Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Standardprozess Datenschutz bei öffentlichen Digitalisierungsvorhaben

Handreichung III

„Rahmendatenschutzkonzept, Datenschutz-konzept & Datenschutz-Folgenabschätzung“

Allgemeiner Teil

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

Diese Handreichung unterstützt die Umsetzung der Vorgaben des **Standardprozesses Datenschutz bei öffentlichen Digitalisierungsvorhaben** zu → **PPS 24 - „Chancen und Risikomanagement“** und → **PPS 25 „Stakeholdermanagement“**).

Die vorliegende Handreichung enthält eine kommentierte Grundstruktur für die ab diesem Punkt des Projektes zu erstellenden **Rahmendatenschutzkonzepte (→ ANLAGE 1**) sowie **Datenschutzkonzepte** mit ggf. anzuschließender **Datenschutzfolgenabschätzung (→ ANLAGE 2)**.

Inhaltlich schließen diese Dokumente an die datenschutzrechtliche Vorprüfung i. R. d. **Projektumfeldanalyse** und **Machbarkeitsprüfung (PPS 10 und PPS 15)** nach → **Handreichung I** an und vertiefen diese.

Diese Handreichung unterscheidet dabei 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 **(→ ANLAGE 1)**
- Eine öffentliche Stelle führt ein IT-Fachverfahren (vaIKT) / einen Basisdienst (vuIKT) ein oder ein allgemeines Digitalisierungsvorhaben durch **(→ ANLAGE 2)**

Diese Handreichung wird durch das **für die Bewertung der Einhaltung der Datenschutzanforderungen zuständige Mitglied des Projektteams** genutzt (→ PPS 7 „Projektteam zusammenstellen“). Dabei sind für die Umsetzung der Methodik in ANLAGE 1 und 2 **vertiefte Datenschutzkenntnisse erforderlich**. Das Projektteam muss vor diesem Hintergrund ggf. zusätzliches Fachpersonal mit den erforderlichen juristischen und technischen Kenntnissen einbeziehen.

2 Datenschutz als Teil des Chancen-, Risiko- und Stakeholdermanagements

Nach den Vorgaben des PMH soll an diesem Punkt der Projektumsetzung die in der Definitionsphase bereits initial durchgeführte Projektumfeldanalyse überarbeitet und ggf. vertieft werden. Dabei geht es darum, auf dem durch die Planung hergestellten neuen Wissensstand Stakeholder und Risiken konkreter und ggf. neu zu bewerten und dazu ein aktives Chancen- und Risikomanagement zu implementieren (s. PMH S. 55).

Auch aus Sicht des Datenschutzes ist an diesem Punkt des Projektes eine systematische Analyse möglicher Datenschutzrisiken zu initialisieren. Dabei sind Verantwortliche ausdrücklich dazu verpflichtet, hinsichtlich der identifizierten Risiken mittels geeigneter TOMs ein angemessenes Schutzniveau für die Betroffenen zu gewährleisten. Diese Risikoanalyse ist dabei in einem **Datenschutzkonzept** und bei vaIKT/vuIKT zusätzlich vorab in einem **Rahmendatenschutzkonzept**, das

von den das Verfahren einsetzenden Behörden nachgenutzt und auf die eigenen Bedürfnisse anzupassen ist, zu dokumentieren. Bei hohen Datenschutzrisiken ist zusätzlich eine **Datenschutzfolgenabschätzung** durchzuführen. Wann dies der Fall ist, lässt sich Art. 35 Abs. 1 DSGVO entnehmen.

Diese rechtlich bindenden Vorgaben zur datenschutzrechtlichen Risikoanalyse sollten als Teil des allgemeinen Chancen-, Risiko- und Stakeholdermanagement verstanden und in dieses integriert werden. So wie auch i. R. d. allgemeinen Chancen-, Risiko- und Stakeholdermanagements baut die strukturierte Datenschutz-Risikoanalyse auf den Ergebnissen der **Vorprüfung** i. R. d. **Projektumfeldanalyse** und **Machbarkeitsprüfung (→ PPS 10 und 15)** nach **→ Handreichung I** auf.

Die vorliegende Handreichung gibt hierfür eine kommentierte Grundstruktur für die Erstellung eines **Rahmendatenschutzkonzeptes (→ ANLAGE 1**) sowie für ein **Datenschutzkonzept** mit ggf. anzuschließender **Datenschutzfolgenabschätzung (→ ANLAGE 2)** vor.

3 Was ist ein Rahmendatenschutzkonzept?

Ein Rahmendatenschutzkonzept:

→ wird durch zuständige Senatsverwaltung bei der Bereitstellung von vaIKT/vuIKT erstellt;

→ dokumentiert Datenschutzrisiken der vaIKT/ vuIKT und erforderliche Abhilfemaßnahmen/ TOMs;

→ Datenschutzkonzepte und DSFAs zu vaIKT/vuIKT können auf zentrale Rahmendatenschutzkonzepte verweisen.

Konkrete Vorgaben zur Erstellung eines Rahmendatenschutzkonzeptes: → **ANLAGE 1**

Führen öffentliche Stellen vaIKT (z. B. IT-Fachverfahren) und vuIKT (z. B. IKT-Basisdienste) ein und verarbeiten mittels dieser pbD, so bleiben sie im Regelfall Verantwortliche (s. → Handreichung I, 3.2.1). Die Entwicklung und Beschaffung zentral bereitgestellter vaIKT/ vuIKT erfolgt jedoch durch die jeweils zuständigen Senatsverwaltungen (siehe für die vaIKT § 20 Abs. 3 S. 1 E-GovG Bln sowie für den Bereich der vuIKT, § 21 Abs. 2 Nr. 3, 11 und § 24 Abs. 2 S. 1 E-GovG Bln).

Vor diesem Hintergrund mangelt es den Verantwortlichen meist an einer ausreichenden Informationsgrundlage zur Durchführung einer vollumfänglichen Risikoanalyse i. S. d. Datenschutzes zu vaIKT/ vuIKT. Diese Grundlagen stellen die zuständigen Senatsverwaltungen in Form von Rahmendatenschutzkonzepten zur Verfügung, die die bereits absehbaren Datenschutzrisiken und erforderlichen Abhilfemaßnahmen/ TOMs dokumentieren.

Die **Erstellung eines Rahmendatenschutzkonzeptes** erfolgt nach **→ ANLAGE I**.

4 Was ist ein Datenschutzkonzept?

Ein Datenschutzkonzept dokumentiert:

→ die Erfüllung der Vorgaben des Datenschutzes, die der Verantwortliche nachweisen muss („Rechenschaftspflicht“);

→ einfache bzw. geringe Datenschutzrisiken, die im Zusammenhang mit einem Digitalisierungsvorhaben entstehen sowie die erforderlichen Abhilfemaßnahmen/ TOMs;

→ die Prüfung und das Ergebnis, ob eine Datenschutz-Folgenabschätzung durchzuführen ist (Schwellwertanalyse).

Konkrete Vorgaben zur Erstellung eines Datenschutzkonzeptes: → **ANLAGE 2**

Die DSGVO enthält keine ausdrücklichen Regelungen zu Datenschutzkonzepten. Grundsätzlich muss der Verantwortliche jedoch nachweisen können, dass er die Vorgaben der DSGVO einhält („**Rechenschaftspflicht**“, Art. 5 Abs. 2 DSGVO). Aus diesem Grund werden Maßnahmen zur Einhaltung der DSGVO v. a. in Datenschutzkonzepten dokumentiert.

Insbesondere sind Verantwortliche dazu verpflichtet, mögliche Risiken zu analysieren, die im Zusammenhang mit der Verarbeitung pbD entstehen und Abhilfemaßnahmen zu bestimmen, die hinsichtlich dieser Risiken ein angemessenes Sicherheitsniveau für die Betroffenen sicherstellen (**→ s. Handreichung I, 3.8**). Risiken für die Rechte und Freiheiten der Betroffenen entstehen auch bei einer rechtmäßigen Verarbeitung personenbezogener Daten, so dass die DSGVO allgemein vorgibt, dass Verantwortliche und Auftragsverarbeiter geeignete TOMs umsetzen, die ein dem Risiko angemessenes Schutzniveau gewährleisten (s. z. B. Art. 32 DSGVO).[1]

Risiken entstehen insbesondere, wenn pbD automatisiert verarbeitet werden, v. a. bei Verwendung neuer Technologien. Daher gibt das BlnDSG ergänzend zur DSGVO in **§ 26 Abs. 2 BlnDSG** vor, dass vor **jeder automatisierten Verarbeitung** pbD stets die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse zu ermitteln und in einem Datenschutzkonzept zu dokumentieren sind.

Schließlich muss der Verantwortliche stets prüfen, inwieweit die im Zusammenhang mit einem Digitalisierungsvorhaben geplante Verarbeitung pbD zu einem **hohen Risiko** führt („**Schwellwertanalyse**“). Für diesen Fall ist die Verantwortliche sodann gem. Art. 35 DSGVO dazu verpflichtet, eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen. Die Entscheidung über Durchführung oder Nichtdurchführung der DSFA ist in jedem Fall mit Angabe von maßgeblichen

[1] Vgl. DSK Kurzpapier Nr. 5 – Datenschutz-Folgenabschätzung, S. 1.

Gründen **schriftlich festzuhalten**.[2] Dies erfolgt sinnvollerweise im Rahmen eines Datenschutzkonzeptes.

Die **Erstellung eines Datenschutzkonzeptes** sowie die Durchführung einer **Schwellwertanalyse** erfolgt nach → **ANLAGE I.**

5 Was ist eine Datenschutz-Folgenabschätzung?

Eine Datenschutzfolgenabschätzung:

→ wird nur bei einem hohen Datenschutzrisiko durchgeführt („Schwellwertanalyse“);

→ dokumentiert hohe Datenschutzrisiken, die im Zusammenhang mit einem Digitalisierungsvorhaben entstehen sowie die erforderlichen Abhilfemaßnahmen/ TOMs;

→ richtet sich nach den genauen Vorgaben der DSGVO (Art. 35 Abs. 1, 7 sowie EG 84, 90).

Konkrete Vorgaben zur Erstellung einer Datenschutzfolgenabschätzung: → **ANLAGE 2**

Eine DSFA ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten.

Die DSFA ist ausdrücklich in der DSGVO geregelt (Art. 35 Abs. 1, 7 DSGVO sowie EG 84, 90). Sie ist durchzuführen, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein **hohes Risiko** für die Rechte und Freiheiten der Betroffenen zur Folge hat. Sie befasst sich insbesondere mit Abhilfemaßnahmen, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann.[3]

Die Prüfung, inwieweit ein hohes Risiko vorliegt, erfolgt i. R. d. „Schwellwertanalyse“, die im Datenschutzkonzept zu dokumentieren ist (siehe unter 3.).

Für die Erstellung einer Datenschutz-Folgenabschätzung dient die → **ANLAGE II „Datenschutzkonzept & Datenschutz-Folgenabschätzung“** als Unterstützung. Die Schwellwertanalyse wird i. R. d. Datenschutzkonzeptes dokumentiert.

[2] Ebenda.
[3] Ebenda.

6 Wer erstellt Datenschutzkonzept, DSFA und Rahmendatenschutzkonzept?

🔔 Die folgenden institutionellen und personellen Zuständigkeiten sind zu beachten:

→ Die **fachverfahrensverantwortliche Senatsverwaltung bzw. nachgeordnete Behörde** erstellt das **Rahmendatenschutzkonzept zu vaIKT** (v.a. IT-Fachverfahren).

→ Die **Senatskanzlei/ IKT-Steuerung** erstellt das **Rahmendatenschutzkonzept zu vuIKT** (v.a. IKT-Basisdiensten).

→ Die **datenschutzrechtlich Verantwortliche** (im Regelfall die die vaIKT/ vuIKT nutzende Stelle) muss das **Datenschutzkonzept** und ggf. die **DSFA** erstellen.

→ **Personell** ist das für Datenschutz zuständige **Mitglied des Projektteams (→ PPS 7)** zuständig und nutzt die hierfür eingeplanten **personellen und finanziellen Ressourcen (→ PPS 20/ 21)**.

→ Die **behDSB beraten das Projektteam** (keine Erstellung oder „Freigabe" der Dokumente).

→ Die **BlnBDI** kann **beratend zu speziellen Fragen** einbezogen werden.

Die **Verantwortliche** ist rechtlich zur Erstellung von DSK und ggf. DSFA verpflichtet (s. o.). Die datenschutzrechtliche Einordnung, welche der an einem Digitalisierungsvorhaben beteiligten öffentlichen Stellen als Verantwortliche bzw. Auftragsverarbeiter zu bewerten sind, erfolgt bereits i. R. d. **Projektumfeldanalyse & Machbarkeitsprüfung** in → PPS 10 und 15 **(→ Handreichung I)**.

Die Erstellung des **RDSK** erfolgt durch die für die **vaIKT/vuIKT** zuständigen **Senatsverwaltungen bzw. fachverfahrensverantwortlichen Behörden**.

Auftragsverarbeiter sind dazu verpflichtet, die Verantwortlichen bei der Erstellung von DSK und DSFA **zu unterstützen** (siehe v. a. Art. 28 Abs. 3 lit. f DSGVO).

Die konkrete Erstellung dieser Datenschutzdokumente muss durch die personellen Ressourcen der Verantwortlichen erfolgen. Das bedeutet, dass zunächst das **Mitglied des Projektteams** zuständig ist, das für **Datenschutz zuständig erklärt** wurde (**→ PPS 7**). Soweit erforderlich, muss dieses sodann das erforderliche juristische und technische Fachpersonal in geeigneten kooperativen Formaten einbeziehen. Dazu nutzt es die in der Planungsphase des Projekts vorgesehen **personellen und finanziellen Ressourcen** (Personal- und Sachmittelplanung → PPS 20/21).

Es fällt nicht in den Aufgabenbereich der **behDSB**, diese Datenschutzdokumente zu Digitalisierungsvorhaben zu erstellen. Die behDSB werden vorrangig beratend tätig (insbesondere i. R. v. DSFA, s. Art. 35 Abs. 2; 39 Abs. 1 lit. c DSGVO).

Die behDSB erfüllen ihre allgemeine Überwachungsrolle zur Einhaltung der DSGVO und weiterer Datenschutzvorschriften (s. Art. 39 Abs. 1 lit. b DSGVO) i. R. v. Digitalisierungsvorhaben nur soweit, als dass ihre jeweilige Behörde dabei tatsächlich pbD verarbeitet. Bei vaIKT/ vuIKT ist dies normalerweise nur insoweit der Fall, als dass die zuständige Senatsverwaltung das jeweilige IT-Fachverfahren bzw. den jeweiligen IKT-Basisdienst auch selbst nutzt.

Ein reines **Outsourcing der Erstellung der Datenschutzdokumente**, z. B. an Beratungsunternehmen, ist **nicht möglich**. Soweit externe Beratungsleistungen einbezogen werden, ist sicherzustellen, dass diese über den erforderlichen technischen und juristischen Sachverstand zum Datenschutz verfügen. Ferner muss das Projektteam den Auftrag an externe Beratungsfirmen genau definieren und die Umsetzung steuern, da andernfalls eine Qualitätssicherung nicht gewährleistet werden kann. Als **Grundlage der Beauftragung** sollten die methodisch strukturellen Vorgaben der **ANLAGEN I und II** dienen.

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)[4]	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.[5]
Europäischer Datenschutzausschuss (EDSA)[6]	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.

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

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

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

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.[7]
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. [8]
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.[9]
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

[7] Siehe Art. 4 Nr. 1 DSGVO

[8] 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).

[9] 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).

ANLAGE 1 – Rahmendatenschutzkonzept

→Siehe separates Dokument zum Download auf www.datenschutz-berlin.de/standardprozess

ANLAGE 2 – Datenschutzkonzept und Datenschutzfolgenabschätzung

→Siehe separates Dokument zum Download auf www.datenschutz-berlin.de/standardprozess