ePrivacyseal GmbH

Kriterienkatalog DE

(inkl. Anforderungen nach EU-DSGVO)

Juli 2016

Das Datenschutzgütesiegel der ePrivacyseal GmbH zertifiziert dem jeweiligen Antragsteller, dass sein Angebot mit den im nachfolgenden Kriterienkatalog näher spezifizierten Kriterien, die sich im Teil A an den Anforderungen des deutschen Datenschutzrechtes und im Teil B an den zusätzlichen Anforderungen der EU-Datenschutzgrundverordnung (EU-DSGVO) orientieren, im Einklang steht. Im Einzelnen wird damit die Einhaltung folgender Bestimmungen bestätigt:

Teil A

I. Allgemeine Grundsätze

1. Grundsätze der Datenvermeidung und Datensparsamkeit

Die Gebote zur Datenvermeidung und Datensparsamkeit müssen berücksichtigt werden (§ 3a BDSG). Bei der Auswahl und Gestaltung des Systems ist daher der Grundsatz, nur so wenig

personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen, zu berücksichtigen.

- Werden personenbezogene Daten, soweit dies nach den Verwendungszwecken möglich ist und dies keine im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert, anonymisiert oder pseudonymisiert?

- Soweit personenbezogene Daten erhoben bzw. verarbeitet und genutzt werden: Ist vorab geprüft worden, ob nicht auch die Möglichkeit der Anonymisierung oder Pseudonymisierung dieser Daten in Betracht kommt?

- Werden nur die personenbezogenen Daten erhoben bzw. verarbeitet und genutzt, die für den Verwendungszweck unbedingt erforderlich sind?

- Sind ausreichende Maßnahmen getroffen worden, die Menge der zu verarbeitenden Daten möglichst gering zu halten? Wenn ja, welche?

- Werden bei jedem Verwendungsschritt ggf. nicht mehr für den ursprünglichen Verarbeitungszweck erforderliche Daten umgehend gelöscht?

- Wie wird die Löschung bzw. Anonymisierung und Pseudonymisierung der Daten umgesetzt?

- Erfolgt die Anonymisierung bzw. Pseudonymisierung zum frühestmöglichen Zeitpunkt?

- Ist im Falle einer Pseudonymisierung von Daten gewährleistet, dass diese Daten nicht mit wenig Aufwand wieder „depseudonymisiert" werden können?

- Sind die Mitarbeiter hinsichtlich der Grundsätze der Datenvermeidung und Datensparsamkeit ausreichend geschult?

2. Transparenz

a) Beschreibung des Produkts / der Dienstleistung

Dem Nutzer muss eine klar verständliche Beschreibung des angebotenen Produkts bzw. der angebotenen Dienstleistung zur Verfügung gestellt werden.

- Wird dem Nutzer eine klar verständliche Beschreibung des angebotenen Produkts bzw. der angebotenen Dienstleistung zur Verfügung gestellt?

- Wird diese Beschreibung immer auf dem aktuellen Stand gehalten?

- Werden in dieser Beschreibung der Fluss der Datenverarbeitung sowie etwaige Datenübermittlungen bzw. Zugriffsrechte hinreichend deutlich?

b) Informationspflichten

Der Antragsteller muss die folgenden Informationspflichten erfüllen, soweit Gegenstand der Zertifizierung ein Onlineangebot ist:

- Enthält das Online-Angebot eine ausreichende Anbieterkennzeichnung?

- Gibt es ein den Anforderungen von § 5 TMG entsprechendes Impressum?

- Wird kommerzielle Kommunikation (also Werbung, z. B. per E-Mail) klar als solche gekennzeichnet und ist das Unternehmen, welches diese verschickt, klar identifizierbar?

- Soweit Angebote zur Verkaufsförderung wie Preisnachlässe, Zugaben und Geschenke angeboten werden: Sind diese für den Nutzer klar erkennbar und sind die Bedingungen für ihre Inanspruchnahme leicht zugänglich sowie klar und eindeutig?

- Werden etwaige Preisausschreiben oder Gewinnspiele mit Werbecharakter klar als solche identifiziert und sind deren Teilnahmebedingungen einfach zugänglich sowie in transparenter Weise erläutert?

- Wird in Werbe-E-Mails weder der Absender, noch der kommerzielle Charakter der Nachricht verschleiert?

- Wird der Nutzer in klar verständlichen Worten im Rahmen einer Datenschutzerklärung über die Datenverarbeitung, insbesondere Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten, hinreichend aufgeklärt?

- Ist die Unterrichtung über die Datenerhebung korrekt und vollständig?

- Falls die Daten auch außerhalb der EU/EWR verarbeitet werden: Wird der Nutzer darüber informiert?

- Falls Nutzungsprofile erstellt werden: Wird der Nutzer darauf sowie auf sein Widerspruchsrecht hingewiesen?

- Erfolgt eine ausreichende Information über Cookies, Weblogs, Analyse- bzw. Tracking-Dienste etc.?

- Ist die Datenschutzerklärung jederzeit abrufbar?

- Soweit eine Weitervermittlung zu einem anderen Diensteanbieter erfolgt:

    - Wird dem Nutzer diese Weitervermittlung angezeigt?

    - Geschieht dies in verständlicher Weise?

3. Zweckbindung und Zweckänderung

Der Antragsteller hat bei der Datenspeicherung, -verarbeitung und -nutzung sicherzustellen, dass die erhobenen Daten nur gemäß ihrer Zweckbestimmung verarbeitet werden oder dass eine gesetzlich zulässige Zweckänderung gegeben ist.

- Ist sichergestellt, dass die erhobenen Daten nur gemäß ihrer Zweckbestimmung verarbeitet werden?

- Wird dazu der Zweck dokumentiert, für den die personenbezogenen Daten erhoben werden?

- Werden die Datensätze mit den entsprechenden Zwecken versehen?

- Wird die Verarbeitung der Daten protokolliert, um ggf. Zweckänderungen nachweisen zu können?

4. Trennungsgebot

Der Antragsteller hat zu gewährleisten, dass bei seiner Datenverarbeitung das Trennungsgebot beachtet wird. Das Trennungsgebot verlangt, dass die Daten, die zu

unterschiedlichen Zwecken erhoben wurden, getrennt voneinander verarbeitet werden können.

- Falls Daten unterschiedlichen Ursprungs an einer zentralen Stelle gespeichert werden: Ist technisch bzw. organisatorisch gewährleistet, dass das Auslesen einzelner Datensätze nur und ausschließlich zweckgebunden erfolgen kann?

- Sofern es sich um IT-Dienstleister handelt: Ist bei mehreren Kunden gewährleistet, dass die Datenverarbeitungssysteme so ausgestaltet sind, dass sich die Datenbereiche der Kunden nicht versehentlich überschneiden und dadurch Daten des einen Kunden von anderen mit ausgelesen werden können?

II. Zulässigkeit der Datenverarbeitung

1. Zulässigkeit der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten

a) Personenbezogene Daten werden nur erhoben, verarbeitet oder genutzt, weil entweder ein Gesetz dieses zulässt oder der Betroffene eingewilligt hat.

b) Sofern eine Einwilligung des Betroffenen einzuholen ist, ist sicherzustellen, dass sie auf der freien Entscheidung des Betroffenen beruht. Zudem ist bei der Einholung der Einwilligung auch sicherzustellen, dass zugleich auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalls erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hingewiesen wird. Der Antragsteller muss ferner sicherstellen, dass die Einwilligung in der gesetzlich vorgesehenen Form eingeholt wird.

- Ist ein gesetzlicher Erlaubnistatbestand zur Verarbeitung der Daten, z. B. gem. der §§ 28 ff. BDSG oder der §§ 67a ff. SGB X vorhanden?

- Falls dies nicht der Fall ist: Ist eine Einwilligung des Betroffenen Nutzers in wirksamer Weise eingeholt worden?

- Ist die Formulierung einer vorgegebenen Einwilligungserklärung hinreichend konkret, d. h. sind die erforderlichen Angaben zu der datenverarbeitenden Stelle, der Art von Daten, die verarbeitet werden sollen, geplanten Übermittlung sowie den Empfängern dieser

etwaigen Übermittlung, Zweck der Datenverarbeitung sowie zudem auch ein Hinweis auf die Widerrufbarkeit dieser Einwilligung sowie deren Freiwilligkeit vorhanden?

- Sind die in § 4 a BDSG monierten Formvorschriften eingehalten worden? Ist also die Einwilligung schriftlich erteilt worden, es sei denn, dass wegen besonderer Umstände eine andere Form angemessen ist?

- Sofern diese Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt wird: Ist die Einwilligung besonders hervorgehoben?

- Wenn die Einwilligung über ein elektronisches Medium wie E-Mail bzw. das Internet eingeholt werden soll, kann dies entweder nach § 13 Abs. 2 TMG oder nach § 4 Abs. 1 Satz 3 BDSG auch elektronisch erfolgen.

- Werden die Einwilligungen so gesammelt/archiviert, dass für jeden einzelnen Kunden bei Anfrage die gegebene Einwilligung als Nachweis-Beleg geliefert werden kann?

2. Besondere Arten personenbezogener Daten

Sollte der jeweilige Antragsteller besondere Arten personenbezogener Daten im Sinne von § 3 Abs. 9 BDSG für eigene Geschäftszwecke erheben, verarbeiten oder nutzen, ist insbesondere sicherzustellen, dass die Voraussetzungen des § 28 Abs. 6-9 BDSG eingehalten werden.

Besonders sensible Daten gem. § 3 Abs. 9 BDSG sind Angaben über die rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Sofern diese verarbeitet werden sollen, gelten zudem die folgenden Anforderungen:

- Soweit es um eine Datenerhebung und -speicherung für eigene Geschäftszwecke im Sinne des § 28 BDSG geht, sind die Einschränkungen des § 28 Abs. 6 bis 9 BDSG zu beachten.

- Die Datenerhebung und Speicherung dieser besonders sensiblen Daten für eigene Geschäftszwecke ist, sofern der Betroffene nicht wirksam eingewilligt hat, zulässig, wenn

- dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außer Stande ist, seine Einwilligung zu geben,

- es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,

- dies zu Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder

- dies zur Durchführung wissenschaftlicher Forschungen erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht übernommen und nur unter unverhältnismäßigem Aufwand erreicht werden kann.

- Das Erheben von besonderen Arten personenbezogener Daten ist zudem zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen.

- Für einen anderen Zweck dürfen diese besonders sensiblen Daten nur unter der Voraussetzung des § 28 Abs. 6 Nr. 1 bis 4 und des § 28 Abs. 7 Satz 1 übermittelt oder genutzt werden. Zudem ist eine Übermittlung oder Nutzung auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist.

3. Erhebung und Verarbeitung von Nutzungsdaten sowie Erstellung von Nutzungsprofilen

Bei bloßem Seitenaufruf des Nutzers muss der Antragsteller sicherstellen, dass nur die nach § 15 Abs. 1 TMG zulässigen Nutzungsdaten erhoben werden. Sofern der Antragsteller Nutzungsprofile unter einem Pseudonym für Zwecke der Werbung, Marktforschung oder

bedarfsgerechten Gestaltung von Telemedien erstellt, muss er sicherstellen, dass die Anforderungen des § 15 Abs. 3 TMG beachtet werden.

- Welche Nutzungsdaten werden erhoben?
- Durch wen werden diese Nutzungsdaten erhoben
- Werden diese Nutzungsdaten auch gespeichert? Wenn ja: Durch wen und für wie lange?
- Wann werden die Nutzungsdaten gelöscht?
- Werden nur Nutzungsdaten erhoben, die für die Erbringung bzw. Abrechnung des angebotenen Dienstes erforderlich sind?
- Ist sichergestellt, dass die Nutzungsdaten zu keinem anderen Zweck verarbeitet werden?
- Werden nur Nutzungsdaten gespeichert, die für die Abrechnung des angebotenen Dienstes erforderlich sind?
- Werden darüber hinaus auch Bestandsdaten erhoben?
- Sofern auch die IP-Adresse erhoben wird: vom wem wird die IP-Adresse erhoben und zu welchem Zweck?
- Wird die IP-Adresse auch gespeichert? Wenn ja: für wie lange?
- Sofern Cookies eingesetzt werden:
    - Welche Arten von Cookies werden eingesetzt?
    - Kann der Nutzer dem Setzen der Cookies widersprechen?
    - Werden die in den Cookies gespeicherten Daten ausgelesen? Wenn ja: Erfolgt eine Speicherung dieser Daten? Zu welchem Zweck?
    - Liegt eine entsprechende Einwilligung des Nutzers vor?
- Sofern Analyse- bzw. Tracking-Dienste eingesetzt werden: Sind diese datenschutzrechtlich unbedenklich?

III. Gewährleistung der Betroffenenrechte

Der Antragsteller hat zu gewährleisten, dass die gesetzlich verankerten Betroffenenrechte in effektiver Weise durchsetzbar sind und dass die dazu erforderlichen technischen und organisatorischen Maßnahmen eingerichtet worden sind. Dazu zählen insbesondere die folgenden Rechte bzw. Verpflichtungen:

1. Recht auf Auskunft

- Sind alle Informationen, die der Nutzer benötigt, um seinen Auskunftsanspruch geltend zu machen, leicht auffindbar?
- Bezieht sich die Auskunftsmöglichkeit auf den vollständigen Auskunftsanspruch, also auf alle gespeicherten Daten, Zweck- und Rechtsgrundlage, Herkunft und Empfängerkreis?
- Wird bei einem Auskunftsverlangen in hinreichender Weise sichergestellt, dass der Anfragende zur Erteilung der Auskunft berechtigt ist?
- Wenn diese personenbezogenen Daten an den Anfragenden übermittelt werden, erfolgt dabei eine Protokollierung der Übermittlung?

2. Recht auf Berichtigung unrichtiger Daten

- Sobald die Unrichtigkeit von personenbezogenen Daten festgestellt wird, werden diese unverzüglich korrigiert?
- Gibt es eine automatisierte Berichtigungsbearbeitung?
- Ist sichergestellt, dass auch die Empfänger vorangegangener Datenübermittlung über diese Berichtigung in Kenntnis gesetzt werden?

3. Recht auf Löschung bzw. Sperrung personenbezogener Daten

- Werden personenbezogene Daten vollständig und irreversibel gelöscht?
- Nach welchen Zeiträumen werden diese Daten gelöscht?

- Ist sichergestellt, dass die zunächst gelöschten Daten nicht wiederhergestellt werden können?

- Ist sichergestellt, dass an Empfänger vorangegangener Datenübermittlungen diese Löschungen weitergeleitet werden?

- Sofern an die Stelle einer Löschung der Daten eine Sperrung tritt, weil der Löschung ein Hindernis entgegensteht, muss gewährleistet sein, dass diese gespeicherten personenbezogenen Daten gekennzeichnet werden, um ihre weitere Verarbeitung oder Nutzung einzuschränken. Gibt es eine Möglichkeit, die Datensätze so zu kennzeichnen, dass sie zwar gespeichert bleiben, aber nicht im Rahmen der normalen Verarbeitung genutzt werden?

- Wird diese Sperrung durch ein hinreichendes Verfahren gewährleistet?

- Gibt es eine Protokollierung sowohl hinsichtlich des Zeitpunkts aber auch des Auftraggebers bzgl. der Sperrung sowie auch ggf. eine Aufhebung dieser Sperre?

4. Widerspruchsrechte der Betroffenen

Dem Nutzer steht ein Widerspruchsrecht gegen die Erhebung, Verarbeitung oder Nutzung seiner Daten zu. Auf einen Widerspruch des Betroffenen muss die weitere Verarbeitung seiner personenbezogenen Daten unterbleiben, sofern die schutzwürdigen Interessen des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der datenverarbeitenden Stelle überwiegen.

- Ist gewährleistet, dass ein solcher Widerspruch unverzüglich berücksichtigt wird?

- Wird gewährleistet, dass nach erfolgtem Widerspruch die entsprechenden Daten umgehend gelöscht werden?

- Ist sichergestellt, dass solche Widersprüche auch am Empfänger vorangegangener Datenübermittlungen weitergeleitet werden?

5. Weiterleitungs- und Unterrichtungspflicht i.S.d. § 6 Abs. 2 BDSG

Wenn mehrere Stellen zur Speicherung der persönlichen Daten eines Nutzers berechtigt sind, sind diese Stellen verpflichtet, etwaige Anfragen eines Nutzers an diejenige Stelle, die die Daten tatsächlich gespeichert hat, weiterzuleiten. Darüber hinaus ist auch der Nutzer über diese Weiterleitung des Vorbringens und auch über die zuständige Stelle zu unterrichten.

- Falls derartige Anfragen eines Betroffenen eingehen, muss gewährleistet sein, dass diese unverzüglich an die Stelle, die die Daten tatsächlich gespeichert hat, weitergeleitet werden. Ist dies der Fall?

- Ist gewährleistet, dass auch der Betroffene über diese Weiterleitung seine Anfrage sowie auch die zuständige Stelle umgehend unterrichtet wird?

IV. Datenschutzmanagement

Die Gesamtorganisation des Antragstellers berücksichtigt die Belange des Datenschutzes, so dass hinreichende Standards und Regelungen vorhanden sind, die die Erreichung der Datenschutzziele gewährleisten.

1. Datenschutzbeauftragter

Das Unternehmen des Antragstellers hat die Bestellung eines betrieblichen bzw. externen Datenschutzbeauftragten gem. § 4f BDSG darzulegen, soweit dies nach den gesetzlichen Anforderungen erforderlich ist.
§ 4 f BDSG sieht vor, dass unter bestimmten Voraussetzungen ein Datenschutzbeauftragter bestellt werden muss. Dies ist der Fall, wenn der Antragsteller zu einer der folgenden Stellen gehört:

- Öffentliche Stelle, die personenbezogene Daten automatisiert verarbeitet.

- Nicht öffentliche Stelle, die personenbezogene Daten automatisiert verarbeitet, wenn in der Regel 10 oder mehr Personen ständig mit der automatisierten Verarbeitung dieser personenbezogenen Daten beschäftigt sind.

- Öffentliche und nicht öffentliche Stellen, die personenbezogene Daten „auf andere Weise“ – also nicht automatisiert – erheben, verarbeiten oder nutzen, wenn in der Regel damit mindestens 20 Personen beschäftigt sind.

Da jede Benutzung von Internet oder E-Mail in der Praxis bereits indiziert, dass damit eine automatisierte Verarbeitung verbunden ist, sind in aller Regel heut zu Tage fast alle Datenverarbeitungen auch automatisiert. Dabei ist es unerheblich, welchen arbeitsrechtlichen Status diese Personen haben, also ob sie Arbeitnehmer, freie Mitarbeiter oder z. B. Auszubildende sind. Es ist vielmehr ausreichend, wenn diese Mitarbeiter auch nur eine geringe Beteiligung an den Verarbeitungsvorgängen haben, soweit dabei ein Zugriff dieser Mitarbeiter auf personenbezogene Daten nicht ausgeschlossen werden kann.

- Ferner haben nicht öffentliche Stellen, die eine automatisierte Verarbeitung vornehmen, unabhängig von der Anzahl der mit dieser automatisierten Verarbeitung beschäftigten Personen immer einen Datenschutzbeauftragten zu bestellen,

    - wenn diese Verarbeitung einer Vorabkontrolle im Sinne des § 4d BDSG unterliegen oder

    - wenn diese nicht öffentlichen Stellen personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeiten,

- Sofern diese Voraussetzungen gegeben sind, ist ein Datenschutzbeauftragter wirksam bestellt worden?

2. Verfahrensverzeichnis

Der Antragsteller hat das Vorliegen eines Verfahrensverzeichnisses gem. § 4e BDSG zu dokumentieren, soweit dies nach den gesetzlichen Anforderungen erforderlich ist.

- Ist ein Verfahrensverzeichnis bzw. eine Verarbeitungsübersicht vorhanden, in der zumindest die folgenden Angaben enthalten sind:

    a) Name oder Firma der verantwortlichen Stelle,

    b) Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufenen Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,

    c) Anschrift der verantwortlichen Stelle,

    d) Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung,

e) Eine Beschreibung der betroffenen Personengruppen unter diesbezüglichen Daten oder Datenkategorien,

f) Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,

g) Regelfristen für die Löschung der Daten,

h) Eine geplante Datenübermittlung in Drittstaaten,

i) Eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 BDSG zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

3. Auftragsdatenverarbeitung

Der Antragsteller hat, soweit dies erforderlich ist, Auftragsdatenverarbeitungsverträge gem. § 11 BDSG abzuschließen.

- Erfolgt eine Datenverarbeitung durch Dritte?
- Ist eine derartige Datenverarbeitung durch ein Drittunternehmen zulässig? Vgl. dazu u.a. § 203 StGB, § 80 Abs. 5 SGB V.
- Ist ein entsprechender Auftragsdatenverarbeitungsvertrag abgeschlossen worden?
- Sind in diesem Vertrag die nach § 11 Abs. 2 BDSG festzulegenden Einzelheiten bestimmt worden?
- Gibt es hinreichende technische und organisatorische Maßnahmen, die insbesondere auch die Bindung des Auftragnehmers an die Weisungen der verantwortlichen Stelle gewährleisten?
- Sind die hinreichenden technischen und organisatorischen Maßnahmen auf Ihre Einhaltung überprüft worden und wurde das Ergebnis der Prüfung dokumentiert?

4. Technische und organisatorische Sicherheitsmaßnahmen

Der Antragsteller muss darlegen, dass in seinem Unternehmen hinreichende technische und organisatorische Sicherheitsmaßnahmen im Sinne des § 9 BDSG implementiert worden sind. Erforderlich sind solche Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

In der Anlage zu § 9 BDSG sind Anforderungen an die technischen und organisatorischen Sicherheitsmaßnahmen, die von Unternehmen zur Erreichung eines einheitlichen gesetzlichen Mindeststandards gestellt werden, enthalten. Hinsichtlich der dabei zu treffenden Maßnahmen gibt es für die Unternehmen einen gewissen Spielraum, so dass es das Unternehmen in der Hand hat, die jeweilige konkrete Ausgestaltung zu wählen. Da es dabei höchst unterschiedliche Gestaltungsmöglichkeiten hinsichtlich der Erreichung der Mindeststandards gibt, sind die nachfolgenden Fragen lediglich als Indiz bzw. Beispiele dafür zu verstehen, dass diese Mindestanforderungen erfüllt werden.

a) Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren, wobei der Begriff räumlich zu verstehen ist, beispielsweise durch:

- Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte, wobei die Anforderungen von § 6c BDSG zu beachten sind
- Schlüssel / Schlüsselvergabe
- Türsicherung (elektrische Türöffner usw.)
- Werkschutz, Pförtner
- Überwachungseinrichtung wie z.B. Alarmanlage, Video-/Fernsehmonitor, wobei die Anforderungen von § 6b BDSG zu beachten sind

b) Zugangskontrolle

Das Eindringen Unbefugter in und Nutzen von Datenverarbeitungssystemen ist zu verhindern durch technische (Kennwort-/Passwortschutz) und organisatorische

(Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung.

- Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
- Zugriff auf Server nur mit persönlichem Konto und speziell definierten Zugangsrechten (Nutzergruppen)
- Einrichtung eines Benutzerstammsatzes pro User
- Verschlüsselung von Datenträgern bzw. Datenverkehr zwischen den Servern
- Vergabe von Admin-Accounts
- Nur befugte Personen haben Zugang zu den Serversystemen

c) Zugriffskontrolle

Unerlaubte Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen sind zu verhindern durch bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung.

- Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte), z.B. durch Rechteverwaltung und Zugriffskontrolle
- Einrichtung eines Benutzerverwaltungssystems
- Benutzer- und Rechteverwaltung nur durch klar definierte Mitarbeiter der IT
- Einsatz von professionellen und sicheren Archivierungslösungen
- Zuverlässige Löschung von Daten bzw. Datenträgern

d) Weitergabekontrolle

Die Aspekte der Weitergabe personenbezogener Daten sind zu regeln, z.B. hinsichtlich der elektronischen Übertragung, Datentransport, Übermittlungskontrolle, etc. Dazu

zählen auch Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträgern (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung.

- Absicherung der elektronischen Kommunikationswege, z.B. durch Einrichten von geschlossenen Netzwerken oder Verfahren zur Verschlüsselung von zu übertragenden Daten
- Tunnelverbindung (VPN = Virtual Private Network)
- Elektronische Signatur
- Protokollierung
- Transportsicherung, z.B. durch Verwendung von sicheren Transportbehältern für Datenträger

e) Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten, z.B. durch Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind.

- Detaillierte Protokollierungs- und Protokollauswertungssysteme hinsichtlich der Erstellung, Veränderung und Entfernung von Datensätzen

f) Auftragskontrolle

Soweit eine Auftragsdatenverarbeitung i.S.d. § 11 BDSG gegeben ist: Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten durch Maßnahmen (technisch sowie organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer.

- Eindeutige Vertragsgestaltung
- Formalisierte und damit standardisierte Erteilung von Aufträgen (Auftragsformular) bzw. Weisungen

- Kriterien zur Auswahl des Auftragnehmers
- Klare Kompetenzabgrenzungen
- Kontrolle der Vertragsausführung

g) Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen durch physikalische bzw. logistische Maßnahmen zur Datensicherung.

- Backup-Verfahren
- Spiegeln von Festplatten, z.B. RAID-Verfahren
- Regelmäßige Erstellung von vollwertigen Sicherungskopien und deren Auslagerung an anderen Ort
- Regelmäßiges Testen der Datenwiederherstellung
- Unterbrechungsfreie (akkugestützte) Stromversorgung
- Virenschutz / Firewall
- Erstellung eines Notfallkonzepts und entsprechender schriftlicher Unterlagen

h) Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten. Daher sind Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken zu gewährleisten.

- Vergabe von Zugriffsberechtigungen/-beschränkungen
- Verschlüsselte Speicherung von personenbezogenen Daten, damit diese im Falle eines versehentlichen Abrufs durch Dritte nicht von diesen gelesen werden können
- Speicherung auf physikalisch getrennten Systemen (Trennung nach Kompetenzen und Aufgabengebieten)

5. Innerbetriebliche Regelungen

Der Antragsteller muss darlegen, dass in seinem Unternehmen hinreichende innerbetriebliche Regelungen, insbesondere auch für die Mitarbeiter, zum Thema Datenschutz existieren.

- Sind alle mit der Datenverarbeitung beschäftigten Mitarbeiter auf das Datengeheimnis verpflichtet worden?
- Sind in den Unternehmen systematische Regelungen zum Umgang mit personenbezogenen Daten vorhanden?
- Sind für die Mitarbeiter Anweisungen vorhanden für die zum Thema Datenschutz aufkommenden Fragen?
- Werden die Mitarbeiter in regelmäßigen Abständen für das Thema Datenschutz sensibilisiert bzw. finden in regelmäßigen Abständen entsprechende Schulungen statt?

Teil B

Zusätzliche Anforderungen nach der EU-Datenschutzgrundverordnung („DSGVO“):

1. **Grundsätze für die Verarbeitung personenbezogener Daten:**
   Die Grundsätze zur Verarbeitung personenbezogener Daten nach Art. 5 DSGVO müssen berücksichtigt werden.

   - Werden personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet? Werden also die Grundsätze der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz erfüllt?

   - Werden personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben? Werden sie nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet?

   - Werden personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt („Datenminimierung“)?

   - Werden personenbezogene Daten sachlich richtig und erforderlichenfalls auf den neusten Stand erfasst? Sind Maßnahmen getroffen, damit personenbezogene Daten, die unrichtig sind, unverzüglich gelöscht oder berichtigt werden können?

   - Werden personenbezogene Daten in einer Form gespeichert, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke für die sie verarbeitet werden, erforderlich ist?

   - Werden personenbezogene Daten in einer Weise verarbeitet, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet,

einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung oder unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

2. Rechtmäßigkeit der Verarbeitung:

Ist die Verarbeitung personenbezogener Daten rechtmäßig, weil:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

3. Zweckänderung:

Kommt es zu einer Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden? Beruht diese auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedsstaaten?

Sofern dies nicht der Fall ist: Ist die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar im Sinne von Art. 6 Abs. 4 DSGVO?

Ist bei der Prüfung dieser Vereinbarkeit folgendes berücksichtigt worden:

a) die Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,

b) der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,
c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,
d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

4. Rechtmäßigkeit der Einwilligung:

Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

Sofern dies durch eine schriftliche Erklärung erfolgt,

- ist sichergestellt, dass diese Erklärung, sofern sie noch andere Sachverhalte betrifft, in verständlicher und leicht zugänglicher Form in der klaren und einfachen Sprache erfolgt, und zwar dergestalt, dass sie von den anderen Sachverhalten klar zu unterscheiden ist?

- Ist sichergestellt, dass die betroffene Person das Recht besitzt, ihre Einwilligung jederzeit zu widerrufen? Ist sichergestellt, dass der Widerruf der Einwilligung so einfach erfolgen kann, wie die Erteilung der Einwilligung? Wird die betroffene Person vor Abgabe der Einwilligung von ihrem Widerspruchsrecht in Kenntnis gesetzt?

- Ist die Einwilligung freiwillig erfolgt? Ist dabei dem Umstand Rechnung getragen worden, ob u. a. die Erfüllung eines Vertrages, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrages nicht erforderlich sind?

- Ist sichergestellt, sofern es um die Einwilligung eines Kindes geht, dass das Kind das 16. Lebensjahr vollendet hat?

5. Verarbeitung besonderer Kategorien personenbezogener Daten:

Sollte der Antragsteller besondere personenbezogene Daten verarbeiten, sind die Voraussetzungen des Art. 9 DSGVO einzuhalten.

Besondere personenbezogene Daten sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgeht, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Die Verarbeitung ist unzulässig, es sei denn:

a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach EU Recht oder dem Recht der Mitgliedstaaten kann das Verbot durch die Einwilligung der betroffenen Person gar nicht aufgehoben werden,

b) die Verarbeitung ist erforderlich, damit der Verantwortliche oder die

betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist,

c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben,

d) die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden,

e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,

f) die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich,

g) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und

angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich,

h) die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich,

i) die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich, oder

j) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 erforderlich.

6. Gewährleistung der Rechte der betroffenen Person:

Der Antragsteller hat zu gewährleisten, dass die in den Art. 12 ff. DSGVO näher spezifizierten Rechte der betroffenen Personen sichergestellt sind. Dazu zählen insbesondere folgende Rechte bzw. Verpflichtungen:

Transparente Information, Kommunikation und Modalitäten:

- Erhält die betroffene Person alle Informationen, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt? Das gilt insbesondere für Informationen, die sich speziell an Kinder richtet.
- Erfolgt die Übermittlung der Informationen schriftlich oder in anderer Form, ggf. auch elektronisch?
- Werden der betroffenen Person, sofern personenbezogene Daten erhoben werden, folgendes mitgeteilt:

  a) der Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
  b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
  c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
  d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
  e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
  f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

- Werden zusätzlich zu den vorgenannten Informationen der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung gestellt sind, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

  a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

  b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

  c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a DSGVO beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

  d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

  e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

  f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 DSGVO und – zumindest in diesen Fällen – aussagekräftige

Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

- Ist sichergestellt, dass der Antragsteller, sofern personenbezogene Daten für einen anderen Zweck weiterverarbeitet werden sollen, als den, für den die personenbezogenen Daten erhoben wurden, die betroffene Person vor dieser Weiterverarbeitung darüber informiert?

7. Auskunftsrechte der betroffenen Person:

- Ist sichergestellt, dass die betroffene Person gem. Art. 15 DSGVO das Recht hat, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden?

  Sofern dies der Fall ist, ist sichergestellt, dass die Person ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen besitzt:

  a) die Verarbeitungszwecke;

  b) die Kategorien personenbezogener Daten, die verarbeitet werden;

  c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;

  d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

  e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung

der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

8. **Recht auf Berichtigung:**

Es ist sicherzustellen, dass die betroffene Person gem. Art. 16 DSGVO das Recht hat, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen.

Weiter ist sicherzustellen, dass unter Berücksichtigung der Zwecke der Verarbeitung die betroffene Person das Recht hat, die Vervollständigung unvollständig personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen.

9. Recht auf Löschung („Recht auf Vergessen werden"):

Ist sichergestellt, dass die betroffene Person ihr Recht gem. Art. 17 DSGVO durchsetzen kann, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden und der Verantwortliche verpflichtet ist, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.

d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

Dies gilt nur dann nicht, sofern die Voraussetzungen des Art. 17 Abs. 3 DGSVO vorliegen.

10. Recht auf Einschränkung der Verarbeitung:

Es ist sicherzustellen, dass die betroffene Person gem. Art. 18 DSGVO das Recht besitzt, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

a) die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem Verantwortlichen

ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen,

b) die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;

c) der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder

d) die betroffene Person Widerspruch gegen die Verarbeitung gemäß Artikel 21 Absatz 1 eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

11. Recht auf Datenübertragbarkeit:

Es ist sicherzustellen, dass die betroffene Person das Recht besitzt und auch wirksam durchsetzen kann, das ihm zustehende Recht auf Datenübertragbarkeit gem. Art. 20 DSGVO durchzusetzen.

12. Widerspruchsrechte:

Der jeweils betroffenen Person muss gem. Art. 21 DSGVO das Recht eingeräumt werden, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 e oder f DSGVO erfolgt ist, Widerspruch einzulegen.

- Das Widerspruchsrecht gilt auch für ein auf Art. 6 Abs. 1 e und f DSGVO gestütztes Profiling.
- Es ist sicherzustellen, dass der Verantwortliche im Falle eines Widerspruches die personenbezogenen Daten nicht mehr verarbeitet, es sei denn, er kann

zwingende schutzwürdige Gründe im Sinne von Art. 21 Abs. 1 DSGVO nachweisen.

- Sofern personenbezogene Daten verarbeitet werden, um Direktwerbung zu betreiben, hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.
- Es ist sicherzustellen, dass im Falle eines entsprechenden Widerspruches die personenbezogenen Daten dieser Person nicht mehr der Verarbeitung für Zwecke der Direktwerbung zur Verfügung stehen.
- Es ist sicherzustellen, dass die betroffene Person spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf die ihr zustehenden Widerspruchsrechte hingewiesen wird.

13. Automatisierte Entscheidungen im Einzelfall einschließlich Profiling:

Es ist gem. Art. 22 DSGVO sicherzustellen, dass eine betroffene Person das Recht besitzt, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – ruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Diese Voraussetzung gilt nicht, wenn die entsprechende Entscheidung:

a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,

b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder

c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

Liegt einer der vorgenannten Fälle vor, ist sicherzustellen, dass der Verantwortliche angemessene Maßnahmen trifft, um die Rechte und Freiheiten sowie die berechtigten Interessen der Betroffenen zu wahren. Ferner dürfen entsprechende Entscheidungen nicht auf besonderen Kategorien personenbezogener Daten beruhen, sofern nicht die Voraussetzungen von Art. 9 Abs. 2 DSGVO a oder g erfüllt sind.

14. Auftragsverarbeitung:

Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so ist sicherzustellen, dass dieser nur mit Auftragsverarbeitern arbeitet, die hinreichend Garantien dafür bieten, das geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

- Es ist sicherzustellen, dass der Auftragsverarbeiter keinen weiteren Auftragsverarbeiter ohne vorherigen gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch nehmen kann.

- Die Verarbeitung durch einen Auftragsverarbeiter darf nur auf der Grundlage eines Vertrages erfolgen oder eines anderen Rechtsinstruments nach Maßgabe von Art. 28 Abs. 3 DSGVO der den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind.

  Ein entsprechender Vertrag hat insbesondere vorzusehen, dass der Auftragsverarbeiter:

  a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener

Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

c) alle gemäß Artikel 32 DSGVO erforderlichen Maßnahmen ergreift;

d) die in den Absätzen 2 und 4 von Art. 28 DSGVO genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

e) angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten unterstützt;

g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht,

h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt

und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

- Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten in Namen des Verantwortlichen auszuführen, so werden diesen weiteren Auftragsverarbeiter im Wege eines Vertrages dieselben Datenschutzpflichten auferlegt, die in dem Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind, wobei zusätzlich hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt.

15. Verzeichnis von Verarbeitungstätigkeiten:

Es ist sicherzustellen, dass die Antragstellerin ein Verzeichnis aller Verarbeitungstätigkeiten führt, dass ihrer Zuständigkeit unterliegt. Dieses Verzeichnis hat insbesondere folgende Angaben zu enthalten:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

b) die Zwecke der Verarbeitung;

c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe

des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO.

- Es ist weiter sicherzustellen, dass jeder Auftragsverarbeiter ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung führt, welches folgendes enthält:

  a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;

  b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;

  c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

  d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO.

Jedes Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann. Die vorgenannten Verpflichtungen gelten nur für Unternehmen oder Einrichtungen, die mehr als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Person birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien einschließt.

16. Sicherheit der Verarbeitung:

Die Antragstellerin hat unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zweck der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Diese Maßnahmen haben insbesondere folgendes einzuschließen:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

- Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die

Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

17. Datenschutz-Folgenabschätzung:

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche gem. Art. 35 DSGVO vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

- Eine Datenschutz-Folgenabschätzung ist insbesondere in folgenden Fällen erforderlich:

  a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

  b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 DSGVO oder

  c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche;

- Diese Folgenabschätzung erhält zumindest folgende Angaben:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigtenInteressen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragenwird.

18. Datenschutzbeauftragter:

Der Antragsteller hat einen Datenschutzbeauftragten zu benennen, wenn:

a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,

b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder

c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen

und Straftaten gemäß Artikel 10 DSGVO besteht.

- Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 DSGVO genannten Aufgaben
- Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

19. Übermittlung personenbezogener Daten an Drittländer oder andere internationale Organisationen:

Es ist sicherzustellen, dass jede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, nur dann zulässig ist, wenn der Verantwortliche und der Auftragsverarbeiter die in Art. 44 DSGVO niedergelegten Voraussetzungen einhalten.

- Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlungen bedarf keiner besonderen Genehmigung.

- Falls kein Beschluss nach Artikel 45 Absatz 3 DSGVO von der Kommission vorliegt, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

Die vorgenannten geeigneten Garantien können bestehen in:

a) einem rechtlich bindenden und durchsetzbaren Dokument zwischen den Behörden oder öffentlichen Stellen,

b) verbindlichen internen Datenschutzvorschriften gemäß Artikel 47 DSGVO,

c) Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 DSGVO erlassen werden,

d) von einer Aufsichtsbehörde angenommenen Standarddaten-schutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 DSGVO genehmigt wurden,

e) genehmigten Verhaltensregeln gemäß Artikel 40 DSGVO zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen, oder

f) einem genehmigten Zertifizierungsmechanismus gemäß Artikel 42 DSGVO zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen.

- Vorbehaltlich der Genehmigung durch die zuständige Aufsichtsbehörde können solche geeigneten Garantien auch insbesondere bestehen in:

  a) Vertragsklauseln, die zwischen dem Verantwortlichen oder dem Auftragsverarbeiter und dem Verantwortlichen, dem Auftragsverarbeiter oder dem Empfänger der personenbezogenen Daten im Drittland oder der internationalen Organisation vereinbart wurden, oder

b) Bestimmungen, die in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen aufzunehmen sind und durchsetzbare und wirksame Rechte für die betroffenen Personen einschließen.

- Eine Übermittlung kann auch auf der Basis verbindlicher interner Datenschutzvorschriften gem. Art. 47 DSGVO erfolgen.

- Die Ausnahmen gem. Art. 49 DSGVO sind zu berücksichtigen.