Zertifizierungkriterien

Basismodul

Version 2.0 vom
14.8.2024

INHALTSVERZEICHNIS

1 Vorwort

1.1 Voraussetzung für die Akkreditierung

Voraussetzung für die Akkreditierung ist neben der Erfüllung der Anforderungen des Art 43 Abs 2 DSGVO und der Zertifizierungsstellen- Akkreditierungs-Verordnung (ZeStAkk-V), BGBl II 79/2021 idgF, die Einhaltung der genehmigten Zertifizierungskriterien.

2 Einführung

2.1 Einhaltung der genehmigten Zertifizierungskriterien

Die Zertifizierung nach Art. 42 Abs. 1 DSGVO wird von der nach Art. 43 Abs. 1 und 2 DSGVO akkreditierten Zertifizierungsstelle auf der Grundlage der von der zuständigen Aufsichtsbehörde nach Art. 42 Abs. 5 DSGVO genehmigten Zertifizierungskriterien erteilt. Die Einhaltung der genehmigten Zertifizierungskriterien kann als ein Element für den Nachweis der Einhaltung der Verpflichtungen aus der DSGVO verwendet werden.

2.2 Gesamtheit

Diese Zertifizierungskriterien bilden alle Aspekte der Datenverarbeitung hinreichend genau ab und schaffen insgesamt einen relevanten Mehrwert. Eine Zertifizierung nach Art. 42 Abs. 1 DSGVO auf der Grundlage dieser Zertifizierungskriterien kann nur in ihrer Gesamtheit (d.h. in Bezug auf alle auf den Bewertungsgegenstand anwendbaren Kriterien dieses Katalogs) erfolgen, nicht aber nur in Bezug auf bestimmte darin enthaltene oder wiedergegebene Aspekte oder Kriterien.

2.3 Keine Garantie

Die vorliegenden Kriterien sind kein Mechanismus, der das Vorhandensein geeigneter Garantien gemäß Artikel 42 (2) und Artikel 46 (2) lit f DSGVO für die internationale Übermittlung personenbezogener Daten nachweist.

2.4 Verantwortliche

Die Zertifizierung nach Artikel 42 (Erwägungsgrund 100 GDPR) DSGVO auf der Grundlage der vorliegenden Kriterien soll es dem für die Verarbeitung Verantwortlichen ermöglichen, "nachzuweisen", dass die zertifizierte Verarbeitung personenbezogener Daten in strenger Übereinstimmung mit der DSGVO erfolgt.

2.5 Klare Definition des Evaluierungsgegenstandes

Der Kunde muss den Evaluierungsgegenstand klar definieren, damit alle Verarbeitungstätigkeiten in den Geltungsbereich der Zertifizierung fallen.

2.6 Verarbeitung personenbezogener Daten

Unternehmen und Organisationen in ihrer Gesamtheit sowie Verarbeitungsvorgänge, die keine Verarbeitung personenbezogener Daten beinhalten, können nicht zertifiziert werden.

2.7 Transparenz

Die Zertifizierung der Verarbeitung personenbezogener Daten im Rahmen der Datenschutz-Grundverordnung ist ein Mittel zur Verbesserung der Transparenz bei der Einhaltung der Datenschutz-Grundverordnung (Erwägungsgrund 100 der Datenschutz-Grundverordnung). Das übergeordnete Ziel der Zertifizierung besteht darin, allen Beteiligten die Gewissheit zu geben, dass ein Verarbeitungsvorgang bestimmte Anforderungen erfüllt. Der Wert der Zertifizierung liegt im Grad des Vertrauens, das durch die unparteiische und kompetente Überprüfung der Einhaltung der festgelegten Anforderungen durch Dritte vermittelt wird.

2.8 Verweise in (Klammern)

Die Verweise auf Normen dieser Zertifizierungskriterien (in Klammer angeführt) sollen den Benutzer unterstützen, sind aber nicht als Auflistung aller Normen zu verstehen, die für die Erfüllung des Kriteriums relevant sind.

2.9 Überschriften in kursiver Schrift

Alle Überschriften, die im gesamten Dokument in kursiver Schrift dargestellt sind, enthalten nicht die eigentlichen Zertifizierungskriterien, sondern stellen eine kurze Beschreibung der nachfolgenden Zertifizierungskriterien dar.

2.10 Konformität und tatsächliche Umsetzung

Wenn einzelne Kriterien dieser Zertifizierungskriterien die Bereitstellung von (dokumentierten) Informationen oder Unterlagen erfordern, müssen diese Dokumente und Informationen auf Konformität mit den anwendbaren Bestimmungen sowie auf ihre tatsächliche Umsetzung innerhalb der relevanten Verarbeitungssysteme (einschließlich der anwendbaren technischen und organisatorischen Maßnahmen) gemäß dem Evaluierungsziel überprüft werden.

2.11 Geeignete Maßnahmen

Soweit einzelne Kriterien auf die Ergreifung "geeigneter" Maßnahmen abstellen, müssen die angewandten Maßnahmen das jeweilige Schutzniveau tatsächlich durch eine quantitative oder qualitative Verbesserung der durchgeführten Schutzmaßnahmen beeinflussen. Ob eine Maßnahme oder ein Maßnahmenbündel angemessen ist, hängt von den konkreten Umständen und Bedingungen der jeweiligen Verarbeitung ab, die Gegenstand der Evaluierung ist. Darüber hinaus muss die Zertifizierungsstelle die Angemessenheit der durchgeführten Maßnahmen anhand der Bewertungsmethoden überprüfen.

2.12 Standardisierte Verfahren

Wenn bestimmte Kriterien besagen, dass der Kunde über geeignete standardisierte Verfahren verfügen muss, bedeutet dies, dass der Kunde diese Verfahren tatsächlich anwenden muss; diese Anwendung muss vom Kunden nachgewiesen und von der Zertifizierungsstelle überprüft werden. Dies gilt auch für dokumentierte Informationen (siehe 2.10) oder Maßnahmen, über die der Kunde gemäß diesen Zertifizierungskriterien verfügen muss.

3 Ziel der Bewertung

3.1 Einzelne oder Bündel von Verarbeitungsvorgängen

Die vorliegenden Zertifizierungskriterien können als ein Element verwendet werden, mit dem die Einhaltung der Verpflichtungen der für die Datenverarbeitung Verantwortlichen nach der DSGVO in Österreich nachgewiesen werden kann. Wie bereits unter 2.3 ausgeführt, dienen die vorliegenden Kriterien nicht als M e c h a n i s m u s , der das Vorhandensein angemessener Garantien nach Art. 42 (2) und Art. 46 (2) lit. f DSGVO für die internationale Übermittlung personenbezogener Daten nachweist. Gegenstand der Bewertung können einzelne Datenverarbeitungsvorgänge im Sinne von Art. 4 Nr. 2 DSGVO (z.B. ein Anmeldeverfahren) oder ein Bündel von Datenverarbeitungsvorgängen (z.B. das Einstellungsverfahren) sein, die in ihrer Gesamtheit relevant und sinnvoll sind.

3.2 Spezifikation des Auswertungsgegenstandes

Im Rahmen des Zertifizierungsantrages hat der Auftraggeber der Zertifizierungsstelle eine eindeutige und umfassende Spezifikation des Auswertungsgegenstandes vorzulegen. Eine solche Spezifikation des Auswertungsgegenstandes erfolgt durch die Benennung und eine detaillierte und vollständige Beschreibung des Auswertungsgegenstandes, einschließlich einer grafischen Beschreibung des Datenflusses, der Zwecke der Datenverarbeitung, seiner Anwendungsbereiche sowie aller Definitionen und Erläuterungen, die zum Verständnis dieser Spezifikation notwendig sind.
Darüber hinaus sind die spezifischen Datenverarbeitungstätigkeiten des Evaluationsgegenstandes und etwaige Berührungspunkte zu anderen, vom Evaluationsgegenstand getrennten Verarbeitungstätigkeiten anzugeben. Soweit dies zur Abgrenzung erforderlich ist, sind Verarbeitungsvorgänge aufzuführen, die nicht unter den Auswertungstarif fallen. Der Ausschluss dieser Vorgänge ist zu begründen.

Darüber hinaus ist ein Verzeichnis der für die Verarbeitung eingesetzten Soft- und Hardware (=Infrastruktur der Verarbeitung") und ein Verzeichnis aller an der Verarbeitung beteiligten Partner (einschließlich weiterer Datenverarbeiter ["Unterauftragsverarbeiter"] und der vollständigen Postanschriften ihres Sitzes sowie aller Standorte, an denen relevante Verarbeitungsvorgänge stattfinden) ungeachtet ihrer datenschutzrechtlichen Rolle ([Mit-]Verantwortlicher oder Auftragsverarbeiter) vorzulegen.

Schließlich sind die Gründe für die Zuweisung der Rolle des Auftraggebers als Verantwortlicher in Bezug auf die Verarbeitungsvorgänge, die Gegenstand der Evaluierung sind, sowie der Partner spezifischen Verarbeitungsvorgänge) zu dokumentieren und der Zertifizierungsstelle zur Bewertung vorzulegen.
Die Überlegungen in den Leitlinien 07/2020 des EDPB zu den Begriffen des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters in der DSGVO in ihrer neuesten Fassung sowie die Rechtsprechung des EuGH sind bei der Rollenverteilung zu berücksichtigen.

3.3 Vereinbarung des Evaluierungsgegenstandes

Mit der Annahme des Antrags auf Zertifizierung durch die Zertifizierungsstelle wurde der Evaluierungsgegenstand zwischen dem Kunden und der Zertifizierungsstelle vereinbart. Die Zertifizierungsstelle muss bewerten, ob die gesamte Verarbeitung personenbezogener Daten, die Gegenstand des Evaluierungsziels ist, den Anforderungen dieser Zertifizierungskriterien entspricht.

4 Normative Referenzen

4.1 GDPR bzw. DSGVO

GDPR: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (General Data Protection Regulation; GDPR, ABl. L 2016/119, 1 in der jeweils geltenden Fassung).

4.2 DSG

DSG: (Österreichisches) Bundesgesetz über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz; DSG, BGBl. I 165/1999 idgF).

4.3 ZeStAkk-V:

ZeStAkk-V: Verordnung der österreichischen Aufsichtsbehörde über die Anforderungen an die Akkreditierung einer Zertifizierungsstelle (BGBl. II 79/2021 idgF).

4.4 EN ISO 17065:2012

EN ISO 17065:2012 Konformitätsbewertung - Anforderungen an Stellen, die Produkte, Verfahren und Dienstleistungen zertifizieren.

4.5 Die ISO/IEC 27000

Die ISO/IEC 27000-Reihe (auch ISO/IEC 27000-Familie oder kurz ISO27k genannt) ist eine Reihe von Informationssicherheitsstandards, die von der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) veröffentlicht werden. Der Schwerpunkt liegt auf bewährten Maßnahmen, Methoden, Praktiken und Verfahren im Unternehmen zur Organisation der Informationssicherheit.

4.6 ISO/IEC 29134

ISO/IEC 29134 Informationstechnologien - Sicherheitstechniken - Leitlinien für die Bewertung der Auswirkungen auf die Privatsphäre. Diese Norm ist ein Leitfaden für Informationstechnologien - Sicherheitstechniken - Datenschutzfolgenabschätzung.

5 Bedingungen

5.1 Allgemein

Soweit für diese Zertifizierungskriterien keine normativen Begriffe gemäß 5.2 (normative Begriffe) definiert sind, sind die Legaldefinitionen des Art 4 DSGVO zu verwenden.

5.2 Standardspezifische Begriffe

Kunde:
Ein Kontrolleur, der die Zertifizierung beantragt oder für die Einhaltung des Zertifizierungsprogramms verantwortlich ist.

Auftragsverarbeiter:
Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet (Art. 4 Nr. 8 GDPR).

Automatisierte Einzelentscheidung, einschließlich Profiling:
Eine ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung, einschließlich Profiling, die für die betroffene Person rechtliche Folgen nach sich zieht oder s i e in ähnlicher Weise erheblich beeinträchtigt.
Besondere Kategorien von personenbezogenen Daten: Personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person (= Art 9 (1) GDPR).

Betroffene Person:
Jede identifizierte oder identifizierbare natürliche oder juristische Person, die sich von dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter unterscheidet und auf die sich die verarbeiteten Daten beziehen (Art. 4 Nr. 1 DSGVO).

Dienst der Informationsgesellschaft:
Jede Dienstleistung, die elektronisch, in der Regel gegen Entgelt, im Fernabsatz und auf individuellen Abruf des Empfängers erbracht wird, insbesondere der Online-Vertrieb von Waren und Dienstleistungen, Online-Informationsangebote, Online-Werbung, elektronische Suchmaschinen und Datenabfragemöglichkeiten sowie Dienste, die Informationen über ein elektronisches Netz übertragen, den Zugang zu einem solchen Netz vermitteln oder die Informationen eines Nutzers speichern.

Dokumentation:
Eine überprüfbare Aufzeichnung und/oder ein Bestand an Informationen, faktischen und/oder rechtlichen Schlussfolgerungen, Vereinbarungen, Abläufen, Prozessen und Maßnahmen zum Nachweis der Einhaltung der Verpflichtungen aus der Datenschutz-Grundverordnung und dieser Zertifizierungskriterien.

Dokumentierte Informationen:
Die spezifischen Informationen, die eine Dokumentationspflicht zum Zweck der Dokumentation erfüllen (5.2.7 Dokumentation). Dazu gehören z.B. (und damit nicht nur) physische und elektronische Textdokumente, Audio- und/oder Videoaufzeichnungen von Richtlinien und sonstigen Arbeitsanweisungen, die in der Organisation des Auftraggebers genehmigt und verwendet werden, interne und externe Vereinbarungen (z.B. Betriebsvereinbarungen, Vereinbarungen nach Art 26, 28 oder 44 ff. DSGVO), Datenschutzhinweise, Verfahrensabläufe, Muster von Einwilligungserklärungen, Datenschutz-Folgenabschätzungen, Organisationsstrukturen und Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit.

Drittland:
Ein Staat, der nicht Mitglied der Europäischen Union ist und nicht als Teil des Europäischen Wirtschaftsraums durch Assoziierung als solcher behandelt wird.

Empfänger:
Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der die personenbezogenen Daten offengelegt werden, unabhängig davon, ob es sich um einen Dritten handelt oder nicht. Öffentliche Stellen, die personenbezogene Daten im Rahmen einer besonderen Untersuchung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erhalten können, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch diese öffentlichen Stellen muss in Übereinstimmung mit den geltenden Datenschutzvorschriften entsprechend den Zwecken der Verarbeitung erfolgen (= Art. 4 Nr. 9 DSGVO).

Gemeinsame Verantwortlichkeit:
Zwei oder mehr für die Verarbeitung Verantwortliche, die gemeinsam die Zwecke und Mittel der Verarbeitung festlegen (=Art 26 (1) Satz 1 DSGVO).

Instrument der internationalen Übermittlung personenbezogener Daten:
Ein Angemessenheitsbeschluss nach Art. 45 DSGVO, eine geeignete Schutzmaßnahme nach Art. 46 DSGVO oder eine Ausnahmeregelung für besondere Situationen im Sinne von Art. 49 DSGVO.

Internationale Organisation:
Eine völkerrechtliche Organisation und ihre Unterorgane oder jede andere Einrichtung, die durch ein Abkommen zwischen zwei oder mehreren Ländern oder auf der Grundlage eines solchen Abkommens gegründet wurde.

Kategorie der personenbezogenen Daten:
Die Beschreibung der personenbezogenen Daten nach typo- logischen Gesichtspunkten (z.B. Name, Kontaktdaten, Bankdaten).

Personenbezogene Daten:
Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind (= Art. 4 Nr. 1 DS-GVO).

Profiling:
Jede Form der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Standort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

Technische und organisatorische Maßnahmen:
Maßnahmen, die der Kunde oder der Prozess ergreift, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, wie in Art. 32 (1), Art. 5 (1) lit. f, 24-25 und 28 GDPR definiert.

Standhaftigkeit:
Eine allgemeine, ungeschriebene Rechtsmaxime, nach der jeder, der am Rechtsleben teilnimmt, zu seinem Wort und seinem Verhalten stehen muss und nicht ohne triftigen Grund dem widersprechen darf, was er zuvor vertreten hat und worauf sich andere verlassen haben.

Ziel der Bewertung:
Der personenbezogene Datenverarbeitungsvorgang oder eine Reihe von personenbezogenen Datenverarbeitungsvorgängen, deren Übereinstimmung mit dem Zertifizierungsprogramm und diesen Zertifizierungskriterien in einem Zertifizierungsverfahren überprüft wird/werden.

Datenschutz-Folgenabschätzung:
Ein Prozess, der sicherstellen soll, dass der für die Datenverarbeitung Verantwortliche die Risiken für den Schutz der Privatsphäre, die sich aus dem Evaluierungsgegenstand ergeben, ordnungsgemäß identifiziert und handhabt, indem er geeignete technische und organisatorische Maßnahmen festlegt, um ein Sicherheitsniveau zu gewährleisten, das den identifizierten Risiken in Bezug auf

Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und -dienste, die Gegenstand des Evaluierungsgegenstands sind, angemessen ist.

6 Rechenschaftspflicht

Unter Rechenschaftspflicht versteht man ein Bündel von Rechtfertigungs- und Dokumentationspflichten, die in erster Linie den für die Verarbeitung Verantwortlichen betreffen. In jedem Fall muss der für die Verarbeitung Verantwortliche als Rechenschaftspflichtiger die Einhaltung aller Kriterien dieses Katalogs sicherstellen und dokumentieren, d.h. mit den Grundsätzen für die Verarbeitung von personenbezogenen Daten. Darüber hinaus muss auch eine Risikobewertung durchgeführt und dokumentiert werden, um die Anforderungen der Artikel 24 und 25 der Datenschutz-Grundverordnung zu erfüllen.
Zur Rechenschaftspflicht gehören auch der rechtskonforme Einsatz von Auftragsverarbeitern und Unterauftragsverarbeitern, die Führung von Aufzeichnungen über Verarbeitungstätigkeiten und der spezifizierte Umgang mit Verletzungen des Schutzes personenbezogener Daten.
Kommt die Risikoanalyse zu dem Ergebnis, dass eine Verarbeitung mit hohen Risiken verbunden ist, muss eine Datenschutz- Folgenabschätzung gemäß Artikel 35 DSGVO durchgeführt werden. Im Ergebnis werden aber auch die Bestimmungen zur Einhaltung d e r anderen Datenverarbeitungsgrundsätze in die Rechenschaftspflicht aufgenommen, so dass die verantwortlichen Stellen erklären können, dass sie die Einhaltung und Umsetzung der DSGVO flächendeckend sicherstellen und dokumentieren müssen.

6.1 Nachweis der Einhaltung (Rechenschaftspflicht) in Bezug auf alle Kriterien

Der Kunde verfügt über dokumentierte Informationen, die belegen, dass diese Zertifizierungskriterien in Bezug auf den Evaluierungsgegenstand erfüllt werden. (Art. 5 Abs. 2 GDPR.).
Dazu gehört, dass der Kunde in Bezug auf den Evaluierungsgegenstand alle in den Zertifizierungskriterien vorgesehenen Richtlinien und Prozesse anwendet, dass er innerhalb seiner Organisation klare Zuständigkeiten in Bezug auf alle damit zusammenhängenden Datenschutzangelegenheiten geschaffen hat, dass er entsprechende Meldeverfahren unter Einbeziehung der Führungsebene implementiert hat und dass er sicherstellt, dass der Datenschutzbeauftragte g e m ä ß Artikel 37 DSGVO in alle damit zusammenhängenden Datenschutzangelegenheiten einbezogen wird.

6.2 Datenschutz-Folgenabschätzung

Durch die Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO hat der Verantwortliche vor Beginn der Verarbeitungstätigkeit zu prüfen, welche Risiken für die Rechte und Freiheiten natürlicher Personen entstehen können und welche technischen und organisatorischen Maßnahmen zur Bewältigung dieser Risiken getroffen werden sollten.
Eine Datenschutz-Folgenabschätzung ist in jedem Fall obligatorisch, wenn unter anderem eine Verarbeitung unter Einsatz 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 hat. Eine ausführliche Beschreibung der in diesem Zusammenhang relevanten Fälle findet sich in Kapitel 7.1.3.

6.2.1 Schwellenwertanalyse

Der Auftraggeber verfügt über dokumentierte Informationen, ob die Durchführung einer Datenschutz-Folgenabschätzung für jede vom Evaluierungsgegenstand erfasste Datenverarbeitung erforderlich ist (Schwellenwertanalyse), weil voraussichtlich ein hohes Risiko besteht auf die Rechte und Freiheiten natürlicher Personen. Im Rahmen dieser Schwellenwertanalyse muss der Kunde zumindest auf die folgenden Aspekte eingehen:

a) Art, Umfang, Kontext und Zweck der Datenverarbeitung;
b) Bewertung der Folgen für den Schutz der spezifischen personenbezogenen Daten;
c) Beschreibung und Bewertung der wahrscheinlichen Risiken;
d) Die unter 6.2.3 (Fälle, in denen eine Datenschutz-Folgenabschätzung nach Art. 35 Abs. 4 DSGVO in jedem Fall durchgeführt werden muss) aufgeführten Rechts- und Verwaltungsvorschriften sowie die im angesprochenen Leitfaden der Art. 29 Datenschutzgruppe ("Guidelines on Data Protection Impact Assessment (DPIA) und die Feststellung, ob die Verarbeitung „wahrscheinlich zu einem hohen Risiko" im Sinne der Verordnung 2016/679 führt) auf Seite 9 - 11. Bewertung und Begründung, ob die Meinung der betroffenen Personen oder ihrer Vertreter eingeholt werden soll.

6.2.2 Keine Datenschutz-Folgenabschätzung

Kommt der Auftraggeber in der Schwellenwertanalyse zu dem Schluss, dass keine Datenschutz-Folgenabschätzung durchgeführt werden muss, so muss er über eine Dokumentation der entsprechenden Gründe verfügen. In diesem Fall muss der Kunde über Verfahren verfügen, die sicherstellen, dass eine dokumentierte Datenschutz-Folgenabschätzung durchgeführt und zur Verfügung gehalten wird, die die Datenschutzbedürfnisse der personenbezogenen Daten im konkreten Kontext der Verarbeitungstätigkeit bestimmt und den Kunden in die Lage versetzt, geeignete technische und organisatorische Maßnahmen gemäß Punkt 8 (Technische und organisatorische Maßnahmen) anzuwenden.
Sie umfasst auch eine Identifizierung, Analyse und Kategorisierung der potenziellen Auswirkungen (Schwere) und der Wahrscheinlichkeit jedes identifizierten Risikos für die Rechte der betroffenen Personen auf der Grundlage einer festgelegten, validierten und dokumentierten Methodik, um kohärente und aussagekräftige Ergebnisse zu gewährleisten. (Einen maßgeblichen Überblick über die anerkannten Risikomanagementstandards für IKT

finden Sie unter https://www.enisa.europa.eu/publications/risk-management-standards. (FN3: Für die dokumentierte Risikoanalyse siehe auch das https://www.enisa.europa.eu/risk-level-tool der ENISA.)

Die angewandten technischen und organisatorischen Maßnahmen müssen in der Lage sein, die Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit personenbezogener Daten zu gewährleisten (z. B. zufällige oder unrechtmäßige Zerstörung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugter Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten), wobei der Stand der Technik, die Implementierungskosten sowie die Art, der Umfang, der Kontext und die Zwecke der Verarbeitung zu berücksichtigen sind.

6.2.3 Zwingende Datenschutz-Folgenabschätzung

Der Kunde führt eine Datenschutz-Folgenabschätzung durch, wenn die Verarbeitungstätigkeit nicht in der Verordnung der Datenschutzbehörde über Ausnahmen von der Datenschutz-Folgenabschätzung aufgeführt ist und die Schwellenwertanalyse wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt; dies ist zumindest in den folgenden Fällen der Fall:

a) Es muss eine systematische und umfassende Bewertung der personenbezogenen Daten natürlicher Personen auf der Grundlage einer automatisierten Verarbeitung, einschließlich Profiling, erfolgen, die wiederum als Grundlage für Entscheidungen dient, die Rechtswirkungen gegenüber natürlichen Personen entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen; Art 35 Abs 3 lit a GDPR.
b) Es werden besondere Kategorien personenbezogener Daten gemäß Artikel 9 (1) DSGVO erhoben oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 DSGVO verarbeitet (Art 35 Abs 3 lit a GDPR.)
c) Öffentlich zugängliche Bereiche werden systematisch und in großem Umfang überwacht (Art 35 Abs 3 lit a GDPR.)
d) Die Verarbeitung ist in der Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchgeführt werden muss (DSFA-V BGBl II 2018/278), aufgelistet;
e) Mindestens zwei der in Nr. 248, Seite 9 - 11, der Leitlinien der Art. 29 Datenschutzgruppe ("Guidelines on Data Protection Impact Assessment (DPIA) and answering the question whether a processing operation is likely to result in a high risk in the meaning of Regulation 2016/679") genannten Kriterien sind erfüllt.

6.2.4 Einholung eines Rats des Datenschutzbeauftragten

Bei der Durchführung einer Datenschutz-Folgenabschätzung holt der Kunde den dokumentierten Rat (5.2.7 Dokumentation) des Datenschutzbeauftragten ein, sofern ein solcher vorhanden ist (Art. 35 Abs. 2 GDPR.).
Darüber hinaus sind unbeschadet des Schutzes wirtschaftlicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitung gegebenenfalls die dokumentierten Stellungnahmen (5.2.7 Dokumentation) der betroffenen Personen sowie ihrer Vertreter zu der beabsichtigten

Verarbeitung einzuholen. (Art. 35 Abs. 9 GDPR.) Der Auftraggeber führt eine Datenschutz-Folgenabschätzung gemäß den 6.2.3 mit mindestens folgendem Inhalt:

a) Systematische Beschreibung der beabsichtigten Verarbeitungsvorgänge, der Zwecke der Datenverarbeitung und eine Beschreibung des berechtigten Interesses gemäß Art 35 (7) lit a DSGVO;
b) Bewertung der Notwendigkeit und Verhältnismäßigkeit der Datenverarbeitung;
c) Bewertung der Risiken für die Rechte und Freiheiten der betroffenen
d) Personen;
e) geplante Abhilfemaßnahmen zur Bewältigung der Risiken, einschließlich Schutzmaßnahmen, Sicherheitsvorkehrungen und Verfahren.

6.2.5 Hohes Risiko

Ergibt sich aus den dokumentierten Informationen nach 6.2.4 ein hohes Risiko nach 6.2.1 lit. c) und kann der Auftraggeber keine Maßnahmen nach 6.2.4 lit. d) ergreifen, muss der Auftraggeber über dokumentierte Informationen verfügen, dass die Aufsichtsbehörde gemäß Art. 36 DSGVO konsultiert wurde sowie dass das Ergebnis dieser Konsultation berücksichtigt und umgesetzt wurde, es sei denn, die Aufsichtsbehörde hat ein Verbot der Verarbeitung wegen Nichtkonformität der Verarbeitung mit der DSGVO ausgesprochen.

6.2.6 Kontinuierliche Bewertung

6.2.6.1 Schwellenwertanalyse

Der Kunde muss über Verfahren für die Überprüfung der Schwellenwertanalyse, der Analyse der Auswirkungen auf den Schutz der Privatsphäre und der Datenschutz-Folgenabschätzung verfügen, die einer anerkannten Methodik folgen (Für einen maßgeblichen Überblick über beispielhafte anerkannte Risikomanagementstandards für IKT siehe https://www.enisa.europa.eu/publications/risk-management-standards. Für die dokumentierte Risikoanalyse siehe auch (als Beispiel) das "Online-Tool für die Sicherheit der Verarbeitung personenbezogener Daten" der ENISA.) und die außerdem sicherstellen, dass nicht nur die ursprüngliche, ursprünglich erstellte Dokumentation der jeweiligen Analyse/Überprüfung verfügbar ist, sondern auch diejenige ihrer Überprüfung und gegebenenfalls Überarbeitung, insbesondere wenn die Überprüfung die Notwendigkeit einer Überarbeitung ergeben hat.
Für alle Versionen enthält die Dokumentation ein Datum, die Genehmigung durch die verantwortliche Person sowie deren Unterschrift und wird für einen Zeitraum von mindestens drei Jahren aufbewahrt. (FN10: Art 35 Abs 11 und Art 32 Abs 1 lit d DSGVO.)

6.2.6.2 Überprüfung der jeweiligen Analyse oder Bewertung

Eine Überprüfung der jeweiligen Analyse oder Bewertung ist gemäß diesem Verfahren in jedem Fall nach einer Verletzung des Schutzes personenbezogener Daten, die den Evaluationsgegenstand betrifft, durchzuführen, wenn neue Bedrohungen auftreten oder sich die mit den zertifizierten Datenverarbeitungsvorgängen verbundenen Risiken oder die Verarbeitungsparameter

oder die verwendeten Technologien ändern. Das Ergebnis der Überprüfung ist zu dokumentieren und muss in jedem Fall enthalten, ob eine Neubewertung/Überarbeitung der jeweiligen Analyse oder Bewertung einschließlich der entsprechenden Gründe erforderlich ist.

6.3 Gemeinsame Kontrolleure

Legen zwei oder mehr für die Verarbeitung Verantwortliche gemeinsam die Zwecke und Mittel der Verarbeitung fest, so sind sie gemeinsam für die Verarbeitung Verantwortliche.
Sie legen ihre jeweiligen Verantwortlichkeiten für die Einhaltung der Verpflichtungen nach dieser Verordnung, insbesondere hinsichtlich der Ausübung der Rechte der betroffenen Person und ihrer jeweiligen Informationspflichten nach den Artikeln 13 und 14, in transparenter Weise durch eine Vereinbarung zwischen ihnen fest, sofern und soweit die jeweiligen Verantwortlichkeiten der für die Verarbeitung Verantwortlichen nicht durch das Unionsrecht oder das Recht der Mitgliedstaaten, dem die für die Verarbeitung Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Kontaktstelle für betroffene Personen benannt werden.

6.3.1 Gemeinsame Verarbeitung

Sofern der Kunde gemeinsam für die Verarbeitung Verantwortliche identifiziert hat die an den Verarbeitungen beteiligt sind, die Gegenstand des Evaluierungsziels sind, muss die Vereinbarung mit jedem gemeinsam für die Verarbeitung Verantwortlichen die folgenden Anforderungen erfüllen, um sicherzustellen, dass die gesamte(n) gemeinsame(n) Verarbeitung(en) die Zertifizierungskriterien vollständig erfüllt (erfüllen); jede Bestimmung in einer solchen Vereinbarung muss die faktischen Umstände der relevanten Verarbeitungen widerspiegeln und mit ihnen übereinstimmen: (Art. 26 Abs. 1 GDPR.).

6.3.1.1 Rechtsverbindlichkeit

Abschluss in schriftlicher und rechtsverbindlicher Form für die Vertragsparteien; Zuweisung der Verantwortlichkeiten für die Einhaltung der Rechte der betroffenen Personen gemäß Art. 12 bis 22, Art. 34 DSGVO, einschließlich (insbesondere, aber nicht ausschließlich) des Rechts, über die Verarbeitung personenbezogener Daten gemäß den folgenden Bestimmungen informiert zu werden Art 13f. GDPR;

6.3.1.2 Zuweisung der Verantwortlichkeiten

Zuweisung der Verantwortlichkeiten für die Einhaltung der Rechte der betroffenen Personen gemäß Art. 12 bis 22, Art. 34 DSGVO, einschließlich (insbesondere, aber nicht ausschließlich) des Rechts, über die Verarbeitung personenbezogener Daten gemäß den folgenden Bestimmungen informiert zu werden.

6.3.1.3 Umsetzung der Datenschutzgrundsätze

Umsetzung der allgemeinen Datenschutzgrundsätze (Artikel 5 GDPR);

6.3.1.4 Bestimmung der Rechtsgrundlagen für die Datenverarbeitung(en) (Artikel 6 DSGVO) sowie der geltenden Ausnahmen vom Verbot der Verarbeitung sensibler Daten (Artikel 9 DSGVO);

6.3.1.5 Zuweisung der Zuständigkeiten für die Durchführung einer Schwellenwertanalyse sowie einer Datenschutz-Folgenabschätzung oder - falls erforderlich - einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) einschließlich der Umsetzung geeigneter Sicherheitsmaßnahmen (Art. 32 DSGVO);

6.3.1.6 Zuweisung der Verantwortung für die Benachrichtigung der zuständigen Aufsichtsbehörde(n) im Falle einer Datenschutzverletzung (Artikel 33 DSGVO);

6.3.1.7 Sicherstellung des Einsatzes von ausschließlich geeigneten Datenverarbeitern und Abschluss eines Datenverarbeitungsvertrags (Art. 28 DSGVO);

6.3.1.8 Sicherstellung, dass personenbezogene Daten unter Einhaltung von Kapitel V der DSGVO in Drittländer übermittelt werden;

6.3.1.9 Festlegung von Kontaktstellen bei jedem gemeinsam für die Verarbeitung Verantwortlichen für die betroffenen Personen sowie für die zuständigen Aufsichtsbehörden;

6.3.1.10 Übermittlung des wesentlichen Inhalts der Vereinbarung an die betroffenen Personen durch die gemeinsam für die Verarbeitung Verantwortlichen (Art. 26 Abs. 2 GDPR).

6.3.2. Der Kunde stellt sicher, dass die Rechte der betroffenen Personen gemäß der DSGVO beachtet und eingehalten werden, unabhängig von den Bedingungen der in 6.3.1 genannten Vereinbarung, wenn sie beim und gegenüber dem Kunden ausgeübt werden.

6.3.3. Der Kunde stellt der Zertifizierungsstelle auf Anfrage alle Informationen und Unterlagen zur Verfügung, die für die Bewertung des durchgeführten Verarbeitungsvorgangs erforderlich sind unter gemeinsamer Beherrschung auf die Einhaltung dieser Kriterien.

6.4 Einbindung der Verarbeiter

Soll die Verarbeitung im Auftrag eines für die Verarbeitung Verantwortlichen erfolgen, so setzt dieser nur Auftragsverarbeiter ein, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung den Anforderungen der DSGVO entspricht und der Schutz der Rechte der betroffenen Person gewährleistet ist. Es steht jedem für die Verarbeitung Verantwortlichen frei, einen oder mehrere geeignete

Auftragsverarbeiter einzusetzen. Ein geeigneter Auftragsverarbeiter ist ein solcher, der hinreichende Garantien dafür bietet, dass die Datenverarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und dass der Schutz der Rechte der betroffenen Personen durch geeignete technische und organisatorische Maßnahmen gewährleistet ist.

6.4.1 Wenn der Kunde einen oder mehrere Auftragsverarbeiter in Bezug auf das Ziel der Auswertung einsetzt, müssen dokumentierte Informationen über die folgenden Aspekte enthalten sein, um dem Grundsatz der Rechenschaftspflicht (Art. 5 (2) DSGVO) zu entsprechen:

a) Verfahren, die sicherstellen, dass nur Auftragsverarbeiter eingesetzt werden, die hinreichende Garantien, insbesondere in Bezug auf Fachwissen, Zuverlässigkeit und Ressourcen, dafür bieten, dass geeignete technische und organisatorische Maßnahmen (wie nachstehend unter 8. beschrieben) so umgesetzt werden, dass die Verarbeitung diesen Zertifizierungskriterien entspricht (Art 28 Abs. 1 GDPR.); diese Verfahren verlangen, dass der Auftragsverarbeiter das Vorhandensein geeigneter Garantien je nach Art, Umfang, Umständen und Zwecken der Verarbeitung durch spezifische Nachweise nachweist, bei denen es sich z. B. um Dritt- oder Selbstaudits und entsprechende Zertifizierungen handeln kann. Darüber hinaus können auch Datenschutzinformationen, Nutzungsbedingungen, Aufzeichnungen über Verarbeitungstätigkeiten von Auftragsverarbeitern, Aufzeichnungen über externe Datenschutzaudits, ein Informationssicherheitskonzept, dokumentierte Nachweise über die Einhaltung anerkannter internationaler Normen wie der ISO 27000-Reihe (z. B. ISO/IEC 27017 und 27018 zum Cloud Computing sowie ISO/IEC 27701 zum Datenschutzmanagement) für den für die Verarbeitung Verantwortlichen aussagekräftige Informationen über die Compliance des Auftragsverarbeiters liefern.

b) Verfahren, die sicherstellen, dass schriftliche (Art. 28 Abs. 9 GDPR) Vereinbarungen, einschließlich einer elektronischen Form zwischen dem Auftraggeber und dem Auftragsverarbeiter geschlossen werden, wie z. B. das Vorliegen entsprechender Musterverträge, die als verbindlich für den Abschluss entsprechender Vereinbarungen innerhalb der Organisation des Auftraggebers zu verwenden sind, oder entsprechende Prüfkataloge, die es ermöglichen, die Konformität der Vereinbarung mit den Anforderungen der DSGVO zu prüfen. Diese Vereinbarung muss die vom Auftragsverarbeiter anzuwendenden TOMs enthalten. Neben einer Vereinbarung kann auch ein anderer Rechtsakt im Sinne v o n Art. 28 Abs. 3 DSGVO verwendet werden, für den die gleichen formalen Anforderungen gelten wie für Vereinbarungen.

6.4.2. Die Vereinbarung oder der andere Rechtsakt im Sinne von Art. 28 Abs. 3 DSGVO gemäß 6.4.1 lit. b) muss mindestens die folgenden Aspekte gemäß Art. 28 umfassen (3) GDPR:

a) Gegenstand der Datenverarbeitung;
b) Dauer der Datenverarbeitung;
c) Art und Zweck der Datenverarbeitung;
d) Art der personenbezogenen Daten, die Gegenstand der Datenverarbeitung sind;
e) Kategorien von betroffenen Personen;
f) Verordnung über den Einsatz von Weiterverarbeitern in der Verarbeitungskette;
g) Verpflichtung zur Weitergabe des Inhalts dieser Vereinbarung an weitere Auftragsverarbeiter in der Kette;
h) Pflichten und Rechte des Auftraggebers gegenüber dem Auftragsverarbeiter und hier insbesondere die Verpflichtung,

I. die personenbezogenen Daten nur auf dokumentierte Anweisung des Kunden im Sinne von Art. 28(3) lit. a DSGVO zu verarbeiten, die sich aus dem Vertrag oder einem anderen Rechtsakt ergeben kann,
II. Personen, die an der Verarbeitung beteiligt sind, zur Vertraulichkeit zu verpflichten, solange sie nicht einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen (Art 28 (3) lit b DSGVO,
III. alle erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um ein dem Risiko der Auftragsdatenverarbeitung angemessenes Schutzniveau zu gewährleisten (Art 28 (3) lit c DSGVO),
IV. den Kunden bei der Bearbeitung von Anfragen gemäß 7.5 (Einschränkung der Verarbeitung personenbezogener Daten), 7.6 (Widerspruch aufgrund einer besonderen Situation), 7.4.5 (Zugang zu personenbezogenen Daten), 7.8 (Datenportabilität), 7.9.2 (Berichtigungsverfahren), 7.11 (Recht auf Löschung personenbezogener Daten) und von Meldungen gemäß 6.6 (Verletzung des Schutzes personenbezogener Daten) zu unterstützen und beim Nachweis der Einhaltung der Vorschriften mitzuwirken;
V. die Durchführung einer Datenschutz-Folgenabschätzung gemäß Artikel 35 DSGVO zu ermöglichen; Artikel 35 DSGVO zu ermöglichen;
VI. den Auftraggeber unverzüglich zu informieren, wenn Weisungen gemäß i) gegen die Datenschutz-Grundverordnung oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen;
VII. die nach Beendigung der Auftragsverarbeitung zugänglich gemachten personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben (Art 28 (3) lit g DSGVO);

VIII. dem Auftraggeber eine Verletzung des Schutzes personenbezogener Daten in der Sphäre des Auftragsverarbeiters zu melden (Art. 33 Abs. 2 GDPR)

IX. dem Kunden alle Informationen zur Verfügung stellen, die erforderlich sind, um die Einhaltung der in Artikel 28 DSGVO festgelegten Verpflichtungen nachzuweisen, und Prüfungen, einschließlich Inspektionen, durch den Kunden oder einen anderen von ihm beauftragten Prüfer ermöglichen und dazu beitragen.(Art 28 Abs 3 lit h GDPR)

6.4.3. Setzt der Auftragsverarbeiter im Rahmen einer oder mehrerer "Verarbeitungsketten" andere Auftragsverarbeiter im Sinne von Art. 28 Abs. 2 und 4 DSGVO ("Unterauftragsverarbeiter") ein, stellt der Auftraggeber sicher, dass die mit dem Auftraggeber vereinbarten Pflichten gemäß 6.4.1 (Einsatz eines Auftragsverarbeiters) übertragen werden. Darüber hinaus sorgt er für eine vorherige spezifische oder allgemeine schriftliche Genehmigung der Unterauftragsverarbeiter durch den Auftraggeber sowie als seine Kenntnis und Übersicht über die entsprechend zugelassenen Unterauftragsverarbeiter.

6.4.4. Wenn das Unionsrecht oder das nationale Datenschutzrecht einen Vertrag oder Rechtsakt vorschreibt, muss dieser schriftlich vorliegen, damit er von der Zertifizierungsstelle überprüft werden kann. Jede Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter wird durch einen Vertrag oder einen anderen Rechtsakt nach Unionsrecht oder nationalem (österreichischem) Recht zwischen dem Verantwortlichen und dem Auftragsverarbeiter geregelt.(Art. 28 Abs. 3 GDPR)

6.4.5. Wenn der Kunde Auftragsverarbeiter mit Sitz in einem Drittland einsetzt, stellt er sicher, dass die Anforderungen von Kapitel V der DSGVO gemäß den Bestimmungen von Kapitel 9 (Übermittlung personenbezogener Daten in ein Drittland) eingehalten werden.

6.5 Aufzeichnungen über Verarbeitungstätigkeiten

Um die Einhaltung der DSGVO nachzuweisen, sollte der für die Verarbeitung Verantwortliche Aufzeichnungen über die Verarbeitungstätigkeiten unter seiner Verantwortung führen. Der Zweck der Aufzeichnungen von Verarbeitungstätigkeiten gemäß Artikel 30 DSGVO ist es, einen Überblick über die Verarbeitungstätigkeiten zu geben.

6.5.1. Der Kunde verfügt über dokumentierte Informationen (Art. 30 Abs. 3 GDPR.), die folgenden Informationen enthalten (Art. 30 Abs. 1 GDPR):

a) Die identifizierte Rolle, einschließlich des Namens und der Kontaktdaten, falls zutreffend, des Vertreters und eines gemeinsam für die Verarbeitung Verantwortlichen sowie eines möglichen Datenschutzbeauftragten; (Art 30 Abs 1 lit a GDPR)

b) Für die Verarbeitung festgelegte Zwecke; (Art 30 Abs 1 lit b GDPR)

c) Beschreibung des betroffenen Personenkreises; (Art 30 Abs 1 lit c GDPR)

d) Identifizierte Kategorien von personenbezogenen Daten; (Art 30 Abs 1 lit c GDPR)

e) Beschreibung der Kategorien von Empfängern; (Art 30 Abs 1 lit d GDPR.)

f) Fristen für die Löschung der personenbezogenen Daten; (Art 30 Abs 1 lit f GDPR.)

g) Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, die gemäß diesen Zertifizierungskriterien festgelegt wurden; (Art 30 Abs 1 lit g GDPR.)

h) Information über das Vorliegen einer Übermittlung personenbezogener Daten gemäß 9.2 lit a) (Übermittlung personenbezogener Daten in ein Drittland).

6.5.2. Gegebenenfalls müssen die dokumentierten Informationen gemäß Abschnitt 6.5 (Aufzeichnung von Verarbeitungstätigkeiten) zusätzlich das betreffende Drittland und die Kategorien von Empfängern in diesem Drittland sowie eine Bezeichnung der internationalen Organisation enthalten. (Art 30 Abs 1 lit d, 30 Abs 1 lit e DSGVO.)

6.5.3. Hat der Kunde ein zwingendes berechtigtes Interesse für die Übermittlung in ein Drittland nachgewiesen, so müssen die dokumentierten Informationen im Zusammenhang mit der Verarbeitung die erforderlichen angemessenen Garantien enthalten. (Art 30 Abs 1 lit e, 49 Abs 6 GDPR.)

6.5.4. Zur Umsetzung der Verpflichtung, die Aufzeichnungen über die Verarbeitungstätigkeiten gemäß Art. 30 DSGVO auf Verlangen der Aufsichtsbehörde vorzulegen, benennt der Kunde eine dafür verantwortliche Person. ()Art. 30 Abs. 4 GDPR)

6.6 Verletzung des Schutzes personenbezogener Daten

Gemäß Artikel 4 (12) DSGVO bedeutet "Verletzung des Schutzes personenbezogener Daten" eine Verletzung der Sicherheit, die zur zufälligen oder unrechtmäßigen Zerstörung, zum Verlust, zur Veränderung oder zur unbefugten Weitergabe von oder zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

6.6.1 Der Kunde stellt sicher und dokumentiert, dass eine Verletzung des Schutzes personenbezogener Daten in seinem Unternehmen zur Kenntnis genommen und - entsprechend dem Ergebnis einer Risikoanalyse - der zuständigen Aufsichtsbehörde und ggf. auch den betroffenen Personen mitgeteilt und in jedem Fall gemäß Artikel 33 (5) der Datenschutz-Grundverordnung. Diese Methoden müssen mindestens die folgenden Aspekte abdecken:

Festgelegte Berichts- und Entscheidungsstrukturen;
Benachrichtigung ohne unangemessene Verzögerung gemäß Artikel 33 DSGVO und, sofern möglich, spätestens 72 Tage nach Bekanntwerden der Verletzung des Schutzes personenbezogener Daten, unter Berücksichtigung des Konzepts der "schrittweisen" Benachrichtigung gemäß Artikel 33 Absatz 4 DSGVO (wenn noch nicht alle Umstände des Datenschutzvorfalls bekannt sind); (Art. 33 Abs. 4 GDPR.)
Kann die 72-Stunden-Frist nach Art. 33 Abs. 1 DSGVO nicht eingehalten werden, ist dies ausführlich zu begründen;
Anerkannte Methode, um zu beurteilen, ob ein Risiko oder e i n hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht; (Zum Beispiel könnte das Konzept nach ISO/IEC 29134 (Information technologies - Security techniques - Guidelines for privacy impact assessment) oder die "Recommendations for a methodology of the assessment of severity of personal data breaches" der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) verwendet werden.)
)Dokumentations- und Archivstrukturen (z.B. gemäß Art 33 (5) GDPR); (Art. 33 Abs. 5 GDPR.)
orlage für die Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten, die mindestens die folgenden Informationen enthält:

I. Zeitpunkt des Bekanntwerdens;
II. Art des Verstoßes;
III. Kategorien von betroffenen Personen;
IV. ungefähre Anzahl der betroffenen Personen;
V. Kategorien der betroffenen personenbezogenen Daten;
VI. ungefähre Anzahl der betroffenen Datensätze;
VII. Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
VIII. ergriffene oder vorgeschlagene Maßnahmen zur Wiederherstellung des erforderlichen Schutzes personenbezogener Daten und
IX. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer anderen Kontaktstelle für weitere Informationen.

Der Kunde verfügt über standardisierte Verfahren, so dass jede Verletzung des Schutzes personenbezogener Daten unter Verwendung der in Abschnitt 6.6.1 Buchstabe f) (Meldung einer Verletzung des Schutzes personenbezogener Daten) genannten Vorlage gemeldet und eine Bewertung gemäß Abschnitt 6.6.1 Buchstabe d) (Risikoanalyse) durchgeführt werden kann.

6.6.2 Ergibt die Bewertung nach 6.6.1 lit d) (Risikoanalyse), dass ein Risiko für die Rechte und Freiheiten natürlicher Personen nicht ausgeschlossen werden kann, muss der Kunde über standardisierte Verfahren verfügen, die sicherstellen, dass die Aufsichtsbehörde gemäß Art 33 DSGVO unverzüglich über die Verletzung des Schutzes personenbezogener Daten informiert wird. Diese Unterrichtung umfasst mindestens die Informationen gemäß 6.6.1 lit f) (Meldung einer Verletzung des Schutzes personenbezogener Daten) sowie den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer anderen Kontaktstelle.

6.6.3 Ergibt die Bewertung nach 6.6.1 lit d) (Risikoanalyse), dass wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht, muss der Kunde über standardisierte Verfahren verfügen, um sicherzustellen, dass die betroffenen Personen gemäß Artikel 34 DSGVO über die Verletzung des Schutzes personenbezogener Daten informiert werden. Diese Unterrichtung muss mindestens die Informationen nach 6.6.1 lit f) vii) und viii) (Folgen einer Verletzung des Schutzes personenbezogener Daten und Abhilfemaßnahmen) sowie den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer anderen Kontaktstelle. Darüber hinaus müssen diese Informationen gemäß Artikel 34 DSGVO im Einklang mit 7.3.2 a) und b) (wie in Bezug auf b) anwendbar) stehen.

7 Grundsätze und Rechte der betroffenen Personen

Der Kunde hält die Kriterien in 7.1 (Rechtmäßigkeit (Artikel 6 GDPR), 7.2 (Fairness), 7.4 (Transparenz der Datenverarbeitung (Art 5 Abs 1 lit a GDPR.), 7.9 (Datenrichtigkeit (Art 5 Abs 1 lit d GDPR), 7.10 (Speicherbegrenzung (Art 5 Abs 1 lit e GDPR.), 7.12 (Integrität und Vertraulichkeit (Art 6 Abs 1 lit f GDPR.) und 7.15 (Zweckbindung) ein, die uneingeschränkt erfüllt werden müssen. Darüber hinaus hat der Kunde die Rechte der betroffenen Personen zu beachten, nämlich das Recht auf Auskunft (7.4.5), das Recht auf Berichtigung (7.9.2), das Recht auf Löschung (7.11), das Recht auf Einschränkung der Verarbeitung (7.5), das Recht auf Datenübertragbarkeit (7.8), das Recht auf Widerspruch aus Gründen einer besonderen Situation (7.6) sowie das Recht, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, einschließlich Profiling (7.7), das gewahrt werden muss.

7.1 Rechtmäßigkeit

Ein Grundsatz der Datenverarbeitung ist ihre Rechtmäßigkeit. Danach dürfen personenbezogene Daten nur verarbeitet werden, wenn die betroffene Person entweder eingewilligt hat oder die Verarbeitung zur Durchführung vorvertraglicher Maßnahmen, zur Erfüllung eines Vertrags oder zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, lebenswichtige Interessen geschützt werden müssen, die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, oder wenn berechtigte Interessen an der Verarbeitung bestehen und diese Interessen nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen, die den Schutz personenbezogener Daten erfordern.

7.1.1 Rechtsgrundlagen der Verarbeitung (einschließlich Ausnahmen vom Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Artikel 9 DSGVO).

Der Auftraggeber stellt die Einhaltung sicher und verfügt über dokumentierte Informationen über die Auswahl der anwendbaren Rechtsgrundlage gemäß Art. 6 (1) DSGVO für jede Verarbeitung im Rahmen des Ziels der Auswertung. Zusätzlich zu dieser Rechtsgrundlage muss der Kunde, falls zutreffend, die Einhaltung der Vorschriften sicherstellen und über dokumentierte Informationen über die Auswahl der Ausnahme vom Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Artikel 9 DSGVO verfügen. Diese muss insbesondere die folgenden Aspekte behandeln:

a) Vorhandensein von personenbezogenen Daten;
b) Die Kategorien personenbezogener Daten müssen sorgfältig überprüft werden, insbesondere im Hinblick auf das Vorhandensein besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 1 GDPR.) und personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten; (Artikel 10 GDPR.)

c) Vorliegen von Entscheidungen, die ausschließlich auf einer automatisierten Entscheidungsfindung - einschließlich Profiling - beruhen; (Artikel 22 GDPR.)
d) Bestimmung des eindeutigen und rechtmäßigen Zwecks der Datenverarbeitung; (Art 5 Abs 1 lit b GDPR.)
e) endgültige Festlegung der Rechtsgrundlage; (Art 5 Abs 1 lit a und Art 6 Abs 1 GDPR.)
f) Darlegung der Erwägungen, Argumente, rechtlichen Verpflichtungen, lebenswichtigen Interessen, der im öffentlichen Interesse zu erfüllenden Aufgabe, des berechtigten Interesses oder der behördlichen Aufsicht;
g) gegebenenfalls das Bestehen einer begünstigten politischen, weltanschaulichen, religiösen oder gewerkschaftlichen Stiftung, Vereinigung oder sonstigen gemeinnützigen Organisation; (Art 9 Abs 2 lit d GDPR.)
h) Beurteilung, ob die personenbezogenen Daten für den Zweck angemessen und für die Erreichung des Zwecks unbedingt erforderlich sind. (Art 5 Abs 1 lit c GDPR.)

Die Verarbeitung auf der Grundlage einer geeigneten Rechtsgrundlage muss im Hinblick auf die Verarbeitungstätigkeiten angemessen sein, je nach Art, Kontext, Umfang und Zweck der Verarbeitung. Die Anwendbarkeit der jeweiligen Rechtsgrundlage muss vom Auftraggeber nachgewiesen werden.

7.1.2 Verarbeitung auf der Grundlage der Einwilligung

Die Einwilligung ist eine freiwillige, spezifische, unmissverständliche und in Kenntnis der Sachlage abgegebene Willensbekundung in die Form einer Erklärung oder einer anderen bestätigenden Handlung, mit der die betroffene Person erklärt, dass sie in die Verarbeitung ihrer personenbezogenen Daten einwilligt. Bei verschiedenen Verarbeitungen personenbezogener Daten muss die Einwilligung für jeden Verarbeitungsvorgang gesondert gegeben werden können. Die Erklärung muss immer vor Beginn der Verarbeitung eingeholt werden. Die Gültigkeitsdauer der Einwilligungserklärung hängt vom Umfang der ursprünglich erteilten Einwilligung und von den Erwartungen der betroffenen Person ab.

7.1.1.1 7.1.2.1 Erfolgt die Verarbeitung personenbezogener Daten gemäß 7.1.1 (Rechtmäßigkeit) auf der Grundlage der Einwilligung der betroffenen Person in die Verarbeitung sie betreffender personenbezogener Daten, muss der Auftraggeber über das Verfahren zur Einholung der

Einwilligungserklärung und deren Inhalt informiert sein. (Art 6 Abs 1 lit a GDPR.)

7.1.1.2 7.1.2.2 Die dokumentierten Informationen nach 7.1.1 (Rechtmäßigkeit) müssen in jedem Fall die folgenden Aspekte in Bezug auf das Verfahren zur Einholung der Einwilligungserklärung enthalten:

a) Wird eine Einwilligungserklärung im Rahmen einer schriftlichen Erklärung eingeholt, die auch andere Themenbereiche (Angelegenheiten) regelt, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Weise, in klarer und einfacher Sprache und deutlich abgrenzbar von den anderen Themenbereichen formuliert werden. (Artikel 7 Absatz 2 GDPR.) Dies erfordert einen Aufbau der Einwilligungserklärung, der mindestens wie folgt aussieht:

b)

X. Überschrift:
Aus dem Text muss klar hervorgehen, dass es sich um eine Einwilligungserklärung und nicht um einen allgemeinen Text zum Thema Datenschutz handelt.

XI. Sensibilisierung:
Die Formulare sollten ein "Opt-in-Feld" enthalten, so dass die betroffene Person durch Ankreuzen des Kästchens oder durch eine unmissverständliche Willenserklärung ihre Zustimmung erteilt.

XII. Freiwilligkeit/Wahlfreiheit:
Die betroffene Person muss ihre Einwilligung freiwillig und ohne Druck geben. Sie dürfen keinen Repressalien oder erheblichen Nachteilen ausgesetzt sein und müssen die Möglichkeit haben, die Einwilligung so einfach zu verweigern, wie sie sie geben können. Dazu gehört auch, dass die betroffene Person ihre Einwilligung für alle Zwecke der Verarbeitung personenbezogener Daten, für die eine Einwilligung eingeholt wird, gesondert erklären kann.

XIII. Die Einwilligung sollte keine gültige Rechtsgrundlage für die Verarbeitung personenbezogener Daten in einem bestimmten Fall darstellen, wenn ein eindeutiges Ungleichgewicht zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen besteht, insbesondere wenn es sich bei dem für die Verarbeitung Verantwortlichen um eine Behörde handelt und es daher unwahrscheinlich ist, dass die Einwilligung unter allen Umständen dieser speziellen Situation freiwillig gegeben wurde.

XIV. Platzierung:
Die Einwilligungserklärung sollte unmittelbar vor der Unterschrift (oder vor dem Kreuzfeld) geschlossen werden und nicht irgendwo im Textverlauf.

XV. Hervorhebung:

XVI. Die Einverständniserklärung muss im Druck hervorgehoben werden, wenn sie in einem umfangreicheren Text enthalten ist.

XVII. Klarer Inhalt:
Der Inhalt der Einwilligungserklärung muss klar und verständlich sein; sie muss auf vollständigen Datenschutzinformationen im Sinne von Art 13 (1) lit f DSGVO beruhen. Etwaige Folgen einer Verweigerung müssen angegeben werden.

XVIII. Rückzug:
Es muss ausdrücklich auf die Möglichkeit hingewiesen werden, die Einwilligung zu widerrufen. Der Widerruf der Einwilligung muss genauso einfach möglich sein, wie die Erklärung der Einwilligung abgegeben werden kann.

b) Richtet sich das Ersuchen um Zustimmung durch einen Dienst der Informationsgesellschaft an einen Minderjährigen, der nach den Bestimmungen des anwendbaren nationalen Rechts des Mitgliedstaats eine solche Zustimmung nur mit Zustimmung des Trägers der elterlichen Verantwortung wirksam erteilen kann, so umfasst das Verfahren die Einholung die Zustimmung oder das Einverständnis des Trägers der elterlichen Verantwortung; (Artikel 7 Absatz 3 GDPR.)
c) Die Einwilligung kann von der betroffenen Person jederzeit widerrufen werden; (Artikel 7 Absatz 3 GDPR)
d) Beruht eine Entscheidung, die für die betroffene Person rechtliche Folgen nach sich zieht oder sie in ähnlicher Weise erheblich beeinträchtigt, ausschließlich auf einer automatisierten Verarbeitung auf der Grundlage einer ausdrücklichen Einwilligung (Art 22 Abs 2 lit c GDPR) - einschließlich Profiling -, so hat die betroffene Person zumindest das Recht, sich an den Auftraggeber zu wenden, um ihren Standpunkt darzulegen und die Entscheidung anzufechten. (Art. 22 Abs. 3 GDPR)
e) Erfolgt die Verarbeitung zu mehreren Zwecken, sollte die Einwilligung für jeden dieser Zwecke gesondert erteilt werden. (Erwägungsgrund 32 GDPR)

7.1.1.3 7.1.2.3 Erfolgt die Verarbeitung besonderer Kategorien personenbezogener Daten (Art 9 Abs 2 lit a GDPR) oder zum Zwecke der Durchführung einer ausschließlich auf einer automatisierten Entscheidungsfindung beruhenden Entscheidung, einschließlich Profiling, (Art 22 Abs 2 lit c GDPR) auf der Grundlage einer Einwilligung

der betroffenen Person, so muss diese Einwilligung ausdrücklich und nicht nur durch eine andere bestätigende (konkludente) Handlung erteilt werden. Die Ausdrücklichkeit der Einwilligung wird überprüft, indem sichergestellt wird, dass sie sich direkt auf die Verarbeitung besonderer Kategorien personenbezogener Daten bezieht und ausschließlich durch eine aktive Handlung der betroffenen Person eingeholt wird.

7.1.1.4 7.1.2.4 Um dies zu beweisen, muss der Kunde zusätzlich zu den Kriterien gemäß 7.1.2.2 (Anforderungen an die Wirksamkeit der Zustimmungserklärung) und 7.1.2.3 (ausdrückliche Einwilligung) auch geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person ergreifen und die eingeholten spezifischen Einwilligungen dokumentieren. (Art. 22 Abs. 4 GDPR).

7.1.3 Verarbeitung zum Zwecke der Durchführung vorvertraglicher Maßnahmen

Ist die Datenverarbeitung für die Durchführung vorvertraglicher Maßnahmen erforderlich, so ist die Verarbeitung insoweit rechtmäßig. Das bedeutet, dass die für die Erstellung eines Angebots oder für die Anbahnung eines Vertragsverhältnisses erforderlichen personenbezogenen Daten ausschließlich zum Zweck des Vertragsabschlusses verarbeitet werden dürfen. Die geltenden Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten nach Art. 6 (1) lit. b DSGVO im Rahmen der Erbringung von Online-Diensten für betroffene Personen durch den Europäischen Datenschutzausschuss müssen beachtet werden.

7.1.1.1 7.1.3.1 Werden personenbezogene Daten gemäß 7.1.1 (Rechtmäßigkeit) zum Zwecke der Durchführung vorvertraglicher Maßnahmen auf Antrag des Betroffenen verarbeitet, so hat der Auftraggeber Informationen über die beabsichtigten vertraglichen Beziehungen und eine Begründung, warum die konkrete Datenverarbeitung für die Durchführung vorvertraglicher Maßnahmen objektiv erforderlich ist, dokumentiert. (Art 22 Abs 2 lit a GDPR)

7.1.1.2 7.1.3.2 Erfolgt eine Verarbeitung personenbezogener Daten zum Zwecke der Durchführung einer ausschließlich auf einer automatisierten Verarbeitung - einschließlich Profiling - beruhenden Entscheidung, die für die Erfüllung eines Vertrags erforderlich ist, so muss56 der Kunde zusätzlich zu den unter 7.1.1 (Rechtmäßigkeit) genannten Kriterien durch dokumentierte Informationen nachweisen, dass das Recht auf ein menschliches Eingreifen seitens des Kunden, auf Darlegung des eigenen

Standpunkts und auf Anfechtung der Entscheidung gewahrt wird. (Art. 22 Abs. 3 GDPR)

7.1.4 Verarbeitung zum Zweck der Vertragserfüllung

Die Verarbeitung muss für die Erfüllung des Vertrags, bei dem die betroffene Person Vertragspartei ist, erforderlich sein. Der Umfang der Vertragserfüllung richtet sich nach dem Zweck des Vertrages. Die Erfüllung des Vertrages umfasst sowohl die Haupt- als auch die Nebenleistungen. Die Verarbeitung muss daher objektiv für einen Zweck erforderlich sein, der ein wichtiger Teil der Erfüllung der vertraglichen Verpflichtung zugunsten der betroffenen Person ist.

7.1.1.3 7.1.4.1 Werden personenbezogene Daten gemäß 7.1.1 (Rechtmäßigkeit) zum Zwecke der Erfüllung eines Vertrages mit der betroffenen Person verarbeitet, so muss der Auftraggeber über dokumentierte Informationen über das betreffende Vertragsverhältnis und eine Begründung verfügen, warum die spezifische Verarbeitung personenbezogener Daten für die Erfüllung des Vertrages objektiv notwendig ist. (Art 6 Abs 1 lit b GDPR)

7.1.1.4 7.1.4.2 Werden besondere Kategorien personenbezogener Daten auf der Grundlage eines Vertrages mit einem Angehörigen der Heilberufe verarbeitet,59 hat der Auftraggeber zusätzlich zu 7.1.4 (Verarbeitung zum Zwecke der Vertragserfüllung) sicherzustellen, dass diese Daten ausschließlich von oder unter Aufsicht von Fachpersonal verarbeitet werden und dass dieses Fachpersonal einem gesetzlichen Berufsgeheimnis oder einer solchen Schweigepflicht unterliegt. (FN 61: Art 22 Abs 2 lit a GDPR). Dies gilt auch für das dem Fachpersonal unterstellte Personal.

7.1.1.5 7.1.4.3. Erfolgt eine Verarbeitung personenbezogener Daten zum Zwecke der Durchführung einer ausschließlich auf einer automatisierten Verarbeitung - einschließlich Profiling - beruhenden Entscheidung, die für die Erfüllung eines Vertrags erforderlich ist, und hat die Entscheidung rechtliche Auswirkungen auf die betroffene Person oder beeinträchtigt sie in ähnlicher Weise erheblich, so hat der Auftraggeber (FN 61: Art 22 Abs 2 lit a GDPR) anhand von dokumentierten Informationen zusätzlich zu den in 7.1.4 (Rechtmäßigkeit) durch dokumentierte Informationen nachweisen, dass geeignete Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person ergriffen wurden und dass der Auftraggeber die Pflichten nach Art 13 (2) lit f und Art 14 (2) lit g DSGVO erfüllt hat. In diesem Zusammenhang muss der Auftraggeber zumindest Maßnahmen ergriffen haben, die es der betroffenen Person ermöglichen, zumindest das Recht auf ein

menschliches Eingreifen seitens des Auftraggebers auszuüben, ihren eigenen Standpunkt darzulegen und die Entscheidung anzufechten. (FN 62: Art. 22 Abs. 3 GDPR)

7.1.5 Verarbeitung zum Zweck der Erfüllung einer rechtlichen Verpflichtung

Die Verarbeitung ist rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Die Verarbeitung bedarf einer Rechtsgrundlage entweder im Unionsrecht oder im Recht eines Mitgliedstaats. Ein Gesetz allein kann auch die Grundlage für mehrere Verarbeitungen bilden, sofern auf eine Rechtsvorschrift der Europäischen Union oder eines Mitgliedstaats verwiesen wird.

7.1.1.6 7.1.5.1 Werden personenbezogene Daten gemäß 7.1.1 (Rechtmäßigkeit) zur Erfüllung einer rechtlichen Verpflichtung verarbeitet, so muss der Auftraggeber über dokumentierte Informationen zu den folgenden Aspekten verfügen. (FN:63: Art 6 Abs 1 lit c GDPR)

a) Bezeichnung der rechtlichen Verpflichtung unter Angabe der Rechtsvorschrift des Unionsrechts oder des Rechts des Mitgliedstaats, dem der Kunde unterliegt (FN 64: Art 6 Abs 3, 9 Abs 2 lit h GDPR)
b) gegebenenfalls die Bezeichnung des Tarifvertrags nach dem Recht des Mitgliedstaats, aus dem sich für den Kunden eine rechtliche Verpflichtung in Bezug auf das Arbeitsrecht und das Recht der sozialen Sicherheit und des sozialen Schutzes ergibt, sowie die (FN 65: Art 9 Abs 2 lit b GDPR)
c) Umstände, aus denen hervorgeht, warum der Kunde dieser gesetzlichen Verpflichtung unterliegt; (FN 66: Art 6 Abs 1 lit c GDPR)

7.1.1.7 7.1.5.2 dokumentierte Informationen verfügen, wonach die entsprechende Verpflichtung mit den Anforderungen an den Eingriff in das Grundrecht auf Datenschutz vereinbar ist. Eine solche Bewertung muss mindestens die folgenden Aspekte umfassen: (FN 67: Art. 6 Abs. 3 Unterabs. 2 GDPR).

a) ob der Zweck der Verarbeitung in dieser Rechtsgrundlage festgelegt ist;
b) ob ein im öffentlichen Interesse liegendes Ziel verfolgt wird, das in einem angemessenen Verhältnis zu dem angestrebten legitimen Ziel steht.

Enthält die Rechtsgrundlage spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften der DSGVO, unter anderem die allgemeinen Bedingungen für die Rechtmäßigkeit der Verarbeitung durch den für die Verarbeitung Verantwortlichen, die Arten von Daten, die Gegenstand der Verarbeitung sind, die betroffenen Personen, die Stellen, an die die personenbezogenen Daten weitergegeben werden dürfen, und die Zwecke, für die sie weitergegeben werden dürfen, die Zweckbindung, die Speicher-

fristen, die Verarbeitungsvorgänge und die Verarbeitungsverfahren, einschließlich der Maßnahmen zur Gewährleistung einer rechtmäßigen und fairen Verarbeitung, wie sie in Kapitel IX für andere besondere Verarbeitungssituationen vorgesehen sind, weist der Kunde durch dokumentierte Informationen nach, dass diese besonderen Bestimmungen der rechtlichen Verpflichtungen eingehalten werden.

7.1.1.8 7.1.5.3 Der Kunde verfügt in den folgenden Fällen zusätzlich zu 7.1.5 (Verarbeitung zum Zweck der Erfüllung einer rechtlichen Verpflichtung) über dokumentierte Informationen über die geeigneten Garantien für die Grundrechte und/oder der betroffenen Person, die in der einschlägigen rechtlichen Verpflichtung vorgesehen ist:

c) Die Verarbeitung bezieht sich auf besondere Kategorien personenbezogener Daten und erfolgt zur Erfüllung einer rechtlichen Verpflichtung nach dem Arbeitsrecht, dem Recht der sozialen Sicherheit oder dem Sozialschutzrecht, (FN 68: Art 9 Abs 2 lit b GDPR.)

d) Wenn die Verarbeitung personenbezogener Daten zum Zwecke einer Einzelentscheidung erfolgt, die ausschließlich auf einer automatisierten Verarbeitung, einschließlich der Datenverarbeitung, beruht und rechtliche Auswirkungen auf die betroffene Person hat oder sie in ähnlicher Weise erheblich beeinträchtigt. (FN 69: Art 22 Abs 2 lit b GDPR)

7.1.6 Verarbeitung zum Schutz lebenswichtiger Interessen

Die Verarbeitung ist rechtmäßig, wenn sie zur Wahrung lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist.

7.1.1.9 7.1.6.1 Werden personenbezogene Daten gemäß 7.1.1 (Rechtmäßigkeit) zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person verarbeitet, so muss der Auftraggeber über dokumentierte Informationen zu den folgenden Aspekten verfügen: (FN 70: Art 6 Abs 1 lit d GDPR).

a) Situationen und Umstände, in denen eine Bearbeitung sofort und dringend erforderlich ist;

b) bei der Verarbeitung besonderer Kategorien personenbezogener Daten die Umstände, Situationen und Tatsachen, aus denen sich ergibt, dass die betroffene Person aus physischen oder rechtlichen Gründen nicht in der Lage ist, ihre Einwilligung zu

geben, (FN 71: Art 9 Abs 2 lit c GDPR) und wie der Kunde diesen Umstand in der konkreten Situation feststellt;

c) Fehlen einer anderen Rechtsgrundlage für die Verarbeitung (FN 72: Nach Erwägungsgrund 46 Satz 2 DSGVO sind lebenswichtige Interessen nur als subsidiäre Erlaubnis zur Verarbeitung der Daten zu verstehen; daher muss zunächst geprüft werden, ob eine andere Rechtsgrundlage anwendbar ist.

e)

7.1.7 Verarbeitung zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt

Die Verarbeitung ist rechtmäßig, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt und dem für die Verarbeitung Verantwortlichen anvertraut wurde. Daher ist die Datenverarbeitung muss für die im Gesetz genannten Zwecke tatsächlich erforderlich sein. Außerdem muss die Verarbeitung hier auf einer unionsrechtlichen Grundlage oder auf einem Gesetz des Mitgliedstaates beruhen, dem der für die Verarbeitung Verantwortliche unterliegt.

7.1.1.10 7.1.7.1 Werden personenbezogene Daten gemäß 7.1.1 (Rechtmäßigkeit) zur Wahrnehmung einer Aufgabe im öffentlichen Interesse verarbeitet, so muss der Auftraggeber über dokumentierte Informationen zu den folgenden Aspekten verfügen: (FN 73: Art 6 Abs 1 lit e GDPR)

a) Beschreibung der entsprechenden Aufgabe;
b) Beschreibung der Aspekte und Umstände, die auf ein öffentliches Interesse hindeuten;
c) im Falle der Verarbeitung besonderer Kategorien personenbezogener Daten die Darlegung der Aspekte und Umstände, die das erhebliche öffentliche Interesse belegen; (FN 74: Art 9 Abs 2 lit g GDPR)
d) Nachweis der Beauftragung des Auftraggebers mit der Erfüllung des Auftrags im öffentlichen Interesse auf der Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten, dem der Auftraggeber unterliegt. (FN: 75: Artikel 6 Absatz 3 GDPR)

7.1.1.11 7.1.7.2 Im Hinblick auf die Aufgabe im öffentlichen Interesse hat der Auftraggeber Informationen dokumentiert, nach denen die entsprechende unionsrechtliche oder mitgliedstaatliche Vorschrift, in der die öffentliche Aufgabe festgelegt ist, mit den Anforderungen an den Eingriff in das Grundrecht auf Datenschutz vereinbar ist. Eine solche Prüfung muss

mindestens die folgenden Aspekte umfassen: (FN 76: Art. 6 Abs. 3 Unterabs. 2 GDPR)

a) ob der Zweck der Verarbeitung in dieser Rechtsgrundlage angegeben ist; und
b) ob ein im öffentlichen Interesse liegendes Ziel verfolgt wird, das in einem angemessenen Verhältnis zu dem angestrebten legitimen Ziel steht.

f)

7.1.1.12 7.1.7.3 Der Auftraggeber muss über dokumentierte Informationen verfügen, die belegen, dass die Rechtsgrundlage für die Wahrnehmung einer Aufgabe im öffentlichen Interesse den Kern des Rechts auf Datenschutz respektiert und angemessene und spezifische Maßnahmen zum Schutz der Grundrechte und Interessen der betroffenen Person vorsieht, und zwar in folgenden Fällen:

a) Verarbeitung besonderer Kategorien personenbezogener Daten auf der Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten und aus Gründen eines wichtigen öffentlichen Interesses; (FN 77: Art 9 Abs 2 lit g GDPR)
b) Verarbeitung besonderer Kategorien personenbezogener Daten auf der Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten und aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit; (FN 78: Art 9 Abs 2 lit i GDPR)
c) Verarbeitung besonderer Kategorien personenbezogener Daten auf der Grundlage des Unionsrechts und des Rechts der Mitgliedstaaten und aus Gründen des öffentlichen Interesses, der Archivierung, der wissenschaftlichen oder historischen Forschung oder für statistische Zwecke. (FN 79: Art 9 Abs 2 lit j, 89 Abs 1 GDPR)

g)

h)

7.1.8 Verarbeitung in Ausübung öffentlicher Gewalt

Öffentliche Gewalt ist die Ausübung hoheitlicher Aufgaben und Befugnisse durch einen Mitgliedstaat oder die Europäische Union.

i)

7.1.1.13 7.1.8.1 Werden personenbezogene Daten gemäß 7.1.1 (Rechtmäßigkeit) zur Ausübung öffentlicher Gewalt verarbeitet, so muss der Auftraggeber

über dokumentierte Informationen zu den folgenden Aspekten verfügen. (FN 80: Art 6 Abs 1 lit e GDPR)

a) Beschreibung der entsprechenden Aufgabe bei der Ausübung der Amtsgewalt;

b) Nachweis der Betrauung des Kunden, wonach der Kunde auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats betraut wurde.

7.1.1.14 7.1.8.2 Gegenüber der ausübenden Behörde hat der Auftraggeber Informationen dokumentiert, wonach die entsprechende Verpflichtung mit den Vorgaben für den Eingriff in das Grundrecht auf Datenschutz vereinbar ist.

Eine solche Bewertung muss mindestens die folgenden Aspekte berücksichtigen: (FN 81: Art. 6 Abs. 3 Unterabs. 2 GDPR)

a) ob der Zweck der Verarbeitung in dieser Rechtsgrundlage angegeben ist oder die Verarbeitung für die Ausübung öffentlicher Gewalt erforderlich ist, die dem Auftraggeber übertragen wurde, und

b) ob ein im öffentlichen Interesse liegendes Ziel verfolgt wird, das in einem angemessenen Verhältnis zu dem angestrebten legitimen Ziel steht.

j)

k)

7.1.1.15 7.1.8.3 Der Auftraggeber muss über dokumentierte Informationen verfügen, um nachzuweisen, dass die Rechtsgrundlage für die Wahrnehmung einer Aufgabe im öffentlichen Interesse den Kern des Rechts auf Datenschutz respektiert und angemessene und spezifische Maßnahmen vorsieht, um die Grundrechte und Interessen der betroffenen Person in den folgenden Fällen zu schützen. (FN 82: Art. 6 Abs. 2 GDPR)

l)

m) Verarbeitung besonderer Kategorien personenbezogener Daten auf der Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten und aus Gründen eines wichtigen öffentlichen Interesses; (FN 83: Art 9 Abs 2 lit g GDPR)

n) Verarbeitung besonderer Kategorien personenbezogener Daten auf der Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten und aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit; (FN 84: Art 9 Abs 2 lit i GDPR)

o) Verarbeitung besonderer Kategorien personenbezogener Daten auf der Grundlage des Unionsrechts und des Rechts der Mitgliedstaaten und aus Gründen des öffentlichen Interesses, der Archivierung, der wissenschaftlichen oder historischen Forschung oder für statistische Zwecke. (FN 85: Art 9 Abs 2 lit j, 89 Abs 1 GDPR)

p)

7.1.9 Verarbeitung für die Zwecke der berechtigten Interessen

Die Datenverarbeitung ist rechtmäßig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz der personenbezogenen Daten erfordern, überwiegen. Die Interessenabwägung erfolgt in drei Prüfschritten: Zunächst muss das berechtigte Interesse ermittelt werden. Dann wird geprüft, ob die Verarbeitung der personenbezogenen Daten zur Erreichung des Zwecks oder zur Wahrung des berechtigten Interesses erforderlich ist. Schließlich erfolgt eine Interessenabwägung, bei der die Interessen im Hinblick auf die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen dürfen.

7.1.1.16 7.1.9.1 Erfolgt die Verarbeitung personenbezogener Daten gemäß 7.1.1 (Rechtmäßigkeit) zur Wahrung eines berechtigten Interesses des Auftraggebers (einschließlich der Begründung, Geltendmachung oder Verteidigung von Rechtsansprüchen (FN 86: Art 9 Abs 2 lit f GDPR, Art 17 Abs 3 lit e GDPR), auch wenn besondere Datenkategorien betroffen sind) oder eines Dritten, so ist dieser über die durchgeführte Interessenabwägung dokumentiert zu informieren: (FN 87: Art 6 Abs 1 lit f GDPR)

7.1.1.17 7.1.9.2 Bei der Durchführung der Interessenabwägung nach 0 (Wahrung des berechtigten Interesses des Auftraggebers) hat der Auftraggeber mindestens die folgenden Aspekte zu berücksichtigen:

a) Die endgültige Feststellung der Art und Quelle des Interesses des Kunden oder eines Dritten;
b) Die tatsächliche und aktuelle Wahrnehmung des g e m ä ß lit. a) ermittelten Inhalts durch den Auftraggeber;
c) Die berechtigten Erwartungen der betroffenen Personen aufgrund ihrer Beziehung zu dem für die Verarbeitung Verantwortlichen;
d) die Erforderlichkeit der Datenverarbeitung zur Erreichung des nach Buchstabe a) bestimmten Zwecks;
e) Die Beschreibung, inwiefern die Verarbeitung ein Risiko für die betroffenen Personen darstellt;
f) sowie zusätzliche Garantien, die der für die Verarbeitung Verantwortliche anwendet, um unangemessene Auswirkungen auf die betroffenen Personen z u verhindern.

7.1.10 Verarbeitung durch eine Stiftung, einen Verein oder eine andere Einrichtung ohne Erwerbszweck

Werden besondere Kategorien personenbezogener Daten von einer Stiftung, einem Verein oder einer anderen gemeinnützigen Einrichtung (FN 88: Art 9 Abs 2 lit d GDPR) *mit politischen, philosophischen, religiösen oder gewerkschaftlichen Zielen gemäß 7.1.1 (Rechtmäßigkeit) im Rahmen ihrer rechtmäßigen Tätigkeiten mit angemessenen Garantien verarbeitet, muss der für die Verarbeitung Verantwortliche nachweisen:*

a) ihre politischen, philosophischen, religiösen oder gewerkschaftlichen Ziele,
b) die Legitimität der Tätigkeit,
c) geeignete Garantien, um sicherzustellen, dass die personenbezogenen Daten nicht ohne die Zustimmung der betroffenen Personen außerhalb dieser Stelle weitergegeben werden, und
d) der Bezug der Verarbeitung ausschließlich zu den Mitgliedern oder ehemaligen Mitgliedern der Einrichtung oder zu Personen, die im Zusammenhang mit deren Zwecken regelmäßig mit ihr in Kontakt stehen.

7.1.11 Verarbeitung von öffentlich zugänglichen Informationen

Werden besondere Kategorien personenbezogener Daten gemäß 7.1.1 (Rechtmäßigkeit) vom Auftraggeber verarbeitet, weil die betroffene Person sie offenkundig öffentlich gemacht hat, muss der Auftraggeber über dokumentierte Informationen verfügen, die belegen, dass eine Interessenabwägung unter Berücksichtigung des Zwecks und des Kontextes der Veröffentlichung vorgenommen wurde. (FN 89: Art 9 Abs 2 lit e GDPR)

7.1.12 Verarbeitung zu einem anderen Zweck

Werden personenbezogene Daten gemäß 7.1.1 (Rechtmäßigkeit) für einen anderen Zweck als den, für den sie erhoben wurden, verarbeitet, muss der Kunde nachweisen, dass die in der DSGVO festgelegten Grundsätze und insbesondere die Un-

terrichtung der betroffenen Person über diese anderen Zwecke und über ihre Rechte, einschließlich des Widerspruchsrechts, gewährleistet sind. Um festzustellen, ob die Verarbeitung für einen anderen Zweck mit dem Zweck, für den die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, muss der Kunde unter anderem die folgenden Elemente und Faktoren berücksichtigen und dokumentierte Informationen über das Ergebnis dieser Vereinbarkeitsprüfung vorlegen. (FN 90: Artikel 6 Absatz 4 GDPR)

a) Alle Informationen gemäß 7.1.1 (Rechtmäßigkeit) über die Verarbeitung für einen anderen Zweck als den, für den die personenbezogenen Daten erhoben wurden ("Weiterverarbeitung");
b) wenn aufgrund des Ergebnisses unter lit. a) alle Voraussetzungen des jeweils anwendbaren Gesetzes der Rechtmäßigkeit vorliegen;
c) wenn aufgrund des Ergebnisses nach lit. a) eine Verarbeitung besonderer Kategorien personenbezogener Daten erfolgt, alle dokumentierten Informationen nach 7.1.1 lit b) (Rechtmäßigkeit);
d) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung; (FN 91: Art 6 Abs 4 lit a GDPR)
e) den Kontext, in dem die personenbezogenen Daten erhoben wurden, wobei insbesondere die Beziehung zwischen der betroffenen Person und dem Kunden darzulegen ist; (FN 92: Art 6 Abs 4 lit b GDPR)
f) Arten personenbezogener Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden; (FN 93: Art 6 Abs 4 lit c GDPR)
g) Mögliche Folgen der beabsichtigten Weiterverarbeitung für die betroffene Person (FN 94: Art 6 Abs 4 lit d GDPR) nach Durchführung einer Bewertung gemäß 7.1.9 (Verarbeitung zur Wahrung berechtigter Interessen);
h) Das Vorhandensein geeigneter Sicherheitsvorkehrungen. FN 95: Art 6 Abs 4 lit e GDPR)

7.1.13 Verarbeitung zu Archivierungszwecken im öffentlichen Interesse, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

Werden personenbezogene Daten gemäß 7.1.1 (Rechtmäßigkeit) zu im öffentlichen Interesse liegenden Archivierungszwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken verarbeitet, so erhält der Auftraggeber unter[96] die folgenden zusätzlichen dokumentierten Informationen:

a) das Vorhandensein angemessener Garantien für die Rechte und Freiheiten der betroffenen Personen;
b) Vorhandensein von technischen und organisatorischen Maßnahmen zur Wahrung der Grundsätze der Datenverarbeitung, insbesondere des Zwecks der Datenminimierung, wie z. B. Pseudonymisierung;
c) Begründung, warum die Verarbeitung personenbezogener Daten zur Erreichung des Zwecks erforderlich ist.

7.2 Fairness

Der Grundsatz der Verarbeitung nach Treu und Glauben ist ein übergreifender Grundsatz, der besagt, dass personenbezogene Daten nicht in einer Weise verarbeitet werden dürfen, die der betroffenen Person einen ungerechtfertigten Nachteil bringt, die in keiner Weise diskriminierend, unerwartet oder irreführend ist. Die Maßnahmen und Garantien zur Umsetzung des Grundsatzes der Verarbeitung nach Treu und Glauben unterstützen auch die Rechte und Freiheiten der betroffenen Personen, insbesondere die in Kapitel III der DS-GVO verankerten Rechte. Als übergreifendes Prinzip ist der Grundsatz der Lauterkeit mit vielen Verpflichtungen der Datenschutz-Grundverordnung verknüpft, die in diesen Zertifizierungskriterien behandelt werden. Die Einhaltung des Grundsatzes der Fairness erfordert daher die Einhaltung aller Zertifizierungskriterien, einschließlich, aber nicht beschränkt auf den vorliegenden Punkt 7.2.

7.2.1. Der Auftraggeber stellt die Einhaltung des Grundsatzes der fairen Verarbeitung (Fairness-Prinzip) (FN 97: Art 5 Abs 1 lit a GDPR) bei allen Verarbeitungsvorgängen im Rahmen des Target of Evaluation sicher. Der Auftraggeber dokumentiert alle Maßnahmen, die zu diesem Zweck ergriffen wurden.

Diese Maßnahmen müssen mindestens die folgenden Aspekte abdecken:

a) Der Auftraggeber prüft, ob die Datenverarbeitung im Rahmen des Evaluationsgegenstandes zu einer Diskriminierung oder Ausbeutung der betroffenen Personen führen kann. Im Rahmen der Bewertung ist insbesondere zu berücksichtigen, ob personenbezogene Daten schutzbedürftiger Gruppen verarbeitet werden, wie z. B. Kinder, Arbeitnehmer, ältere Menschen oder Menschen mit Beeinträchtigungen. Der Kunde muss Maßnahmen ergreifen, um festgestellte Fälle von Diskriminierung oder Ausbeutung zu beseitigen.

   Dazu gehört auch, dass Personen mit Beeinträchtigungen, wie z. B. Sehbehinderungen, geeignete Wege zur Ausübung ihrer Betroffenenrechte zur Verfügung gestellt werden. Darüber hinaus muss sichergestellt werden, dass es keine ungerechtfertigte Diskriminierung aufgrund von Merkmalen der betroffenen Personen wie Geschlecht, Alter oder sexuelle Ausrichtung gibt, insbesondere im Zusammenhang mit einer automatisierten Einzelentscheidung gemäß Artikel 22 DSGVO.
b) Zusätzlich zu Punkt 7.3 (Transparente Informationen und Modalitäten für die Ausübung der Rechte der betroffenen Person) werden die Mitarbeiter des Auftraggebers darin geschult, Anfragen der betroffenen Person ohne unnötige Verzögerung an die zuständige interne Abteilung des Auftraggebers zur weiteren Bearbeitung weiterzuleiten;
c) Richtet sich die Datenverarbeitung an Kinder, so ist sicherzustellen, dass die Anforderungen des Art. 12 Abs.. 1 GDPR für eine kinderfreundliche Sprache umgesetzt wurden;
d) Der Kunde darf das Risiko seines Unternehmens nicht auf die betroffene Person übertragen (z. B. durch Allgemeine Geschäftsbedingungen). (FN 100: So darf beispielsweise in den Geschäftsbedingungen des Kunden nicht festgelegt werden, dass die betroffene Person und nicht der für die Verarbeitung Verantwortliche für die Umsetzung der Datensicherheitsmaßnahmen gemäß Artikel 32 DSGVO verantwortlich ist.)
e)

7.2.2. Der Kunde überprüft die in Punkt 7.2.1 genannten Maßnahmen mindestens alle 12 Monate und passt sie gegebenenfalls an. Der Kunde dokumentiert die E r g e b n i s s e jeder Überprüfung. Falls bestellt, kon-

sultiert und dokumentiert der Kunde den Rat des Datenschutzbeauftragten hinsichtlich der Durchführung und Überprüfung aller unter Punkt 7.2.1 genannten Maßnahmen.

7.2.3. Bei der Durchführung und Überprüfung der in Ziffer 7.2.1 genannten Maßnahmen wird der Auftraggeber die höchstrichterliche Rechtsprechung, insbesondere des EuGH, sowie die einschlägigen Papiere des EDPB (FN 101: Siehe insbesondere EDPB-Leitlinien 4/2019 zu Art 25 - Data Protection by Design and by Default, Version 2.0, Kapitel 3.3.) zum Thema Fairnessprinzip beachten und berücksichtigen.

7.3 Transparente Informationen und Modalitäten für die Ausübung der Rechte der betroffenen Person

Es sollten Modalitäten vorgesehen werden, die der betroffenen Person die Ausübung ihrer Rechte nach dieser Verordnung erleichtern, einschließlich Mechanismen für die Beantragung und gegebenenfalls die unentgeltliche Erlangung insbesondere des Zugangs zu und der Berichtigung oder Löschung von personenbezogenen Daten sowie die Ausübung des Widerspruchsrechts. Der für die Verarbeitung Verantwortliche sollte auch die Möglichkeit vorsehen, Anträge auf elektronischem Wege zu stellen, insbesondere wenn personenbezogene Daten auf elektronischem Wege verarbeitet werden. Der für die Verarbeitung Verantwortliche sollte verpflichtet sein, Ersuchen der betroffenen Person unverzüglich, spätestens jedoch innerhalb eines Monats, zu beantworten und zu begründen, wenn er nicht beabsichtigt, einer solchen Aufforderung nachzukommen.

7.3.1 Verfahren zur Erleichterung der Ausübung der Rechte der betroffenen Person nach 7.5 (Einschränkung der Verarbeitung personenbezogener Daten), 7.6 (Widerspruch aus Gründen einer besonderen Situation), 7.7 (Recht, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, einschließlich Profiling), 7.4.2 (Informationspflicht), 7.4.3 (Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden), 7.4.5 (Zugang zu personenbezogenen Daten), 7.8 (Datenübertragbarkeit), 7.9.2 (Recht auf Berichtigung) und 7.11 (Recht auf Löschung personenbezogener Daten – FN 102: Art. 12 Abs. 2 GDPR) gewährleistet zumindest,

a) Benennung eines Verantwortlichen für die Wahrung der Rechte der betroffenen Personen;

b) Angabe der Kontaktdaten des Kunden, über die er mit mehreren Kommunikationsmitteln kontaktiert werden kann, in jedem Fall per E-Mail, Telefon und Post;
c) die Bestätigung des Empfangs eines Antrags im Sinne der genannten Bestimmung unverzüglich und unabhängig von den nachfolgenden Maßnahmen des Kunden in Bezug auf den Antrag;
d) dass der Kunde sich nicht weigern darf, dem Antrag der betroffenen Person auf Ausübung ihrer Rechte nachzukommen, es sei denn, der Kunde weist nach, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, und (FN:103: Art. 12 Abs. 2 GDPR.)
e) dass der Kunde bei begründeten Zweifeln an der Identität der antragstellenden natürlichen Person die zur Bestätigung der Identität der betroffenen Person erforderlichen zusätzlichen Informationen einholt, einschließlich einer schriftlichen Anweisung an die betroffene Person, wie sie sich unter Berücksichtigung des Grundsatzes der Datenminimierung ordnungsgemäß identifizieren kann. (FN 104: Art. 12 Abs. 6 GDPR)

7.3.2 Darüber hinaus müssen diese Verfahren das Vorhandensein von dokumentierten Informationen gewährleisten, die belegen, dass alle entsprechenden Informationen und Mitteilungen zur Wahrnehmung der Rechte der betroffenen Person und deren Ausübung zur Verfügung stehen.

a) in knapper, transparenter, verständlicher und leicht zugänglicher Form, unter Verwendung klarer und einfache Sprache, insbesondere bei Informationen, die sich speziell an ein Kind richten (FN 105: Art. 12 Abs. 1 Satz 1 GDPR); dokumentierte Informationen in Bezug auf Informationen, die sich speziell an ein Kind richten, müssen zumindest den Nachweis enthalten, dass die Fähigkeit, solche Informationen zu verstehen, an Kindern getestet wurde und dass die Ergebnisse dieser Tests bei der Abfassung der endgültigen Fassung der Informationen berücksichtigt wurden;
b) kostenlos (FN106: Art. 12 Abs. 5 GDPR) - es sei denn, der Kunde beschließt, bei offensichtlich unbegründeten oder übermäßigen Anfragen, insbesondere aufgrund ihres Wiederholungscharakters, eine angemessene Gebühr unter Berücksichtigung der Verwaltungskosten für die Bereitstellung der Informationen oder Mitteilungen oder die Durchführung der angeforderten Maßnahmen (FN 107: Art. 12 Abs. 5 Nr. 1 GDPR) zu erheben,
c) (FN108 : Art. 12 Abs. 1 Satz 2 GDPR.) Auf Antrag der betroffenen Person stellen die Verfahren sicher, dass die Informationen münd-

lich erteilt werden können, sofern die Identität der betroffenen Person auf andere Weise nachgewiesen wird. (FN109: Art. 12 Abs. 1 Satz 2 GDPR)

7.3.3 Darüber hinaus müssen diese Verfahren sicherstellen, dass die Meldungen nach 7.5 (Einschränkung der Verarbeitung personenbezogener Daten), 7.6 (Widerspruch aufgrund besonderer Umstände), 7.7 (Recht, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, einschließlich Profiling), 7.4.2 (Informationspflicht), 7.4.3 (Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden), 7.4.5 (Zugang zu personenbezogenen Daten), 7.8 (Datenübertragbarkeit), 7.9.2 (Berichtigungsverfahren) und 7.11 (Recht auf Löschung personenbezogener Daten) wird der betroffenen Person unverzüglich, auf jeden Fall aber innerhalb eines Monats nach Eingang des Antrags, zur Verfügung gestellt. (FN110 : Art. 12 Abs. 3 Satz 1 GDPR)

7.3.4 Verlängert der Auftraggeber die Einmonatsfrist nach Eingang der Anfrage um bis zu zwei Monate, so stellt er in jedem Einzelfall eine dokumentierte Information über die jeweilige Notwendigkeit einer solchen Verlängerung sicher, die sich in der (FN 111: Art. 12 Abs. 3 Satz 2 GDPR). In diesem Fall muss der Kunde die betroffene Person innerhalb eines Monats nach Eingang des Antrags unter Angabe der Gründe für die Verzögerung unterrichten. (FN 112: Art 12 Abs 3 Satz 3 GDPR)

7.3.5 Wird der Kunde auf das Ersuchen der betroffenen Person hin nicht tätig, so sorgt er dafür, dass die betroffene Person unverzüglich, spätestens jedoch innerhalb eines Monats nach Eingang des Ersuchens, über die Gründe für das Nichttätigwerden oder die Erhebung einer angemessenen Gebühr unter Berücksichtigung der Verwaltungskosten für die Bereitstellung der Informationen oder Mitteilungen oder die Durchführung der beantragten Maßnahme (FN113: Art. 12 Abs. 5 Nr. 1 GDPR) sowie über die Möglichkeit einer Beschwerde bei einer Aufsichtsbehörde und eines gerichtlichen Rechtsbehelfs informiert wird. (FN114: Artikel 12 Absatz 4 GDPR). Gründe für den Verzicht auf Maßnahmen können unter anderem sein, dass der Kunde nicht der für die Verarbeitung Verantwortliche der personenbezogenen Daten ist, auf die sich die Anfrage bezieht, dass die Anfrage der betroffenen Person offensichtlich unbegründet oder übertrieben ist, (FN115: Art. 12 Abs. 5 GDPR) insbesondere wegen ihres wiederholten Charakters, oder dass eine Ausnahme nach Artikel 23 DSGVO vorliegt. (FN116: Artikel 23 GDPR).

7.3.6 Wenn der Kunde aufgrund eines offensichtlich unbegründeten oder übermäßigen Ersuchens oder einer Ausnahme nach Artikel 23 DSGVO nicht tätig wird, muss der Kunde sicherstellen, dass dokumentierte Informationen

vorliegen, die den Charakter des Ersuchens als übermäßig oder offensichtlich unbegründet belegen (FN117: Art 15 Abs 5 letzter Satz GDPR), bzw. über die genaue gesetzgeberische Maßnahme im Unionsrecht oder im Recht der Mitgliedstaaten, die Gründe für die Anwendung einer solchen gesetzgeberischen Maßnahme sowie eine dokumentierte Bewertung der Erfüllung der Voraussetzungen für eine solche gesetzgeberische Maßnahme gemäß Artikel 23 (1) und (2) DSGVO, nämlich dass die Beschränkung den Kern der Grundrechte und - freiheiten respektiert und eine notwendige und verhältnismäßige Maßnahme in einer demo- kratischen Gesellschaft ist, um ein in Artikel 23 (1) DSGVO genanntes Thema zu schützen, und dass die gesetzgeberische Maßnahme spezifische Bestimmungen gemäß Artikel 23 (2) DSGVO enthält.

7.4 Transparenz der Verarbeitung personenbezogener Daten

Transparenz spielt eine wichtige Rolle bei der Durchsetzung der Rechte der betroffenen Personen. Nur wenn die betroffene Person ausreichend informiert ist, kann sie ihre Rechte Daher muss der betroffenen Person ausreichende Transparenz über die Erhebung, die Verwendung, den Zugang zu ihren personenbezogenen Daten und den Umfang der Verarbeitung der personenbezogenen Daten gewährt werden. Darüber hinaus müssen alle Informationen und Mitteilungen in einer leicht zugänglichen und verständlichen Form sowie in einer einfachen und verständlichen Sprache erfolgen.

7.4.1 Transparente Datenverarbeitung

Der Kunde stellt sicher, dass personenbezogene Daten auf transparente Weise verarbeitet werden. Zu diesem Zweck muss der Kunde alle in Punkt 7.4 genannten Kriterien erfüllen. (FN118: Art 5 Abs 1 lit a GDPR)

7.4.2 Informationspflicht bei der Erhebung personenbezogener Daten bei der betroffenen Person (Informationspflicht)

Die Informationspflichten gelten für den für die Datenverarbeitung Verantwortlichen. Es geht darum, die betroffene Person über die Datenverarbeitung und die ihr zustehenden Rechte zu informieren, bevor sie personenbezogene Daten zur Verfügung stellt oder wenn sie Daten von einem Dritten erhält.

7.4.1.1 Der Kunde muss über dokumentierte Informationen verfügen, aus denen hervorgeht, dass die betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten (FN119: Art. 13 Abs. 1, 13 Abs. 4, 14 Abs. 5 GDPR) informiert wurde und dass geprüft wurde, welche Aspekte relevant und

notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten. (FN120: Art. 13 Abs. 2 GDPR)

7.4.1.2 Der Nachweis nach 7.4.2 muss in jedem Fall die folgenden Aspekte umfassen: (FN121: Art. 13 Abs. 1 GDPR)

a) Name und Kontaktdaten des Auftraggebers;
b) gegebenenfalls der im Europäischen Wirtschaftsraum benannte Vertreter;
c) die Kontaktdaten des Datenschutzbeauftragten, falls zutreffend;
d) Zweck der Datenverarbeitung;
e) Rechtsgrundlage für die Datenverarbeitung;
f) Ggf. die berechtigten Interessen des Auftraggebers oder eines Dritten
g) Empfänger oder die Kategorien von Empfängern;
h) Ggf. die Absicht, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, und das Vorhandensein oder Nichtvorhandensein eines Angemessenheitsbeschlusses der Kommission oder, im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absätze 1 und 2 DSGVO, einen Hinweis auf die geeigneten oder angemessenen Garantien und wie eine Kopie davon zu erhalten ist oder wo sie verfügbar sind.

7.4.1.3 Zusätzlich zu den Aspekten nach 7.4.2.2 umfasst der Nachweis nach 7.4.2 die folgenden Aspekte, soweit sie zur Gewährleistung einer fairen und transparenten Verarbeitung erforderlich sind:

a) Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer; (FN122: Art 13 Abs 2 lit b GDPR)
b) Belehrung über die folgenden Rechte:
   I. Recht auf Zugang; (FN123: Art 13 Abs 2 lit b GDPR)
   II. Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung; (FN124: Art 13 Abs 2 lit b GDPR)
   III. Recht auf Widerspruch gegen die Verarbeitung (FN125: Art 13 Abs 2 lit b, Art 21 Abs 4 GDPR)
   IV. Recht auf Datenübertragbarkeit; (FN126: Art 13 Abs 2 lit b GDPR)
   V. Recht auf jederzeitigen Widerruf der Einwilligung, ohne dass die Rechtmäßigkeit der auf der Einwilligung beruhenden Verarbeitung nach Art. 6 (1) lit. a oder Art. 9 (2) lit. a DSGVO vor dem Widerruf berührt wird; (FN127: Art 13 Abs 2 lit c GDPR)
   VI. Recht auf Beschwerde bei der Aufsichtsbehörde (FN128: Art 13 Abs 2 lit d GDPR)

Klärung der Frage, ob die Bereitstellung personenbezogener Daten gesetzlich oder vertraglich vorgeschrieben oder für den Abschluss eines Vertrags erforderlich ist; (FN129: Art 13 Abs 2 lit e GDPR)

Klärung der Frage, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten zur Verfügung zu stellen, und welche Folgen die Nichtbereitstellung der Daten haben würde; (FN130: Art 13 Abs 2 lit e GDPR)
Informationen über das Bestehen einer automatisierten Entscheidungsfindung, einschließlich der Einreichung von Anträgen gemäß Art. 22 Abs. 1 und 4 DSGVO und zumindest in diesen Fällen sinnvolle Informationen über die involvierte Logik sowie die Tragweite und die beabsichtigten Auswirkungen einer solchen Verarbeitung für die betroffene Person (FN131: Art 13 Abs 2 lit f GDPR)

7.4.1.4 Die Informationspflicht nach 7.4.2 gilt nicht, wenn und soweit die betroffene Person bereits über die Informationen verfügt. (FN132: Artikel 13 Absatz 4 GDPR) Falls sich der Auftraggeber auf diese Ausnahme beruft, muss er deren Anwendbarkeit in Bezug auf das Ziel der Auswertung nachweisen.

7.4.3 Informationen, die zu erteilen sind, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden.

7.4.3.1 Werden personenbezogene Daten nicht vom Auftraggeber bei der betroffenen Person erhoben, so sind die Nachweise gemäß 7.4.2 (Informationspflicht) zu erbringen und müssen in jedem Fall die folgenden zusätzlichen Aspekte enthalten (FN133: Art. 14 Abs. 1 GDPR).

a) Kategorien der verarbeiteten personenbezogenen Daten (FN134: Art 14 Abs 1 lit d DSGVO,
b) soweit dies für eine faire und transparente Verarbeitung erforderlich ist, die Quelle, aus der die personenbezogenen Daten stammen, und gegebenenfalls, ob sie aus öffentlich zugänglichen Quellen stammen (FN135: Art. 14 Abs. 1 lit. f GDPR).

7.4.3.2 Der Kunde muss dokumentierte Informationen darüber liefern, dass die Informationspflicht gemäß 7.4.3 (personenbezogene Daten werden nicht bei der betroffenen Person erhoben) vorgesehen ist

a) innerhalb einer angemessenen Frist nach Erhalt der personenbezogenen Daten, spätestens jedoch innerhalb eines Monats, unter Berücksichtigung der besonderen Umstände, unter denen die personenbezogenen Daten verarbeitet werden (FN136: Art 14 Abs 3 lit a GDPR),
b) wenn die personenbezogenen Daten für die Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Kommunikation mit dieser Person (FN 137: Art 14 Abs 3 lit b GDPR);
c) wenn eine Weitergabe an einen anderen Empfänger beabsichtigt ist, spätestens bei der ersten Weitergabe der personenbezogenen Daten (FN 138: Art 14 Abs 3 lit a GDPR) oder

7.4.4 Die Informationspflicht nach 7.4.3 (personenbezogene Daten werden nicht bei der betroffenen Person erhoben) gilt jedoch nicht, wenn

a) die betroffene Person bereits über die Informationen verfügt (FN139: Art 14 Abs 5 lit a GDPR);
b) die Bereitstellung dieser Informationen sich als unmöglich erweist oder mit unverhältnismäßigem Aufwand verbunden wäre, insbesondere bei Verarbeitungen für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke, vorbehaltlich der in Artikel 89 Absatz 1 genannten Bedingungen und Garantien, oder soweit die in Absatz 1 des vorliegenden Artikels genannte Verpflichtung die Verwirklichung der Ziele dieser Verarbeitung unmöglich machen oder ernsthaft beeinträchtigen könnte. In solchen Fällen ergreift der für die Verarbeitung Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten und der berechtigten Interessen der betroffenen Person, einschließlich der Veröffentlichung der Informationen FN140: Art 14 Abs 5 lit b GDPR);
c) die Einholung oder Weitergabe ausdrücklich durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgesehen ist, dem der für die Verarbeitung Verantwortliche unterliegt und das angemessene Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsieht (FN141: Art 14 Abs 5 lit c GDPR); oder
d) wenn die personenbezogenen Daten aufgrund einer durch das Unionsrecht oder das Recht der Mitgliedstaaten geregelten Verpflichtung zur Wahrung des Berufsgeheimnisses, einschließlich einer gesetzlichen Geheimhaltungspflicht, vertraulich bleiben müssen (FN142: Art 14 Abs 5 lit d GDPR).

Falls sich der Auftraggeber auf eine oder mehrere dieser Ausnahmen beruft, muss er die Anwendbarkeit in Bezug auf den Evaluationsgegenstand nachweisen.

7.4.5 Zugang zu personenbezogenen Daten

7.4.5.1 Der Kunde muss über dokumentierte Informationen verfügen, die belegen, dass Verfahren zur Bereitstellung der folgenden Informationen vorhanden sind:

a) Bestätigung, ob die betreffenden personenbezogenen Daten v e r a r b e i t e t werden (FN143: Art. 15 Abs. 1 GDPR);

b) Informationen über die verarbeiteten personenbezogenen Daten (FN144: Art. 15 Abs. 1, 15 Abs. 3 GDPR);

7.4.5.2 Der Nachweis gemäß 7.4.5.1 lit. a) (Bestätigung der Verarbeitung) hat jedenfalls folgende Angaben zu enthalten (FN145: Art. 15 Abs. 1 GDPR):

a) Verarbeitungszwecke, die mit dem Ziel der Bewertung verfolgt werden (FN146: Art 15 Abs 1 lit a GDPR);
b) Kategorien personenbezogener Daten, die zur Erreichung des unter Buchstabe a) genannten Zwecks verarbeitet werden Kategorien der verarbeiteten personenbezogenen Daten(FN147: Art 15 Abs 1 lit b GDPR);
c) wenn die Kategorien nach Buchstabe b) nicht bei der anfragenden Person erhoben worden sind, alle verfügbaren Informationen über die Herkunft der Daten(FN148: Art 15 Abs 1 lit g GDPR);
d) Klärung des Vorliegens einer automatisierten Entscheidungsfindung gemäß 5.2.3 (Automatisierte Einzelfallentscheidung) und ggf. die zugrunde liegende Logik, der Anwendungsbereich und die beabsichtigten Auswirkungen (FN149: Art 15 Abs 1 lit h GDPR);
e) Empfänger oder Kategorien von Empfängern, an die die unter Buchstabe b) genannten Kategorien personenbezogener Daten weitergegeben werden (FN150: Art 15 Abs 1 lit c GDPR);
f) Aufbewahrungsfrist oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Frist mit zur Erreichung des Zwecks gemäß Buchstabe a) (FN151: Art 15 Abs 1 lit d GDPR);
g) das Bestehen des Rechts, von dem für die Verarbeitung Verantwortlichen die Berichtigung oder Löschung personenbezogener Daten oder die Einschränkung der Verarbeitung personenbezogener Daten der betroffenen Person zu verlangen oder gegen eine solche Verarbeitung Widerspruch einzulegen (FN152: Art 15 Abs 1 lit e GDPR), sowie das Recht, eine Beschwerde bei der Aufsichtsbehörde einzureichen (FN153: Art 15 Abs 1 lit f GDPR);
h) Gegebenenfalls die geeigneten Garantien, die gemäß 9.4 (verbindliche unternehmensinterne Vorschriften), 9.5 (Standard-Datenschutzklauseln der Europäischen Kommission), 9.6 (Standard-Datenschutzklauseln einer Aufsichtsbehörde), 9.7 (genehmigte Verhaltenskodizes), 9.8 (genehmigter Zertifizierungsmechanismus) oder 0 (genehmigte Vertragsklauseln) im Falle einer Übermittlung von Kategorien gemäß Buchstabe b) an ein Drittland oder eine internationale Organisation umgesetzt werden (FN154: Art. 15 Abs. 2 GDPR).

7.4.5.3 Das Verfahren nach 7.4.5.1 lit a) (Bestätigung der Verarbeitung) muss zumindest angemessene Verantwortlichkeiten vorsehen und sicherstellen, dass die Recherche nach personenbezogenen Daten der anfragenden Person nicht nur die automatisierte Datenverarbeitung durch den

Auftraggeber, sondern auch die manuelle Datenverarbeitung in Ablagesystemen nach Art 4 Nr. 6 DSGVO umfasst. .

7.4.5.4 Der Nachweis nach 7.4.5.1 lit b) (Information über verarbeitete Daten) hat jedenfalls zusätzlich zu den Informationen nach 7.4.5.2 auch durch dokumentierte Informationen sicherzustellen, dass (FN155: Art. 15 Abs. 3 GDPR)

a) eine Kopie der von den Kategorien gemäß 7.4.5.3 lit b) (Auskunft über verarbeitete Daten) bereitgestellten Informationen an die Person, die die Auskunft beantragt, ausgegeben werden kann; und
b) die Bereitstellung in einem gemeinsamen elektronischen Format möglich ist.

7.4.5.5 Das Verfahren nach Abschnitt 7.4.5.4 Buchstabe a) (Kopie der personenbezogenen Daten) muss außerdem Folgendes enthalten ein System zur Abwägung zwischen den Gründen der betroffenen Person und den Rechten und Freiheiten anderer Personen (FN156: Artikel 15 Absatz 4 GDPR).

7.4.5.6 Beruht eine Entscheidung ausschließlich auf einer automatisierten Verarbeitung einschließlich Profiling, hat die betroffene Person zumindest das Recht, eine Person des für die Verarbeitung Verantwortlichen hinzuzuziehen, und die dokumentierten Informationen müssen gemäß 6.5 (Aufzeichnungen über Verarbeitungstätigkeiten) aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer solchen Verarbeitung enthalten (FN157: Art 15 Abs 1 lit h GDPR). Dies gilt nach Art. 22 Abs. 2 lit. b und Abs. 3 DSGVO jedoch nicht, wenn der Verantwortliche durch Unionsrecht oder das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt und das auch geeignete Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person vorsieht, dazu ermächtigt ist.

7.5 Einschränkung der Verarbeitung von personenbezogenen Daten

7.5.1 Der Kunde muss über dokumentierte Informationen verfügen, die belegen, dass organisatorische und technische Maßnahmen vorhanden sind, die es den betroffenen Personen erleichtern, von dem für die Verarbeitung Verantwortlichen die Einschränkung der Verarbeitung personenbezogener Daten zu verlangen, wenn einer der folgenden Fälle vorliegt (FN158: Art. 18 Abs. 1 GDPR:

a) Die Richtigkeit der personenbezogenen Daten wird während eines Zeitraums bestritten, der dem Kunden die Möglichkeit gibt, die Richtigkeit der personenbezogenen Daten zu überprüfen;159

b) die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Verwendung der personenbezogenen Daten verlangt (FN160: Art 18 Abs 1 lit b GDPR);
c) der Auftraggeber die personenbezogenen Daten nicht mehr benötigt, die betroffene Person sie aber zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt (FN161: Art 18 Abs 1 lit c GDPR);
d) bis zur Prüfung, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen, nachdem die betroffene Person gemäß Artikel 21 (1) DSGVO Widerspruch gegen die Verarbeitung eingelegt hat (FN162: Art 18 Abs 1 lit d GDPR).

7.5.2 Der entsprechende Nachweis muss auch dokumentierte Informationen enthalten, aus denen hervorgeht, dass die Einschränkung der Verarbeitung nur aus den folgenden Gründen aufgehoben wird (FN163: Art. 18 Abs. 2 GDPR) und nach Unterrichtung der betroffenen Person: (FN164: Art. 18 Abs. 3 GDPR)

a) Mit der Zustimmung der betroffenen Person;
b) für die Begründung, Ausübung oder Verteidigung von Rechtsansprüchen;
c) um die Rechte einer anderen natürlichen oder juristischen Person zu schützen;
d) aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaates.

7.5.3 Hat der Kunde personenbezogene Daten an Empfänger weitergegeben, so muss er über dokumentierte Informationen zur Unterrichtung der Empfänger über die Einschränkung der Verarbeitung verfügen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden (FN165: Artikel 19 GDPR). Wird ein Empfänger nicht entsprechend unterrichtet, so müssen die dokumentierten Informationen umfassende Gründe enthalten, warum eine solche Unterrichtung nicht möglich oder mit einem unverhältnismäßigen Aufwand verbunden ist. Unangemessener Aufwand kann z.B. vorliegen, wenn die Kontaktdaten der Empfänger nicht vorhanden sind und nur zu diesem Zweck neu erhoben werden müssten oder die Information - unter Berücksichtigung der Bedeutung und des Wertes der Informationen über die Empfänger für die Betroffenen - kostenintensiv wäre.

7.5.4 Der Kunde muss über dokumentierte Informationen verfügen, die belegen, dass die Verarbeitung personenbezogener Daten eingeschränkt wurde oder

wird, wenn die betroffene Person dies beantragt und einer der folgenden Aspekte gegeben ist:

a) Die Richtigkeit der personenbezogenen Daten wird während eines Zeitraums bestritten, der dem Kunden die Möglichkeit gibt, 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 Verwendung der personenbezogenen Daten verlangt;
c) der Auftraggeber die personenbezogenen Daten nicht mehr benötigt, die betroffene Person sie aber zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt.
d) bis zur Prüfung, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen, nachdem die betroffene Person gemäß Artikel 21 (1) DSGVO Widerspruch gegen die Verarbeitung eingelegt hat.

7.5.5 Der entsprechende Nachweis muss auch dokumentierte Informationen enthalten, aus denen hervorgeht, dass die Einschränkung der Verarbeitung nur aus den folgenden Gründen und nach Unterrichtung der betroffenen Person aufgehoben wird:

a) Mit der Zustimmung der betroffenen Person;
b) für die Begründung, Ausübung oder Verteidigung von Rechtsansprüchen;
c) um die Rechte einer anderen natürlichen oder juristischen Person zu schützen;
d) aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaates.

7.5.6 Hat der Kunde personenbezogene Daten an Empfänger weitergegeben, so muss er über dokumentierte Informationen verfügen, um die Empfänger über die Einschränkung der Verarbeitung zu informieren, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.

7.6 Einspruch aufgrund einer besonderen Situation

Werden personenbezogene Daten rechtmäßig auf der Grundlage eines berechtigten Interesses oder zur Erfüllung einer Aufgabe verarbeitet, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, besteht für die betroffenen Personen weiterhin die Möglichkeit, der Verarbeitung aufgrund der besonderen Situation zu widersprechen und damit die Datenverarbeitung wirksam

zu untersagen. Besondere Vorschriften über den Widerspruch gegen die Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken sowie in Fällen von Direktmarketing sind zu beachten.

7.6.1 Hat der Kunde seine Verarbeitung auf 7.1.7 (Verarbeitung zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt) oder auf 7.1.8 (Verarbeitung in Ausübung öffentlicher Gewalt) oder 7.1.9 (Verarbeitung zur Wahrung berechtigter Interessen) gestützt, muss der Kunde über dokumentierte Informationen verfügen, aus denen hervorgeht, dass die Verarbeitung personenbezogener Daten eingestellt wird, wenn die betroffene Person dies aus Gründen, die sich aus ihrer besonderen Situation ergeben, beantragt (FN 166: Art. 21 Abs. 1, 21 Abs. 3 GDPR).

7.6.2 Der Nachweis nach 7.6 (Einspruch wegen besonderer Sachlage) ist bei mindestens die folgenden Aspekte behandeln:

a) Verfahren zur Abwägung zwischen den Gründen der betroffenen Person, die sich aus ihrer besonderen Situation ergeben, und den vorrangigen berechtigten Gründen des Kunden;
b) Beurteilung, ob ein Fall von Direktmarketing oder Profiling vorliegt (FN167: Art. 21 Abs. 2 GDPR);
c) alle nach 7.1.9 (Verarbeitung zur Wahrung berechtigter Interessen) erforderlichen Aspekte.

7.7 Recht, keiner Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung, einschließlich Profiling, beruht

7.7.1 Der Kunde stellt sicher und verfügt über dokumentierte Informationen, aus denen hervorgeht, dass eine ausschließlich auf einer automatischen Verarbeitung, einschließlich Profiling, beruhende Entscheidung, die der betroffenen Person gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, nicht auf besonderen Kategorien personenbezogener Daten im Sinne von Artikel 9 Absatz 1 beruht, es sei denn, Buchstabe (a) (Verarbeitung auf der Grundlage einer ausdrücklichen Einwilligung gemäß 7.1.2.3) oder (g) (Verarbeitung aus Gründen eines wichtigen öffentlichen Interesses gemäß 7.1.7.3) von Artikel 9 (2) gilt und geeignete Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person vorhanden sind (FN168: Art. 22 Abs. 4 GDPR), und nur durchgeführt werden, wenn

a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und einem für die Verarbeitung Verantwortlichen erforderlich sind (FN169: Art 22 Abs 2 lit a GDPR);

b) nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem der für die Verarbeitung Verantwortliche unterliegt, zulässig ist und das außerdem geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person vorsieht (FN170: Art 22 Abs 2 lit b GDPR); oder
c) auf der Grundlage der ausdrücklichen Zustimmung der betroffenen Person (FN171: Art 22 Abs 2 lit c GDPR);

7.7.2 Darüber hinaus muss der Kunde über dokumentierte Informationen verfügen, die belegen, dass die automatisierte Verarbeitung, einschließlich Profiling, die zu einer Entscheidung nach 7.7.1 a) und c) führt, auf geeigneten Maßnahmen zum Schutz der Rechte der betroffenen Person beruht und Freiheiten und berechtigten Interessen, zumindest das Recht auf ein persönliches Gespräch mit dem für die Verarbeitung Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung, wenn diese auf 7.7.1 a) oder b) oder c) beruht (FN172: Art 22 Abs 3 GDPR);

7.8 Übertragbarkeit von Daten

7.8.1. Stützt der Auftraggeber die Datenverarbeitung auf die Punkte 7.1.2.1 (Verarbeitung auf der Grundlage einer Einwilligung), 7.1.3 (Verarbeitung zum Zwecke der Durchführung vorvertraglicher Maßnahmen) oder 7.1.4 (Verarbeitung zum Zwecke der Vertragserfüllung), so muss er über dokumentierte Informationen verfügen, die belegen, dass Verfahren vorhanden sind, die es den betroffenen Personen ermöglichen, personenbezogene Daten in einem strukturierten, allgemein gebräuchlichen und maschinenlesbaren Format zu erhalten und an Dritte zu übermitteln (FN173: Art. 20 Abs. 1 GDPR).

7.8.2 Die dokumentierten Informationen nach 7.8.1 (Nachweis der Möglichkeit, personenbezogene Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln) müssen auch nachgewiesene Verfahren enthalten, mit denen personenbezogene Daten der betroffenen Personen direkt an einen Dritten übermittelt werden können (FN 174: Art. 20 Abs. 2 GDPR).

7.8.3 Die dokumentierten Informationen nach 7.8.1 (Nachweis der Möglichkeit, personenbezogene Daten in einem strukturierten, gängigen und maschinenlesbaren Format an die betroffene Person zu übermitteln) oder 7.8.2 (Verfahren zur Übermittlung an Dritte) müssen auch ein System zur Abwägung der Gründe der betroffenen Person und der Rechte und Freiheiten anderer Personen enthalten (FN 174: Art. 20 Abs. 4 GDPR).

7.9 Genauigkeit der Daten

7.9.1 Genauigkeit der Verarbeitung

Der Kunde muss über dokumentierte Informationen verfügen, die belegen, dass Verfahren vorhanden sind, die sicherstellen, dass personenbezogene Daten korrekt sind und, falls erforderlich, auf dem neuesten Stand gehalten werden. Diese Verfahren sehen vor, dass je nach dem Gegenstand der Verarbeitung in regelmäßigen Abständen überprüft wird, ob Aktualisierungen erforderlich sind, und dass dem Aktualisierungsbedarf Rechnung getragen wird (FN176: Art 5 Abs 1 lit d GDPR).

7.9.2 Verfahren zur Berichtigung

Diese dokumentierten Informationen umfassen in jedem Fall Verfahren, mit denen sichergestellt wird, dass personenbezogene Daten, die in Bezug auf die Zwecke, für die sie verarbeitet werden, unrichtig sind, unabhängig von einem entsprechenden Antrag der betroffenen Person unverzüglich gelöscht oder berichtigt werden (FN177: Art 5 Abs 1 lit d GDPR).

7.9.1.1 Das Verfahren nach 7.9.2 (Berichtigungsverfahren) ermöglicht es den betroffenen Personen, die unverzügliche Berichtigung unrichtiger personenbezogener Daten zu verlangen (FN178: Artikel 16 GDPR).

7.9.1.2 Das Verfahren nach 7.9.2 (Berichtigungsverfahren) ermöglicht es den betroffenen Personen, die Vervollständigung unvollständiger personenbezogener Daten zu beantragen (FN179: Artikel 16 GDPR).

7.9.1.3 Das Verfahren nach 7.9.2.2 (Berichtigungsverfahren) ermöglicht es betroffenen Personen, eine ergänzende Erklärung aufnehmen zu lassen, so dass sichergestellt ist, dass der Auftraggeber diese Erklärung bei Bewertungen, Beurteilungen und Entscheidungen bei der Verarbeitung der personenbezogenen Daten berücksichtigt (FN180: Artikel 16 GDPR).

7.9.1.4 Hat der Kunde personenbezogene Daten an Empfänger weitergegeben, so muss er über dokumentierte Informationen verfügen, um die Empfänger über jede Berichtigung, Vervollständigung oder ergänzende Erklärung gemäß 7.9.1, 7.9.2 und 7.9 (Datenrichtigkeit) zu informieren (FN181: Artikel 19 GDPR).

7.10 Beschränkung der Speicherung

Der Grundsatz der Beschränkung der Aufbewahrung sieht vor, dass personenbezogene Daten nur so lange aufbewahrt werden dürfen, wie dies zur Erreichung des Zwecks erforderlich ist.

7.10.1 Löschungsroutinen

Der Kunde muss über dokumentierte Informationen verfügen, die belegen, dass Verfahren vorhanden sind, die sicherstellen, dass personenbezogene Daten in einer Form aufbewahrt werden, die die Identifizierung einer betroffenen Person nicht länger zulässt, als es für die in 7.1.1 lit d) (Rechtmäßigkeit) genannten Zwecke erforderlich ist (FN181: Art 5 Abs 1 lit e GDPR).

7.10.2 Lagerzeiten

Die dokumentierten Informationen nach 7.10 (Speicherbegrenzung) sollen Fristen für die Löschung personenbezogener Daten vorsehen - es sei denn, eine Löschung ist nicht möglich, weil z.B. Archivierungszwecke nach Art. 89 (1) DSGVO verfolgt werden (FN183: Art 30 Abs 1 lit f GDPR).

7.10.3 Konzept der Löschung

Die Informationen nach 7.10.1 (Löschroutinen) müssen ein Regelwerk zur Löschung personenbezogener Daten enthalten, das sich an der DIN-66398 oder einer vergleichbaren Regelung (FN184: DIN 66398:2016-05 i.d.g.F., Leitfaden zur Entwicklung eines Löschkonzeptes mit Ableitung von Löschfristen für personenbezogene Daten) orientiert und die in der Norm beschriebenen Verfahren, Löschregeln und Strukturen beinhaltet.

7.11 Recht auf Löschung der personenbezogenen Daten

Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der für die Verarbeitung Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, wenn einer der in Artikel 17 Absatz 1 DSGVO genannten Gründe vorliegt.

7.11.1 Der Kunde muss über dokumentierte Informationen verfügen, die belegen, dass Verfahren vorhanden sind, die sicherstellen, dass personenbezogene Daten auf erneute Anfrage der betroffenen Person unverzüglich gelöscht werden, wenn eine Anspruchsvoraussetzung erfüllt ist (FN185: Art 17 Abs 1 lit a bis f DSGVO und kein außergewöhnlicher Umstand vorliegt (FN186: Art 17 Abs 3 lit a bis e GDPR).

7.11.2 Das Verfahren unter 7.11 (Recht auf Löschung personenbezogener Daten) enthält in jedem Fall das System zur Abwägung der Gründe der betroffenen Person und des Rechts auf freie Meinungsäußerung (FN187: Art 9 GDPR, 17 Abs 3 lit a GDPR) sowie des Interesses des Auftraggebers an der Speicherung zur Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen (FN188: Art 17 Abs 3 lit e DSGVO).

7.11.3 Hat der Kunde personenbezogene Daten an Empfänger weitergegeben, muss er über dokumentierte Informationen verfügen, um die Empfänger über die Löschung gemäß 7.11 (Recht auf Löschung der personenbezogenen Daten) (FN189: Artikel 19 GDPR) zu informieren.

7.11.4 Sofern der Kunde personenbezogene Daten veröffentlicht und deren Löschung gemäß 7.11 (Recht auf Löschung personenbezogener Daten) angeordnet hat, muss er über dokumentierte Informationen verfügen, die

sicherstellen, dass Dritte darüber informiert werden, dass ein Betroffener die Löschung aller Verknüpfungen zu den personenbezogenen Daten sowie von Kopien oder Replikationen beantragt hat (FN190: Art. 17 Abs. 2 GDPR).

7.11.5 Das Verfahren nach Nummer 7.11 (Recht auf Löschung personenbezogener Daten) umfasst in jedem Fall die folgenden Aspekte:

a) Ermittlung der verfügbaren Technologien und der Implementierungskosten für geeignete Maßnahmen zur Benachrichtigung Dritter (FN191: Art. 17 Abs. 2 GDPR);
b) Angabe der Folgen für die Rechte und Freiheiten der betroffenen Person, falls Dritte nicht über die Löschung informiert werden;
c) Abwägung der Interessen des Auftraggebers an lediglich technisch und wirtschaftlich realisierbaren Maßnahmen mit den Interessen der betroffenen Person an der Löschung personenbezogener Daten bei Dritten.

7.12 Integrität und Vertraulichkeit

Der Grundsatz der Integrität soll sicherstellen, dass die verarbeiteten personenbezogenen Daten nicht unrechtmäßig absichtlich oder versehentlich geändert oder gelöscht werden. Der Grundsatz der Vertraulichkeit soll sicherstellen, dass personenbezogene Daten nicht für Personen zugänglich sind, die nicht zum Zugriff auf die Daten berechtigt sind.

Der Kunde hat Informationen gemäß Punkt 8 (technische und organisatorische Maßnahmen) dokumentiert, die belegen, dass Verfahren vorhanden sind, die sicherstellen, dass personenbezogene Daten in einer Weise verarbeitet werden, die ihre Integrität und Vertraulichkeit gewährleistet (FN192: Art 5 Abs 1 lit f GDPR).

7.13 Minimierung der Datenmenge

Der Grundsatz der Datenminimierung soll sicherstellen, dass die Verarbeitung personenbezogener Daten dem Zweck angemessen und sachdienlich ist und sich auf das für die Zwecke der Verarbeitung erforderliche Maß beschränkt.

Der Kunde muss über dokumentierte Informationen verfügen, die belegen, dass Verfahren vorhanden sind, die sicherstellen, dass personenbezogene Daten angemessen, relevant und auf die Zwecke der Verarbeitung beschränkt sind, um die Verarbeitung personenbezogener Daten zu vermeiden, die für die Erreichung der Zwecke der Verarbeitung nicht erforderlich sind (FN193: Art 5 Abs 1 lit c GDPR.

7.14 Datenschutz durch Technik und Datenschutz durch Voreinstellungen

Der Grundsatz des "eingebauten Datenschutzes" soll sicherstellen, dass der für die Verarbeitung Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der von der Verarbeitung ausgehenden Risiken für die Rechte und Freiheiten natürlicher Personen sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst geeignete technische und organisatorische Maßnahmen, wie z. B. die Pseudonymisierung, durchführt. Die Kommission trifft technische und organisatorische Maßnahmen, wie z. B. die Pseudonymisierung, die darauf abzielen, Datenschutzgrundsätze wie die Datenminimierung wirksam umzusetzen und die erforderlichen Sicherheitsvorkehrungen in die Verarbeitung einzubeziehen, um die Anforderungen dieser Verordnung zu erfüllen und die Rechte der betroffenen Personen zu schützen. Gemäß dem Grundsatz des Datenschutzes durch Voreinstellungen hat der für die Verarbeitung Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, um sicherzustellen, dass standardmäßig nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den spezifischen Zweck der Verarbeitung erforderlich ist. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherdauer und ihre Zugänglichkeit. Insbesondere muss durch solche Maßnahmen sichergestellt werden, dass personenbezogene Daten nicht durch Voreinstellungen einer unbestimmten Zahl von natürlichen Personen ohne Zutun des Einzelnen zugänglich gemacht werden. Dieser Grundsatz gewährleistet somit unter anderem die Einhaltung des Grundsatzes der Datenminimierung.

7.14.1 Datenschutz durch Design

Der Auftraggeber muss über dokumentierte Informationen verfügen, die belegen, dass Verfahren in Bezug auf das Ziel der Auswertung vorhanden sind und angewandt werden, um sicherzustellen, dass unter Berücksichtigung des Stands der Technik, der Kosten der Umsetzung und der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie der unterschiedlichen Wahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen - wie z. B. Pseudonymisierung - sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der tatsächlichen Verarbeitung umgesetzt werden. Es müssen geeignete technische und organisatorische Maßnahmen - wie z.B. Pseudonymisierung - sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der tatsächlichen Verarbeitung getroffen werden (FN194: Art. 25 Abs. 1 DSGVO, siehe hierzu auch die Leitlinien 4/2019 des Europäischen Datenschutzausschusses). Für die Auslegung dieses Kriteriums sind die Leitlinien der EDPB Guidelines 4/2019 zu Art 25 Data Protection by Design and by Default, Version 2.0, zu berücksichtigen.

7.14.2 Standardmäßiger Datenschutz:

Der Kunde muss über dokumentierte Informationen verfügen, die belegen, dass Verfahren in Bezug auf das Ziel der Bewertung vorhanden sind und angewandt werden, um sicherzustellen, dass standardmäßig nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen Verarbeitungszweck erforderlich ist (FN195: Art. 25 Abs. 2 GDPR).

Aus den dokumentierten Informationen muss auch hervorgehen, dass sich die getroffenen technischen und organisatorischen Maßnahmen auf die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherdauer und ihre Zugänglichkeit beziehen und dass die Standardeinstellungen personenbezogene Daten nicht einer unbestimmten Zahl von natürlichen Personen zugänglich machen.

7.15 Zweckbindung

Der Grundsatz der Zweckbindung soll sicherstellen, dass personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; die Weiterverarbeitung zu im öffentlichen Interesse liegenden Archivierungszwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken ist nicht als unvereinbar mit dem ursprüngliche Zwecke gemäß Artikel 89 (1) GDPR.

7.15.1 Der Kunde muss über dokumentierte Informationen verfügen, um sicherzustellen, dass personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden (FN196: Art 5 Abs 1 lit b GDPR). Eine solche dokumentierte Information muss nicht nur eine Begründung enthalten, warum die vom Evaluierungsziel erfassten Verarbeitungszwecke festgelegt, eindeutig und rechtmäßig sind, sondern auch eine verbindliche interne Politik in Bezug auf eine mögliche Verwendung der für diese Verarbeitungszwecke erhobenen personenbezogenen Daten für verbotene Zwecke.

7.15.2 Erfolgt eine Weiterverwendung zu im öffentlichen Interesse liegenden Archivierungszwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken, muss der Auftraggeber über dokumentierte Informationen verfügen, die das Vorliegen der jeweiligen Zwecke belegen und zeigen, dass die Verarbeitung für diese Zwecke erforderlich ist. Aus diesen dokumentierten Informationen muss hervorgehen, warum pseudonymisierte Daten nicht ausreichen, um diese Zwecke zu erreichen. Darüber hinaus müssen die dokumentierten Informationen belegen, dass die implementierten Schutzmaßnahmen für die Rechte und Freiheiten der betroffenen Personen angemessen sind,

insbesondere um den Grundsatz der Datenminimierung zu gewährleisten (FN197: Art. 89 Abs. 1 GDPR).

7.15.3 Wenn der Kunde die Rechte der betroffenen Personen in Bezug auf die Verarbeitung personenbezogener Daten gemäß Artikel 89 (2) und (3) DSGVO auf der Grundlage des jeweiligen Unionsrechts oder des Rechts der Mitgliedstaaten nicht einhalten möchte, muss der Kunde das Vorhandensein dokumentierter Informationen sicherstellen, die Gründe für die Einhaltung solcher Ausnahmen mit den Bedingungen und Garantien unter 7.15.2. und für ihre Notwendigkeit für die Erfüllung des jeweiligen Zwecks sowie dafür enthalten, warum die vollständige Einhaltung des eingeschränkten Rechts der betroffenen Personen die Erreichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen würde.

8 Technische und organisatorische Maßnahmen

Technische und organisatorische Maßnahmen sind alle Handlungen und Vorkehrungen, die dazu beitragen, personenbezogene Daten datenschutzkonform zu verarbeiten. Technische Maßnahmen sind Maßnahmen, die auf dem Einsatz von Technik beruhen. Organisatorische Maßnahmen betreffen strukturelle Vorkehrungen und/oder Arbeitsanweisungen.

Auf der Grundlage einer Risikoanalyse nach 6.2.2 oder einer Datenschutz- Folgenabschätzung nach 6.2.3, die einer kontinuierlichen Bewertung nach 6.2.6 unterliegt, hat der Auftraggeber alle Maßnahmen umzusetzen, die den identifizierten Risiken und dem spezifischen Datenverarbeitungskontext in Bezug auf den Evaluationsgegenstand entsprechen und geeignet sind, das angemessene Schutzniveau zu gewährleisten. Anhang I (einschließlich seiner Anlage) enthält als integraler Bestandteil dieser Zertifizierungskriterien technische und organisatorische Maßnahmen, die der Auftraggeber mindestens umsetzen muss, um einen angemessenen Schutz der Rechte und Freiheiten der betroffenen Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten.

Für den Fall, dass bestimmte Maßnahmen des Anhangs I nicht umgesetzt werden, muss der Antragsteller der Zertifizierungsstelle angemessene und ausführliche Unterlagen zur Begründung dieser Entscheidung vorlegen. Für jede nicht umgesetzte Sicherheitsmaßnahme sind in den Unterlagen die Gründe anzugeben, warum der Antragsteller sich gegen ihre Umsetzung entschieden hat, einschließlich einer Bewertung des damit verbundenen Risikominderungspotenzials und einer Kosten-Nutzen-Analyse. Auf Verlangen der Zertifizierungsstelle muss der Antragsteller eine Liste der nicht umgesetzten Maßnahmen des Anhangs I vorlegen.

Die Nichtdurchführung von Sicherheitsmaßnahmen darf nicht mit der Entscheidung des Antragstellers begründet werden, ein höheres Restrisiko in Kauf zu nehmen. Zu den akzeptablen Begründungen für die Nichtdurchführung einer Sicherheitsmaßnahme gehören die folgenden:

- Die Maßnahme hat keine Auswirkungen auf das Restrisiko der Datenverarbeitung;
- Die Maßnahme ist nicht auf den spezifischen Kontext der Datenverarbeitung anwendbar.

Der spezifische Datenverarbeitungskontext kann insbesondere davon abhängen:

a) Anzahl, Ausbildung und Erfahrung des an der Verarbeitung beteiligten Personals,
b) den Umfang der Verarbeitung in Bezug auf die Zahl der betroffenen Personen und die Kategorien der verarbeiteten personenbezogenen Daten,
c) die Schutzbedürftigkeit der betroffenen Personen und der über sie gespeicherten Datenkategorien und
d) die Gegebenheiten vor Ort sowie die verwendeten Verarbeitungssysteme und Technologien

9 Übermittlung von personenbezogenen Daten in ein Drittland

Die DSGVO setzt einen Rahmen für die Verarbeitung personenbezogener Daten innerhalb des Europäischen Wirtschaftsraums. Dies bedeutet, dass jede Übermittlung personenbezogener Daten innerhalb des Europäischen Wirtschaftsraums einer innerstaatlichen Übermittlung gleichkommt. Für alle anderen Länder der Welt (=Drittländer) geht die DSGVO von einem niedrigeren Schutzniveau für personenbezogene Daten aus, so dass entweder die Angemessenheit von der Europäischen Kommission festgestellt werden muss oder die für die Verarbeitung Verantwortlichen, die eine Übermittlung in ein Drittland vornehmen wollen, zusätzliche Maßnahmen ergreifen müssen, um das erforderliche Schutzniveau gemäß Kapitel V der DSGVO zu gewährleisten, es sei denn, die angemessenen Garantien gemäß Artikel 46 DSGVO bleiben in Bezug auf die Übermittlung in ein Drittland wirksam oder es gilt eine Ausnahmeregelung gemäß Artikel 49 DSGVO. Folglich müssen die folgenden Kriterien erfüllt sein, wenn die Verarbeitung personenbezogener Daten im Rahmen des Ziels der Evaluierung die Übermittlung in ein Drittland beinhaltet; die vorliegenden Kriterien sind jedoch kein Mechanismus, der eine angemessene Garantie gemäß Art 46 (2) lit f DSGVO für die internationale Übermittlung von Daten darstellen kann:

9.1 Anforderungen

9.1.1. Die folgenden Kriterien sind nur anwendbar, wenn eine Übermittlung personenbezogener Daten in ein Drittland in das Zielgebiet der Evaluierung fällt. Zu diesem Zweck führt der Kunde ein Verzeichnis aller Übermittlungen personenbezogener Daten in Drittländer, die unter das Ziel der Evaluierung fallen, und hält dieses Verzeichnis auf dem neuesten Stand.

9.1.2 Voraussetzung für die Übermittlung personenbezogener Daten in Drittländer ist, dass der Auftraggeber die Anforderungen dieser Zertifizierungskriterien erfüllt, insbesondere die Anforderungen an die Grundsätze für die Verarbeitung personenbezogener Daten und die Rechtmäßigkeit der Verarbeitung gemäß Kapitel 0. Sind diese nicht erfüllt, ist die Übermittlung rechtswidrig und wird ausgesetzt, wenn z.B. keine Rechtsgrundlage im Sinne von Art. 6 Abs. 1 DSGVO besteht.

9.1.3 Bei der Umsetzung der in Kapitel 9 der vorliegenden Zertifizierungskriterien festgelegten Anforderungen berücksichtigt der Kunde die in den Empfehlungen 01/2020 des EDPB zu Maßnahmen, die Übermittlungsmechanismen ergänzen, um die Einhaltung des EU-Niveaus des Schutzes personenbezogener Daten zu gewährleisten, Schritt 1 bis Schritt 6, dargestellten Prüfungsschritte ("Fahrplan"). Ebenso die einschlägige Rechtsprechung des Europäischen Gerichtshofs und der zuständigen nationalen Aufsichtsbehörde und/oder der zuständigen nationalen Gerichte zum Thema Kapitel V der Datenschutz-Grundverordnung muss beachtet werden.

9.1.4 Der Kunde gewährleistet die Einhaltung von Kapitel V der DSGVO bei allen Übermittlungen personenbezogener Daten in Drittländer, die unter das Ziel der Bewertung fallen. In Übereinstimmung mit Kapitel V der DSGVO muss der Kunde daher überprüfen, dass jede derartige Übermittlung auf einem der folgenden Übermittlungsmechanismen beruht:

a) Angemessenheitsentscheidungen gemäß Artikel 45 DSGVO (siehe Punkt 9.3);
b) Verbindliche unternehmensinterne Vorschriften gemäß Art. 46 (2) lit b und Art. 47 DSGVO (siehe Punkt 9.4 für Details); Verbindliche unternehmensinterne Vorschriften gemäß Art. 46 (2) lit b und Art. 47 DSGVO (siehe Punkt 9.4 für Details);
c) Standard-Datenschutzklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO (Einzelheiten siehe Punkt 9.5); Standard-Datenschutzklauseln gemäß Art. 46 (2) lit c GDPR (siehe Punkt 9.5 für Details);

d) Standard-Datenschutzklauseln einer Aufsichtsbehörde gemäß Art 46 (2) lit d DSGVO (siehe Punkt 9.6 für Details); Standard-Datenschutzklauseln einer Aufsichtsbehörde gemäß Art 46 (2) lit d DSGVO (siehe Punkt 9.6 für Details);
e) Genehmigte Verhaltenskodizes gemäß Art. 46 (2) lit. e DSGVO (siehe Punkt 9.7 für Details);
f) Anerkannte Zertifizierungsmechanismen gemäß Art 46 (2) lit e DSGVO (Einzelheiten siehe Punkt 9.8); Anerkannte Zertifizierungsmechanismen g e m ä ß Art 46 (2) lit e DSGVO (Einzelheiten siehe Punkt 9.8);
g) Genehmigte Vertragsklauseln gemäß Art. 46 (3) lit. a DSGVO (siehe Punkt 9.9 für Details);
h) Ausnahmeregelungen für besondere Situationen gemäß Artikel 49 DSGVO (siehe Punkt 9.10 und 9.12 für Einzelheiten).

Alle anderen Übermittlungsmechanismen des Kapitels V der Datenschutz-Grundverordnung, die oben nicht aufgeführt sind, können im Rahmen der vorliegenden Zertifizierungskriterien nicht berücksichtigt werden. Darüber hinaus stellen die vorliegenden Zertifizierungskriterien keinen Mechanismus dar, der eine angemessene Schutzmaßnahme gemäß Artikel 42 und Artikel 46 (2) Buchstabe f DSGVO darstellen kann.

9.2 Umsetzung und Dokumentation der rechtlichen Grundlagen der Datenübermittlung

9.2.1 Der Kunde bewertet und dokumentiert die Gründe für die Auswahl, Bewertung und Wirksamkeit der in Punkt 9.1.2 genannten Übermittlungsmechanismen (einschließlich ergänzender Maßnahmen, falls erforderlich) im Falle einer (geplanten) Übermittlung personenbezogener Daten in ein Drittland. Der Kunde konsultiert und dokumentiert den Rat des Datenschutzbeauftragten im Hinblick auf diese Bewertung, falls er dazu bestellt wird.

Diese Bewertung ist auf dem neuesten Stand zu halten und muss mindestens die nachstehenden Aspekte abdecken; falls diese Aspekte die Durchführung bestimmter Maßnahmen durch den Kunden erfordern, ist die Umsetzung (FN198: Dies gilt zumindest für die nachstehenden Buchstaben b) und d) nachzuweisen und ebenfalls zu dokumentieren:

a) Bestimmung des Drittlandes oder der Drittländer (einschließ- de
Empfänger), in das/die personenbezogene Daten gemäß dem de
Bewertung (siehe auch Punkt 9.1.1) übermittelt werden (so-

b) C

c) Wenn unter lit b) die Anwendung eines Übermittlungsverfahrens nach Art. 45 DSGVO (Angemessenheitsbeschluss) festgestellt wurde, Feststellung der Anwendbarkeit des Angemessenheitsbeschlusses auf die Übermittlung(en) personenbezogener Daten;

d) Wurde unter lit b) die Anwendung eines Übermittlungsmechanismus nach Art 46 bis 47 DSGVO (angemessene Garantien, einschließlich verbindlicher unternehmensinterner Vorschriften) festgelegt, muss der Kunde sowohl die Rechtslage als auch die Praxis der Behörden in dem jeweiligen Drittland (oder den jeweiligen Ländern) bewerten und analysieren, um festzustellen, ob die angemessenen Garantien in der Praxis eingehalten werden können und ein angemessenes Schutzniveau für die betroffenen Personen in der EU bieten, deren personenbezogene Daten von der Übermittlung in ein Drittland betroffen sind.

Ein Schutzniveau ist angemessen, wenn die übermittelten personenbezogenen Daten
in dem Drittland ein Schutzniveau, das im Wesentlichen dem im EWR gewährleisteten Schutzniveau entspricht. Bei der Bewertung der Rechtslage und der Praxis der Behörden in dem jeweiligen Drittland, auf die im obigen Absatz Bezug genommen wird, ist daher zu prüfen, ob die europäischen Grundgarantien im Rahmen der Überwachungsmaßnahmen der Behörden in diesem Drittland eingehalten werden, die in Folgendem bestehen:

i) Datenverarbeitung sollte auf klaren, präzisen und zugänglichen Regeln beruhen;
II) Notwendigkeit und Verhältnismäßigkeit im Hinblick auf die verfolgten legitimen Ziele müssen nachgewiesen werden;
III) ein unabhängiger Kontrollmechanismus sollte vorhanden sein und
IV) dem Einzelnen müssen wirksame Rechtsmittel zur Verfügung stehen.

Die Empfehlungen 2/2020 des Europäischen Datenschutzausschusses zu den europäischen Grundgarantien für Überwachungsmaßnahmen in ihrer jeweils geltenden Fassung oder eine sie ersetzende Empfehlung sind bei der Durchführung der genannten Bewertung zu berücksichtigen, insbesondere (aber nicht ausschließlich) im Anhang 2.

e) Kommt die Prüfung nach lit. d) zu dem Ergebnis, dass der festgelegte Übermittlungsmechanismus kein im Wesentlichen gleichwertiges Schutzniveau wie das im EWR garantierte in dem Drittland bietet, muss der Kunde

- nach einer dokumentierten Bewertung - technische und - falls erforderlich -
- begleitende organisatorische und vertragliche Zusatzmaßnahmen, zusätzlich zu den bereits durch den festgelegten Übermittlungsmechanismus gewährleisteten Maßnahmen, um die Risiken für die Verarbeitung personenbezogener Daten, die sich aus der Bewertung des Drittlandes in Bezug auf seine Gesetze und Praktiken ergeben, wirksam zu beheben. Eine wirksame Abhilfe wird durch ergänzende Maßnahmen erreicht, wenn sie - unter Berücksichtigung des festgelegten Übermittlungsmechanismus - die in dieser Bewertung festgestellten spezifischen Mängel beheben und dadurch sicherstellen, dass das durch die DSGVO garantierte Schutzniveau nicht untergraben wird, dass die festgelegten angemessenen Garantien eingehalten werden können und dass die Rechtsvorschriften und Praktiken des Drittlandes diese ergänzenden Maßnahmen nicht beeinträchtigen, so dass ihre Wirksamkeit verhindert wird. Empfehlungen 1/2020 zu Maßnahmen zur Ergänzung der Übermittlungsmechanismen zur Sicherstellung des Niveaus der Bei der Überprüfung der Auswahl und der Wirksamkeit der vom Kunden ergriffenen ergänzenden Maßnahmen ist die Empfehlung des Europäischen Datenschutzausschusses zum Schutz personenbezogener Daten nach dem Unionsrecht in ihrer jeweils geltenden Fassung oder eine sie ersetzende Empfehlung des EDSB zu berücksichtigen.

f) Jegliche (zusätzlichen) Bestimmungen oder Bedingungen des Übertragungsmechanismus dürfen weder direkt

noch indirekt im Widerspruch zur Gewährleistung eines angemessenen Schutzniveaus stehen, das durch die vom Kunden angewandten und nachgewiesenen angemessenen Schutzmaßnahmen und/oder ergänzenden Maßnahmen garantiert wird.

g) Wenn unter Buchstabe b) die Anwendung einer Ausnahmeregelung für bestimmte Situationen gemäß Artikel 49 DSGVO festgelegt wurde, die ausführliche Begründung des Vorliegens der jeweiligen Bedingungen im Zusammenhang mit der konkreten Übermittlung oder einer Reihe von Übermittlungen;

h) Verfahren des Kunden zur Gewährleistung einer mindestens jährlichen Überwachung und Überprüfung, gegebenenfalls in Zusammenarbeit mit dem Datenimporteur, der Anwendbarkeit des Angemessenheitsbeschlusses, der Wirksamkeit der geeigneten Garantien (einschließlich etwaiger zusätzlicher Maßnahmen) sowie der Anwendbarkeit einer Ausnahmeregelung gemäß Artikel 49 DSGVO. Die Überprüfung der Wirksamkeit geeigneter Garantien (einschließlich etwaiger zusätzlicher Maßnahmen) muss eine Bewertung etwaiger Änderungen der rechtlichen und praktischen Situation in den Drittländern seit der letzten Überprüfung sowie der Auswirkungen etwaiger Änderungen auf die Gewährleistung eines angemessenen Schutzniveaus umfassen.

9.2.2 Die Anwendbarkeit eines Angemessenheitsbeschlusses auf die Übermittlung personenbezogener Daten in das Drittland, die Übereinstimmung der Übermittlung mit den vom Auftraggeber festgelegten angemessenen

Garantien sowie deren faktische Umsetzung und rechtliche Existenz, die Umsetzung und Wirksamkeit etwaiger zusätzlicher Maßnahmen des Auftraggebers zur Gewährleistung eines angemessenen Schutzniveaus sowie die Anwendbarkeit einer Ausnahmeregelung nach Art. 49 DSGVO müssen vom Auftraggeber nachgewiesen und von der Zertifizierungsstelle überprüft werden (siehe auch 2.10 und 2.12).

9.3 Datenübermittlung auf der Grundlage einer Angemessenheitsentscheidung

9.3.1 Wenn der Kunde die Übermittlung auf das Vorliegen eines Angemessenheitsbeschlusses der Europäischen Kommission für das Drittland gemäß Art. 45 DSGVO stützt, muss der Kunde zusätzlich die folgenden Nachweise erbringen:

a) Dokumentation der Fassung der Angemessenheitsentscheidung;
b) Datum der ersten Überprüfung der Gültigkeit der Angemessenheitsentscheidung im Amtsblatt der Europäischen Union;
c) Datum der nächsten Überprüfung der Anwendbarkeit und Gültigkeit der Angemessenheitsentscheidung.

9.3.2. Der Kunde muss die Maßnahmen dokumentieren, die im Hinblick auf Übermittlungen auf der Grundlage eines Angemessenheitsbeschlusses ergriffen werden, wenn dieser Angemessenheitsbeschluss widerrufen wird. Solche Maßnahmen können z. B. in der Aussetzung oder Beendigung der Übermittlung sowie in der Einrichtung eines anderen Übermittlungsmechanismus bestehen.

9.4 Verbindliche Unternehmensregeln

Verbindliche Unternehmensregeln sind Regeln einer Unternehmensgruppe, die ein angemessenes Schutzniveau für die interne Übermittlung personenbezogener Daten auf Dauer gewährleisten sollen. Solche Datenschutzregeln gewährleisten ein globales Schutzniveau innerhalb einer Unternehmensgruppe.

9.4.1 Stützt der Auftraggeber die Übermittlung auf genehmigte verbindliche unternehmensinterne Vorschriften (BCR) gemäß Art. 46 Abs. 2 lit. b DSGVO,

so muss der Auftraggeber über die folgenden dokumentierten Informationen verfügen:

a) Dokumentation der Version der BCR;
b) Überprüfung des Anwendungsbereichs der BCR für die jeweilige Übertragung;
c) Wie betroffene Personen über die BCR und die Aspekte gemäß Art 47 (2) lit d, e, f DSGVO zusätzlich zu den Bestimmungen gemäß Art 13 und Art 14 DSGVO informiert werden (FN199: Art 47 Abs 2 lit g GDPR);
d) BCR-Beschwerdeverfahren und
e) durchsetzbare Rechte für die betroffenen Personen (FN200: Art 47 Abs 2 lit i GDPR).

9.4.2 Der Kunde muss über standardisierte Verfahren verfügen, die sicherstellen, dass die Verpflichtung nach 9.4.1 lit b), c), d) (Übermittlung personenbezogener Daten in ein Drittland) mindestens alle zwölf Monate überprüft und an die aktuelle Situation angepasst wird.

9.5 Standard-Datenschutzklauseln der Europäischen Kommission

Die Europäische Kommission hat Standard-Datenschutzklauseln veröffentlicht, deren Vereinbarung zwischen dem Datenexporteur in der EU und einem Datenimporteur in einem Drittland ein angemessenes Schutzniveau beim Datenimporteur gewährleisten soll.

9.5.1 Soweit der Auftraggeber den Standarddatenschutzklauseln der Europäischen Kommission gemäß Art. 46 Abs. 2 lit. c DSGVO zugestimmt hat, stehen dem Auftraggeber die folgenden zusätzlichen dokumentierten Informationen zur Verfügung:

a) Festlegung des Durchführungsrechtsakts der Europäischen Kommission;
b) Datum der Zustimmung zur Anwendung der Standarddatenschutzklauseln gemäß Buchstabe a);
c) Festlegung eines Moduls der anzuwendenden Standarddatenschutzklauseln;
d) Bewertung des Datenimporteurs und der Rechtslage im Sitzland des Datenimporteurs, um festzustellen, ob der Datenimporteur in der Lage ist, die Verpflichtungen aus den Standarddatenschutzklauseln zu erfüllen, und - falls dies nicht der Fall ist - ob zusätzliche Maßnahmen erforderlich sind (Folgenabschätzung für den Datentransfer).

9.5.2 Der Kunde verfügt über standardisierte Verfahren, die sicherstellen, dass die Dokumentation gemäß 9.5.1 mindestens alle zwölf Monate überprüft und an zwischenzeitliche Änderungen angepasst wird.

9.5.3 Für den Fall, dass die Anwendung des ermittelten Instruments (zumindest) zweifelhaft erscheint, verfügt der Kunde über standardisierte Verfahren, wie er mit diesem Umstand umgehen kann. Diese Verfahren müssen mindestens die folgenden Aspekte abdecken:

a) Feste Berichts- und Entscheidungsstrukturen, um zu entscheiden, ob die Datenübermittlung (noch) rechtmäßig ist oder nicht;
b) Verfahren zur sofortigen Aussetzung der Datenübermittlung im Hinblick auf die konkrete Datenverarbeitung;
c) Verfahren für Identifizierung von und Umsetzung zusätzlicher geeignete Maßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus;
d) Verfahren zur Beendigung der Datenübermittlung im Hinblick auf die konkrete Datenverarbeitung;
e) Verfahren zur Unterrichtung der Aufsichtsbehörde gemäß der Vereinbarung.

9.6 Standard-Datenschutzklauseln einer Aufsichtsbehörde

Zusätzlich zu den EU-Standard-Datenschutzklauseln kann jede Aufsichtsbehörde auch eigene Standard-Datenschutzklauseln ausarbeiten. Nach Genehmigung durch die Europäische Kommission können diese Vertragsklauseln zwischen einem Datenexporteur in der EU und einem Datenimporteur in einem Drittland ebenfalls verwendet werden, um ein angemessenes Schutzniveau zu gewährleisten.

9.6.1 Soweit der Auftraggeber Standarddatenschutzklauseln einer Aufsichtsbehörde gemäß Art. 46 Abs. 2 lit. d DSGVO vereinbart hat, stehen dem Auftraggeber zusätzlich die folgenden dokumentierten Informationen zur Verfügung:

a) Festlegung der spezifischen Standarddatenschutzklauseln und der zuständigen Aufsichtsbehörde;
b) Datum der Zustimmung zur Anwendung der Standarddatenschutzklauseln gemäß Buchstabe a).

9.6.2 Der Kunde verfügt über standardisierte Verfahren, die sicherstellen, dass die Dokumentation gemäß 9.6.1 mindestens alle zwölf Monate überprüft und an zwischenzeitliche Änderungen angepasst wird.

9.6.3 Der Kunde muss über standardisierte Verfahren verfügen, um mit folgenden Umständen umgehen zu können die zumindest gewisse Zweifel an der Anwendung des ermittelten Instruments aufkommen lassen. Diese Verfahren müssen zumindest die folgenden Aspekte abdecken:

a) Feste Berichts- und Entscheidungsstrukturen, um zu entscheiden, ob die Datenübermittlung (noch) rechtmäßig ist oder nicht;
b) Verfahren zur sofortigen Aussetzung der Datenübermittlung im Hinblick auf die konkrete Datenverarbeitung;
c) Verfahren für Identifizierung von und Umsetzung zusätzlicher geeignete Maßahmen zur Gewährleistung eines angemessenen Datenschutzniveaus;
d) Verfahren zur Beendigung der Datenübermittlung im Hinblick auf die konkrete Datenverarbeitung;
e) Verfahren zur Unterrichtung der Aufsichtsbehörde gemäß der Vereinbarung.

9.7 Genehmigte Verhaltenskodizes

Verhaltenskodizes sollen die branchen- und sektorspezifische Selbstregulierung stärken und damit die DSGVO branchenspezifisch konkretisieren. Sind genehmigte Verhaltenskodizes für die Übermittlung personenbezogener Daten in Drittstaaten vorgesehen und genehmigt, kann eine solche Datenübermittlung in Verbindung mit einer rechtsverbindlichen und durchsetzbaren Verpflichtung des Datenimporteurs im Drittstaat unter Berufung auf die Verhaltenskodizes erfolgen.

9.7.1 Sofern der Kunde einen genehmigten Verhaltenskodex gemäß Art. 46 Abs. 2 lit. e DSGVO als Übermittlungsmechanismus festgelegt hat, stehen dem Kunden die folgenden zusätzlichen dokumentierten Informationen zur Verfügung:

a) Referenz und Datum der Allgemeinen Gültigkeitserklärung der Europäischen Kommission;
b) Anwendungsbereich der Verhaltenskodizes und Darstellung der Anwendbarkeit für die konkrete Verbringung in ein Drittland;
c) Nachweis, dass der Datenimporteur den genehmigten Verhaltenskodizes unterliegt;
d) Aufzeichnungen über das Intervall und die Ergebnisse von Überwachungsaudits.

9.7.2 Der Kunde verfügt über standardisierte Verfahren, die sicherstellen, dass die Dokumentation nach 9.7.1 lit. c), d) (Nachweis der Unterordnung des Datenimporteurs unter die genehmigten Verhaltenskodizes, Aufzeichnung der Überwachungsaudits) mindestens alle zwölf Monate überprüft und an zwischenzeitliche Änderungen angepasst wird.

9.7.3 Der Kunde muss über standardisierte Verfahren verfügen, um mit Umständen umgehen zu können, die zumindest gewisse Zweifel an der Anwendung des ermittelten Instruments aufkommen lassen. Diese Verfahren müssen zumindest die folgenden Aspekte abdecken:

a) Feste Berichts- und Entscheidungsstrukturen, um zu entscheiden, ob die Datenübermittlung (noch) rechtmäßig ist oder nicht;
b) Verfahren zur sofortigen Aussetzung der Datenübermittlung im Hinblick auf die konkrete Datenverarbeitung;
c) Verfahren für Identifizierung von und Umsetzung zusätzlicher geeignete Maßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus;
d) Verfahren zur Beendigung der Datenübermittlung im Hinblick auf die konkrete Datenverarbeitung;
e) Verfahren zur Unterrichtung der Aufsichtsbehörde gemäß der Vereinbarung.

9.8 Anerkannter Zertifizierungsmechanismus

Mit Hilfe von Bescheinigungen können angemessene Garantien für Datenexporte in Drittländer nachgewiesen werden. Dies ist jedoch nur in Verbindung mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Datenimporteurs im Drittland möglich.

9.8.1 Sofern der Auftraggeber einen zugelassenen Zertifizierungsmechanismus gemäß Art. 46 Abs. 2 lit. f DSGVO als Übermittlungsmechanismus identifiziert hat, stehen dem Auftraggeber die folgenden zusätzlichen dokumentierten Informationen zur Verfügung:

a) Benennung der genehmigten Zertifizierungskriterien;
b) Bezugnahme auf die Stellungnahme des Europäischen Datenschutzausschusses;
c) Verfahrensnummer des Genehmigungsbescheids der zuständigen Aufsichtsbehörde;
d) Umfang der Zertifizierungskriterien und Darstellung der Anwendbarkeit für die spezifische Verbringung in ein Drittland;

e) Nachweis einer entsprechenden Konformitätsbestätigung durch den Datenimporteur;
f) Aufzeichnungen über das Intervall und die Ergebnisse von Überwachungs- und Neuzertifizierungsaudits.

9.8.2 Der Kunde verfügt über standardisierte Verfahren, die sicherstellen, dass die Dokumentation nach 9.8.1 lit. d), e), f) (Umfang der Zertifizierungskriterien sowie Vorlage zur Übermittlung in ein Drittland, Konformitätsbestätigung des Datenimporteurs, Aufzeichnung des Intervalls und des Ergebnisses von Überwachungs- und Rezertifizierungsaudits) mindestens im Abstand von zwölf Monaten überprüft und an zwischenzeitliche Änderungen angepasst wird.

9.8.3 Der Kunde muss über standardisierte Verfahren verfügen, um mit Umständen umgehen zu können, die zumindest gewisse Zweifel an der Anwendung des ermittelten Instruments aufkommen lassen. Diese Verfahren müssen zumindest die folgenden Aspekte abdecken:

a) Feste Berichts- und Entscheidungsstrukturen, um zu entscheiden, ob die Datenübermittlung (noch) rechtmäßig ist oder nicht;
b) Verfahren zur sofortigen Aussetzung der Datenübermittlung im Hinblick auf die konkrete Datenverarbeitung;
c) Verfahren für Identifizierung von und Umsetzung zusätzlicher geeignete Maßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus;
d) Verfahren zur Beendigung der Datenübermittlung im Hinblick auf die konkrete Datenverarbeitung;
e) Verfahren zur Unterrichtung der Aufsichtsbehörde gemäß der Vereinbarung.

9.9 Genehmigte Vertragsklauseln

Einzelne Vertragsklauseln zwischen dem Datenexporteur in der EU und dem Datenimporteur in dem Drittland können einen angemessenen Schutz für die Übermittlung personenbezogener Daten in ein Drittland darstellen, wenn sie von der zuständigen Aufsichtsbehörde genehmigt worden sind.

9.9.1 Sofern der Kunde über eigene genehmigte Vertragsklauseln gemäß Art. 46 Abs. 3 lit. a DSGVO verfügt, stehen dem Kunden die folgenden zusätzlichen dokumentierten Informationen zur Verfügung:

a) Datum der Vereinbarung der Vertragsklauseln;
b) Verfahrensnummer des Genehmigungsbescheids der zuständigen Aufsichtsbehörde.

9.9.2 Der Kunde verfügt über standardisierte Verfahren, die sicherstellen, dass die Dokumentation nach 9.9.1 (Bewertung des Datenimporteurs) mindestens alle zwölf Monate überprüft und an zwischenzeitliche Änderungen angepasst wird.

9.9.3 Der Kunde muss über standardisierte Verfahren verfügen, um mit Umständen umgehen zu können, die zumindest gewisse Zweifel an der Anwendung des ermittelten Instruments aufkommen lassen. Diese Verfahren müssen zumindest die folgenden Aspekte abdecken:

a) Feste Berichts- und Entscheidungsstrukturen, um zu entscheiden, ob die Datenübermittlung (noch) rechtmäßig ist oder nicht;
b) Verfahren zur sofortigen Aussetzung der Datenübermittlung im Hinblick auf die konkrete Datenverarbeitung;
c) Verfahren für Identifizierung von und Umsetzung zusätzlicher geeignete Maßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus;
d) Verfahren zur Beendigung der Datenübermittlung im Hinblick auf die konkrete Datenverarbeitung;
e) Verfahren zur Unterrichtung der Aufsichtsbehörde gemäß der Vereinbarung.

9.10 Nach Unionsrecht nicht zulässige Übermittlungen oder Offenlegungen (FN201: Artikel 48 GDPR)

Einige Drittländer erlassen Gesetze, Verordnungen und andere Rechtsakte, die die Verarbeitungstätigkeiten von natürlichen und juristischen Personen, die der Rechtsprechung der Mitgliedstaaten unterliegen, direkt regeln sollen. Dazu können Urteile von Gerichten oder Entscheidungen von Verwaltungsbehörden in Drittländern gehören, die einen für die Verarbeitung Verantwortlichen oder einen Auftragsverarbeiter verpflichten, personenbezogene Daten zu übermitteln oder offenzulegen, und die nicht auf einer internationalen Übereinkunft, wie einem Rechtshilfevertrag, beruhen, die zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat in Kraft ist. Die extraterritoriale Anwendung dieser Gesetze, Verordnungen und sonstigen Rechtsakte kann gegen das Völkerrecht verstoßen und die Verwirklichung des in der Union durch diese Verordnung gewährleisteten Schutzes natürlicher Personen behindern. Übermittlungen sollten nur zulässig sein, wenn die Bedingungen dieser Verordnung für eine Übermittlung in Drittländer erfüllt sind. Dies kann unter anderem der Fall sein, wenn die Weitergabe aus einem wichtigen Grund des öffentlichen Interesses erforderlich ist, der im Unionsrecht oder im Recht eines Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, anerkannt ist (FN202: Erwägungsgrund 115 GDPR).

Ist der Kunde einem Urteil eines Gerichts oder einer Entscheidung einer Verwaltungsbehörde eines Drittlandes unterworfen, das bzw. die den Kunden verpflichtet, personenbezogene Daten

an ein Drittland zu übermitteln oder offenzulegen, so darf der Kunde eine solche Übermittlung oder Offenlegung an ein Drittland unbeschadet anderer Übermittlungsgründe gemäß diesem Kapitel nur dann begründen, wenn eine solche Übermittlung oder Offenlegung auf einer internationalen Übereinkunft, wie z. B. einem Rechtshilfevertrag, beruht, die zwischen dem suchenden Drittland und dem Mitgliedstaat der für die beabsichtigte Übermittlung oder Offenlegung zuständigen Aufsichtsbehörde in Kraft ist.

9.11 Ausnahmeregelungen für besondere Situationen (FN203: Artikel 49 GDPR)

Soweit der Auftraggeber das Vorliegen einer besonderen Situation nach 9.11.1 bis 9.11.8 (Ausnahmen für besondere Situationen) in Bezug auf eine Übermittlung personenbezogener Daten in ein Drittland im Rahmen des Auswertungsziels festgestellt hat, muss der Auftraggeber neben den fallspezifischen Informationen auch Informationen über die Berücksichtigung des Ausnahmecharakters der besonderen Situation, insbesondere in Bezug auf die gelegentliche und nicht wiederholte Auftreten solcher Übermittlungen, wie sie in den Leitlinien des EDPB zu Ausnahmen von Artikel 49 gemäß der Verordnung 2016/679 genannt werden (FN204: Siehe die Leitlinien des EDPB zu Ausnahmen von Artikel 49 der Verordnung 2016/679, abrufbar unter: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_deroga- tions_en.pdf.)

Behörden können sich bei der Ausübung ihrer öffentlichen Befugnisse nicht auf bestimmte Situationen berufen, die in Artikel 49 Absatz 1 Buchstaben a, b und c sowie Absatz 1 Unterabsatz 1 DSGVO beschrieben sind (FN205: Art. 49 Abs. 3 GDPR).

9.11.1 Ausdrückliche Zustimmung

Eine der besonderen Situationen für die Übermittlung personenbezogener Daten in ein Drittland ist die ausdrückliche Zustimmung der betroffenen Person.
Soweit der Auftraggeber die Übermittlung auf das Vorliegen einer ausdrücklichen Einwilligung einer betroffenen Person stützt, muss (FN206: Art. 49 Abs. 1 Unterabs. 1 lit. a DSGVO) über die gemäß 7.1.2.2 (Einholung der Einwilligungserklärung) erforderlichen dokumentierten Informationen zu der konkreten Datenübermittlung verfügen. Darüber hinaus muss die betroffene Person auf das Risiko hingewiesen werden, das mit der Übermittlung, in die sie einwilligt, verbunden ist, insbesondere darauf, dass ihre personenbezogenen Daten einem unangemessenen Zugriff öffentlicher Stellen zu Überwachungszwecken ausgesetzt sein könnten und dass sie nicht über einen wirksamen Rechtsbehelf gegen einen solchen Zugriff verfügen (Art 49 Abs 1 lit a DSGVO).

9.11.2 Durchführung von vorvertraglichen Maßnahmen

Eine der besonderen Situationen für die Übermittlung personenbezogener Daten in ein Drittland ist die Notwendigkeit der Übermittlung für die Durchführung vorvertraglicher Maßnahmen. So können beispielsweise die Daten der Kunden eines Reisebüros an Hotels übermittelt werden, die den Aufenthalt des Kunden organisieren.

Soweit der Auftraggeber die Übermittlung auf die Durchführung einer vorvertraglichen Maßnahme stützt, stehen dem Auftraggeber unter (FN207: Art. 49 Abs. 1 Unterabs. 1 lit. b DSGVO) die folgenden zusätzlichen dokumentierten Informationen zur Verfügung:

a) Art des Vertrags;
b) Zusammenfassung der für die Vertragsanbahnung erforderlichen personenbezogenen Daten;
c) Erwägung der Gründe, warum diese Daten für die Verarbeitung erforderlich sind.

9.11.3 Leistung eines Kontakts

Eine der besonderen Situationen für die Übermittlung personenbezogener Daten in ein Drittland ist die Notwendigkeit der Übermittlung für die konkrete Vertragserfüllung.

Sofern der Kunde die Übermittlung auf die Erfüllung eines Vertrages stützt,[208] stehen dem Kunden neben den in 9 (Übermittlung personenbezogener Daten in ein Drittland) vorgesehenen Rechten die folgenden zusätzlichen dokumentierten Informationen zur Verfügung:

a) Art des Auftrags;
b) Zusammenfassung der für die Vertragserfüllung erforderlichen personenbezogenen Daten.

9.11.4 Abschluss oder Erfüllung eines Vertrags zugunsten der betroffenen Person

Eine der besonderen Situationen für eine Übermittlung personenbezogener Daten in ein Drittland ist die Notwendigkeit des Abschlusses oder der Erfüllung eines Vertrags zugunsten der betroffenen Person. Dabei ist die betroffene Person nicht der Vertragspartner selbst, sondern eine andere Person oder ein Unternehmen.

Soweit die Übermittlung auf den Abschluss oder die Erfüllung eines Vertrags zugunsten der betroffenen Person gestützt wird, stehen dem Auftraggeber unter (FN209: Art. 49 Abs. 1 Unterabs. 1 lit. c DSGVO) folgende zusätzliche dokumentierte Informationen zur Verfügung:

a) Art des Vertragsverhältnisses;
b) begünstigte betroffene Person;

c) Zusammenfassung der personenbezogenen Daten, die für die Erfüllung oder den Abschluss des Vertrags erforderlich sind;
d) Bestimmung des Nutzens für die betroffene(n) Person(en).

9.11.5 Wichtige Gründe des öffentlichen Interesses

Sofern der Kunde die Übermittlung auf die Notwendigkeit aus wichtigen Gründen des öffentlichen Interesses stützt (FN210: Art. 49 Abs. 1 Unterabs. 1 lit. d DSGVO), muss der Kunde auch über die unter 7.1.7.2 und 7.1.7.3 (Rechtmäßigkeit FN211: Art. 49 Abs. 4 GDPR) geforderten dokumentierten Informationen in Bezug auf die konkrete Datenübermittlung verfügen. In diesen dokumentierten Informationen sind außerdem die spezifische(n) Bestimmung(en) des Unionsrechts und/oder des Rechts eines Mitgliedstaats und deren Anwendbarkeit auf den Kunden zu bestimmen, in denen das öffentliche Interesse anerkannt wird.

9.11.6 Begründung, Ausübung, Verteidigung von Rechtsansprüchen

Eine der besonderen Situationen für eine Übermittlung personenbezogener Daten in ein Drittland im Einzelfall ist eine Übermittlung zur Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen.

Soweit der Auftraggeber die Übermittlung auf die Notwendigkeit zur Begründung, Ausübung oder Verteidigung von Rechtsansprüchen stützt, stehen dem Auftraggeber unter (FN212: Art 49 Absatz 1 Unterabsatz 1 Buchstabe e DSGVO) die folgenden zusätzlichen dokumentierten Informationen zur Verfügung:

a) Darstellung des konkreten Rechtsanspruchs;
b) Weitergabe von personenbezogenen Daten, die für die Begründung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sind;
c) Bewertung der Erforderlichkeit;
d) Nachweis der ursprünglichen rechtmäßigen Sammlung im Sinne von 7.1 (Rechtmäßigkeit).

9.11.7 Schutz der lebenswichtigen Interessen

Eine Übermittlung in ein Drittland, die zur Wahrung lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich ist, ist zulässig, wenn die betroffene Person aus physischen oder rechtlichen Gründen nicht einwilligen kann.

Sofern der Kunde die Übermittlung auf den Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen stützt, wenn die betroffene Person physisch oder rechtlich nicht in der Lage ist, seine Zustimmung zu erteilen (FN213: Art. 49 Abs. 1 Unterabsatz 1 lit. f DSGVO), verfügt der Kunde über die unter 7.1.6 (Verarbeitung zum Schutz lebenswichtiger Interessen) geforderten dokumentierten Informationen in Bezug auf die spezifische Datenübermittlung.

9.11.8 Übertragung aus einem öffentlichen Register

Die Übertragung aus einem öffentlichen Register der Europäischen Union oder eines Mitgliedstaates ist zulässig, wenn die betreffenden Informationen für die Öffentlichkeit bestimmt sind.

Sofern die Übermittlung aus einem Register erfolgt, das nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und das entweder der Öffentlichkeit im Allgemeinen oder jeder Person, die ein berechtigtes Interesse nachweisen kann, zur Einsichtnahme offen steht, stehen dem Auftraggeber unter (FN214: Art. 49 Abs. 1 Unterabsatz 1 lit. g GDPR) folgende zusätzliche dokumentierte Informationen zur Verfügung:

a) Darstellung der unionsrechtlichen oder mitgliedstaatlichen Voraussetzungen für den Zugang zum Register (FN215: Art. 49 Abs. 1 Unterabsatz 1 lit. g GDPR),
b) wenn ein berechtigtes Interesse für die Einsichtnahme in das Register erforderlich ist, die Vorlage desselben gemäß 7.1.9 (Verarbeitung zur Wahrung berechtigter Interessen) im Einzelfall (FN216: Art. 49 Abs. 1 Unterabsatz 1 lit. g GDPR),
c) Maßnahmen, die sicherstellen, dass der Inhalt des Registers nicht in seiner Gesamtheit übermittelt wird (FN217: Art. 49 Abs. 2 GDPR).

9.12 Schutz der zwingenden berechtigten Interessen des Auftraggebers

Eine Übermittlung personenbezogener Daten in ein Drittland zur Wahrung zwingender schutzwürdiger Interessen darf nur erfolgen, wenn die Übermittlung nicht wiederholt wird, nur eine begrenzte Zahl von Betroffenen betrifft und zur Wahrung der zwingenden schutzwürdigen Interessen erforderlich ist, sofern in der Interessenabwägung die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen.
Wenn der Auftraggeber die Übermittlung auf zwingende berechtigte Interessen stützt, gemäß Art 49 (1) Unterabsatz 2 GDPR muss der Kunde auch über folgende Unterlagen verfügen

a) die zwingenden berechtigten Interessen, die verfolgt werden, sowie eine Abwägung dieser Interessen mit den Interessen und den Rechten und Freiheiten der betroffenen Personen, die diese Interessen nicht überwiegen;
b) die Notwendigkeit der Übermittlung zur Wahrung der zwingenden berechtigten Interessen;
c) die Bewertung aller Umstände der Datenübermittlung, wie die Art der personenbezogenen Daten, der Zweck und die Dauer der geplanten Verarbeitung(en) sowie die Situation im Herkunftsland, im Drittland und im Endbestimmungsland;
d) die angemessenen Sicherheitsvorkehrungen, die für diese Bewertung vorgesehen sind;
e) der Unterrichtung der Aufsichtsbehörde und der Unterrichtung der betroffenen Personen über die Übermittlung zusätzlich zu den Informationen gemäß Art. 13 (1) lit. f DSGVO;

f) die Tatsache, dass die spezifische Übertragung nicht wiederholt wird, und
g) sie betrifft nur eine begrenzte Anzahl von Betroffenen.

10 Zusammenarbeit mit der Aufsichtsbehörde

Der für die Verarbeitung Verantwortliche oder der Auftraggeber arbeitet mit der Aufsichtsbehörde zusammen. Ein direkter Ansprechpartner für die Aufsichtsbehörde kann ein ernannter Datenschutzbeauftragter sein.

Der Kunde muss über standardisierte Verfahren verfügen, um sicherzustellen, dass Anfragen der zuständigen Aufsichtsbehörde bearbeitet werden und er mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenarbeitet (FN218: Artikel 31 GDPR).
Unabhängig davon, ob ein Datenschutzbeauftragter benannt ist oder nicht, muss er über Datenschutzbeauftragte und eine elektronische Kontaktadresse für datenschutzrelevante Anfragen verfügen, auf die mindestens einmal täglich zugegriffen wird.

11 Benennung und Aufgaben des Datenschutzbeauftragten

11.1 Der Kunde muss unter Berücksichtigung der Anforderungen von Art. 37 (1) DSGVO über dokumentierte Informationen darüber verfügen, ob seine Organisation verpflichtet ist, einen Datenschutzbeauftragten zu benennen oder nicht, und zwar aufgrund der Verarbeitungen, die Gegenstand des Ziels der Bewertung sind. Die Auslegung dieser Anforderungen muss dem Arbeitsdokument Nr. 243 der Artikel-29-Datenschutzgruppe (FN219: wp243rev01_de (datenschutzkonferenz-online.de). folgen.

11.2 Die Anforderungen, die gemäß Artikel 37 GDPR zu berücksichtigen sind, sind:

11.2.1 die Verarbeitung erfolgt durch eine Behörde oder eine öffentliche Einrichtung, mit Ausnahme von Gerichten, die in ihrer gerichtlichen Eigenschaft handeln (FN220: Art 37 Abs 1 lit a GDPR);

11.2.2 die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters aus Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Überwachung der betroffenen Personen in großem Umfang erfordern (FN221: Art 37 Abs 1 lit b GDPR); oder

11.2.3 die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der Verarbeitung besonderer Datenkategorien gemäß Artikel 9 oder personenbezogener Daten über strafrechtliche

Verurteilungen und Straftaten gemäß Artikel 10 in großem Umfang besteht (FN222: Art 37 Abs 1 lit c GDPR).

11.3. Kommt der Auftraggeber zu dem Schluss, dass ein Datenschutzbeauftragter zu bestellen ist, hat er die ordnungsgemäße Meldung der Kontaktdaten des Datenschutzbeauftragten an die zuständige Aufsichtsbehörde und deren Veröffentlichung zu dokumentieren (FN223: Art. 37 Abs. 7 GDPR). Er hat auch die Benennung des Datenschutzbeauftragten sowie dessen ausreichende fachliche Qualifikation und Befähigung zur Erfüllung der in Art 39 DSGVO und § 5 DSG genannten Aufgaben unter Berücksichtigung seines Fachwissens im Bereich des Datenschutzrechts und der Datenschutzpraxis zu dokumentieren (FN224: Art. 37 Abs. 5 GDPR).

11.4 Darüber hinaus verfügt der Kunde über dokumentierte Informationen über die Einhaltung der Anforderungen in Bezug auf seine Position gemäß Artikel 38 GDPR.

11.5 In diesem Zusammenhang muss der Kunde den Nachweis erbringen, dass

11.5.1 Der Datenschutzbeauftragte in allen Fragen, die den Schutz personenbezogener Daten betreffen, ordnungsgemäß und rechtzeitig einbezogen wird (FN225: Art. 38 Abs. 1 GDPR);

11.5.2. Der Auftraggeber unterstützt den Datenschutzbeauftragten bei der Erfüllung der in Art. 39 genannten Aufgaben, indem er ihm die für die Erfüllung dieser Aufgaben erforderlichen Mittel und den Zugang zu den personenbezogenen Daten und den Verarbeitungen, die dem Ziel der Bewertung unterliegen, zur

Verfügung stellt und sein Fachwissen aufrechterhält (FN226: Art. 38 Abs. 2 GDPR);

11.5.3 der Datenschutzbeauftragte erhält keine Anweisungen für die Ausübung dieser Aufgaben (FN227: Art. 38 Abs. 3 GDPR);

11.5.4 wird nicht entlassen oder für die Erfüllung seiner Aufgaben bestraft (FN228: Art. 38 Abs. 3 GDPR);

11.5.5 der Datenschutzbeauftragte kann direkt der höchsten Führungsebene des Unternehmens unterstellt werden (FN2229: Art. 38 Abs. 3 GDPR);

11.5.6 Betroffene Personen können sich bei allen Fragen im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten und der Ausübung ihrer Rechte nach der DSGVO an den Datenschutzbeauftragten wenden (FN230: Art. 38 Abs. 4 GDPR);

11.5.7 der Datenschutzbeauftragte seine Aufgaben unter Einhaltung seiner Geheimhaltungs- oder Vertraulichkeitsverpflichtungen wahrnehmen kann (FN231: Art. 38 Abs. 5 GDPR); (z. B. mittels eines speziellen E-Mail-Kontos, zu dem nur er und sein Personal Zugang haben) und dass

11.5.8. andere Aufgaben und Pflichten des Datenschutzbeauftragten nicht zu einem Interessenkonflikt führen (z. B. indem er seine Aufgaben nicht einem Mitglied des Vorstands oder der Geschäftsführung mit Entscheidungsbefugnis in Bezug auf Verarbeitungen überträgt) (FN232: Art. 38 Abs. 6 GDPR);