DS-GVO der Verantwortliche die zuständige Aufsichtsbehörde konsultieren. Er trifft unter Berücksichtigung der Empfehlungen der Aufsichtsbehörde eine Entscheidung, ob die Verarbeitungsvorgänge angesichts der verbleibenden Restrisiken durchgeführt werden können und ggf. welche zusätzlichen Abhilfemaßnahmen in diesem Fall zum Einsatz kommen sollen. Die Aufsichtsbehörde kann ihrerseits die in Art. 58 DS-GVO genannten Befugnisse ausüben und z. B. eine Warnung, Anweisung oder Untersagung aussprechen (**DSK Kurzpapier Nr. 5, S. 4**).*

10 Fortschreibung DSFA/ Datenschutzmanagement

- Siehe zur Überprüfung und Fortschreibung der DSFA → DSK Kurzpapier Nr. 5, S. 4 f.
- Siehe zum Datenschutzmanagement: 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 zuständigen Senatsverwaltungen, verantwortet (§ 20 Abs. 3 S. 1 E-GovG Bln).

[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.

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).