Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Standardprozess Datenschutz bei öffentlichen Digitalisierungsvorhaben

Handreichung II

Datenschutz im Vergabeverfahren

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
EDSA	Europäischer Datenschutzausschuss
EG	Erwägungsgrund (der DSGVO)
E-GovG Bln	E-Government-Gesetz Berlin
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum
GWB	Gesetz gegen Wettbewerbsbeschränkungen
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)
VgV	Vergabeverordnung
vuIKT	Verfahrensunabhängige IKT

1 Einführung

Die vorliegende Handreichung unterstützt die Umsetzung der Vorgaben des Standardprozesses Datenschutz zu → **PPS 21 „Sachmittelplanung“**. Diese Handreichung wird genutzt durch das für die Bewertung der Einhaltung der Datenschutzanforderungen zuständige Mitglied des Projektteams (→ PPS 7) sowie durch das für die Vergabe zuständige Personal.

Im Rahmen der Sachmittelplanung eines Digitalisierungsvorhabens wird entschieden, ob IKT zur Digitalisierung des Geschäftsprozesses entwickelt oder eingekauft wird (siehe PMH Anlage 8). Soll neue IKT eingeführt bzw. beschafft werden, muss diese Einführung entweder als gesondertes Projekt oder als Teilprojekt nach den Vorgaben für IKT-Projekte (PMH Anlage 9) erfolgen.

Die Beschaffung erfolgt im Regelfall über ein **Vergabeverfahren**, so dass sich das Projektteam frühzeitig mit den zuständigen Vergabestellen in Verbindung setzen muss. Die Vergabeverfahren stellen dann eigene Arbeitspakete dar, die in den Projektstrukturplan aufgenommen werden müssen (s. PMH, S. 48).

Regelmäßig sind i. R. v. Digitalisierungsvorhaben Dienstleistungen oder IT-Anwendungen zu beschaffen, die mit der Verarbeitung pbD verbunden sind. Dabei müssen die Vorgaben des Datenschutzes bereits i. R. d. Vergabeverfahrens Berücksichtigung finden. So weisen auch die Vergabekammern in ihrer Spruchpraxis darauf hin, dass die Einhaltung der datenschutzrechtlichen Anforderungen nach der DSGVO bereits vor der Zuschlagserteilung und nicht erst i. R. d. Auftragsausführung zu prüfen sind.[1]

Die vorliegende Handreichung enthält keine umfassende Betrachtung aller datenschutzrechtlichen Aspekte des Vergabeverfahrens, sondern weist auf einige besonders **praxisrelevante Aspekte** hin. Auch sind keine Hinweise zur Verarbeitung pbD i. R. d. Vergabeverfahrens selbst (z. B. bei der Eignungsprüfung nach §§ 122 ff. GWB sowie §§ 42, 44 ff. VgV) enthalten.

2 Erstellung der Vergabeunterlagen/ Leistungsbeschreibung

Das Transparenzgebots des § 97 Abs. 1 GWB verpflichtet öffentliche Auftraggeber dazu, das Beschaffungsverfahren offen und nachvollziehbar zu gestalten und dabei Leistungsbeschreibungen „so eindeutig und erschöpfend wie möglich“ zu formulieren (§ 121 Abs.

[1] Vgl. BKartA (2. Vergabekammer des Bundes), Beschluss vom 20.06.2023 - VK 2-34/23; 2. red. Ls.; hier wird ferner darauf hingewiesen, dass eine Lösung über die vertragliche Ebene, wonach eine nicht vertragsgemäße Leistungserbringung durch vertragliche Sanktionsmechanismen zu erfassen sei, für den vergaberechtlichen Wettbewerb zu spät kommen.

1 S. 1 GWB).[2] Vor diesem Hintergrund müssen auch die datenschutzrechtlichen Anforderungen so in der Leistungsbeschreibung berücksichtigt werden, dass diese nach Zuschlagserteilung auch tatsächlich umgesetzt werden können. Dies gilt insbesondere für die Vorgaben des Art. 28 DSGVO da zu beschaffende Dienstleistungen, die mit der Verarbeitung pbD verbunden sind (z. B. cloudbasierte Speicherung, Support), im Regelfall als **Auftragsverarbeitung** erbracht werden.

2.1 Kategorisierung der personenbezogenen Daten

Die Vergabeunterlagen müssen eine Kategorisierung der pbD enthalten, die zu verarbeiten sind. Insbesondere bei **Auftragsverarbeitungsleistungen** ist den Bietern andernfalls eine einwandfreie Preiskalkulation nicht möglich, da die Informationen über die zu verarbeitenden pbD Auswirkungen auf das zu gewährende Schutzniveau und die dazu ggf. noch umzusetzenden TOM auf Seiten des Bieters haben können.[3]

Konkret sollte diese Kategorisierung der pbD für die Leistungsbeschreibung genau aufführen, welche Kategorien pbD, insbesondere sensibler Daten i. S. d. Art. 9 Abs. 1 DSGVO, zu welchen Zwecken, auf welcher Rechtsgrundlage und für welche Speicherdauer verarbeitet werden sollen.[4] Hierzu kann auf die Ergebnisse der **Datenschutzprüfung nach → Handreichung I, 3.1** i. R. d. **Projektumfeldanalyse** und **Machbarkeitsprüfung (→ PPS 10 und 15**) zurückgegriffen werden.

2.2 Vollständige Aufstellung der Subunternehmer

In der Praxis setzen Anbieter regelmäßig Subunternehmer ein, die auch die Verarbeitung pbD übernehmen. Auch für die Verarbeitung durch Subunternehmer trägt die Verantwortliche letztlich die datenschutzrechtliche Verantwortung (siehe Art. 28 Abs. 1 DSGVO sowie zu den Vorgaben für den Einsatz von Unter-Auftragsverarbeitern Art. 28 Abs. 2, Abs. 3 lit. d sowie Abs. 4 DSGVO).

Vor diesem Hintergrund sollte bereits i. R. d. Vergabe eine genaue Aufstellung der eingesetzten Subunternehmer und der diesbezüglichen Datenflüsse verlangt werden. Vergaberechtlich kann der Auftraggeber Vorgaben zur Zulässigkeit des Einsatzes von Subunternehmern bei den

[2] Siehe zu den einschlägigen Normen des Vergaberechts, LfD Bayern, Datenschutz als Kriterium im Vergabeverfahren, Orientierungshilfe v. 1. Februar 2024.
[3] Vgl. VK Berlin Beschl. v. 13.9.2019 – VK-B1-13/19, II.B.4, Rn. 109 und 118.
[4] Entsprechend gibt das V-Model XT unter C.1.10.3.3. im Produkt „Vorgaben zum Datenschutz“ u. a. für das Lastenheft verbindlich vor: *„Alle zu verarbeitenden personenbezogenen Daten sind nach ihrem Schutzbedarf zu kategorisieren. Die Kategorisierung ist nachvollziehbar und zusammen mit Erhebungszweck, Rechtsgrundlage, erlaubter Verwendung und Speicherdauer zu dokumentieren“.*

Bewerbern oder Bietern, einschließlich deren Wechsel, machen. Die Bewerber oder Bieter müssen für die von ihnen eingeschalteten Subunternehmer einstehen und sich deren Leistungsteil und gegebenenfalls deren Eignung (sogenannte „Eignungsleihe", § 47 VgV) zurechnen lassen, denn diese sind Bestandteil ihrer Teilnahmeanträge beziehungsweise Angebote, § 36 VgV.[5]

2.3 Leistungsort

Typischerweise stellt sich auch in öffentlichen Digitalisierungsvorhaben die Frage, inwieweit Angebote von Unternehmen berücksichtigt werden können, die nicht innerhalb des EWR sitzen. Sollen diese dabei pbD verarbeiten so ist zu beachten, dass die DSGVO in den Art. 44 ff DSGVO besondere Anforderung an die **Übermittlung von pbD in Drittländer** vorsieht (s. hierzu → **Handreichung I, 3.6**). Vor allem in diesen Fällen bedarf es einer **präzisen Beschreibung des Leistungsorts** in der Leistungsbeschreibung. Dabei ist zu beachten, dass eine Übermittlung in ein Drittland nicht nur dann vorliegt, wenn die Daten in einem Drittland gespeichert werden, sondern bereits etwa dann, wenn ein **Zugriff aus einem Drittland technisch möglich** ist oder die Daten auf einem Bildschirm in einem Drittland angezeigt werden.[6] Die ist häufig im Rahmen von Administrations- und Support-Aufgaben der Fall.

2.3.1 Anbieter in Drittstaaten, insbes. Vereinigte Staaten

Regelmäßig sollen i. R. v. Digitalisierungsvorhaben Auftragsverarbeitungsleistungen von in Drittstaaten, insbesondere den Vereinigten Staaten, ansässigen Anbietern in Anspruch genommen werden. Aber auch Angebote von Dienstleistern, die ihren Sitz in Staaten wie z. B. China haben, sind aufgrund ihrer regelmäßig kostengünstigeren Angebote attraktiv.

Eine Beauftragung eines Anbieters in einem Drittland[7] ist nur dann möglich, wenn ein besonderer Erlaubnisgrund der Art. 44 ff DSGVO vorliegt. Besonders relevant sind sog. **Angemessenheitsbeschlüsse** i. S. d. Art. 45 DSGVO (s. hierzu → **Handreichung I, 3.6**).

Es muss also bereits vor Zuschlagserteilung geprüft werden, ob für das Drittland eines Anbieters ein Angemessenheitsbeschluss besteht. Die EU-Kommission hat hierzu eine **Liste der Angemessenheitsbeschlüsse**[8] veröffentlicht.

---

[5] Vgl. LfD Bayern, Datenschutz als Kriterium im Vergabeverfahren, Orientierungshilfe v. 1. Februar 2024, Rn. 59.

[6] Siehe EDSA Guidelines 05/2021, Version 2.0, Rn. 16.

[7] Siehe EDSA Guidelines 05/2021, Version 2.0, Rn. 22 ff.

[8] Siehe https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

🔔 **Wichtig:** Da **Angemessenheitsbeschlüsse geändert, aufgehoben** oder durch den EuGH – in der Regel rückwirkend – für ungültig erklärt werden können, muss das Vertragswerk unbedingt **Regelungen enthalten, um in einem solchen Fall die Übermittlung in Drittländer sofort beenden** und die Daten zurückholen zu können.

Für die **Vereinigten Staaten** hat die EU-Kommission am 10. Juli 2023 ein Angemessenheitsbeschluss für das **„EU-U.S. Data Privacy Framework"** angenommen (→ Handreichung I, 3.6).[9] Viele Unternehmen, die Daten in den USA verarbeiten, setzen dabei allerdings **Unterauftragnehmer in weiteren Drittländern** ein.

🔔 **Wichtig:** Sollen i. R. e. Vergabe Unternehmen in den Vereinigten Staaten von Amerika in Anspruch genommen werden muss **vor Zuschlagserteilung geprüft** werden, ob das Unternehmen sich unter dem **„EU-U.S. Data Privacy Framework"**[10] freiwillig **zertifiziert** hat. Das Handelsministerium der Vereinigten Staaten hat hierzu eine **Liste**[11] der zertifizierten Unternehmen veröffentlicht.

→**Achtung**: Die Zertifizierung nach dem Privacy Framework unterscheidet in „hr data" (Beschäftigtendaten) und „non hr data". Sollen auch **Beschäftigtendaten** übermittelt werden, was bei Digitalisierungsvorhaben z. B. im Bereich des Supports nicht unüblich ist, so muss auch eine entsprechende **Zertifizierung für „hr data"** vorliegen.

2.3.2 Tochterunternehmen von Unternehmen in Drittländern

Viele große IT-Konzerne aus Drittländern bieten ihre Leistung über **Tochterunternehmen** an, die innerhalb der EU ansässig sind. Auch diese Anbieter können i. R. e. Vergabeverfahrens nicht ohne weiteres beauftragt werden. Es muss zuvor genau geprüft werden, ob nicht auch bei diesen die Gefahr eines Exports der pbD in das Drittland entsteht. So könnte die Drittlands-Muttergesellschaft oder öffentliche Stellen des Drittlandes das Tochterunternehmer anweisen, pbD aus der EU in das Drittland zu übermitteln.

Zwar reicht diese Gefahr allein noch nicht aus, um eine Übermittlung in ein Drittland i. S. d. Art. 44 ff. DSGVO anzunehmen. Soweit ein solcher Anbieter aber, wie im Regelfall, als Auftragsverarbeiter

[9] Der Vorgänger des EU-U.S. Data Privacy Framework, das „EU-U.S. Privacy Shield" ist durch den EuGH per Urteil v. 16. Juli 2020, C-311/18 („Schrems II") beanstandet worden, der den Vereinigten Staaten kein angemessenen Datenschutzniveau attestierte.

[10] Siehe https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

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

tätig wird, so kann diese Gefahr dazu führen, dass die **Zuverlässigkeit i. S. v. Art. 28 Abs. 1 DSGVO fehlt**.[12]

Soll i. R. e. Vergabeverfahrens ein Tochterunternehmen eines Drittlands-Mutterkonzerns beauftragt werden, so sind an die Sorgfalt der Zuverlässigkeitsprüfung i. S. v. Art. 28 Abs. 1 DSGVO (s. allgemein → Handreichung I, 3.3.3) besonders hohe Anforderungen zu stellen:

→ Zunächst sollte geprüft werden, ob für das Drittland des Mutterkonzerns ein **Angemessenheitsbeschluss** vorliegt, wie **oben unter 2.2.1** beschrieben (siehe die **Liste der Angemessenheitsbeschlüsse** der EU-Kommission[13]). Für die **Vereinigten Staaten** liegt ein solcher Angemessenheitsbeschluss vor (s. **oben unter 2.2.1).**

→ Soweit kein Angemessenheitsbeschluss vorliegt, muss noch genauer als sonst geprüft werden, ob sichergestellt ist, dass **technische und/oder organisatorische Maßnahmen** umgesetzt worden sind, die hinreichende Garantien dafür bieten, dass der Auftragsverarbeiter seinen Pflichten nachkommt, insbesondere was das Unterlassen von Verarbeitungen personenbezogener Daten ohne oder gegen die Weisung des Verantwortlichen angeht, im Speziellen auf der Grundlage von Verpflichtungen aus drittstaatlichem Recht.[14]

Zu beachten ist schließlich, dass öffentliche Auftraggeber nach der Rechtsprechung im Vergabeverfahren grundsätzlich darauf vertrauen dürfen, dass der Bieter seinen vertraglichen Zusagen nachkommt und beispielsweise keinen rechtlichen Verpflichtungen unterliegt, die ihn zu Verarbeitungen verpflichten, die nicht durch die Verantwortliche angewiesen sind.[15] Dies bedeutet allerdings nur, dass die Auftraggeber **vergaberechtlich** nicht zu einer Überprüfung verpflichtet sind. Sie sind dazu aber vergaberechtlich berechtigt, und dies auch ohne besonderen Anlass.[16] Vor dem Hintergrund, dass die Auftraggeber als Verantwortliche **aus datenschutzrechtlichen Gründen zu dieser Überprüfung verpflichtet** ist, sollte diese aber bereits i. R. d. Vergabeverfahrens erfolgen.[17]

---

[12] Vgl. DSK-Beschluss v. 31. Januar 2023 „Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten“, Ziff. 1-2; siehe auch 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.

[13] Siehe https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[14] Vgl. DSK-Beschluss v. 31. Januar 2023 „Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten“, Ziff. 2 und zum Prüfkatalog Ziff. 4.

[15] Vgl. OLG Karlsruhe, Beschl. v. 7.9.2022 - 15 Verg 8/22, NZBau 2022, 615 Rn. 35; OLG Düsseldorf, Beschl. v. 19.9.2018 - Verg 17/18, BeckRS 2018, 58390 Rn. 81.

[16] Vgl. OLG Düsseldorf, Beschl. v. 19.9.2018 - Verg 17/18, BeckRS 2018, 58390 Rn. 81; Bergt CR 2022, 629 Rn. 21.

[17] Vgl. Bergt CR 2022, 629.

2.4 Vollständiger Auftragsverarbeitungsvertrag

Es empfiehlt sich ferner, bereits ein vollständiges Muster eines Auftragsverarbeitungsvertrags (AVV) den Vergabeunterlagen zuzufügen. Hier kann der unter Beratung durch die BlnBDI durch die IKT-Steuerung und das ITDZ erstellte **Muster-AVV** genutzt werden.[18] Selbstverständlich muss das AVV-Muster nach Zuschlagserteilung sodann auch bindend zwischen der Verantwortlichen und dem Auftragsverarbeiter abgeschlossen werden.

2.5 Leistungsanforderungen aus Sicht der Informationssicherheit

Neben den spezifischen Datenschutz-Risiken sind im Zusammenhang mit Digitalisierungsvorhaben auch die Risiken der Informationssicherheit zu betrachten (siehe dazu → **Handreichung I, 3.8.5**).

Im Regelfall erfolgt im Zusammenhang mit Vergabeverfahren zu Digitalisierungsvorhaben eine Schutzbedarfsfeststellung nach der IT-Grundschutz-Methodik des BSI.[19] 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.[20] Auch methodisch ist Datenschutz in die Risikoanalyse aus Sicht der Informationssicherheit einzubeziehen, indem insbesondere i. R. d. Schutzbedarfsfeststellung auch das typische Schadensszenarium „Beeinträchtigung des informationellen Selbstbestimmungsrechts“ zu berücksichtigen ist.[21]

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 und können i. R. d. Leistungsbeschreibung eines Vergabeverfahrens berücksichtigt werden.

Die **Risikoanalyse aus Sicht der Informationssicherheit erledigt** dabei jedoch **nicht** bereits die Betrachtung der **Datenschutz-Risiken** (siehe → Handreichung I, 3.5.8). Ferner ist stets darauf zu achten, dass TOMs, die aus Sicht der Informationssicherheit umgesetzt werden sollen, ihrerseits datenschutzkonform eingerichtet sein müssen (z. B. Videoüberwachung zur Objektsicherung,

[18] Siehe: https://b-intern.de/themen/digitalisierung/ikt-vertraege/artikel.1014105.php.
[19] Siehe BSI-Standard 200-2 (IT-Grundschutz-Methodik), 7.5 und 8.2.
[20] Siehe dazu SDM, D 3.2.2, S. 53.
[21] Siehe BSI-Standard 200-2 - IT-Grundschutz-Methodik, 8.2, S. 104.

Cloud-Lösungen zum Malwareschutz oder Protokollierung). Auch dies muss bereits i. R. d. Leistungsbeschreibung berücksichtigt werden.

2.6 Beispiele für datenschutzrechtliche Leistungsanforderungen

In diesem Abschnitt werden Beispiele für datenschutzrechtliche Leistungsanforderungen dargestellt, die nach entsprechender Prüfung für das jeweilige Vergabeverfahren in Betracht gezogen werden können:

Das V-Modell XT führt die folgenden **Anforderungen** und **Ausschlüsse** aus Sicht des Datenschutzes für die Leistungsbeschreibung auf[22]:

- ➔ Personenbezogene Daten müssen bei der Übertragung verschlüsselt werden.
- ➔ Bei der Verschlüsselung von besonderen Kategorien pbD i. S. d. Art. 9 Abs. 1 DSGVO müssen kryptografische Verfahren der höchsten Sicherheitsstufe verwendet werden.
- ➔ Die Authentifizierung von Administrator-Konten muss per Smartcard erfolgen. Für alle übrigen Benutzerkonten ist ein softwarebasiertes Zertifikat zu verwenden.
- ➔ Jede Modifikation von pbD, insbesondere i. S. d. Art. 9 Abs. 1 DSGVO, ist mit Angabe des Zeitstempels, der Kennung des Ändernden und dem bisherigen Wert des Datums zu protokollieren.
- ➔ Es dürfen keine Daten vom System ausgewertet werden, die eine unmittelbare Leistungskontrolle bei der Nutzung des Systems durch einzelne Personen erlauben.
- ➔ Webserver dürfen keine IP-Adressen der Client-Rechner protokollieren.

Eine Liste von Beispielen für Ansatzpunkte zu datenschutzrechtlichen Leistungsanforderungen ist darüber hinaus der **Orientierungshilfe „Datenschutz als Kriterium im Vergabeverfahren“ des LfD Bayern** zu entnehmen.[23]

3 Verfahrenswahl

Schließlich kann auch eine passende Verfahrenswahl die Erfüllung der Vorgaben das Datenschutzes i. R. d. Vergabe fördern. So wird z. B. oberhalb der EU-Schwellenwerte ein Verhandlungsverfahren mit Teilnahmewettbewerb nach § 119 Abs. 5 GWB in Verbindung mit §§ 14 Abs. 3, 17 VgV oder ein wettbewerblicher Dialogs nach § 119 Abs. 6 GWB in Verbindung mit

[22] Vgl. das V-Model XT, C.1.10.3 – „Anforderungen Datenschutz“; siehe darüber hinaus allgemein ISO/IEC 27701 (Entwurf) „Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Datenschutz-Informationsmanagementsysteme - Anforderungen und Leitlinien“, Anhang A PIMS-Referenzmaßnahmenziele und -Maßnahmen für verantwortliche Stellen und Auftragsverarbeiter.

[23] LfD Bayern, Datenschutz als Kriterium im Vergabeverfahren, Orientierungshilfe v. 1. Februar 2024, Rn. 44.

§§ 14 Abs. 3, 18 VgV und unterhalb des EU-Schwellwerts insbesondere die Verhandlungsvergabe mit oder ohne Teilnahmewettbewerb gemäß § 8 Abs. 4 in Verbindung mit § 12 UVgO als praktikabelste Verfahren mit Blick auf den Datenschutz empfohlen.[24]

4 Auswahl geeigneter Auftragsverarbeiter, Hersteller und Produzenten

Schließlich müssen die zuständigen Stellen auf der Grundlage der aus Sicht des Datenschutzes optimierter Leistungsunterlagen geeignete Anbieter auswählen.

Auftragsverarbeiter müsse nicht nur zuverlässig sein (siehe oben 2.3.2), sondern auch verlässlich die Vorgaben der DSGVO zur Sicherheit der Verarbeitung pbD gewährleisten können müssen (Art. 32 DSGVO, siehe allg. → Handreichung I, 4.5). Diese verpflichten auch direkt die Auftragsverarbeiter und nicht nur Verantwortliche. Hierzu empfiehlt sich eine Recherche, inwieweit bei jeweiligen Anbietern zuletzt größere Sicherheitsprobleme aufgetreten sind und ob diese beseitigt werden konnten. Auch sollte geprüft werden, ob **Zertifizierungen** nach BSI und oder auch schon nach DSGVO (Art. 42, 43 DSGVO) bestehen.

Gegenstand der Beschaffung i. R. v. Digitalisierungsvorhaben sind darüber hinaus regelmäßig Hard- und Software-Produkte, die auch zur Verarbeitung pbD genutzt werden. Beschränken sich die **Hersteller oder Produzenten** dabei auf den reinen Verkauf oder die Vermietung der Produkte, so sind sie nicht direkt verpflichtet, den Datenschutz umzusetzen da sie weder Verantwortliche noch Auftragsverarbeiter sind (siehe dazu → Handreichung I, 3.2.1). Insbesondere sind sie nicht unmittelbare Adressaten der Vorgaben der DSGVO zu Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO). Es ist jedoch dringend zu empfehlen, im Rahmen von Vergabeverfahren nur solche Hersteller und Produzenten auszuwählen, die die Vorgaben des Art. 25 DSGVO umsetzen.[25]

[24] LfD Bayern, Datenschutz als Kriterium im Vergabeverfahren, Orientierungshilfe v. 1. Februar 2024, Rn. 60 ff.

[25] EDSA Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Version 2.0 v. 20. Oktober 2020, Rn. 96.

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)[26]	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.[27]
Europäischer Datenschutzausschuss (EDSA)[28]	Der Europäische Datenschutzausschuss ist ein unabhängiges europäisches Gremium. Es ist die Dachorganisation, die die nationalen Datenschutzbehörden der Länder des

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

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

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

	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.
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.[29]
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. [30]
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

[29] Siehe Art. 4 Nr. 1 DSGVO

[30] Siehe DSK Kurzpapier Nr. 18, S. 1.

	und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.[31]
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).
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).

[31] Siehe Datenschutzkonferenz Kurzpapier Nr. 18 - Risiko für die Rechte und Freiheiten natürlicher Personen (DSK Kurzpapier Nr. 18) unter Bezug auf DSGVO EG 75 und 94 S. 2.