

„DSGVO – information privacy standard’: Best-Practice Kriterien (AVVIS-02)

datenschutz cert GmbH
Version 0.7



Inhaltsverzeichnis

1. Einleitung.....	4
2. Umsetzungshinweise.....	5
2.1. P.1 Zulässigkeit der Datenverarbeitung	5
2.2. Besondere Umsetzungshinweise für Rechtsgrundlagen	15
2.3. P.2 Grundsätze.....	20
2.4. P.3 Pflichten des Kunden.....	23
2.5. P.4 Auftragsverarbeitung.....	25
2.6. P.5 Technisch-organisatorische Maßnahmen	28
2.7. P.6 Datenschutz-Management.....	33
2.8. P.7 Datenverarbeitung außerhalb der EU	38
2.9. P.8 Betroffenenrechte	41
3. Referenzen.....	51



Historie

Version	Date	Reason of change	Editor
0.1		Erstellung	Dr. Sönke Maseberg
0.2	10.02.2021	Fortschreibung	Alisha Gühr, Stefanie Bedürftig, Dr. Sönke Maseberg
0.3	25.06.2021	Fortschreibung nach LfDI Bremen Prüfung (20.05.2021)	Alisha Gühr, Dr. Sönke Maseberg, Dr. Irene Karper
0.4	28.10.2021	editorielle Überarbeitung sowie Fortschreibung nach LfDI Bremen Prüfung (20.10.2021)	Alisha Gühr, Dr. Sönke Maseberg, Dr. Irene Karper
0.5	29.08.2023	Überarbeitung sowie Fortschreibung nach Co Review Prüfung der LfDI Berlin, Italien	Alisha Gühr, Dr. Sönke Maseberg, Dr. Irene Karper
0.6	17.12.2024	Finalisierung	Alisha Gühr, Dr. Sönke Maseberg, Dr. Irene Karper
0.7	20.08.2025	Aktualisierung	Alisha Gühr, Dr. Sönke Maseberg, Dr. Irene Karper

Dokumenten-Überwachungsverfahren

Status	Prozess- / Dokumentenbesitzer	Version
final	Dr. Sönke Maseberg	0.7



1. Einleitung

„DSGVO – information privacy standard“ ist das DSGVO-Zertifizierungsprogramm der datenschutz cert GmbH, zu dem auch „Anwendungshinweise, verbindliche Vorgaben und Interpretationen zum Schema (AVVIS)“ gehören.

Das vorliegende Dokument AVVIS-02 enthält Umsetzungshinweise zum Kriterienkatalog [dsc_Kriterien]. Diese Umsetzungshinweise sind zur einheitlichen Interpretation und Auslegung der Kriterien verpflichtend hinzuzuziehen.

Dieses Dokument wird regelmäßig ergänzt und aktualisiert, um der ständigen Entwicklung im Datenschutzrecht gerecht zu werden und stets eine aktuelle Handlungshilfe zu bieten.

Dabei beachten Sie bitte, dass aufgrund der Fülle bestehender Orientierungshilfen und Positionspapiere der verschiedenen nationalen und europäischen Aufsichtsbehörden nicht alle abschließend aufgezählt werden können. Wir empfehlen dem Leser daher stets die aktuellen bestehenden Veröffentlichungen der Datenschutzaufsichtsbehörden zu beobachten. Wir empfehlen ferner auch die aktuelle Literatur und Fachkommentare zu den relevanten geltenden Gesetzen und Rechtsvorschriften heranzuziehen.

2. Umsetzungshinweise

2.1. P.1 Zulässigkeit der Datenverarbeitung

2.1.1. P.1.1 Identifikation Grundlagen

Umsetzungshinweise zum Kriterium

Die Übersicht über die Grundlagen enthält alle Anforderungen, die Einfluss auf den Datenverarbeitungsvorgang haben. Die Identifikation der Grundlagen umfasst insbesondere:

- DSGVO;
- Rechtsgrundlagen aus nationalen Konkretisierungen der DSGVO auf Basis der Öffnungsklauseln;
- Rechtsgrundlagen aus nationalem Recht;
- das Konformitätsbewertungs- bzw. Zertifizierungsprogramm mit dem vorliegenden Kriterienkatalog.

Weitere Grundlagen können sein:

- Auslegungshilfen des Europäischen Datenschutzausschusses (European Data Protection Board, EDPB);
- die Rechtsprechung der Europäischen Gerichtshöfe sowie der nationalen Gerichtsbarkeiten;
- nationale Vorgaben und Auslegungshilfen der Datenschutzaufsichtsbehörden.

Hinsichtlich der rechtlichen Grundlagen kann auch auf das Verzeichnis der Verarbeitungstätigkeiten verwiesen werden.

Die Aktualität der Übersicht setzt eine jährliche sowie anlassbezogene Kontrolle voraus. Änderungen in der Gesetzeslage und Auswirkungen auf die Übersicht sowie die Einschlägigkeit für die Datenverarbeitung sind zu beobachten.

2.1.2. P.1.2 Rechtsgrundlage Vertrag

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [EDSA_2/2019]
- [EDSA_4/2017]

Voraussetzung zur Erfüllung dieses Kriteriums ist das Vorliegen eines ordnungsgemäßen Vertrags oder vorvertraglicher Maßnahmen sowie die Erforderlichkeit jeder einzelnen Datenverarbeitung für die Erfüllung des Vertrags oder vorvertraglicher Maßnahmen. Diese müssen durch den Kunden nachgewiesen werden.

Die Erforderlichkeit der Datenverarbeitung ist restriktiv auszulegen und sollte durch den Verantwortlichen im Vorfeld geprüft werden. Die Erforderlichkeit umfasst keine Datenverarbeitungsvorgänge, die für den Verantwortlichen nützlich sind. Die

Erforderlichkeit der Datenverarbeitung sollte der betroffenen Person transparent dargelegt werden.

Ist die Datenverarbeitung objektiv zur Vertragsdurchführung nicht notwendig, so kann die Datenverarbeitung ggf. auf eine andere Rechtsgrundlage gestützt werden. Wird die Datenverarbeitung alternativ auf die Einwilligung gestützt, ist in diesem Zusammenhang insb. das sog. Kopplungsverbot der Einwilligung zu beachten, s. P 1.4. Bitte beachten Sie in diesem Fall, dass eine echte Wahlmöglichkeit zur Abgabe einer Einwilligung bestehen muss, ohne dass der Erhalt der Leistung versagt wird. Die Einwilligung sollte separat vom Unterzeichnen der Vertragsklauseln eingeholt werden.

Werden bei Verträgen, insb. über Online-Dienste, allgemeine Verarbeitungsklauseln mit in die Verträge aufgenommen, so sollte der Zweck der Verarbeitung angemessen beschrieben werden, also so präzise und klar formuliert werden, dass bei den einzelnen Datenverarbeitungsvorgängen festgestellt werden kann, auf welchem konkreten Zweck diese gestützt wird.

In diesem Kontext sollte für die betroffene Person ersichtlich sein, dass es sich bei der Unterzeichnung von Vorträgen oder dem Akzeptieren von Nutzungsbedingungen nicht um eine erteilte Einwilligung gem. Artikel 6 Absatz 1 Buchstabe a DSGVO handelt.

2.1.3. P.1.3 Rechtsgrundlage berechtigtes Interesse

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [Art.29_WP217]
- [DSK_Direktwerbung]

Relevante Erwägungsgründe: ErwGr. 47, 48, 49, 49, 38, 69, 71 DSGVO.

Bei der Interessensabwägung sind unter anderem die (angemessenen) Erwartungen der betroffenen Personen zum Zeitpunkt und im Zusammenhang mit der Erhebung der personenbezogenen Daten zu berücksichtigen, insb. ob die betroffenen Personen vernünftigerweise erwarten können, dass eine Verarbeitung zu diesem Zweck erfolgen kann.

Zur Begründung des berechtigten Interesses können folgende Prüfschritte erfolgen:

- Schritt 1: Ausschluss anderer Rechtsgrundlagen.
- Schritt 2: Formulierung eines rechtmäßig bestehenden, berechtigten sowie realen Interesses.
- Schritt 3: Prüfung, ob die Verarbeitung notwendig ist, um das verfolgte Interesse zu erreichen oder ob es andere, weniger stark in die Privatsphäre eingreifende Mittel zum Erreichen des genannten Zwecks möglich ist.
- Schritt 4: Herstellung eines vorläufigen Gleichgewichts, indem beurteilt wird, ob das Interesse des für die Datenverarbeitung Verantwortlichen durch die Grundrechte oder Interessen der betroffenen Personen überlagert wird. Insb. Berücksichtigung der Art der Datenverarbeitung, die betroffenen Grundrechte, Stellung der betroffenen Person (z. B. Minderjährigkeit, etc.).



- Schritt 5: Herstellung eines endgültigen Gleichgewichts unter Berücksichtigung zusätzlicher Schutzmaßnahmen: Es sind sorgfältig entsprechende Schutzmaßnahmen zu ermitteln sowie umzusetzen wie z. B. Datenminimierung, verstärkte Nutzung von Anonymisierungstechniken, Technologien zur Stärkung der Privatsphäre, Privacy by Design, Abschätzung der Folgen für die Privatsphäre und den Datenschutz, verstärkte Transparenz, allgemeines und nicht an Bedingungen geknüpftes Widerspruchsrecht (Verweigerung der Verarbeitung), Datenportabilität und verwandte Maßnahmen zur Stärkung der Position der betroffenen Personen.
- Schritt 6: Nachweis der Einhaltung und Gewährleistung von Transparenz: Dokumentation Schritt 1 -5 sowie Mitteilung an die betroffenen Personen.
- Schritt 7: Bei Ausübung des Widerspruchsrechts ist eine Neueinschätzung vorzunehmen und bei Bedarf die Datenverarbeitung einzustellen.

Die Verhinderung von Betrug kann ein berechtigtes Interesse des jeweiligen Verantwortlichen darstellen. Auch die Direktwerbung kann auf ein berechtigtes Interesse gestützt werden, für weitere Umsetzungshinweise vgl: [DSK_Direktwerbung].

Es kann ein berechtigtes Interesse bei Verantwortlichen, die Teil einer Unternehmensgruppe bzw. Gruppe von Einrichtungen sind, darin bestehen, welche personenbezogene Daten von Kunden und Beschäftigten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, zu übermitteln. Die Regelungen zum Datentransfer gem. Art. 44ff. DSGVO in Drittstaaten sind weiterhin zu beachten.

Gem. ErwGr. 49 DSGVO gilt für Netz- und Informationssicherheit bezüglich des überwiegend berechtigten Interesses Folgendes: „Die Verarbeitung von personenbezogenen Daten durch Behörden, Computer-Notdienste (Computer Emergency Response Teams – CERT, beziehungsweise Computer Security Incident Response Teams – CSIRT), Betreiber von elektronischen Kommunikationsnetzen und -diensten sowie durch Anbieter von Sicherheitstechnologien und -diensten stellt in dem Maße ein berechtigtes Interesse des jeweiligen Verantwortlichen dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, d.h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen“.

Die besondere Schutzbedürftigkeit von Kindern ist insbesondere bei der Durchführung einer Interessensabwägung für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden.

Das Widerspruchsrecht ermöglicht betroffenen Personen bei einer Datenverarbeitung, die der Verantwortliche auf das berechtigte Interesse stützt, trotz der besonderen Situation für den Verantwortlichen, Widerspruch einzulegen. Die Verarbeitung kann nach Ausübung des Widerspruchsrechts durch die betroffene Person nur fortgeführt werden, wenn der Verantwortliche darlegen kann, dass ihre zwingenden

berechtigten Interessen Vorrang vor den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person haben.

Bei der Datenverarbeitung zur Direktwerbung ist den betroffenen Personen ein unentgeltliches Widerspruchsrecht gegen die ursprüngliche oder spätere Verarbeitung einschließlich des Profilings zu ermöglichen

2.1.4. P.1.4 Rechtsgrundlage Einwilligung

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [Art.29_WP259]
- [Art.29_WP187]
- [Art.29_WP162]
- [Art.29_WP131]
- [Art.29_WP114]
- [Art.29_WP48]
- [DSK_K.Nr.4]
- [DSK_K.Nr.20]
- [DSK_ErwGr.33_DSGVO]
- [LfDI_Ni-Consent-Layer]
- [EDSA_2_2023]
- [EDSA_8_2024]

Relevante Erwägungsgründe: ErwGr. 32, 33, 43, 155, 171 DSGVO

Nur die jeweils betroffene Person kann einwilligen. Dritte können nicht für eine andere Personen einwilligen. Bitte beachten Sie, dass Ausnahmen nur bei begrenzt einwilligungsfähigen Personen bestehen können. Betroffenen Personen sind alle relevanten Informationen zur Verfügung zu stellen, um in Kenntnis der Sachlage – ohne jeglichen Zweifel – einwilligen können.

Die schriftliche Einholung der Einwilligung erleichtert den Nachweis, z. B. durch eine unterzeichnete Einverständniserklärung, die darlegt, warum ein für die Datenverarbeitung Verantwortlicher personenbezogene Daten sammelt und wie er diese weiterverarbeiten wird.

Die Einwilligung liegt in leicht zugänglicher Form vor, wenn sie offensichtlich platziert und nicht in längeren Textpassagen versteckt wurde. Bitte beachten Sie auch die Hinweise zum sog. „Nudging“ bei der Gestaltung von Consent-Tools.

Die Einwilligung dient nur als Grundlage für den Zweck, für den sie erteilt wurde. Wenn die Verarbeitung mehreren Zwecken dient, ist für alle Verarbeitungszwecke eine Einwilligung abzugeben werden. Eine Ausnahme gilt für Einwilligungen zur wissenschaftlichen Forschung, hier kann eine generelle Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung, unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung, wirksam erteilt werden. Für die Einholung



einer breiten Einwilligung (broad consent) sind die Umsetzungshinweise in [DSK_ErwGr.33_DSGVO] zu beachten.

Einwilligungen, die wirksam im Rahmen der rechtlichen Regelung der Richtlinie 95/46/EG erteilt wurden, bedürfen keiner erneuten Einwilligung der betroffenen Person, wenn die Art und Weise, in der die Einwilligung erteilt wurde, den Bedingungen dieser der DSGVO entspricht.

Bei Vorliegen eines eindeutigen Ungleichgewichts zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen ist nicht von Freiwilligkeit bei der Einwilligung auszugehen.

Bitte beachten Sie, dass sich die Freiwilligkeit durch das Vorliegen einer Wahlmöglichkeit zur Abgabe der Einwilligung. Eine Wahlmöglichkeit liegt nicht vor, wenn die Einwilligung nicht verweigert oder zurückgezogen werden kann, ohne Nachteile zu erleiden bzw. dem Risiko einer Täuschung, Einschüchterung oder Nötigung.

Ein Ungleichgewicht zwischen dem Verantwortlichen und der betroffenen Person liegt insb. im Verhältnis zu einer Behörde vor, in diesem Fall besteht tendenziell kein Wahlrecht zur Abgabe einer Einwilligung gegenüber der Behörde. Hier sind andere Rechtsgrundlagen einschlägig.

Auch im Beschäftigtenverhältnis liegt ein typisches Ungleichgewicht zwischen dem Verantwortlichen und der betroffenen Person vor. Eine Einwilligung kann nur als frei qualifiziert werden, wenn ein reales Wahlrecht auf Arbeitnehmerseite vorliegt. Weitere Regelungen dazu enthalten Art. 88 der DSGVO sowie ErwGr. 155 DSGVO.

Wird die Erteilung der Einwilligung an den Erhalt einer Leistung gekoppelt (sog. „Take-it-or-leave-it“ Situationen), ist dies als ein erheblicher Nachteil in der Leistungsverweigerung für die betroffenen Personen aufzufassen. Kein erheblicher Nachteil liegt z. B. bei einer alternativ kostenpflichtig angebotenen Leistung vor. Zur Abwägung ist [EDSA_8_2024] zu beachten. Um die Freiwilligkeit einer Einwilligung nachzuweisen, kann der Verantwortliche darlegen, dass die Erfüllung eines Vertrags nicht von der Einwilligung in eine Datenverarbeitung abhängig ist, die zur Erbringung dieser Leistung nicht erforderlich ist.

Bei entgegenstehendem Recht der Union oder der Mitgliedstaaten kann eine Unwirksamkeit der Einwilligung vorliegen, vgl. P.7.1 Datenübermittlung in Drittstaaten.

Für eine wirksame Einwilligung gem. Art. 49 Abs. 1 lit. a) DSGVO ist zunächst eine ausdrückliche Einwilligung in die Weitergabe ihrer Daten für den konkreten Fall erforderlich. Die betroffene ist Person im Vorfeld explizit über mögliche Risiken derartiger Datenübermittlungen aufzuklären, insb. über das unzureichende Datenschutzniveau und die Vereitelung von Betroffenenrechten.

Eine Alternative Rechtsgrundlage für die Fortführung der Datenverarbeitung bei Widerruf der Einwilligung kann sich aus Art 17 Abs. 3 DSGVO ergeben, nämlich wenn die Verarbeitung erforderlich ist zur

- Ausübung des Rechts auf freie Meinungsäußerung und Information;
- zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt,

erfordert, zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;
- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89
- Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Der Kunde (als Verantwortlicher) ist verantwortlich dafür, nachzuweisen, dass alternative Rechtsgrundlage einschlägig ist für den konkreten Fall.

2.1.5. P.1.5 Rechtsgrundlage rechtliche Verpflichtung

Umsetzungshinweise zum Kriterium

Relevante Erwägungsgründe: ErwGr. 45 DSGVO.

Bitte beachten Sie, dass eine Datenverarbeitung auf Grundlage einer rechtlichen Verpflichtung voraussetzt, dass die rechtliche Verpflichtung eine Grundlage im Recht der Union oder der Mitgliedstaaten hat.

Rechtliche Verpflichtungen meint z. B. Datenverarbeitungen im Zusammenhang mit:

- gesetzlichen Aufbewahrungspflichten;
- Beschäftigungsverhältnissen, z. B. für Arbeitsschutz, Sozialversicherungsträger oder das Finanzamt;
- Personenverkehr;
- Buchführungsunterlagen;
- Aufzeichnungspflichten;
- Infektionsschutz.

Zur rechtmäßigen Datenverarbeitung sollten insb. folgende Punkte berücksichtigt werden:

- Zweckgebundenheit und mögliche Beschränkungen der Rechtsgrundlage, auf die die Datenverarbeitung gestützt wird;
- Zulässigkeit der Datenverarbeitung für die konkrete Art(en) der personenbezogenen Daten;
- Notwendigkeit der Datenverarbeitung;
- Was sind die konkreten Anforderungen der Rechtsgrundlage hinsichtlich Weitergabe an Dritte, Aufbewahrungsfrist sowie zusätzlich zu ergreifenden Maßnahmen?

2.1.6. P.1.6 Rechtsgrundlage lebenswichtige Interessen

Umsetzungshinweise zum Kriterium

Relevante Erwägungsgründe: ErwGr. 46, 112DSGVO.

Die Zulässigkeit der Datenverarbeitung aufgrund lebenswichtiger Interessen umfasst die Datenverarbeitung zum Schutz bestimmter höchstpersönlicher Rechtsgüter, die unumkehrbar geschädigt werden können, wie die körperliche Unversehrtheit oder das Leben (Epidemien, humanitären Notfällen, Katastrophen). Zu beachten ist die vorrangige Regelung des Art. 9 DSGVO.

Folgende Elemente sind bei einer Datenverarbeitung aufgrund lebenswichtiger Interessen zu berücksichtigen:

- Darlegung der Notwendigkeit der Datenverarbeitung, um die lebenswichtigen Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.
- Feststellung der relevanten lebenswichtigen Interessen.
- Sicherstellung, dass tatsächlich keine Einwilligung der betroffenen Person eingeholt werden kann, bzw. bei einer anderen natürlichen Person eine andere Rechtsgrundlage für die konkrete Datenverarbeitung einschlägig ist.

In einigen Fällen kann die Datenverarbeitung wichtigen Gründen des öffentlichen Interesses als auch lebenswichtigen Interessen der betroffenen Person dienen, sodass die Verarbeitung auf beide Rechtsgrundlagen gestützt werden kann.

Insgesamt ist der Begriff lebenswichtige Interessen restriktiv auszulegen, schwerwiegende finanzielle Interessen fallen nicht in den Anwendungsbereich der Norm.

2.1.7. P.1.7 Rechtsgrundlage öffentliches Interesse

Umsetzungshinweise zum Kriterium

Relevante Erwägungsgründe: ErwGr. 45, 55 DSGVO

Eine Verarbeitung personenbezogener Daten aus Gründen des öffentlichen Interesses liegt bei einer staatlichen Stelle vor, wenn diese zu verfassungsrechtlich oder völkerrechtlich verankerten Zielen von staatlich anerkannten Religionsgemeinschaften personenbezogene Daten verarbeitet.

Zur rechtmäßigen Datenverarbeitung können folgende Punkte berücksichtigt werden:

- Zweckgebundenheit und mögliche Beschränkungen der Rechtsgrundlage, auf die die Datenverarbeitung gestützt wird
- Anforderungen der Rechtsgrundlage hinsichtlich Weitergabe an Dritte, Aufbewahrungsfrist, Art der personenbezogenen Daten sowie zusätzlich zu ergreifend Maßnahmen
- Tatsächliche Erforderlichkeit der Verarbeitung personenbezogener Daten für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde

- Sicherstellung der Einhaltung der Vorgaben
- Ggf. erforderlicher Genehmigungspflichten durch die zuständige Aufsichtsbehörde

2.1.8. P.1.8 Verarbeitung bei besonderen Kategorien personenbezogener Daten

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [EDSA_3/2020]
- [Art.29_WP131]
- [Art.29_WP 91]
- [DSK_K.Nr.17]

Relevante Erwägungsgründe: 35, 52, 53, 54, 56, 91 DSGVO.

Die Erforderlichkeit der Datenverarbeitung kann insb. aus dem Arbeits-, Sozialversicherungs- und Sozialschutzrechts, dem Unionsrecht, dem Recht der Mitgliedstaaten oder Kollektivvereinbarungen nach dem Recht der Mitgliedstaaten erwachsen.

Bitte beachten Sie spezialgesetzliche Regelungen, welche sich aus dem nationalen Recht der Mitgliedsstaaten ergeben können. Ggf. hat der Verantwortliche bei der Datenverarbeitung aufgrund der jeweiligen konkreten spezialgesetzlichen Regelungen (in Deutschland gelten z. B. Art. 9 Abs. 2 lit. b, g, h, i und j DSGVO i.V.m. §§ 22 Abs. 1, 27 und 28 BDSG) zusätzliche Maßnahmen zur Wahrung der Interessen der betroffenen Personen zu treffen. Zudem können branchenspezifische Anforderungen an die Rechtmäßigkeit eines bestimmten Datenverarbeitungsvorgangs, der die Verarbeitung besonderer Kategorien personenbezogener Daten umfasst, bestehen.

Dabei ist zu beachten, ob das anwendbare Recht des Mitgliedstaates Garantien vorsieht, welche einzuhalten sind. Sofern die Verarbeitung auf einem Tarifvertrag basiert, muss dieser den Anforderungen bestehender gesetzlich festgelegter Garantien entsprechen.

Besondere personenbezogene Daten sind weit auszulegen, bspw. können Abbildungen und Videos Hinweise auf besondere personenbezogene Daten enthalten.

Insb. im Zusammenhang mit Freitextfeldern ist die Möglichkeit der Verarbeitung aller Arten von Daten, auch besondere personenbezogene Daten zu beachten.

Werden Daten für gesundheitsbezogene Zwecke verarbeitet, so ist zu berücksichtigen, dass die Verarbeitung im Interesse einzelner natürlicher Personen und der Gesellschaft insgesamt erforderlich sein sollte, z. B. im Zusammenhang mit der Verwaltung der Dienste und Systeme des Gesundheits- oder Sozialbereichs, einschließlich der Verarbeitung dieser Daten durch die Verwaltung und die zentralen nationalen Gesundheitsbehörden zwecks Qualitätskontrolle, Verwaltungsinformationen und der allgemeinen nationalen und lokalen Überwachung des Gesundheitssystems oder des, zu wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken, die auf Rechtsvorschriften der Union oder der Mitgliedstaaten beruhen, die einem im

öffentlichen Interesse liegenden Ziel dienen müssen, sowie für Studien, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden.

Die Verarbeitung genetischer Daten im Bereich des Arbeitsrechts ist grundsätzlich verboten. Nur unter wirklich außergewöhnlichen Umständen und unter Berücksichtigung des Verbots ihrer Verarbeitung, das bereits in mehreren Mitgliedstaaten in Kraft ist, kann die Verarbeitung rechtmäßig erfolgen.

Zur rechtmäßigen Datenverarbeitung gem. Art. 9 Abs. 2 c) sind insb. folgende Punkte zu berücksichtigen:

„Die Verarbeitung muss sich auf wesentliche Einzelinteressen der betroffenen Person oder einer anderen Person beziehen und sie muss - im medizinischen Kontext - für eine lebensrettende Behandlung in einer Situation notwendig sein, in der die betroffene Person nicht in der Lage ist, ihre Absichten zum Ausdruck zu bringen (...) Und ist somit nicht zur Rechtfertigung der Verarbeitung personenbezogener medizinischer Daten für andere Zwecke als die Behandlung der betroffenen Person verwendet werden, wie z. B. für die Durchführung allgemeiner medizinischer Forschung, die erst in der Zukunft zu Ergebnissen führen wird“, vgl. [Art.29_WP131].

Sind die besonderen personenbezogenen Daten öffentlich verfügbare / veröffentlicht, gleichen diese einer ausdrücklichen Zustimmung, da beide auf einer frei getroffenen Entscheidung der betroffenen Person beruhen. Voraussetzung ist aber, dass die Daten von der betroffenen Person offenkundig öffentlich gemacht werden. Besteht ein begründeter Zweifel, dass personenbezogene Daten von der betroffenen Person offenkundig veröffentlicht wurden, ist Art. 9 Abs. 2 lit. e DSGVO nicht anwendbar.

Folglich kann die Verarbeitung personenbezogener Daten, die über einen Pressebeicht veröffentlicht wurden, in den meisten Fällen nicht auf diese Grundlage gestützt werden, personenbezogene Daten, die regelmäßig in einem öffentlichen Telefonbuch veröffentlicht wurden hingegen schon.

Zur Verarbeitung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken im Zusammenhang mit der COVID-19- Pandemie ist folgende Leitlinien vom EDSA zu beachten: [EDSA_3/2020].

Zur rechtmäßigen Datenverarbeitung gem. Art. 9 Abs. 2 lit. d) DSGVO berücksichtigen Sie bitte folgende Aspekte:

- Werden die personenbezogenen Daten von einer Stelle verarbeitet, die nicht gewinnorientiert ist? Wird ein politisches, philosophisches, religiöses oder gewerkschaftliches Ziel verfolgt und erfolgt die Verarbeitung im Rahmen der rechtmäßigen Tätigkeit der Stelle?
- Bezieht sich die Verarbeitung tatsächlich nur auf die (ehemaligen) Mitglieder der Körperschaft oder auf Personen, die im Zusammenhang mit den Zielen der Körperschaft regelmäßige Kontakte mit ihr haben?
- Erfolgt die Weitergabe der Daten nur mit Zustimmung der betroffenen Personen?

Die Datenverarbeitung politischer Parteien im Zusammenhang mit Wahlen kann, sofern jedenfalls geeignete Garantien vorgesehen werden, ggf. zur Einhaltung des demokratischen Systems (öffentliches Interesse) erforderlich sein.

Die Unterstützungspflichten des Auftragsverarbeiters ergeben sich aus der Weisung im Vertrag zur Auftragsverarbeitung. Dies kann z. B. umfassen, dass der Auftragsverarbeiter Kenntnis über die verarbeiteten Kategorien von Daten hat.

2.1.9. P1.9 Verarbeitung bei strafrechtlichen Verurteilungen und Straftaten

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [DSK_K.Nr.14]

Die Zulässigkeit der Verarbeitung richtet sich nach den Erlaubnistatbeständen des Art. 6 DSGVO. Es können sich gesonderte Rechtsgrundlagen aus nationaler Gesetzgebung der Mitgliedsstaaten ergeben, vgl. auch P.1.1.

Hinweise auf mögliche Straftaten und die damit verbundene Übermittlung personenbezogener Daten im Zusammenhang mit derselben Straftat durch den Verantwortlichen an eine zuständige Behörde können als berechtigtes Interesse des Verantwortlichen angesehen werden. Dies ist nicht gegeben, wenn die Verarbeitung mit einer rechtlichen, beruflichen oder sonstigen verbindlichen Pflicht zur Geheimhaltung unvereinbar ist.

Bitte beachten Sie, dass spezielle Regelungen, z. B. in Deutschland § 26 Abs. 1 BDSG, die Verarbeitung personenbezogener Daten von Beschäftigten zur Aufdeckung von Straftaten regeln. Demnach ist die Datenverarbeitung rechtmäßig, wenn tatsächliche Anhaltspunkte dokumentiert vorliegen, die den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, sofern die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der / des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insb. Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

2.1.10. P.1.10 Datenverarbeitung im Auftrag

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [EDSA_07/2020]
- [BayLfDI_Auftragsverarb.]
- [DSK_K.Nr.13]

Ein „Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Sie bestimmt nicht über die Zwecke und Mittel der Datenverarbeitung und ist vertraglich an die Weisung des Verantwortlichen gebunden. Die Auftragsverarbeitung basiert auf Art. 28 DSGVO.

Hat der Vertrag zwischen Verantwortlichen und Auftragsverarbeiter die IT-Wartung oder Fernwartung zum Gegenstand und besteht beim Auftragsverarbeiter die Möglichkeit auf personenbezogene Daten zuzugreifen, so liegt auch eine Verarbeitung i.S.d. Art. 4 Nr. 2 DSGVO (z. B. Auslesen, Abfragen, Verwenden) vor, sodass

entsprechend ein Auftragsverarbeitungsvertrag gem. Art. 28 DSGVO zu schließen ist; bei einer ausschließlich technischen Wartung der IT-Infrastruktur jedoch nicht.

Keine Auftragsverarbeitung ist hingegen die Inanspruchnahme fremder Fachleistungen bei einem eigenständigen Verantwortlichen wie beispielsweise Berufsgeheimnisträgers (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer), Inkassobüros mit Forderungsübertragung, Bankinstituts für den Geldtransfer oder Postdienstes für den Brieftransport.

Die Weitergabe personenbezogener Daten an den Auftragsverarbeiter, dessen Verarbeitung im Auftrag er durchführt, bedarf i.d.R. keiner weiteren Rechtsgrundlage i.S.d. Art. 6 bis 10 DSGVO als derjenigen, auf die der Verantwortliche selbst die Verarbeitung stützt. Die Zulässigkeit der Datenverarbeitung auf Seite des Verantwortlichen obliegt der Verantwortung des Verantwortlichen.

Für weitere Umsetzungshinweise vgl. auch: [EDSA_07/2020], [BayLfDI_Auftragsverarb.].

2.2. Besondere Umsetzungshinweise für Rechtsgrundlagen

2.2.1. Einschränkungen der Rechtsgrundlagen aufgrund ePD (Datenschutzrichtlinie für elektronische Kommunikation)

Bis die geplante E-Privacy-Verordnung in Kraft tritt, ist die E-Privacy-Richtlinie noch heranzuziehen. Teile der E-Privacy-Richtlinie sind im Gesetz gegen den unlauteren Wettbewerb umgesetzt. Das seit 1.12.2021 geltende Telekommunikations-Telemedien Datenschutzgesetz (TTDSG) enthält neue Datenschutzbestimmungen in der Telekommunikation und Telemedien.

Die Richtlinie enthält besondere Bestimmungen über die Verarbeitung von Verkehrs- und Standortdaten, die im Zusammenhang mit der Bereitstellung elektronischer Kommunikationsdienste erzeugt werden. Ebenfalls geregelt wird die Verwendung von Cookies und anderen im Endgerät eines Teilnehmers oder Nutzers gespeicherten Informationen und über die Herstellung unerbetener Direktmarketingkontakte zu Nutzern. Die Umsetzung erfolgte zum Teil in das TTDSG und in das TKG. Die DSGVO sieht in bestimmten Fällen (z.B. Verkehrsdaten) keine Regelung vor. Setzt das TTDSG die Vorgaben der Richtlinie ePD also um, so gelten diese als spezieller und gehen gemäß Art. 95 DSGVO den Vorgaben der DSGVO vor.

Die ePD findet Anwendung die für die Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der EU.

Im Falle der Verarbeitung personenbezogener Daten die Verwendung von Cookies, ähnlichen Technologien oder unerbetene Direktmarketingkontakte, richtet sich die Datenverarbeitung nunmehr nach § 25 TTDSG, welcher die Anforderungen des Art. 5 Abs. 3 ePD umsetzt. Es gelten die festgelegten Verpflichtungen für jede Stelle, die Informationen platziert und / oder Informationen abrufen, die bereits in den Endgeräten der betroffenen Personen gespeichert sind. Gemäß § 25 Abs. 1 TTDSG ist ein Personenbezug nicht erforderlich und erweitert somit den Anwendungsbereich bzw. dieser geht über den Anwendungsbereich der DSGVO hinaus. Es ist unerheblich, ob die Stelle,

die die Informationen platziert oder liest, ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter ist.

Die Begriffe "elektronisches Kommunikationsnetz", "öffentliches Kommunikationsnetz" und "elektronischer Kommunikationsdienst" sind in Art. 2 der ePD (Rahmenrichtlinie) definiert, die Begriffe "Verkehrsdaten", "Standortdaten" usw. in Art. 2 der ePD (umgesetzt in das TTDSG).

Art. 13 der ePD (unerbetene Nachrichten) ist eine allgemeine Bestimmung, die nicht nur für elektronische Kommunikationsdienste gem. der Definition der Rahmenrichtlinie gilt, sondern auch für alle anderen Dienste, die unerbetene Nachrichten verwendet. Art. 13 der ePD ist in § 7 UWG umgesetzt.

2.2.2. Zu Cookies

§ 25 TTDSG setzt die Anforderungen des Art. 5 Abs. 3 ePD um. Damit soll der Umgang mit Speichertechnologien geschaffen werden, die Zugriff auf Endgeräte von Anwendern haben. Cookies sind kleine Textdateien, die auf der Festplatte des Nutzers abgelegt werden und verschiedene Werte beinhalten können. Sie erlauben es, Informationen über einen bestimmten Zeitraum vorzuhalten und den Rechner bzw. das Endgerät des Besuchers zu identifizieren.

Zu Cookies sind insb. folgende Vorgaben zu beachten:

- [DSK_Telemedien]
- [LfDI_Ni-Consent-Layer]
- [EDSA_05/2020]
- [EDSA_01/2023]
- [Art.29_WP194]

Relevante Vorschriften: § 25 TTDSG; Art. 6 Abs. 1 lit. a, 7 DSGVO

Relevante Erwägungsgründe: ErwGr. 32 DSGVO. Die technische Seite der Speicherung solcher Informationen (HTTP-Cookies, Flash-Cookies, Silverlight-Cookies, Tracking Pixel und andere Techniken) auf dem Gerät des Nutzers ermöglichen verschiedene Methoden zur Nachverfolgung und somit einen Personenbezug. Es ist zu prüfen, welche Art von Cookies im Client des Nutzers platziert werden. Beispiele sind:

- Standard-HTTP-Cookies;
- Lokal freigegebene Objekte (Flash-Cookies);
- Silverlight Isolated Storage;
- History Caching;
- In RGB-Werten gespeicherte Cookies (in speziellen PNG-Dateien);
- In HTTP-ETags gespeicherte Cookies;
- Verschiedene HTML 5-Techniken (Sitzungs-, lokale, globale und Datenbankspeicherung);
- Speicherung von Benutzerdaten (Internet Explorer);
- Browser / Geräte-Fingerprinting (siehe z. B. unter <https://panopticklick.eff.org/>).

Zum Zwecke der Werbung oder Marktforschung ist eine Einwilligung der Teilnehmer oder Nutzer erforderlich, (§ 25 Abs. 1 S. 2 TTDSG i.V.m. Art. 7 DSGVO). Die Einwilligung ist nur wirksam, wenn gemäß § 25 Abs. 1 S. 2 TTDSG die Anforderungen des Art. 6 Abs. 1 lit. a, 7 DSGVO eingehalten werden.

Für eine Beurteilung der Wirksamkeit einer Einwilligung werden folgende Anforderungen gesetzt [DSK_Telemedien]:

- Einwilligung der Endnutzer des Endgeräts
- Zeitpunkt der Einwilligung
- Informiertheit der Einwilligung
- unmissverständliche und eindeutig bestätigende Handlung
- Bezug auf den konkreten Einzelfall
- Freiwilligkeit der Willensbekundung
- Widerrufsmöglichkeit, die ebenso einfach sein muss wie die Erteilung.

Die Einwilligung für einwilligungsbedürftige Datenverarbeitungsvorgänge kann durch ein „Consent-Tool“, eine vorgeschaltete Abfrage beim ersten Aufruf einer Website / Web-App, eingeholt werden. Die Einwilligung ist vor der Datenverarbeitung einzuholen. Zu den Anforderungen an die rechtmäßige Gestaltung und technischen Umsetzung eines Consent-Layers vgl. [LfDI_Ni-Consent-Layer], [EDSA_05/2020], [EDSA_01/2023].

Das Impressum sowie die Datenschutzerklärung dürfen nicht vom sog. Consent-Layer verdeckt werden und damit stets erreichbar sein [LfDI_Ni-Consent-Layer]

Eine rechtmäßige Einwilligung, entsprechend den Anforderungen der DSGVO, liegt bei einer eindeutig bestätigenden Handlung der betroffenen Person vor (Opt-In). Vorab angekreuzte Opt-in-Boxen führen nicht zur wirksamen Einwilligung [EDSA_01/2023], [ErwGr. 32]. Konkludente Einwilligungen durch Schweigen oder Untätigkeit der betroffenen Person stellen keine wirksame Einwilligung i.S.d. DSGVO dar. Irreführende Farbgestaltungen und Kontrastierungen sind unzulässig, daher ist die Sichtbarkeit der Optionen zu gewährleisten.

Der Ablehnen Button sollte auf dem ersten Layer sichtbar dargestellt werden [EDSA_01/2023], [DSK_Telemedien], [LfDI_Ni-Consent-Layer].

Eine „Widerruf-Schaltfläche“ sollte stets sichtbar zur Verfügung stehen, die jederzeit zugänglich ist. Erforderlich sei, dass der Widerruf jederzeit und ebenso einfach wie die Erteilung der Einwilligung möglich ist.

„Tracking“, eine Datenverarbeitung zur websiteübergreifenden Nachverfolgung des individuellen Nutzerverhaltens, bedarf in der Regel einer vorherigen Einwilligung, vgl. EuGH, 1.10.2019, C-673/17. Die Legitimation dieser Datenverarbeitung ergibt sich daher lediglich aus § 25 Abs. 1 S. 2 TTDSG i.V.m. Art. 6 Abs. 1 lit. a, 7 DSGVO.

Die betroffene Person ist insoweit einfach und transparent zu informieren, als dass es ihr möglich ist, in Kenntnis der konkreten Sachlage die Reichweite der Einwilligung abzugeben und zu verstehen.

Gestaltungen, um den Endnutzer zur Erteilung einer Einwilligung zu bewegen, sog. „Nudging“ oder auch „Dark Pattern“, bedürfen einer Einzelprüfung, da diese nicht grundsätzlich unzulässig sind [LfDI_Ni-Consent-Layer]. Folglich dürften farbliche Unterscheidungen zwischen Einwilligung und Ablehnung noch nicht als unzulässig zu bewerten sein. Eine Gesamtbetrachtung ist erforderlich und verlangt eine Prüfung, wonach der Nutzer zur Ablehnung nicht unzumutbare Schritte durchlaufen muss. Mehrstufige Cookie-Layer unterliegen daher einer strengen Einzelfallprüfung.

Die Einbindung eines Pixels zur Profilbildung kann nicht auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden, da der Nutzer keine Widerspruchsmöglichkeit hat oder durch sonstige Weise zum Ausdruck bringen kann, dass er die Profilbildung durch einen Dritten nicht wünscht. Als Rechtsgrundlage kann hier die Einwilligung als Rechtsgrundlage herangezogen werden.

Bei der Verwendung von unbedingt erforderlichen Cookies nach § 25 Abs. 2 Nr. 2 TTDSG ist eine Einwilligung nicht einzuholen. Insbesondere fallen technisch erforderliche Cookies i.S.d. § 25 Abs. 2 Nr. 2 TTDSG in diese Kategorie. Das können unter anderem funktionale Cookies für Komfortfunktionen sein oder Session Cookies, die nach jeder Sitzung gelöscht werden. Sog. Performance Cookies, die zu analytischen Zwecken eingesetzt werden, können nicht als „unbedingt erforderliche“ Cookies subsumiert werden [Art.29_WP194] und benötigen eine Einwilligung.

Zwingend erforderliche Cookies sollten in einer Liste vorgehalten werden sowie gegenüber einer Behörde nachgewiesen werden können. Dieses Working Paper [Art.29_WP194] bietet einen Überblick über zwingend erforderliche Cookies, wobei die Aufzählungen nicht abschließend sind.

Die Verarbeitung personenbezogener Daten bei der Erbringung von Telemediendiensten kann gegebenenfalls zur Vertragsdurchführung oder aufgrund einer Interessenabwägung rechtmäßig erfolgen.

Art. 6 der Richtlinie ePD betrifft ausschließlich die Speicherung von Verkehrsdaten durch den Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen Kommunikationsdienstes. Die DSGVO sieht weiterhin keine Vorgaben für den Umgang mit Verkehrsdaten vor. § 9 TTDSG setzt nun die Vorgaben des Art. 6 der Richtlinie ePD um. Aufgrund von Art. 95 DSGVO gehen speziellere Vorgaben der ePD der DSGVO vor, sodass § 9 TTDSG neben der DSGVO anwendbar ist und der DSGVO daher vorgeht.

Das TTDSG beinhaltet keine Legaldefinition für Verkehrsdaten und verweist mithin über § 2 Abs. 1 TTDSG auf § 3 Nr. 70 TKG. Danach sind Verkehrsdaten „Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind“. Der Begriff der Verkehrsdaten ist daher sehr weit zu verstehen, sodass alle Daten erfasst sind, die mit der Übermittlung / Weiterleitung einer Nachricht in ein TK-Netz in Verbindungen stehen.

Gemäß § 9 Abs. 1 dürfen Verkehrsdaten nur verarbeitet werden, sowie diese zum Aufbau und zur Aufrechterhaltung der Telekommunikation, zur Entgeltabrechnung oder zum Aufbau weiterer Verbindungen erforderlich ist. Der nichtabschließende Katalog von § 9 Abs. 1 Nr. 1 bis 5 TTDSG ist hierbei zu beachten. Die Löschung der Verkehrsdaten muss unverzüglich nach Beendigung der Verbindung erfolgen, § 9 Abs. 1 S. 2 TTDSG.

In Fällen der teilnehmerbezogenen Verkehrsdaten ist die Einwilligung gemäß § 9 Abs. 2 S. 1 TTDSG i.V.m. Art. 6 Abs. 1 lit. a, 7 DSGVO einzuholen. Beispielhaft zu nennen ist die Nutzung von Verkehrsdaten zur Vermarktung von Telekommunikationsdiensten.

In Bezug auf Protokolldateien, die von Website-Betreibern geführt werden, ist diese Bestimmung nicht anwendbar. Vielmehr kann Art. 6 Abs. 1 lit. f DSGVO als Rechtsgrundlage angesehen werden (vgl. EuGH, 19.10.2016, C-582/14).

2.2.3. Besonderheiten für Videosprechstunden gemäß § 365 Absatz 1 SGB V

Im Rahmen der Videosprechstunde sind des Weiteren die Anforderungen an die technischen Verfahren zur Videosprechstunde gemäß § 365 Absatz 1 SGB V zu berücksichtigen. Danach hat der Gesetzgeber bestimmte Verbände befugt, datenschutzrechtliche Anforderungen an Videosprechstunden zu konkretisieren. Beispiel ist die Anlage 31b zum Bundesmantelvertrag-Ärzte (BMV-Ä) mit der Vereinbarung über die Anforderungen an die technischen Verfahren zur Videosprechstunde gemäß § 365 Absatz 1 SGB V. Gleichlautende Regelungen liegen ferner vor für Zahnärzte, Pflegedienste und Psychologen.

Im Rahmen von Videosprechstunden ist zusätzlich § 2a Absatz 2 der Anlage 31b BMV-Ä (bzw. die gleichlautenden Vorschriften für Zahnärzte, Pflegedienste und Psychologen) i.V.m. § 365 SGB V zu beachten. Hiernach darf die Verarbeitung von personenbezogenen Daten auch im Auftrag nur im Inland, in einem Mitgliedsstaat der Europäischen Union oder in einem diesem nach § 35 Absatz 7 des Ersten Buches Sozialgesetzbuch gleichgestellten Staat, oder, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat erfolgen.

Eine datenschutzrechtlich unzulässige Übermittlung von personenbezogenen Daten in ein Drittland liegt auch vor, wenn der entsprechende Server von einer in der EU ansässigen Gesellschaft betrieben wird, die ihrerseits Teil eines Konzerns mit Drittstaatenbezug ist. Insbesondere beim Betrieb von Telemedien kommen Technologien zum Einsatz, wo auch eine Datenübermittlung in einen Drittstaat zur Folge hat.

Beim Betrieb einer Videosprechstunde werden Technologien eingesetzt, die es ermöglichen, personenbezogene Daten von Nutzenden zu verschiedenen Zwecken zu verarbeiten. Dies gilt insbesondere für den Einsatz von Cookies, mittels derer Informationen auf den Geräten der Nutzenden abgelegt und verwaltet werden können, die bei der Verwendung eindeutiger Kennungen (sog. UIDs) eine Identifikation bzw. Zuordnung zu einer natürlichen Person zulassen. Erfolgt der Einsatz von Cookies auf einer Videosprechstundenwebsite, so fallen diese ebenfalls in den Anwendungsbereich des § 25 TTDSG.

Folglich orientiert sich die Prüfung der Videosprechstunde auch an § 25 TTDSG mit der Ausnahme, dass Dienstleister in Drittstaaten ohne Angemessenheitsbeschluss nicht eingesetzt werden können.

Eine Übermittlung von personenbezogenen Daten (bspw. nach Indien) mittels Cookies oder anderweitigen Technologie darf daher zu keinem Zeitpunkt im Rahmen der Videosprechstunde erfolgen. Personenbezogene Daten, die im Zusammenhang mit der regelmäßigen Nachverfolgung durch einen Dienstleister mit Drittstaatenbezug

verarbeitet werden, sind absolut unzulässig und können auch nicht auf Grundlage einer Einwilligung übermittelt werden.

2.3. P.2 Grundsätze

2.3.1. P.2.1 Privacy-by-Design

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [EDSA_4/2019]
- [DSK_S-D-M_V.2.ob]
- [PRIPARE]

Relevante Erwägungsgründe: 78 DSGVO.

Der Verantwortliche bzw. der Auftragsverarbeiter soll seinen Datenverarbeitungsvorgang bereits während der Konzeption und Entwicklung auf besonders datenschutzfreundlichen Bedingungen ausrichten. Dabei ist zu beachten, dass sich die Verpflichtung auf jegliche Verarbeitungen, welche durch Auftragsverarbeiter durchgeführt werden erweitert. Die regelmäßige Kontrolle der Auftragsverarbeiter durch Verantwortliche sollte diesen Aspekt umfassen.

Als mögliche methodische Grundlagen für die Entwicklung geeigneter Maßnahmen können z.B. folgende Modelle herangezogen werden:

- PRIPARE (PReparing Industry to Privacy-by-design by supporting its Application in Research)
- SDM (Standard-Datenschutzmodell)

2.3.2. P.2.2 Privacy-by-Default

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [EDSA_4/2019]
- [DSK_S-D-M_V.2.ob]
- [PRIPARE]

Relevante Erwägungsgründe: 78 DSGVO.

Der Verantwortliche bzw. der Auftragsverarbeiter soll datenschutzfreundliche Voreinstellungen für jegliche Verarbeitungen personenbezogener Daten achten. Dabei ist zu beachten, dass sich die Verpflichtung auf jegliche Verarbeitungen, welche durch Auftragsverarbeiter durchgeführt werden erweitert. Die regelmäßige Kontrolle der Auftragsverarbeiter durch Verantwortliche sollte diesen Aspekt umfassen.

Der Nutzer soll die datenschutzfreundlichste Lösung der Verarbeitung ohne weiteres Zutun erhalten.

Insbesondere bei der Gestaltung von Consent-Tools, Datenschutz oder Profileinstellungen sollte diesem Grundsatz besondere Beachtung zukommen.

Die Gestaltung des Datenschutz-Managementsystem (DSMS) folgt einer strukturierten Methodik mit PDCA-Zyklus („Plan-Do-Check-Act“, „Planen-Umsetzen-Überprüfen-Handeln“). Dies impliziert einen regelmäßigen Zyklus zur Verbesserung, Pflege und Aufrechterhaltung des DSMS und einer regelmäßigen Überprüfung und, sofern erforderlich, Anpassung der getroffenen Maßnahmen.

Als mögliche methodische Grundlagen für die Entwicklung geeigneter Maßnahmen können z.B. folgende Modelle herangezogen werden:

- PRIPARE (PReparing Industry to Privacy-by-design by supporting its Application in Research)
- SDM (Standard-Datenschutzmodell)

2.3.3. P.2.3 Zweckbindung

Umsetzungshinweise zum Kriterium

Relevante Erwägungsgründe: 50 DSGVO.

Eine Möglichkeit, die Umsetzung dieses datenschutz-rechtlichen Grundsatzes nachzuweisen („Rechenschaftspflicht“), ist, für alle verwendeten Datenarten deren Zweck zu analysieren und zu prüfen, dass die Datenverarbeitung abschließend diesem Zweck genügt. Dazu sind ferner entsprechende Prozesse und weitere Regelungen und Dokumente (Verzeichnis der Verarbeitungstätigkeiten, Richtlinien, Hinweise, Anweisungen oder Verfahren zur Kontrolle der Umsetzung) zu berücksichtigen.

Eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke ist nicht unvereinbar mit dem ursprünglichen Zweck. Gegebenenfalls sind jedoch Rechte des Betroffenen, wie z. B. eine Widerspruchsmöglichkeit zu achten. Um festzustellen, ob eine Verarbeitung zu einem anderen Zweck mit dem ursprünglichen Zweck vereinbar ist, sind die Verbindungen zwischen den Zwecken, der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, die Art der personenbezogenen Daten, die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen sowie das Vorhandensein geeigneter Garantien zu berücksichtigen.

Für Auftragsverarbeiter ergeben sich die Zwecke aus dem Vertrag zur Auftragsverarbeitung und den Weisungen des Verantwortlichen.

Die Weiterverarbeitung personenbezogener Daten für andere Zwecke als den / die Zweck(e), für den / die sie ursprünglich erhoben wurden, ist nur erlaubt, wenn die Verarbeitung mit den Zwecken vereinbar ist, für die die personenbezogenen Daten ursprünglich erhoben wurden. In einem solchen Fall ist keine rechtliche Grundlage erforderlich, die von derjenigen getrennt ist, die die Erhebung der personenbezogenen Daten erlaubte.

In einem solchen Fall ist die betroffene Person über diesen anderen Zweck und alle relevanten weiteren Informationen (Verarbeitung für einen anderen Zweck gem. Art. 13 Abs. 3 bzw. Art. 14 Abs. 4 des DSGVO) zu informieren.

2.3.4. P.2.4 Datenminimierung

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [DSK_S-D-M_V.2.ob]

Relevante Erwägungsgründe: 39 DSGVO.

Eine Möglichkeit, die Umsetzung dieses datenschutz-rechtlichen Grundsatzes nachzuweisen („Rechenschaftspflicht“), ist, für alle verwendeten Datenarten deren „Minimalität“ zu analysieren und zu prüfen, d.h. dass diese Datenarten für die Datenverarbeitung unverzichtbar sind. Dazu sind ferner entsprechende Prozesse und weitere Regelungen und Dokumente (Verzeichnis der Verarbeitungstätigkeiten, Richtlinien, Hinweise, Anweisungen oder Verfahren zur Kontrolle der Umsetzung) zu berücksichtigen.

Für die Verarbeitung sind nur die Daten zu erfassen, die für Verarbeitung erforderlich sind. Erforderlichkeit i.S.d. Norm liegt vor, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann.

Für Auftragsverarbeiter ergeben sich die Zwecke aus dem Vertrag zur Auftragsverarbeitung und den Weisungen des Verantwortlichen.

Für weitere Umsetzungshinweise vgl. auch: Das Standard-Datenschutzmodell Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, V. 2.ob.

2.3.5. P.2.5 Richtigkeit

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [DSK_S-D-M_V.2.ob]
- [EDSA_4/2019]

Relevante Erwägungsgründe: 39 DSGVO.

Eine Möglichkeit, die Umsetzung dieses datenschutz-rechtlichen Grundsatzes nachzuweisen („Rechenschaftspflicht“), ist, die dazu etablierten Prozesse und ihre Wirksamkeit darzulegen. Dazu sind ferner entsprechende Prozesse und weitere Regelungen und Dokumente (Verzeichnis der Verarbeitungstätigkeiten, Richtlinien, Hinweise, Anweisungen oder Verfahren zur Kontrolle der Umsetzung) zu berücksichtigen.

Der Grundsatz der Richtigkeit personenbezogener Daten steht im Einklang mit zahlreichen Betroffenenrechten, wie das Recht auf Berichtigung oder Löschung.

Der Umfang der Verpflichtung, die sich für den Verantwortlichen aus dem Grundsatz der Richtigkeit ergibt, ist weit auszulegen: Es sind alle vertretbaren Schritte zu unternehmen, um unrichtige personenbezogene Daten zu löschen oder zu berichtigen.

Für Auftragsverarbeiter ergibt sich die Richtigkeit personenbezogener Daten aus dem Vertrag zur Auftragsverarbeitung und den Weisungen des Verantwortlichen.

Für weitere Umsetzungshinweise vgl. auch: Das Standard-Datenschutzmodell Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, V. 2.ob.

2.3.6. P.2.6 Speicherbegrenzung

Umsetzungshinweise zum Kriterium

Relevante Erwägungsgründe: 30, 39 DSGVO

Eine Möglichkeit, die Umsetzung dieses datenschutz-rechtlichen Grundsatzes nachzuweisen („Rechenschaftspflicht“), ist, für alle verwendeten Datenarten deren Aufbewahrungsfristen zu analysieren und zu prüfen, dass die Daten nicht länger als erforderlich gespeichert werden. Dazu sind ferner entsprechende Prozesse und weitere Regelungen und Dokumente (Verzeichnis der Verarbeitungstätigkeiten, Richtlinien, Hinweise, Anweisungen oder Verfahren zur Kontrolle der Umsetzung) zu berücksichtigen.

Die Speicherfrist ist auf das erforderliche Mindestmaß zu beschränken. Der Verantwortliche oder der Auftragsverarbeiter kann durch geeignete Löschkonzepte, z. B. in Orientierung an DIN 66398, die Sicherstellung der Einhaltung von Fristen nachweisen, z. B. durch Festlegung einer regelmäßigen Überprüfung der Löschrufen. Aufbewahrungsfristen aus anderen Gesetzen können sich auf die Speicherbegrenzung auswirken.

Eine Ausnahme gilt für personenbezogene Daten, die ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gem. Art. 89 Abs. 1 DSGVO verarbeitet werden, sofern geeignete technische und organisatorische Maßnahmen getroffen wurden.

Für Auftragsverarbeiter ergeben sich die Löschrufen aus dem Vertrag zur Auftragsverarbeitung und den Weisungen des Verantwortlichen.

2.3.7. P.2.7 Treu und Glauben

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [EDSA_4/2019]

Relevante Erwägungsgründe: 39 DSGVO

2.4. P.3 Pflichten des Kunden

2.4.1. P.3.1 Informationspflichten des Kunden

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [DSK_K.Nr.10]
- [EDSA_4 / 2019]

Relevante Erwägungsgründe: 39, 58, 60, 61, 62 DSGVO.

Die Informationen, die der Verantwortliche betroffenen Personen mitteilt, ergeben sich aus den Art. 13 und 14 sowie 15 bis 22 und 34 DSGVO, vgl. auch nachfolgende Kriterien aus P.3.1.

Die Informationen können je nach Art des Datenverarbeitungsvorgangs z. B. in einer Datenschutzerklärung, in einem Impressum, in Leitfäden, Informationsblättern oder auf Hinweisschildern wiedergegeben werden.

Die Informationen können in Kombination mit standardisierten, maschinenlesbaren Bildsymbolen bereitgestellt werden.

Um eine faire und transparente Verarbeitung zu gewährleisten umfasst die Informationspflicht auch Angaben über die Umstände und Rahmenbedingungen bezüglich der Datenverarbeitung. Die betroffenen Personen sollten darüber in Kenntnis sein, welche Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang dies geschieht bzw. künftig geschehen wird.

Die Informationen können der Verständlichkeit halber mit zusätzlich visuellen Elementen versehen werden. Richtet sich die Verarbeitung an Kinder, sollten aufgrund der besonderen Schutzwürdigkeit von Kindern Informationen und Hinweise in einer klaren und einfachen Sprache erfolgen, sodass ein Kind die Information verstehen kann, dabei ist insb. die Altersgruppe der betroffenen Kinder zu berücksichtigen.

Eine Verarbeitung nach Treu und Glauben erlaubt es nicht, dark patterns zu verwenden, um die betroffenen Personen zu einem bestimmten Verhalten zu verleiten, das dem für die Verarbeitung Verantwortlichen zugutekommt und die betroffene Person einem unerwarteten Risiko aussetzt.

Eine Ausnahme von der Informationspflicht kann bestehen, wenn die betroffene Person nachweislich bereits über die Informationen verfügt. Zudem kann eine Ausnahme von der Informationspflicht, sofern die Erhebung nicht bei der betroffenen Person erfolgt, bestehen, wenn es dem Verantwortlichen unmöglich ist, die Informationen zu erteilen oder dies einen unverhältnismäßigen Aufwand erfordern würde, sofern der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person ergreift und die Informationen öffentlich bereitstellt. Die Informationen müssen der betroffenen Person ebenfalls nicht erteilt werden, wenn die Erlangung oder Offenlegung der Daten durch Rechtsvorschriften, denen der Verantwortliche unterliegt ausdrücklich geregelt ist und geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen oder die personenbezogenen dem Berufsgeheimnis unterliegen und daher vertraulich behandelt werden müssen.

Anforderungen an die Informationspflichten bei Dritt- und Direkterhebung, siehe [DSK_K.Nr.10].

Im Hinblick auf das Transparenzgebot sollte der Verantwortliche stets den Nachweis einer ordnungsgemäßen Erledigung der Informationspflichten erbringen können.

2.5. P.4 Auftragsverarbeitung

2.5.1. P.4.1 Vertrag zur Auftragsverarbeitung (AV-Vertrag)

Umsetzungshinweise zum Kriterium

Bei standardisierten Massengeschäften werden I.d.R., auch unter Unternehmern, vorformulierte Vertragsklauseln (Allgemeine Geschäftsbedingungen, AGB) eingesetzt, die wirksam im Sinne des jeweiligen AGB-Rechts sein müssen. Im (vorformulierten oder individuell ausgehandelten) AV-Vertrag wird auch das anwendbare Recht aufgenommen. Der AV-Vertrag muss als ein Bestandteil des Hauptvertrags zwingend mit diesem verknüpft sein und inhaltlich Konnektivität aufweisen.

Der Vertrag kann unbeschadet eines individuellen Vertrags auch ganz oder teilweise auf Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gem. den Art. 42 und 43 erteilten Zertifizierung sind.

Beim Vertragsschluss wird der passende Vertragstyp gewählt. I.d.R. wird bei der Festlegung des Vertragstyps eine Schwerpunktbetrachtung aller Leistungen aus Sicht der betroffenen Person vorgenommen.

Gegenstand sowie Dauer des Auftrages werden durch einen Start- und Endpunkt oder den Verweis auf eine unbestimmte Nutzungszeit festgelegt.

Neben dem Kernvertrag sollten die verwendeten und Stand der Technik entsprechenden technischen und organisatorischen Maßnahmen in einer zusätzlichen Anlage dem Vertrag angefügt werden, so dass diese der betroffenen Person bekannt sind.

Im Vertrag ist festzulegen, ob die Auftragsverarbeitung potenziell in der EU oder in Drittstaaten stattfindet und relevante Drittstaaten benannt werden.

Die vorherige gesonderte oder allgemeine schriftliche Genehmigung zum Einsatz von Subauftragnehmern ist zwingender Bestandteil eines rechtskonformen AV-Vertrags. In dem Vertrag zur Auftragsverarbeitung zwischen Auftragsverarbeiter und Verantwortlichem kann eine allgemeine schriftliche Genehmigung vereinbart werden, sofern der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung der eingesetzten Subauftragnehmer informiert und dem Verantwortlichen die Möglichkeit gewährt innerhalb einer angemessenen Frist einen Einspruch zu erheben.

Die Weisungsbefugnisse sind zwingender Bestandteil eines rechtskonformen AV-Vertrags. Aus dem Vertrag sollte genaustens hervorgehen, welche Personen bei dem Verantwortlichen zur Erteilung von Weisungen befugt sind.

2.5.2. P.4.2 Umsetzung der Maßnahmen gem. AV-Vertrag

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [DSK_K.Nr.13]

Der Auftragsverarbeiter ist verpflichtet die personenbezogenen Daten nur aufgrund der Weisung des Auftraggebers zu verarbeiten. Hierzu können Weisungsberechtigte und weisungsempfangsberechtigte Personen vereinbart werden.

Die Verpflichtung von Mitarbeitern des Auftragsverarbeiters, welche mit der Verarbeitung von personenbezogenen Daten im Auftrag betraut sind, zur Verschwiegenheit kann etwa im Arbeitsvertrag erfolgen. Sollten gesonderte Vertraulichkeitsanforderungen bestehen, etwa gem. § 203 StGB im deutschen Recht, sind Mitarbeiter auch diesbezüglich zu verpflichten.

Die vertraglich vereinbarten und für die Datenverarbeitung geeigneten technischen und organisatorischen Maßnahmen sind vom Auftragsverarbeiter umzusetzen, jederzeit dem Stand der Technik zu entsprechen und werden bei Bedarf angepasst. Zum Begriff bzw. Technologieniveau "Stand der Technik" vgl. 2.6.1. P.5.1.

Daraus ergibt sich, dass die technischen und organisatorischen Maßnahmen in gewisser Regelmäßigkeit im Hinblick auf Technologiestände überprüft und bei Bedarf nachzubessern sind.

Ist eine allgemeine schriftliche Genehmigung zum Einsatz weiterer Auftragsverarbeiter vereinbart, ist zu beachten, dass der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informiert, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Eine bloße Mitteilung z. B. auf der Webseite ist nicht ausreichend. Ist der Verantwortliche nicht mit dem Einsatz des Subauftragnehmers einverstanden ermöglicht ihm der Auftragsverarbeiter ohne Einschaltung dieses Subdienstleisters fortzufahren und oder die Kündigung des Vertragsverhältnisses mit dem Auftragsverarbeiter.

Der Auftragsverarbeiter kann nur Subauftragnehmer einsetzen, sofern er mit diesen einen Vertrag zur Auftragsverarbeitung geschlossen hat, welcher die Anforderungen des Art. 28 DSGVO erfüllt und ein Datenschutzniveau entsprechend der DSGVO gewährleistet wird. Der Auftragsverarbeiter stellt sicher, dass die Subunternehmer die geeigneten technischen und organisatorischen Maßnahmen umgesetzt haben.

Zur Unterstützungspflicht des Auftragsverarbeiters zählen z. B.:

- die Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person;
- die Einhaltung der in den Art. 32 bis 36 DSGVO Pflichten (Sicherheit der Verarbeitung, Meldung von Datenschutzverletzungen an die Aufsichtsbehörde, Benachrichtigung von betroffenen Personen bei Datenschutzverletzungen, Datenschutz-Folgenabschätzung und vorherige Konsultation), insb.
 - die unverzügliche Berichterstattung an den Auftraggeber bei einer Datenschutzverletzung;
 - die Feststellung von relevanten Verletzungsereignissen;
 - Unterstützung bei der Einhaltung der Informationspflichten gegenüber der betroffenen Person; dazu gehört auch die unverzügliche Bereitstellung relevanter Informationen.

Der Auftragsverarbeiter kann die Löschung oder Rückgabe der Daten wie vertraglich mit dem Verantwortlichen vereinbart umsetzen.

Der Auftragsverarbeiter kann sicherstellen, dass dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung zur Verfügung gestellt werden und Überprüfungen ermöglicht werden, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden.

2.5.3. P.4.3 Audit

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [BayLDA_GoodPractice]
- [EDSA_o7/2020]

Relevante Erwägungsgründe: 81 DSGVO.

Die Erfüllung dieses Kriteriums dient dazu, dass der Verantwortliche bzw. Auftragsverarbeiter sicherstellt, dass er nur Auftragsverarbeiter einsetzt, die hinreichende Garantien dafür bieten, dass durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt. Bestenfalls sollten nur Dienstleister genutzt werden, die die Garantien (in Form von Dokumenten) zur Verfügung stellen können und die über Fachwissen und Ressourcen verfügen, zuverlässig sind und hinreichende Garantien bieten.

Der Verantwortliche ist verpflichtet, die Angemessenheit der Garantien zu beurteilen und nachweisen zu können, dass er gewissenhaft alle Anforderungen der DSGVO berücksichtigt hat. Zum Nachweis können Dokumente wie z. B. Datenschutzerklärung, Nutzungsbedingungen, Aufzeichnungen Verarbeitungstätigkeiten, Archivverwaltungspolitik, Informationssicherheitspolitik, Berichte über externe Audits, anerkannte internationale Zertifizierungen, wie die ISO 27000er Serie, herangezogen werden.

Die Beurteilung, ob die Garantien ausreichend sind hängt von der konkreten Art der Verarbeitung ab und ist im Einzelfall unter Berücksichtigung vom Umfang, Kontext und Zweck der Verarbeitung abhängig.

Mögliche Maßnahmen zur Kontrolle eines Dienstleisters:

- Nachweise auf Dokumentationsbasis, etwa durch ausgefüllten Fragebogen;
- Remote-Audits;
- Vor-Ort Kontrollen;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Datenschutzbeauftragter oder Auditoren);
- Zertifikat eines Informationssicherheits-Managementsystems (z. B. ISO/IEC 27001 oder ISO 27001 auf der Basis von IT-Grundschutz);
- Nachweis genehmigter Verhaltensregeln gem. Art. 40 DSGVO;
- Nachweis genehmigtes Zertifizierungsverfahren gem. Art. 42 DSGVO.

Die Umsetzungshinweise der ISO/IEC 27002, Kapitel 15 sind anwendbar.

2.6. P.5 Technisch-organisatorische Maßnahmen

2.6.1. P.5.1 Festlegung geeigneter Maßnahmen

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [DSK_S-D-M_V.2.ob]
- [TeleTrust_StdT]

Zur Durchführung einer Analyse zur Festlegung geeigneter Maßnahmen sei auf die verschiedenen Methoden verwiesen, die sich weltweit etabliert haben, etwa ISO/IEC 27001, ISO/IEC 27005, BSI-Standard 200-3, Standard-Datenschutz-Modell.

Bei der Festlegung geeigneter Maßnahmen ist insb. der Stand der Technik zu berücksichtigen. Das Technologieniveau „Stand der Technik“ ist angesiedelt zwischen dem innovativeren Technologiestand „Stand der Wissenschaft und Forschung“ und dem bewährten Technologiestand „allgemein anerkannten Regeln der Technik“. Diese drei Technologiestände werden von den Kategorien „allgemeine Anerkennung“ und "Bewährung in der Praxis" flankiert.“ (Drei-Stufen-Theorie nach Kalkar-Entscheidung), vgl. [TeleTrust_StdT]. Getroffene Maßnahmen entsprechend dem Stand der Technik sind am wirkvollsten, was die Erreichung der gesetzlichen Schutzziele betrifft.

Technische Maßnahmen im Stadium „Stand der Wissenschaft und Forschung“ sind hingegen noch sehr dynamisch und nicht ausreichend etabliert, wodurch mögliche Sicherheitsrisiken bzgl. der Datensicherheit bestehen können, sodass auf diesen Stand zur Festlegung geeigneter Maßnahmen nicht abgestellt werden darf.

Zur Konkretisierung „Stand der Technik“ vgl. auch ISO/IEC 27001, ISO/IEC 27002 oder IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Die Analyse zur Festlegung geeigneter Maßnahmen kann als Basis für die sich anschließende Datenschutz-Folgenabschätzung gem. P.6.5 herangezogen werden.

2.6.2. P.5.2 Zutrittskontrolle (Vertraulichkeit und Integrität auf Ebene der physischen Zutritte)

Umsetzungshinweise zum Kriterium

Mögliche Maßnahmen der Zutrittskontrolle (insb. zum physikalischen Zutritt zu Gebäuden) sind:

- Sicherheitszonenkonzept;
- Empfang;
- Besucherregelung;
- Einbruchmeldeanlage (EMA) mit Alarmierung / Aufschaltung Wachdienst;
- Videoüberwachung;
- Absicherung Fenster und Türen;

- Perimeterschutz;
- elektronisches Schließsystem;
- Schlüsselvergabe / Schlüsselrückgabe;
- Protokollierung von Zutritten.

Die Umsetzungshinweise aus ISO/IEC 27002, Kapitel 11 sind anwendbar.

2.6.3. P.5.3 Zugangskontrolle (Vertraulichkeit und Integrität auf Ebene der Systemzugänge)

Umsetzungshinweise zum Kriterium

Zur Umsetzung des Kriteriums sind insb. folgende Vorgaben zu beachten:

- [DSK_Online-Dienste]

Mögliche Maßnahmen der Zugangskontrolle (insb. zum Zugang auf IT-Systeme) sind:

- sichere Kennwörter (Passwort-Policy, individuelle Kennungen);
- Zwei-Faktor-Authentifizierungen;
- Vergabe und Entzug von Zugangsberechtigungen mit regelmäßiger Inventur;
- Protokollierung;
- Firewall;
- Virenschutz;
- Software- / Patch-Management;
- VPN-Zugänge (insb. für externe Dienstleister);
- Bildschirmschoner;
- Einschränkung der Nutzung privater Datenträger;
- Verschlüsselung der Festplatten.

Die Umsetzungshinweise aus ISO/IEC 27002, Kapitel 9 sind anwendbar.

2.6.4. P.5.4 Zugriffskontrolle (Vertraulichkeit und Integrität auf Ebene der Anwendungszugriffe)

Umsetzungshinweise zum Kriterium

Mögliche Maßnahmen der Zugriffskontrolle (insb. zum Zugriff auf Applikationsebene) sind:

- Berechtigungskonzepte;
- restriktive Gestaltung von Zugriffen und Berechtigungen;
- sichere Kennwörter (Passwort-Policy, individuelle Kennungen);
- Protokollierungen von Zugriffen;
- revisionsfähige Dokumentationen der Benutzerprofile;
- gesicherte Schnittstellen (USB, Netzwerke etc.).

Die Umsetzungshinweise aus ISO/IEC 27002, Kapitel 10, 12 und 13 sind anwendbar.

2.6.5. P.5.5 Transportkontrolle (Vertraulichkeit und Integrität auf Transport-Ebene)

Umsetzungshinweise zum Kriterium

Mögliche Maßnahmen der Transport- und Weitergabekontrolle sind:

- Sicherung der elektronischen Übertragung mit Nutzung geeigneter Protokolle, etwa VPN, IPsec;
- verschlüsselte Kommunikation;
- Verschlüsselung der Datenträger;
- Istaufnahme der Verschlüsselungsroutinen mit Angabe der Algorithmen und Methoden zum Schlüssel-Management;
- Nutzung anerkannter kryptographischer Mechanismen und hinreichend geeigneter Schlüssel und Parameter;
- versiegelte Transportbehälter;
- Nachweis über Versand.

Die Umsetzungshinweise aus ISO/IEC 27002, Kapitel 10, 12 und 13 sind anwendbar.

2.6.6. P.5.6 Trennungskontrolle

Umsetzungshinweise zum Kriterium

Mögliche Maßnahmen für die Trennungskontrolle sind:

- logische und / oder physikalische Trennung der Datenbestände bzw. Datenbanken;
- Benutzerrechteverwaltung;
- Unterweisungen der Mitarbeiter zur Trennungskontrolle;
- Funktionstrennung.

Die Umsetzungshinweise aus ISO/IEC 27002, Kapitel 12 und 13 sind anwendbar.

2.6.7. P.5.7 Eingabekontrolle

Umsetzungshinweise zum Kriterium

Mögliche Maßnahmen sind:

- Benutzeridentifikation / -authentisierung;
- Protokollierung von Log-In / Log-Out;
- Protokollierung von Datensatzanpassungen.

Die Umsetzungshinweise aus ISO/IEC 27002, Kapitel 12.4 sind anwendbar.

2.6.8. P.5.8 Verfügbarkeitskontrolle

Umsetzungshinweise zum Kriterium

"Hinreichend verfügbar" orientiert sich dabei an den notwendigen Verfügbarkeitsanforderungen (etwa gem. Vertrag). Dazu gehört sowohl die reine Erreichbarkeit der Systeme, als auch die Belastbarkeit sowie die Wiederherstellbarkeit der Systeme im Schadensfall.

Mögliche Maßnahmen der Verfügbarkeitskontrolle zum Schutz vor Verlust oder Zerstörung sind:

- Betriebskontinuitätsmanagement (Business Continuity Management, BCM), beispielsweise gem. BSI-Standard 200-4, ISO 22301 oder ISO 22313;
- Feuerlöscher, Brandfrühsterkennung, Rauchmelder, Brandmeldeanlage, Brandabschnitte;
- Klimatisierung Serverraum;
- unterbrechungsfreie Stromversorgung (USV);
- redundante Serverräume / Rechenzentren;
- redundante Netzanbindung.
- Zuverlässigkeit / Belastbarkeit: Fehlerfreie Funktion der DV-Systeme bzw. der genutzten Anwendungen (Frühwarnsysteme, Kapazitätsprognosen etc.); Die DV-Systeme müssen resilient gegen Störungen von außen sein, um eine vollständige Sicherheit der Daten zu gewährleisten.
- Wiederherstellbarkeit: Eine schnelle Wiederherstellung der Daten in einem technischen oder physischen Zwischenfall ist zu gewährleisten (Backup-Routinen, Notfallpläne etc.).

Die Umsetzungshinweise aus ISO/IEC27002, Kapitel. 11.1.4, 11.2.1, 11.2.2, 11.2.4, 12.3.1 und 17 sind anwendbar.

2.6.9. P.5.9 Pseudonymisierung / Anonymisierung

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [Art.29_WP216]
- [BfDI_Anonymisierung]

Relevante Erwägungsgründe: 26,28 DSGVO.

Pseudonymisierung bedeutet, dass personenbezogene Daten ohne Hinzuziehung weiterer Informationen einer Person nicht mehr zugeordnet werden können bzw. dürfen. Dabei ist zwischen der Anonymisierung und Pseudonymisierung zu unterscheiden. Bei der Pseudonymisierung werden die Informationen auf verschiedene Tabellen aufgeteilt.

Eine Anonymisierung zielt hingegen unter Zuhilfenahme von Anonymisierungstechniken darauf ab, den Personenbezug von Daten so aufzuheben, „dass eine Re-Identifizierung praktisch nicht durchführbar ist, weil der Personenbezug nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden kann“ [BfDI_Anonymisierung]. Eine absolute Anonymisierung liegt hingegen vor, wenn unter keinen Umständen eine Re-Identifizierung möglich ist. Dies ist in den wenigstens Fällen möglich.

Bitte beachten Sie daher, dass für die Beurteilung, ob eine hinreichende Anonymisierung vorliegt, insb. nach allgemeinem Ermessen die wahrscheinlich der verwendeten Mittel des Kunden (oder eines Dritten) zu berücksichtigen sind, die eine direkte oder indirekte Identifizierung ermöglichen. Dabei sind die objektiven Faktoren, wie insb. der erforderliche Aufwand sowie Kosten anhand des aktuellen Stands der Technik sowie technologische Entwicklungen zu berücksichtigen.

Die Anonymisierung personenbezogener Daten stellt eine Verarbeitung dar, wofür es ebenfalls einer Rechtsgrundlage bedarf. Stimmt der der Zweck der Anonymisierung mit dem der ursprünglichen Erhebung überein, handelt es sich um eine Weiterverarbeitung, die auch über die ursprüngliche Rechtsgrundlage legitimiert werden darf. Für die Beurteilung der Vereinbarkeit mit dem Erhebungszweck vgl. Kriterien Art. 6 Abs. 4 DSGVO.

Möglicher Ansätze und mögliche Maßnahmen zur Pseudonymisierung / Anonymisierung sind:

- Istaufnahme der personenbezogenen Daten, die pseudonymisiert werden;
- Istaufnahme der personenbezogenen Daten, die anonymisiert werden;
- Informationen zur De-Pseudonymisierung (Verfahrensbeschreibung, 4-Augen-Prinzip, Freigabeprozess);
- Angabe der Methode / Algorithmen;
- ggf. Istaufnahme der Verschlüsselungsroutinen mit Angabe der Algorithmen und Methoden zum Schlüssel-Management;
- ggf. Nutzung anerkannter kryptographischer Mechanismen und hinreichend geeigneter Schlüssel und Parameter.

2.6.10. P.5.10 Überprüfung, Bewertung und Evaluierung

Umsetzungshinweise zum Kriterium

Bitte beachten Sie, dass im Hinblick auf den technischen Fortschritt ständig die Wirksamkeit technisch und organisatorischer Maßnahmen zu überprüfen und, sofern erforderlich, nachzubessern ist, sodass durch die getroffenen technischen und organisatorischen Maßnahmen das geforderte Schutzniveau der DSGVO gewährleistet wird.

Zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen gehören beispielsweise:

- interne Audits;
- Penetrationstests (für IT-Systeme und Anwendungen).

Für die Durchführung interner Audits kann ISO 19011 herangezogen werden.

Die Umsetzungshinweise der ISO/IEC 27001, 9.2 sowie ISO/IEC 27002, Abs. 18.2 sind anwendbar.

2.7. P.6 Datenschutz-Management

2.7.1. P.6.1 Fortlaufende Datenschutz-Kontinuität

Umsetzungshinweise zum Kriterium

Für Datenschutz-Managementsysteme existieren verschiedene Standards, die herangezogen werden können, beispielsweise:

- ISO/IEC 27701, hier wird ein Informationssicherheits-Managementsystem (gem. ISO/IEC 27001) um Datenschutz-Aspekte ergänzt;
- ITIL für Prozesse;
- Standard-Datenschutzmodell (SDM) der deutschen Datenschutz-Aufsichtsbehörden.

Das Datenschutz-Managementsystem (DSMS) folgt einer strukturierten Methodik mit PDCA-Zyklus („Plan-Do-Check-Act“, „Planen-Umsetzen-Überprüfen-Handeln“). Dies impliziert einen regelmäßigen Zyklus zur Verbesserung, Pflege und Aufrechterhaltung des DSMS.

2.7.2. P.6.2 Datenschutzbeauftragter

Umsetzungshinweise zum Kriterium

Bitte beachten Sie, dass sich ergänzende oder strengere Anforderungen an die Bestellung eines DSB aus dem nationalen Recht der Mitgliedstaaten ergeben können.

Besteht eine Pflicht zur Benennung eines DSB, so ist z. B. gemäß §§ 6 Abs. 4, 38 Abs. 2 des deutschen BDSG die Abberufung des DSB nur zulässig, wenn § 626 BGB entsprechend angewendet wird. Die Kündigung des Arbeitsverhältnisses ist nur zulässig, wenn Tatsachen vorliegen, welche die Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen.

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [DSK_K.Nr.12]
- [DSK_Bestellpflicht_DSB]
- [Art.29_WP243.01]

Der Datenschutzbeauftragte kann eine interne oder externe Person sein.

Es kann gegebenenfalls ein gemeinsamer Datenschutzbeauftragter für Unternehmensgruppen, mehrere Behörden oder öffentliche Stellen benannt werden.

Der Datenschutzbeauftragte sollte leicht erreichbar sein. Die Kontaktdaten müssen verfügbar gemacht und Mitarbeitern bekannt sein. Betroffene Personen sowie Mitarbeiter können den Datenschutzbeauftragten zu allen Fragen des Datenschutzes kontaktieren.

Der Verantwortliche bzw. der Auftragsverarbeiter binden den Datenschutzbeauftragten ordnungsgemäß und frühzeitig in alle Fragen des Datenschutzes ein, unterstützen ihn und stellen sicher, dass er weisungsfrei bzgl. der Aufgaben des Datenschutzbeauftragten agieren kann. Weisungsfrei bedeutet, dass keine Anweisungen erteilt werden dürfen bzgl. der Vorgehensweise und Bewertung von vorliegenden Dachverhalten, z. B. ob die Aufsichtsbehörde benachrichtigt werden soll.

Zu den Aufgaben des Datenschutzbeauftragten zählen u.a.:

- Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten;
- Überwachung der Einhaltung der Vorgaben;
- Sensibilisierung und Schulung der Mitarbeiter;
- Unterstützung bei der Datenschutz-Folgenabschätzung;
- Zusammenarbeit mit der Aufsichtsbehörde.

Um Interessenskonflikten beim Datenschutzbeauftragten durch andere wahrzunehmende Aufgaben zu vermeiden, sollte ausgeschlossen werden, dass der Datenschutzbeauftragte Positionen innehat, bei der Zweck sowie Mittel der Datenverarbeitung festgelegt sind.

In Deutschland ist bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs regelmäßig von der Bestellpflicht eines DSB wegen der umfangreichen Verarbeitung besonderer personenbezogener Daten auszugehen vgl. [DSK_Bestellpflicht_DSB].

2.7.3. P.6.3 Verpflichtung auf Vertraulichkeit / Schulungen

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [DSK_K.Nr.19]

In der DSGVO wird das Datengeheimnis nicht konkret beschrieben. Es lässt sich jedoch eine Pflicht zur „Wahrung der Vertraulichkeit“ für Beschäftigte ableiten. Hierzu können Art. 5 Abs. 1 lit. f, Art. 28 Abs. 3, Art. 29 sowie Art. 32 Abs. 4 DSGVO näher hinzugezogen werden. Demnach sollte ein Verantwortlicher bzw. Auftragsverarbeiter bei der Durchführung der Arbeiten nur Beschäftigte einstellen, die auf die Vertraulichkeit sowie Einhaltung datenschutzrechtlicher Vorgaben verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Beschäftigte in diesem Sinne sind auch: „Auszubildende, Praktikanten, Referendare, Leiharbeiter und ehrenamtlich Tätige mit einzubeziehen. Soweit die Verschwiegenheit von Beschäftigten im öffentlichen Bereich gesetzlich oder tariflich ausdrücklich geregelt ist, muss eine solche Verpflichtung nicht erfolgen.“ [DSK_K.Nr.19].

Dies kann z. B. erfolgen durch eine Verpflichtungserklärung für Beschäftigte zur Wahrung der Vertraulichkeit Schulungen oder andere geeignete Sensibilisierungsmaßnahmen, Einbeziehung in regelmäßige Treffen zum Datenschutz und zur IT-Sicherheit oder Leitlinien zum Umgang mit Daten und klare Tätigkeitsbeschreibungen in Bezug auf die Verarbeitung von personenbezogenen Daten. Relevante Regeln, Richtlinien

und Verfahrensanweisungen sollen Mitarbeitern verfügbar gemacht und bekannt sein.

Ferner sollen regelmäßige Schulungen nach Bedarf zum Datenschutz stattfinden und die Teilnahme der Mitarbeiter an den Schulungen nachvollziehbar sein.

2.7.4. P.6.4 Verzeichnis von Verarbeitungstätigkeiten

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [DSK_K.Nr.1]

Das Verzeichnis der Verantwortlichen hat nach Art. 30 Abs. 1 DSGVO wesentliche Angaben zur Verarbeitung zu beinhalten; das Verzeichnis des Auftragsverarbeiters umfasst Angaben zu allen Kategorien der von ihm im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung. Die notwendigen Angaben ergeben sich direkt aus dem Kriterium.

Eine allgemeine und detaillierte Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen empfiehlt sich besonders.

Ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen – und somit eine Pflicht zum Führen eines Verzeichnisses der Verarbeitungstätigkeit – kann auch bei kleinen und mittelständischen Unternehmen (KMUs) bestehen, etwa beim Einsatz von Scoring oder Profiling.

Werden besondere Kategorien personenbezogener Daten oder personenbezogene Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten verarbeitet, so sind die durchgeführten Verarbeitungsvorgänge schriftlich (auch in elektronischer Form möglich) aufzuzeichnen.

Deutschland hat von der Öffnungsklausel Gebrauch, sodass in Deutschland Ausnahme von der Pflicht zum Führen eines solchen Verzeichnisses besteht, wenn der Verantwortliche oder Auftragsverarbeiter weniger als 250 Mitarbeiter beschäftigt und die Datenverarbeitung kein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien einschließt.

2.7.5. P.6.5 Datenschutz-Folgenabschätzung

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [Art.29_WP248.01]
- [DSK_K.Nr.5]
- [DSK_S-D-M_V.2.ob]

Relevante Erwägungsgründe: 75, 84, 92 DSGVO.

Die Abschätzung der Folgen sollte vor der Durchführung der vorgesehenen Verarbeitungsvorgänge erfolgen.

Es sollte entsprechend geprüft werden, ob einer der o.g. Verarbeitungsvorgänge vorliegt und somit eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen ist, oder sich aufgrund von Gesetzen der Mitgliedsstaaten oder Anforderungen des EDSA in der jeweils aktuellen Fassung oder speziellen Umständen das Erfordernis einer DSFA ergibt. Eine DSFA sollte insb. bei umfangreichen Verarbeitungsvorgängen, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten und eine große Zahl von Personen betreffen könnten durchgeführt werden.

Es sollte ein Konzept für die Durchführung einer DSFA entwickelt werden.

Bei der Abschätzung der Folgen ist die Wahrscheinlichkeit, dass die Verarbeitung personenbezogener Daten, die mit der Erbringung der Dienstleistung in Zusammenhang stehen, zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt zu berücksichtigen. Ein solches Risiko liegt insb. dann vor, wenn die Verarbeitung zu einem physischen, materiellen oder immateriellen Schaden führen könnte. Gem. ErwGr. 75 DSGVO z. B. bei : „(...) einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren(...)“. Die Schutzbedürftigkeit natürlicher Personen, insb. die von Kindern ist zu beachten.

Zudem ist zu berücksichtigen, dass bei einer Änderung der Datenverarbeitung sich auch die Risiken im Hinblick auf Art, Umfang, Umstände oder Zweck ändern können und sich entsprechend die Wahrscheinlich des Risikos für die Rechte und Freiheiten natürlicher Personen ändern bzw. erhöhen kann. Auf Grund des technischen Fortschritts unterliegen insb. technische Maßnahmen einem stetigen Wandel.

Ggf. kann es vernünftig und unter ökonomischen Gesichtspunkten zweckmäßig sein, eine Datenschutz-Folgenabschätzung nicht lediglich auf ein bestimmtes Projekt zu beziehen, sondern sie thematisch breiter anzulegen.

Weitere Angaben zu den einzelnen Bestandteilen der Hauptprozessschritte einer DSFA: [DSK_K.Nr.5], vgl. auch [DSK_S-D-M_V.2.ob].

2.7.6. P.6.6 Meldung von Datenschutzverletzungen

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [Art.29_WP250.01]

Erwägungsgründe: 85, 88 DSGVO.

Es sollte schriftlich festgelegt werden, wie im Falle einer Datenschutzverletzung vorzugehen ist. Zuständige Meldestellen, Fristen und Meldewege sind zu definieren. Diese sollten sowohl der Geschäftsführung als auch den Mitarbeitern oder

Unterauftragsnehmer zu jeder Zeit zur Verfügung stehen (Ressourcen müssen hierfür geschaffen werden).

Die Aufsichtsbehörde ist unverzüglich, höchstens jedoch innerhalb von 72 Stunden, nach Kenntnis der Verletzung, zu unterrichten. Kann der Verantwortliche nachweisen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt, ist unter Einhaltung des Grundsatzes der Rechenschaftspflicht keine Meldung erforderlich. Bei einer verfristeten Mitteilung sind die Gründe dafür anzugeben.

Die Meldungspflicht umfasst, dass der Verantwortliche zu untersuchen hat, ob die Verletzung voraussichtlich zu einem hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt, und diese entsprechend unverzüglich von der Verletzung in Kenntnis zu setzen, damit diese die erforderlichen Vorkehrungen treffen können, dabei sind insb. die Art und Schwere der Verletzung sowie deren Folgen und nachteilige Auswirkungen für die betroffene Person zu berücksichtigen.

Die Benachrichtigung an die betroffene Person hat möglichst rasch, in Absprache mit der Aufsichtsbehörde, zu erfolgen. Die Beschreibung enthält die Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene natürliche Person gerichtete Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen dieser Verletzung.

Bei der Meldung sind die Umstände der Verletzung hinreichend zu berücksichtigen, z. B. ob geeignete technische Sicherheitsvorkehrungen getroffen wurden, die die Wahrscheinlichkeit eines Identitätsbetrugs oder anderer Formen des Datenmissbrauchs wirksam verringern. Der Verantwortliche hat bei einer Verletzung des Schutzes personenbezogener Daten rechtzeitig und angemessen zu reagieren, insb. um physischen, materiellen oder immateriellen Schaden oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffenen Personen zu vermeiden.

Bei der Frist zur Meldung sind insb. die Art und Schwere der Verletzung sowie deren Folgen und nachteilige Auswirkungen für die betroffene Person zu berücksichtigen.

Kenntnis liegt beim Verantwortlichen vor, wenn dieser eine hinreichende Gewissheit darüber hat, dass ein Sicherheitsvorfall aufgetreten ist, der zu einer Beeinträchtigung des Schutzes personenbezogener Daten geführt hat.

2.7.7. P.6.7 Zusammenarbeit mit Aufsichtsbehörden

Umsetzungshinweise zum Kriterium

Es sollte schriftlich festgelegt werden, wie im Falle einer Anfrage vorzugehen ist. Zuständige Mitarbeiter sollten entsprechend definiert werden. Diese sollten sowohl der Geschäftsführung als auch den Mitarbeitern oder Unterauftragsnehmer zu jeder Zeit zur Verfügung stehen (Ressourcen müssen hierfür geschaffen werden).

2.8. P.7 Datenverarbeitung außerhalb der EU

2.8.1. P.7.1 Datenübermittlung in Drittstaaten

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [EDSA_QA-C-311/18]
- [EDSA_o2/2018]
- [EDSA_o1/2020]
- [EDSA_o2/2020]
- [EDSA_o7/2022]
- [EDSA_o5_2021]
- EuGH, 16.07.2020 - C-311/18.

Im Einklang mit [EDSA_o5_2021] wird eine Übermittlung durch die folgenden kumulativen Kriterien definiert:

- Der Verantwortliche oder Auftragsverarbeiter (als Exporteur) unterliegt mit der betreffenden Verarbeitung der DSGVO.
- Dieser Verantwortliche oder Auftragsverarbeiter ("Exporteur") stellt einem anderen für die Verarbeitung Verantwortlichen, einem gemeinsam Verantwortlichen oder Auftragsverarbeiter ("Importeur") personenbezogene Daten, die Gegenstand dieser Verarbeitung sind, durch Übermittlung oder auf andere Weise zur Verfügung.
- Der Importeur befindet sich in einem Drittland oder ist eine internationale Organisation, unabhängig davon, ob dieser Importeur in Bezug auf die betreffende Verarbeitung gemäß Artikel 3 der DSGVO der DSGVO unterliegt oder nicht.

Wesentliche Grundlage einer zulässigen Drittstaatenübermittlung ist ein Angemessenheitsbeschluss der EU Kommission nach Art. 45 DSGVO. Die EU Kommission veröffentlicht diese unter https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de.

Liegt kein Angemessenheitsbeschluss vor, können geeignete Garantien nach Art. 46 DSGVO eine Drittstaatenübermittlung rechtfertigen.

Unter anderem spielen hier die EU-Standardvertragsklauseln (Standard Contractual Clauses - SCC) nach Art. 46 Abs. 2 lit. c DSGVO eine Rolle. Dabei ist darauf zu achten, dass diese in der aktuellsten Version unverändert durch die Parteien abgeschlossen wurden. Andere eventuell hinzugefügte Klauseln oder zusätzliche Schutzklauseln dürfen die Verpflichtungen in den SCC nicht untergraben oder negativ beeinflussen oder die Einhaltung der in den SCC enthaltenen Verpflichtungen verhindern.

Auch genehmigte, verbindliche interne Datenschutzvorschriften (Binding Corporate Rules – BCR) können einen Drittstaatentransfer nach Art. 46 Abs. 2 lit. b DSGVO i.V.m. Art. 47 DSGVO rechtfertigen.

Ebenso können genehmigte Zertifizierungsverfahren nach Art. 42 DSGVO gemäß Art. 46 Abs. 2 lit. f DSGVO dazugehören.

Im Einklang mit Art. 42 Absatz 2 DSGVO und der [EDSA_07/2022] über die Zertifizierung als Instrument für Übermittlungen verlässt sich in diesem Fall der Kunde (Exporteur) auf die von den Importeuren in den Drittländern (für die Verarbeitung Verantwortliche oder Auftragsverarbeiter, die gemäß Artikel 3 DSGVO nicht der DSGVO unterliegen) erhaltenen Zertifizierungen. Gegenstand der Zertifizierung ist in diesem Fall die Verarbeitung der aus der EU / dem EWR erhaltenen Daten durch den Datenimporteur in dem Drittland und jeder Vorgang, der unter der Kontrolle des Importeurs steht.

Anhang 1 des [EDSA_07/2022] sieht dabei zusätzliche Anforderungen vor: etwa ist zu prüfen, ob die Zertifizierung des Importeurs mit den Daten und Anwendungsfällen des Exporteurs übereinstimmt. Darüber hinaus muss der Vertrag zur Auftragsverarbeitung mit dem Importeur die Anforderungen umsetzen, insbesondere muss der Importeur darin verpflichtet sein, die verantwortliche Person im Falle von Gesetzesänderungen, welche die Erfüllung der Verpflichtungen aus dem Zertifikat verhindern, zu informieren. Ferner muss gewährleistet sein, dass im Falle von Informations- / Zugangsanfragen der Regierung eine Information erfolgt. Insgesamt ist zu prüfen, ob die Zertifizierung als Instrument für Übermittlungen den Anforderungen des [EDSA_07/2022] genügt.

Unter Beachtung der Rechtssache „Schrems II“, EuGH, 16.07.2020 - C-311/18, reicht das Vorliegen von EUStandardvertragsklauseln oder genehmigten Binding Corporate Rules allein nicht aus.

Vielmehr ist das vom EU-Recht geforderte Schutzniveau in dem betreffenden Drittland einzuhalten, um festzustellen, ob die von den SCC oder den BCR gebotenen Garantien in der Praxis eingehalten werden können. Die Beurteilung obliegt sowohl dem Datenimporteur als auch Exporteur.

Ist dies nicht der Fall, sind zusätzliche Maßnahmen zu ergreifen, um ein im Wesentlichen gleichwertiges Schutzniveau wie im in der EU und EWR (EWR = Europäischer Wirtschaftsraum = EU + Island, Lichtenstein und Norwegen) zu gewährleisten, ohne, dass das Recht des Drittlandes diese zusätzlichen Maßnahmen beeinträchtigt, um ihre Wirksamkeit zu verhindern, vgl. EuGH, 16.07.2020 - C-311/18.

Die Prüfung und Bewertung muss dabei folgende Umstände betrachten:

- Die Regelung der geeigneten Garantien selbst (z.B. SCC, BCR)
- Relevante Aspekte des Rechts im Drittstaat im Hinblick auf den Zugriff auf die personenbezogenen Daten dort durch Sicherheitsbehörden
- Die konkreten Umstände der Drittstaatenübermittlung sowie die vom Datenexporteur ergriffenen zusätzlichen Garantien.

Prüfung und Bewertung sind nachweisbar zu dokumentieren. Bewährtes Mittel ist ein „Transfer Impact Assessment“ – TIA, welches in den SCC, Klauseln 14 und 15 auch so erwähnt wird. Bei einer TIA handelt es sich um eine von einem für die Datenverarbeitung Verantwortlichen oder einem Datenverarbeiter durchgeführte Analyse der Auswirkungen und Sicherheitsimplikationen einer Übermittlung in ein Land außerhalb des EWR, für das die Kommission keine Angemessenheitsfeststellung getroffen hat.

Die Ausnahmen des Art. 49 DSGVO sind zu prüfen, falls weder ein Angemessenheitsbeschluss nach Artikel 45 Absatz 3 vorliegt noch geeignete Garantien nach Artikel 46. Art. 49 Satz 1 lit. a – g DSGVO führt eine Reihe von Ausnahmen auf. Die Leitlinien des EDSA [EDSA_02/2018] sind hier wesentlich.

Ein Beispiel ist die Einwilligung. muss ausdrücklich erfolgen und für den konkreten Fall einer Datenverarbeitung vor der Übermittlung eingeholt werden, sowie in Kenntnis der Sachlage erfolgen, indem die Betroffenen umfangreich über mögliche Risiken der Übermittlung sowie dem Fehlen geeigneter Garantien informiert werden, vgl. für weitere Umsetzungshinweise P.1.4.

Sofern die Datenübermittlung nur in Einzelfällen stattfindet – die Datenverarbeitung nicht wiederholt erfolgt und nur eine begrenzte Zahl von betroffenen Personen betrifft –, kann ausnahmsweise eine rechtmäßige Datenübermittlung in einen Drittstaat vorliegen, sofern die Voraussetzungen des Art. 49 Abs. 1 S. 2 DSGVO vorliegen. Es ist im Einzelfall zu bewerten, ob die Datenübermittlungen sich nicht wiederholt und nur eine begrenzte Zahl von betroffenen Personen betrifft. Die Datenverarbeitung kann sich folglich nur auf Einzelfälle ohne Wiederholungsabsicht stützen. Artikel 49 Satz 2 DSGVO hat einen Ausnahmecharakter. Die darin enthaltenen Ausnahmeregelungen müssen restriktiv ausgelegt werden und beziehen sich hauptsächlich auf gelegentliche und nicht wiederholte Verarbeitungen.

Eine weitere Ausnahme ist aufgrund von wichtigen Gründen des öffentlichen Interesses möglich. Dazu ist vom Datenexporteur sicherzustellen, dass diese Ausnahme durch eine „strenge Notwendigkeitsprüfung“ legitimiert ist und die Rechtsgrundlage in den Rechtsvorschriften der EU oder der Mitgliedstaaten anerkannt ist. Für weitere Ausnahmen vgl. Art. 49 Abs. 1 DSGVO.

Die ergänzenden Maßnahmen sind unter Berücksichtigung aller Umstände der Übermittlung und nach Beurteilung des Rechts des Drittlandes festzulegen. Hilfestellung zur Festlegung geeigneter zusätzlicher Maßnahmen vgl., [EDSA_01/2020] und [EDSA_02/2020]. [EDSA_01/2020] beschreibt dabei Maßnahmen zur Ergänzung von Übermittlungsinstrumenten zur Gewährleistung des EU-Schutzniveaus und Prüfschritte. [EDSA_02/2020] fasst Empfehlungen zusammen, welche Anforderungen zu stellen sind, damit ein angemessenes Schutzniveau festgestellt werden kann.

2.8.2. P.7.2 Vertreter innerhalb der EU

Umsetzungshinweise zum Kriterium

Dieser Vertreter dient als Kontaktstelle für Aufsichtsbehörden oder betroffene Personen. Die Benennung eines Vertreters befreit den Verantwortlichen bzw. Auftragsverarbeiter nicht von seiner Haftung. Die Benennung eines Vertreters ist nicht erforderlich, wenn:

- die Verarbeitung der Daten nur gelegentlich erfolgt und es zu keiner umfangreichen Verarbeitung besonderer Datenkategorien im Sinne von Art. 9 Abs. 1 DSGVO sowie personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO kommt;

- es unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen kommt;
- es sich um eine Behörde oder öffentliche Stelle handelt.

2.9. P.8 Betroffenenrechte

Bitte beachten Sie für dieses Kapitel, dass Betroffenenrechte nur in Bezug auf personenbezogene Daten ausgeübt werden können. Dies gilt auch für pseudonyme Datenbestände, nicht aber für Daten ohne Personenbezug der Daten vor, z. B. bei einer anonymen Datenverarbeitung.

2.9.1. P.8.1 Recht auf Auskunft

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [DSK_K.Nr.6]
- [EDSA_1_2022]

Erwägungsgründe: 59, 63, 64, DSGVO

Es sollte ein Konzept entwickelt werden, das den Umgang mit und die Beantwortung von Anfragen betroffener Personen festlegt und die unkomplizierte Ausübung der Betroffenenrechte ermöglicht.

Eine Ausnahme von dieser Pflicht zur Erfüllung dieses Rechts kann vorliegen, wenn der Verantwortliche nachweisen kann, dass er die betroffene Person nicht identifizieren kann, wobei alle vertretbaren Mittel zu nutzen sind, um die Identität einer Auskunft suchenden betroffenen Person zu überprüfen. Ein Verantwortlicher sollte personenbezogene Daten nicht allein zu dem Zweck speichern, auf mögliche Auskunftersuchen reagieren zu können.

Auftragsverarbeiter sollten ein Konzept zur Unterstützung der Verantwortliche entwickeln, welches die erforderlichen Maßnahmen zur Unterstützung identifiziert und Verantwortlichkeiten sowie Fristen festlegt.

Gegenstand des Auskunftsanspruchs sind ausschließlich die auf die betroffene Person bezogenen Daten, die zum Zeitpunkt der Auskunftserteilung vorhanden sind. Diese Daten sind der betroffenen Person so herauszugeben, wie diese im Unternehmen vorliegen. Eine Aufbereitung darf nicht erfolgen, da damit der Informationsgehalt der Daten verändert werden könnte. Eine ergänzende Erläuterung ist hingegen zulässig.

Sofern der Verantwortliche keine Daten zu dieser Person verarbeitet oder personenbezogene Daten unumkehrbar anonymisiert, ist ebenfalls darüber Auskunft zu erteilen (Negativauskunft).

Eine geeignete Maßnahme, um das Auskunftersuchen wahrzunehmen, wäre die Einrichtung einer organisatorischen Kontaktstelle (mit ausreichend Ressourcen) zur Beauskunftung.

Grundsätzlich hat die Auskunft unentgeltlich zu erfolgen. Macht die betroffene Person ihren Anspruch auf kostenlose Kopie nach Art. 15 Abs. 3 S. 1 DSGVO elektronisch geltend, sind ihr diese vollständigen Informationen (sofern diese nichts anderes angibt) in einem gängigen elektronischen Format zu Verfügung zu stellen. Ab der zweiten vom Betroffenen beantragten Kopie, kann jedoch ein angemessenes Entgelt auf Grundlage der Verwaltungskosten hierfür verlangt werden. Entsprechendes gilt bei offenkundig unbegründeten oder exzessiven Anfragen einer betroffenen Person.

Wie weitreichend der Anspruch auf Kopie aus Art. 15 Abs. 3 DSGVO zu werten ist wird derzeit im diskutiert und von den Gerichten weder einheitlich noch eindeutig beantwortet. Für die Anwendung der [dsc_Kriterien] schließt sich der Programmeigner daher der Meinung von Aufsichtsbehörden aus Bayern und (im Ergebnis) aus Hessen in den aktuellen Tätigkeitsberichten an, auch im Hinblick auf die im Rahmen der DS-RL ergangenen EuGH-Rechtsprechung, den Anspruch auf Kopie auf die durch Art. 15 Abs. 1 DSGVO geforderten Informationen zu begrenzen. Die Kopie ist, sofern nicht anders beantragt, in einem gängigen maschinenlesbaren Format zur Verfügung zu stellen.

Nach Art. 12 Abs. 1 DSGVO ist die Erteilung der Auskunft in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Üblicherweise sind Auskunftersuchen in der Sprache der betroffenen Person zu beantworten. Der Anspruch an die Verständlichkeit der Sprache bestimmt sich anhand der Adressaten. Insbesondere ist zu berücksichtigen, ob die Auskunft an Kinder erteilt wird.

Bei begründeten Zweifeln an der Identität eines Antragstellers kann der Verantwortliche nach Art. 12 Abs. 6 DSGVO zusätzliche Informationen zur Bestätigung der Identität verlangen (z. B. eine Postadresse bei elektronischem Auskunftsantrag).

Das Auskunftsrecht gewährleistet den natürlichen Personen dieses Recht problemlos und in angemessenen Abständen auszuüben.

Der Verantwortliche hat die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums, zu wahren, darf jedoch aufgrund dessen kein Auskunftersuchen verweigern. Bei einer großen Menge an verarbeiteten Daten, kann der Verantwortliche vom Auskunftssuchenden eine Präzisierung der Informationen verlangen, auf die sich das Auskunftersuchen bezieht.

Bei der Korrespondenz und insb. bei der Datenübertragung ist die Vertraulichkeit der Kommunikation zu gewährleisten.

2.9.2. P.8.2 Recht auf Berichtigung

Umsetzungshinweise zum Kriterium

Es sollte ein Konzept entwickelt werden, das den Umgang mit und die Beantwortung von Anfragen betroffener Personen festlegt und die unkomplizierte und zeitnahe Ausübung der Betroffenenrechte ermöglicht. Eine Ausnahme von dieser Pflicht zur Erfüllung dieses Rechts kann vorliegen, sofern der Verantwortliche nachweisen kann, dass er die betroffene Person nicht identifizieren kann, wobei alle vertretbaren Mittel zu nutzen sind, um die Identität einer Auskunft suchenden betroffenen Person zu überprüfen.

Auftragsverarbeiter sollten ein Konzept zur Unterstützung der Verantwortliche entwickeln, welches die erforderlichen Maßnahmen zur Unterstützung identifiziert und Verantwortlichkeiten sowie Fristen festlegt.

Die Systeme des Verantwortlichen bzw. des Auftragsverarbeiters haben die Berichtigung auf technischer und organisatorischer Ebene zuzulassen. Sofern die betroffene Person die Daten nicht selber anpassen kann, muss der Verantwortliche bzw. der Auftragsverarbeiter die Berichtigung der Daten übernehmen. Bei der Berichtigung ist zu beachten, dass diese an allen Speicherorten erfolgt, etwa Backups. Insbesondere sollten auch Prozesse implementiert werden, die sicherstellen, dass bei einer Wiederherstellung von Daten aus einem Backup die Berichtigung auf in der Wiederherstellung übernommen wird.

Unverzüglich meint, dass es zu keiner schuldhaften Verzögerung bei der Berichtigung durch die verantwortliche Stelle kommen darf. Aufwandsbedingt kann eine gewisse Bearbeitungszeit toleriert werden, wobei die Erforderlichkeit sodann begründet werden muss.

Der Begriff Berichtigung umfasst sowohl die Hinzufügung fehlender, aber notwendiger Daten als auch die Löschung / Löschung unnötiger Daten.

2.9.3. P.8.3 Recht auf Löschung

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [DSK.K.Nr.11]
- [EDSA_5/2019]
- [Art.29_WP216]

Erwägungsgründe: 65, 66 DSGVO

Es sollte ein Konzept entwickelt werden, das den Umgang mit und die Beantwortung von Anfragen betroffener Personen festlegt und die unkomplizierte Ausübung der Betroffenenrechte ermöglicht. Eine Ausnahme von dieser Pflicht zur Erfüllung dieses Rechts kann vorliegen, sofern der Verantwortliche nachweisen kann, dass er die betroffene Person nicht identifizieren kann, wobei alle vertretbaren Mittel zu nutzen sind, um die Identität einer Auskunft suchenden betroffenen Person zu überprüfen. Auftragsverarbeiter sollten ein Konzept zur Unterstützung der Verantwortliche entwickeln, welches die erforderlichen Maßnahmen zur Unterstützung identifiziert und Verantwortlichkeiten sowie Fristen festlegt.

Der Verantwortliche hat das Recht auf Löschung sowie das „Recht auf Vergessenwerden“ der betroffenen Personen zu gewährleisten, indem auf Verlangen der betroffenen Person und / oder unter bestimmten Voraussetzungen ohne Verlangen der betroffenen Person eigenständig und unverzüglich die Daten löscht.

Bei Vorliegen eines Widerspruchs ist zu beachten, dass dieser nur gilt, soweit keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen. Das Widerspruchsrecht nach Art. 21 Abs. 1 DSGVO besteht ausschließlich bei Verarbeitungen, die auf Art. 6 Abs. 1 lit. e oder f DSGVO gründen. Für die Lösungsverpflichtung bedarf es dabei

einer Interessenabwägung. Bei Widersprüchen in Bezug auf Direktwerbung ist hingegen keine Begründung notwendig.

Ausnahmen vom Recht auf Löschung / Vergessenwerden bestehen, wenn die Verarbeitung erforderlich ist:

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
- zur Erfüllung einer rechtlichen Verpflichtung, des Verantwortlichen unterliegt oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse;
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gem. Art. 9 Abs. 2 lit. h und i sowie Art. 9 Abs. 3 DSGVO;
- Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke gem. Art. 89 Abs. 1 DSGVO, soweit die Löschung die Verwirklichung dieser Ziele ernsthaft beeinträchtigt
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

Die zeitlich unbegrenzte Verarbeitung der jeweiligen personenbezogenen Daten ist unzulässig; das bedeutet, dass das regelmäßige Erreichen der Zweckmäßigkeit zu überprüfen ist.

Der Verantwortliche kann der betroffenen Person die Möglichkeit gewähren, die Löschung selbst durchzuführen, sofern die Art der Datenverarbeitung dies zulässt. Ist dies nicht möglich, stellt der Verantwortliche sicher, dass die betroffene Person das Recht auf Löschung ihm gegenüber geltend machen kann und die Löschung beim Verantwortlichen erfolgt.

Für Methoden zur Durchführung der Löschung können z.B. die Hilfestellungen genutzt werden:

- [DSK.K.Nr.11]
- [DIN 66399-1]
- [DIN 66391-2]
- [DIN 66399-3]
- [DIN 66398]
- Entsprechende Richtlinien des BSI

Zur Umsetzung einer Löschung kann das Mittel der Anonymisierung gewählt werden. Zu den Anforderungen an eine Anonymisierung beachten Sie bitte die Ausführungen zu P.5.9.

Ist der Verantwortliche gem. Art. 17 Abs. 1 DSGVO zu deren Löschung verpflichtet, hat er personenbezogene Daten, die er öffentlich gemacht hat unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, zu treffen, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten (gleichfalls) verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

Zudem hat der Verantwortliche, weitere Verantwortliche, die die zu löschenden Daten (noch) verarbeiten, über den Antrag des Betroffenen nach Löschung von Links, Kopien oder Replikationen zu informieren; der Verweis auf Unzumutbarkeit ist unwirksam.

Der Verantwortliche hat, sofern er sich auf die Beschränkung des Löschanpruchs beruft, sicherzustellen, dass der Wesensgehalt der Grundrechte und Grundfreiheiten gewahrt bleibt und die Beschränkung eine notwendige und verhältnismäßige Maßnahme darstellt und (zumindest) einem der in Art. 23 Abs. 1 lit. a bis j DSGVO genannten Zwecke dient. In diesem Zusammenhang ist in Deutschland zu beachten, dass § 35 BDSG grundsätzlich eng und im Sinne einer größtmöglichen Transparenz auszulegen ist, wobei die Anwendung der Norm aufgrund des Anwendungsvorrangs der DSGVO auf Einzelfallentscheidungen zu beschränken ist.

2.9.4. P.8.4 Recht auf Einschränkung

Umsetzungshinweise zum Kriterium

Erwägungsgründe: 67 DSGVO

Es sollte ein Konzept entwickelt werden, das den Umgang mit und die Beantwortung von Anfragen betroffener Personen festlegt und die unkomplizierte Ausübung der Betroffenenrechte ermöglicht; darüber hinaus sind die entsprechenden Prozesse zu implementieren und die Implementierung ist nachzuweisen. Auftragsverarbeiter sollten ein Konzept zur Unterstützung der Verantwortliche entwickeln, welches die erforderlichen Maßnahmen zur Unterstützung identifiziert und Verantwortlichkeiten sowie Fristen festlegt.

Sofern eine betroffene Person eine Einschränkung seiner Daten verlangt, ist dies umzusetzen, soweit keine rechtlichen Gründe entgegenstehen.

Der Verantwortliche kann zur Umsetzung die ausgewählten personenbezogenen Daten vorübergehend auf ein anderes Verarbeitungssystem übertragen, für Nutzer diese sperren oder veröffentlichte Daten vorübergehend von einer Website entfernen. Liegt ein automatisiertes Dateisystem vor, so hat die Einschränkung der Verarbeitung grundsätzlich durch technische Mittel zu erfolgen, wodurch eine Weiterverarbeitung bzw. Veränderung unmöglich ist. Zudem ist ein Hinweis bzgl. einer Beschränkung im System notwendig.

Eine Ausnahme von dieser Pflicht zur Erfüllung dieses Rechts kann vorliegen, wenn der Verantwortliche nachweisen kann, dass er die betroffene Person nicht identifizieren kann. Allerdings darf er sich nicht weigern, zusätzliche Informationen zur Identifizierung von der betroffenen Person entgegenzunehmen.

2.9.5. P.8.5 Mitteilungspflicht

Umsetzungshinweise zum Kriterium

Erwägungsgründe: 85, 86, 87, 88 DSGVO

Der Verantwortliche sollte ein Konzept entwickeln, das den Umgang mit den Rechten betroffener Personen festlegt und die unkomplizierte Ausübung der Betroffenenrechte ermöglicht. Auftragsverarbeiter sollten ein Konzept zur Unterstützung der

Verantwortliche entwickeln, welches die erforderlichen Maßnahmen zur Unterstützung identifiziert und Verantwortlichkeiten sowie Fristen festlegt. Dabei sind Maßnahmen zur Umsetzung und Sicherstellung folgender Punkte zu berücksichtigen und zu implementieren. Im Gegensatz zum Recht auf Vergessenwerden bezieht sich diese Verpflichtung auf vorangegangene Übermittlungen an konkrete Empfänger.

Sofern der Verantwortliche nachweisen kann, dass er die betroffene Person nicht identifizieren kann, besteht keine Mitteilungspflicht an die Empfänger der Daten bzw. an die betroffene Person.

2.9.6. P.8.6 Recht auf Datenübertragung

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [Art.29_WP242]

Erwägungsgründe: 68 DSGVO

Der Verantwortliche hat die von den Betroffenen bereitgestellten personenbezogenen Daten in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format den Betroffenen bereitzustellen. Dies dient der Stärkung der Datensouveränität der betroffenen Personen und soll den Wechsel zwischen verschiedenen Anbietern erleichtern. Es greift bei Banken oder Versicherungen genauso wie bei sozialen Netzwerken oder anderen Unternehmen der Informationsgesellschaft.

Um die Datenübertragbarkeit zu ermöglichen, sollte der Verantwortliche ein interoperables Format entwickeln, sodass eine Wiederverwendung der Daten mit geringem Aufwand durch die betroffene Person oder den Verantwortlichen gewährleistet werden kann. Je nach Sektor kann das geeignete Format sowie der Weg der Übermittlung variieren (z. B. sichere E-Mail, SFTP-Server, sichere Web-Schnittstelle oder Web-Portal). Gibt es keine sektortypischen Formate, sollten allseits bekannte Formate (wie XML, JSON oder CSV) verwendet werden. Diese sollten zusammen mit Metadaten, sofern diese sachdienlich sind in der bestmöglichen Granularitätsstufe bereitgestellt werden, sodass ein hohes Abstraktionsniveau bestehen bleibt. Der Inhalt der übermittelten Informationen, einschließlich sachdienlicher Metadaten sollte genau beschrieben werden.

Möglicherweise fehlen aufgrund neuartiger oder proprietärer Dienste gängige Formate, sodass für den Verantwortlichen nicht zwingend eine Pflicht zur Nutzung oder Entwicklung eines interoperablen Formats besteht. Hiervon können ggf. wiederum Ausnahmen bestehen, wenn z. B. die proprietären Dateiformate so marktüblich sind, dass feststeht, dass Mitbewerber diese Formate für den Zweck zweifelsfrei verarbeiten können. Gelten für bestimmte Formate kostenintensive Lizenzbeschränkungen, so werden diese nicht als geeignet angesehen.

Bei großen und komplexen Sammlungen von Daten sollte der Verantwortliche die betroffene Person ermöglichen Definition, Schema und Struktur der personenbezogenen Daten, die bereitgestellt werden könnten, mittels einer Übersicht „in präziser, transparenter, verständlicher und leicht zugänglicher Form“ zu erfassen, z. B. durch die

Verwendung von Dashboards. Sodass benötigte Daten herunterladen oder an einen anderen Verantwortlichen übermitteln werden können.

Geht aus einer Datenportabilitätsanfrage eindeutig die Geltendmachung von Rechten aus den Rechtsvorschriften eines sektorspezifischen Bereichs, sind diese Vorschriften hinzuzuziehen und nicht die der DSGVO. Welche Rechte konkret die betroffenen Personen ausüben möchten, kann mittels einer Einzelfallprüfung festgestellt werden. Das Recht auf Datenportabilität entsprechend der DSGVO kann auch neben den Rechten aus den Rechtsvorschriften eines sektorspezifischen Bereichs stehen.

Zur Datenübermittlung wird auf technischer Ebene eine direkte Übermittlung des vollständigen Datensatzes bzw. Auszüge sowie ergänzend den Einsatz eines automatisierten Werkzeugs, wodurch die relevanten Daten extrahiert werden können empfohlen.

Der Verantwortliche hat auf Antrag der betroffenen Person und soweit es ihm technisch möglich ist, die personenbezogenen Daten direkt an einem anderen Verantwortlichen zu übermitteln. Er hat sicherzustellen, dass die Daten stets sachlich richtig und auf dem neuesten Stand sind.

Zur Umsetzung empfiehlt es sich, dass der Verantwortliche prüft, ob bei den Daten der betroffenen Person andere Personen tangiert sind und durch das Recht auf Empfang der Daten die Rechte und Freiheiten anderer Personen beeinträchtigt werden, z. B. indem die Daten unrechtmäßig an einen neuen Verantwortlichen übermittelt werden.

Die Datenübertragung ist in folgenden Fällen zulässig:

- die Verarbeitung erfolgt auf Basis einer Einwilligung oder eines Vertrages und
- die Verarbeitung erfolgt mithilfe automatisierter Verfahren.

Der Verantwortliche hat dem Recht auf Datenübertragbarkeit nur nachzukommen, wenn die Daten von der betroffenen Person aktiv und wissentlich von der betroffenen Person (z. B. Postanschrift, Nutzernamen, Alter) „bereitgestellt“ wurden oder es sich um „beobachtete Daten, die von der betroffenen Person durch die Nutzung des Dienstes oder des Geräts bereitgestellt werden“ (z. B. Suchverlauf, Verkehrsdaten und Standortdaten, ebenso andere Rohdaten wie die von einem Trackinggerät aufgezeichnete Herzfrequenz).

Die von einer betroffenen Person „bereitgestellten Daten“ sind weit auszulegen; lediglich „aus Rückschlüssen erzeugte Daten“ sowie „abgeleitete Daten“, welche personenbezogene Daten beinhalten und von einem Diensteanbieter erzeugt werden, sind von der Anwendung ausgenommen.

Es sollte ein Konzept entwickelt werden, das den Umgang mit und die Beantwortung von Anfragen betroffener Personen festlegt und die unkomplizierte Ausübung der Betroffenenrechte ermöglicht, insb. Prozesse zur Fristwahrung sind zu implementieren

Eine Ausnahme von dieser Pflicht zur Erfüllung dieses Rechts kann vorliegen, sofern der Verantwortliche nachweisen kann, dass er die betroffene Person nicht identifizieren kann. Der Verantwortliche sollte zur Einhaltung der Maßnahmen ein Authentifizierungsverfahren einführen.

Auftragsverarbeiter sollten ein Konzept zur Unterstützung der Verantwortliche entwickeln, welches die erforderlichen Maßnahmen zur Unterstützung identifiziert und Verantwortlichkeiten sowie Fristen festlegt.

2.9.7. P.8.7 Recht auf Widerspruch

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [DSK_Direktwerbung]

Erwägungsgründe: 69 DSGVO

Es sollte ein Konzept entwickelt werden, wodurch ersichtlich wird, welche Maßnahmen der Verantwortliche bzw. der Auftragsverarbeiter ergreift, der betroffenen Personen die Ausübung eines Widerspruchs ermöglicht.

Auftragsverarbeiter sollten ein Konzept zur Unterstützung der Verantwortliche entwickeln, welches die erforderlichen Maßnahmen zur Unterstützung identifiziert und Verantwortlichkeiten sowie Fristen festlegt.

Zur Umsetzung von Werbewidersprüche, kann die Aufnahme der Daten in eine sog. Werbesperrdatei erfolgen, sodass durch Abgleich mit der Werbesperrdatei sichergestellt wird, dass die Kontaktdaten dieser betroffenen Person nicht verwendet werden. Werbesperrdateien sind im Zusammenhang mit Art. 21 Abs. 3, Art. 17 Abs. 3 lit. b und Art. 6 Abs. 1 Satz 1 lit. f DSGVO zulässig. Die Unterrichtung bzgl. der Beachtung des Werbewiderspruchs hat auch über die Aufnahme der Daten in eine Sperrdatei sowie Sinn und Zweck dessen zu informieren.

Der Werbewiderspruch ist so zu platzieren, dass die betroffene Person beim gewöhnlichen Umgang mit den Vertragsinformationen bzw. der Werbung, Kenntnis erlangt. Das Werbewiderspruchsrecht im Zusammenhang mit Direktwerbung und ggf. Profiling sollte unverzüglich erfolgen. In Einzelfällen kann die Umsetzung des Werbewiderspruchs für Unternehmen unzumutbar sein, z. B., wenn sich die personenbezogenen Daten schon in der Verarbeitung befinden. Optimal werden die betroffenen auf diesen Umstand hingewiesen.

Der Verantwortliche hat, unabhängig von der rechtmäßigen Verarbeitung und der entsprechenden Rechtsgrundlage, das den betroffenen Personen zustehende Widerspruchsrecht wahrzunehmen. Er hat bei einem eingelegten Widerspruch darzulegen, dass „seine zwingenden berechtigten Interessen Vorrang vor den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person haben“, vgl. auch Umsetzungshinweise zu 2.1.3. P.1.3.

Bitte beachten Sie, dass zu prüfen ist, ob Ausnahmen vom Widerspruchsrecht des Art. 21 DSGVO, z. B. aufgrund der Öffnungsklausel des Art. 23 DSGVO besteht, um das Recht auf Widerspruch gegenüber einer öffentlichen Stelle auszuschließen. In Deutschland z. B. ist hier § 36 BDSG relevant.

2.9.8. P.8.8 Recht auf Widerruf bei Einwilligung

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [DSK_K.Nr.20]

Es sollten Prozesse etabliert werden, die die Ausübung und Umsetzung des Widerrufsrechts ermöglichen. Dabei ist zu beachten, dass der Widerruf für die Zukunft wirkt. In der Vergangenheit liegende Verarbeitungsvorgänge personenbezogener Daten auf Grundlage der Einwilligung bleiben weiterhin rechtmäßig.

Auftragsverarbeiter sollten ein Konzept zur Unterstützung der Verantwortliche entwickeln, welches die erforderlichen Maßnahmen zur Unterstützung identifiziert und Verantwortlichkeiten sowie Fristen festlegt.

Es muss vor Abgabe der Einwilligung der betroffenen Person auf die Widerrufsmöglichkeit der Einwilligung hingewiesen werden. Auch sollte darüber informiert werden, wie die betroffene Person die Einwilligung widerrufen kann. Ein Widerrufsverzicht ist nicht zulässig. Zudem ist eine Kontaktmöglichkeit anzugeben, unter welcher ein Widerruf geltend gemacht werden kann. Der Widerruf der Einwilligung ist technisch umsetzbar und genauso leicht für die betroffene Person möglich, wie die Abgabe der Einwilligung. Die Sprache muss leicht verständlich und transparent sein. Das Recht, abgegebene Einwilligungen zu widerrufen, ist für die Einwilligenden deutlich hervorzuheben.

Eine Alternative Rechtsgrundlage für die Fortführung der Datenverarbeitung bei Widerruf der Einwilligung kann sich aus Art 17 Abs. 3 DSGVO ergeben, nämlich wenn die Verarbeitung erforderlich ist zur

- Ausübung des Rechts auf freie Meinungsäußerung und Information;
- zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;
- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89
- Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Der Kunde (als Verantwortlicher) ist verantwortlich dafür, nachzuweisen, dass alternative Rechtsgrundlage einschlägig ist für den konkreten Fall.

2.9.9. P.8.9 Automatisierte Entscheidungen / Profiling

Umsetzungshinweise zum Kriterium

Zur Auslegung des vorliegenden Kriteriums sind insb. folgende Vorgaben zu beachten:

- [Art.29_WP251]

Es sollte ein Konzept entwickelt werden, das den Umgang mit und die Beantwortung von Anfragen betroffener Personen festlegt und die unkomplizierte Ausübung der Betroffenenrechte ermöglicht. Eine Ausnahme von dieser Pflicht kann vorliegen, sofern der Verantwortliche nachweisen kann, dass er die betroffene Person nicht identifizieren kann.

Auftragsverarbeiter sollten ein Konzept zur Unterstützung der Verantwortliche entwickeln, welches die erforderlichen Maßnahmen zur Unterstützung identifiziert und Verantwortlichkeiten sowie Fristen festlegt.

Umsetzungshinweise zum Profiling vgl. insb. [Art.29_WP251].

2.9.10. P.8.10 Beschwerde-Management

Umsetzungshinweise zum Kriterium

Es ist sicherzustellen, dass die Zertifizierungsstelle über Beschwerden, die den Untersuchungsgegenstand oder Konformitätsaussage des Zertifikates betreffen informiert wird. Dies kann etwa folgende Arten von Beschwerden betreffen:

- Unrechtmäßige, missbräuchliche oder missverständliche Nutzung des Zertifikats oder anderer Lizenzzeichen;
- Datenschutzverletzungen mit Relevanz für die Zertifikatsaussage.

Aspekte zu einem Beschwerde-Management sind beispielsweise:

- öffentlich verfügbare Informationen zum Beschwerde-Management inkl. Ansprechpartner und Prozessbeschreibung;
- Definition von Verantwortlichkeiten inkl. Beachtung von etwaigen Interessenskonflikten;
- Bearbeitung von Beschwerden inkl. Ursachenanalyse und Verifikation;
- Rückmeldung an Meldenden;
- Vorgabe von Fristen;
- Weiterbearbeitung von Beschwerden mit Maßnahmendefinition und -verfolgung;
- Prozessbeschreibung über gesamten Prozess;
- Integration des Prozesses in die Organisation.

3. Referenzen

- [Art.29_WP250.ro1] Art. 29-Gruppe, WP 250 rev.01, „Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gem. der Verordnung (EU) 2016/679“, 06.02.2018.
- [Art.29_WP114] Art. 29-Gruppe, WP 114, „Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG“, 24.10.1995.
- [Art.29_WP131] Art. 29-Gruppe, WP 131, „Arbeitspapier zur Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)“, 15.02.2017.
- [Art.29_WP162] Art. 29-Gruppe, WP 162, „Zweite Stellungnahme 4/2009 zum Internationalen Standard der Welt-Anti-Doping-Agentur (WADA) zum Schutz der Privatsphäre und personenbezogener Informationen, zu entsprechenden Vorschriften des WADA-Codes und zu anderen Datenschutzfragen im Bereich des Kampfes gegen Doping im Sport durch die WADA und durch (nationale) Anti-Doping-Organisationen“, 06.04.2009.
- [Art.29_WP187] Art. 29-Gruppe, WP 187, „Stellungnahme 15/2011 zur Definition von Einwilligung“, 13.07.2011.
- [Art.29_WP216] Art. 29-Gruppe, WP 216, „Stellungnahme 5/2014 zu Anonymisierungstechniken“, 10.04.2014.
- [Art.29_WP217] Art. 29-Gruppe, WP 217, „Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gem. Art. 7 der Richtlinie 95/46/EG“, 09.04.2014.
- [Art.29_WP242] Art. 29-Gruppe, WP 242, „Leitlinien zum Recht auf Datenübertragbarkeit“, 05.04.2017.
- [Art.29_WP243.o1] Art. 29-Gruppe, WP 243 rev.01, „Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“)“, 05.04.2017.
- [Art.29_WP248.ro1] Art. 29-Gruppe, WP 248 rev. 01, „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679“, 04.10.2017.
- [Art.29_WP251] Art. 29-Gruppe, WP 251 „Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679“ 06.02.2018.
- [Art.29_WP259.ro1] Art. 29-Gruppe, WP 259 rev.01, „Leitlinien in Bezug auf die Einwilligung gem. Verordnung 2016/679“, 10.04.2018.

- [Art.29_WP48] Art. 29-Gruppe, WP 48, „Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten“, 13.09.2001.
- [Art.29_WP91] Art. 29-Gruppe, WP 91, „Arbeitspapier über genetische Daten“, 17.03.2004.
- [Art.29_WP194] Art. 29-Gruppe, WP 91, „Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht v. 07.06.2012“
- [BayLDA_Good Practice] BayLDA, „Good Practice bei technischen und organisatorischen Maßnahmen - Generischer Ansatz nach Art. 32 DSGVO zur Sicherheit“, 13.10.2020.
- [BayLfDI_Auftragsverarb.] BayLfDI, „Auftragsverarbeitung Orientierungshilfe Version 2.0“, 01.04.2019.
- [BfDI_Anonymisierung] BfDI, „Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche Stand“, 29.06.2020
- [DIN 66391-2] Büro- und Datentechnik - Vernichten von Datenträgern Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern Ausgabe 2012-10
- [DIN 66398] Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten Ausgabe 2016-05
- [DIN 66399-1] Büro- und Datentechnik - Vernichten von Datenträgern Teil 1: Grundlagen und Begriffe Ausgabe 2012-10
- [DIN 66399-3] Büro- und Datentechnik - Vernichten von Datenträgern Teil 3: Prozess der Datenträgervernichtung Ausgabe 2013-02
- [dsc_Kriterien] datenschutz cert GmbH, „Kriterienkatalog zur Zertifizierung einer IT-gestützten Verarbeitung personenbezogener Daten gem. Art. 42 DSGVO („DSGVO – information privacy standard“)“, Version 0.94, 29.08.2023.
- [DSK_Bestellpflicht_DSB] DSK, Beschluss „Bestellpflicht nach Artikel 37 Abs. 1 lit. C Datenschutz-Grundverordnung bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs“, 26.04.2018.
- [DSK_Direktwerbung] DSK, „Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO)“, November 2018.
- [DSK_ErwGr.33_DSGVO] DSK, Beschluss zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ im Erwägungsgrund 33 der DS-GVO, 03.04.2019.

[DSK_K.Nr.1]	DSK, „Kurzpapier Nr. 1 Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DSGVO“, 17.12.2018.
[DSK_K.Nr.10]	DSK, „Kurzpapier Nr. 10 Anforderungen an die Informationspflichten bei Dritt- und Direkterhebung“, 16.01.2018.
[DSK_K.Nr.11]	DSK, „Kurzpapier Nr. 11 Recht auf Löschung / „Recht auf Vergessenwerden“, 17.12.2018.
[DSK_K.Nr.12]	DSK, „Kurzpapier Nr. 12 Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern“, 17.12.2018.
[DSK_K.Nr.13]	DSK, „Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DSGVO“, 17.12.2018.
[DSK_K.Nr.14]	DSK, „Kurzpapier Nummer 14 Beschäftigtendatenschutz“, 24.09.2020.
[DSK_K.Nr.17]	DSK, „Kurzpapier Nr. 17 Besondere Kategorien personenbezogener Daten“, 27.03.2018.
[DSK_K.Nr.19]	DSK, „Kurzpapier Nr. 19 Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DSGVO“, 29.05.2018.
[DSK_K.Nr.20]	DSK, „Kurzpapier Nr. 20 Einwilligung nach der DS-GVO“, 22.02.2019
[DSK_K.Nr.4]	DSK, „Kurzpapier Nr. 4 Beschäftigtendatenschutz“ 24.09.2020.
[DSK_K.Nr.5]	DSK, „Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DSGVO“, 17.12.2018.
[DSK_K.Nr.6]	DSK, „Kurzpapier Nr. 6 Auskunftsrecht der betroffenen Person, Art. 15 DSGVO“, 17.12.2018.
[DSK_Online-Dienste]	DSK, „Orientierungshilfe: Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung“, 29.3.2019.
[DSK_S-D-M_V.2.ob]	DSK, „Das Standard-Datenschutzmodell Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, V. 2.ob“, 17.04.2020.
[DSK_Telemedien]	DSK, „Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien“, März 2019.
[EDPS_4/2017]	EDPS, “Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content”, 14.03.2017.
[EDSA_01/2020]	EDSA, “Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data”, V.2.0, 18.06.2021.

[EDSA_01/2023]	EDSA, "Report of the work undertaken by the Cookie Banner Taskforce", 17.01.2023.
[EDSA_02/2018]	EDSA, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679 vom 25. Mai 2018
[EDSA_05/2020]	EDSA, "Guidelines 05/2020 on consent under Regulation 2016/679" Version 1.1, 11.05, 2020.
[EDSA_05_2021]	EDPB, "Guidelines 05 / 2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR", Version 1.0, 18.11.2021.
[EDSA_07/2020]	EDSA, "Guidelines 07/2020 on the concepts of controller and processor in the GDPR", Version 1.0, 02.09.2020.
[EDSA_07/2022]	EDSA, Guidelines 07/2022 on certification as a tool for transfers vom 30.06.2022
[EDSA_2/2019]	EDSA, „Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gem. Art. 6 Abs. 1 lit. b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen“, Version 2.0, 08.10.2019.
[EDSA_3/2020]	EDSA, „Leitlinien 3/2020 für die Verarbeitung von Gesundheitsdaten für wissenschaftliche Forschungszwecke im Zusammenhang mit dem COVID-19-Ausbruch“, Version 1.1, 21.04.2020.
[EDSA_4/2019]	EDSA, "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default", Version 1.0, 13.11.2019.
[EDSA_5/2019]	EDSA, „Leitlinien 5/2019 zu den Kriterien des Rechts auf Vergessenwerden in Fällen in Bezug auf Suchmaschinen gem. der DSGVO Teil 1“: Version 2.0, 07.07.2020.
[EDSA_2_2023]	EDSA, Verbindlicher Beschluss 2/2023 zu dem von der irischen Aufsichtsbehörde vorgelegten Streitfall betreffend TikTok Technology Limited (Artikel 65 DSGVO), 02.08.2023
[EDSA_1_2022]	EDSA, Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht Version 2.1, 28.03.2023
[EDSA_8_2024]	EDSA, Stellungnahme 08/2024 zur „Wirksamkeit von Einwilligungen im Kontext von „Consent or Pay“-Modellen großer Online-Plattformen“, 17. April 2024
[EDSA_QA-C-311/18]	EDSA, „Häufig gestellte Fragen zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 — Data Protection Commissioner gegen Facebook Ireland Ltd und Maximilian Schrems“, 23.07.2020.



[LfDI_Ni-Consent-Layer] LfDI Niedersachsen, „Handreichung: Datenschutzkonforme Einwilligungen auf Webseiten – Anforderungen an Consent-Layer“, November 2020.

[PRIPARE] PRIPARE Handbook: Methodological Tools to Implement Privacy and Foster Compliance with the GDPR, Version 1.00, 31.12.2015

[TeleTrust_StdT] Bundesverband IT-Sicherheit e.V., „It-Sicherheitsgesetz und Datenschutz-Grundverordnung: „Handreichung zum Stand der Technik“ technischer und organisatorischer Maßnahmen“, Version 1.7, 10.2020.