

Datenschutzrecht

NEU

INHALTSVERZEICHNIS

I. VORWORT

II. WICHTIGSTE BEGRIFFE AUF EINEN BLICK - IN ALPHABETISCHER REIHENFOLGE

III. ANWENDUNGSBEREICH DER DSGVO

1. sachlicher Anwendungsbereich
2. räumlicher Anwendungsbereich

IV. GRUNDSÄTZE DER DATENVERARBEITUNG

1. sachlicher Anwendungsbereich
2. Rechtmäßigkeit der Verarbeitung
 - 2.1 *Voraussetzungen*
 - 2.2 *Verarbeitung zu einem anderen Zweck*
3. Bedingungen für die Einwilligung
 - 3.1 *bereits vorhandene Einwilligung*
 - 3.2 *Form*
 - 3.3 *Freiwilligkeit*
 - 3.4 *Widerrufungsmöglichkeit*
4. Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft
5. Verarbeitung besonderer Kategorien personenbezogener Daten
 - 5.1 *Verbot der Verarbeitung*
 - 5.2 *Ausnahmen vom Verbot der Verarbeitung*
6. Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist

V. RECHTE DER BETROFFENEN PERSONEN

1. Transparenz und Modalitäten
 - 1.1 *Maßnahmen zur Information*
 - 1.2 *Erleichterung der Ausübung der Rechte der betroffenen Person*
 - 1.3 *Informationspflicht über ergriffene Maßnahmen*
 - 1.4 *Information über Gründe für Untätigkeit*
 - 1.5 *Unentgeltlichkeit der Information*
 - 1.6 *Ausnahmen von der Unentgeltlichkeit*
2. Informationspflicht bei Erhebung von personenbezogenen Daten bei der betreffenden Person
3. Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden
 - 3.1 *Umfang der Informationspflicht*
 - 3.2 *Frist für die Information*
 - 3.3 *Information bei der Verarbeitung für andere Zwecke*
 - 3.4 *Unterbleiben der Informationspflicht*
4. Auskunftsrecht der betroffenen Person
5. Recht auf Berichtigung
6. Recht auf Löschung („Recht auf Vergessenwerden“)
7. Recht auf Einschränkung der Verarbeitung
8. Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung
9. Recht auf Datenübertragbarkeit
10. Widerspruchsrecht
11. automatisierte Entscheidung im Einzelfall einschließlich Profiling

VI. FÜR DIE DATENVERARBEITUNG VERANTWORTLICHE UND AUFTRAGS- VERARBEITER

1. Verantwortung des für die Verarbeitung Verantwortlichen
2. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
3. gemeinsam für die Verarbeitung Verantwortliche
4. Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern
5. Auftragsverarbeiter
 - 5.1 *Auswahl*
 - 5.2 *Sub-Auftragsverarbeiter*
 - 5.3 *Grundlage für die Auftragsverarbeitung*
 - 5.4 *Sub-Auftragsverarbeitung*
 - 5.5 *Standardvertragsklauseln und Form*
6. Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters
7. Verzeichnis von Verarbeitungstätigkeiten
 - 7.1 *Inhalt für Verantwortliche*
 - 7.2 *Inhalt für Auftragsverarbeiter*
 - 7.3 *Form*
 - 7.4 *Entfall der Verpflichtung*
8. Zusammenarbeit mit der Aufsichtsbehörde
9. Sicherheit der Verarbeitung
10. Datensicherheitsmaßnahmen nach dem Datenschutz-Anpassungsgesetz
11. Meldung von Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde
 - 11.1 *Frist*
 - 11.2 *Inhalt der Meldung*

12. Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person
 - 12.1 *Voraussetzung für das Erfordernis*
 - 12.2 *Entfall des Erfordernisses*
13. Datenschutz-Folgenabschätzung
 - 13.1 *Voraussetzungen*
 - 13.2 *Inhalt / Umfang*
 - 13.3 *Vorgehensweise für bereits existierende Verarbeitungsvorgänge*
14. vorherige Konsultation
15. Benennung eines Datenschutzbeauftragten
16. Stellung des Datenschutzbeauftragten
17. Aufgaben des Datenschutzbeauftragten
18. Zertifizierung

VII. ÜBERMITTLUNG PERSONENBEZOGENER DATEN AN DRITTLÄNDER ODER AN INTERNATIONALE ORGANISATIONEN

1. allgemeine Grundsätze der Datenübermittlung
2. Datenübermittlung auf Grundlage eines Angemessenheitsbeschlusses
3. Datenübermittlung vorbehaltlich geeigneter Garantien
4. nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung
5. Ausnahme für bestimmte Fälle

VIII. BILDVERARBEITUNG GEMÄß § 12 DATENSCHUTZ-ANPASSUNGSGESETZ

IX. RECHTSBEHELFE, HAFTUNGEN UND SANKTIONEN

1. Recht auf Beschwerde bei einer Aufsichtsbehörde
2. Recht auf wirksamen, gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde

3. Recht auf wirksamen, gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter
4. Vertretung von betroffenen Personen
5. Haftung und Recht auf Schadenersatz
6. allgemeine Bedingungen für die Verhängung von Geldbußen
7. Verwaltungsstrafbestimmungen nach dem Datenschutz-Anpassungsgesetz

X. ANLAGE

- | | |
|------------|---|
| Muster 1 | Checkliste - Status Quo und Anpassungsbedarf |
| Muster 2 | Verzeichnis von Verarbeitungstätigkeiten (Verantwortlicher) |
| Muster 3 | Verzeichnis von Verarbeitungstätigkeiten (Auftragsverarbeiter) |
| Muster 4 | Einwilligungserklärung |
| Muster 5.1 | Auskunftserteilung gemäß Artikel 15 DSGVO
<i>keine Daten werden verarbeitet (Negativauskunft)</i> |
| Muster 5.2 | Auskunftserteilung gemäß Artikel 15 DSGVO
<i>fristgerechte Auskunftserteilung</i> |
| Muster 5.3 | Auskunftserteilung gemäß Artikel 15 DSGVO
<i>fristgerechte Auskunftserteilung - mit Fristverlängerung</i> |
| Muster 5.4 | Auskunftserteilung gemäß Artikel 15 DSGVO
<i>fristgerechte Auskunftserteilung - Übermittlung Drittland</i> |
| Muster 5.5 | Auskunftserteilung gemäß Artikel 15 DSGVO - weitere mögliche Zusätze |
| Muster 6 | Bestellung zum Datenschutzbeauftragten |
| Muster 7 | Meldung an Behörde wg. Meldung Datenschutzbeauftragter |
| Muster 8 | Meldung an Behörde wg. Data Breach |
| Muster 9 | Benachrichtigung von der Verletzung des Schutzes personenbezogener Daten
<i>Meldung an betroffene Person</i> |

- Muster 10 Benachrichtigung von der Verletzung des Schutzes personenbezogener Daten
Auftraggeber an Verantwortlichen
- Muster 11 Vereinbarung über Auftragsverarbeitung
- Muster 12 Vorgehensweise bei Datenschutz-Folgenabschätzung

I. VORWORT

Das vorliegende Handbuch stellt eine zusammenfassende Information über die Datenschutz-Grundverordnung (DSGVO) und die dazu in Österreich im Datenschutz-Anpassungsgesetz enthaltenen Begleitregelungen dar, die die Vorbereitung Ihrer Genossenschaft und Ihrer Mitglieder auf die Neuerungen, die aufgrund der DSGVO resultieren, erleichtern und Hilfestellung zu bestimmten Fragen bieten soll. Es handelt sich dabei um keine abschließende Information. Eine Beratung durch spezialisierte Einrichtungen kann durch das vorliegende Handbuch im Einzelfall nicht ersetzt werden.

Das gegenständliche Handbuch wird in regelmäßigen Abständen unter Einbeziehung allfälliger Neuerungen vor allem auf europäischer Ebene und allfälliger Veröffentlichungen von Mustern seitens der Datenschutzbehörde aktualisiert werden.

Die in den nachfolgenden Kapiteln enthaltenen Ausführungen beschränken sich auf Themengebiete, die für Genossenschaften und ihre Mitglieder von Interesse sein können. Die darüber hinaus in der DSGVO enthaltenen Themenbereiche werden ausgespart.

Abschließend bitte ich Sie, mir allfällige Anregungen / Anmerkungen zukommen zu lassen, die ich dann gerne bei späteren Überarbeitungen berücksichtigen werde.

Dezember 2017

MMag. Barbara POGACAR

II. WICHTIGSTE BEGRIFFE AUF EINEN BLICK - IN ALPHABETISCHER REIHENFOLGE

<i>Aufsichtsbehörde</i>	Aufsichtsbehörde ist eine von einem Mitgliedstaat gemäß Artikel 51 DSGVO eingerichtete, unabhängige staatliche Stelle. In Österreich ist die Datenschutzbehörde Aufsichtsbehörde.
<i>Auftragsverarbeiter</i>	Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
<i>betroffene Aufsichtsbehörde</i>	Betroffene Aufsichtsbehörde ist eine Aufsichtsbehörde, die von der Verarbeitung personenbezogener Daten betroffen ist, weil der Verantwortliche oder der Auftraggeber im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist, diese Verarbeitung erheblicher Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann oder eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde.
<i>betroffene Person</i>	Darunter ist eine Person zu verstehen, über die personenbezogene Daten vorliegen, die die natürliche Person identifizieren oder identifizierbar machen.
<i>Bildaufnahme</i>	Eine Bildaufnahme bezeichnet die durch Verwendung technischer Einrichtungen zur Bildverarbeitung vorgenommene Feststellung von Ereignissen im öffentlichen oder nicht-öffentlichen Raum zu privaten Zwecken. Zur Bildaufnahme gehören auch dabei mitverarbeitete, akustische Informationen.
<i>biometrische Daten</i>	Biometrische Daten sind mit speziellen, technischen Verfahren gewonnene, personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige

Identifizierung dieser natürlichen Person ermöglichen oder bestätigen wie Gesichtsbilder oder daktyloskopische Daten.

Data Breach

Unter einer Verletzung des Schutzes personenbezogener Daten (Data Breach) ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Dateisystem

Unter Dateisystem ist jede strukturierte Sammlung personenbezogener Daten zu verstehen, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.

Datengeheimnis

Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich aufgrund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger, gesetzlicher Verschwiegenheitspflichten geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht.

Datenschutzrat

Der Datenschutzrat ist beim Bundeskanzleramt eingerichtet und nimmt zu Fragen von grundsätzlicher Bedeutung für den Datenschutz Stellung, fördert die einheitliche Fortentwicklung des Datenschutzes und berät die Bundesregierung in rechtspolitischer Hinsicht bei datenschutzrechtlich relevanten Vorhaben.

Dienst der Informationsgesellschaft

Ein Dienst der Informationsgesellschaft ist eine Dienstleistung iSd Artikel 1, Nr. 1 lit. b der Richtlinie über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (RL [EU] 2015/1535).

<i>Dritter</i>	Dritter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.
<i>Einschränkung der Verarbeitung</i>	Darunter ist die Markierung gespeicherter, personenbezogener Daten mit dem Ziel zu verstehen, ihre künftige Verarbeitung einzuschränken.
<i>Einwilligung</i>	Unter Einwilligung der betroffenen Person ist jede freiwillige, für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen, eindeutigen bestätigenden Handlung zu verstehen, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden, personenbezogenen Daten einverstanden ist.
<i>Empfänger</i>	Ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.
<i>genetische Daten</i>	Genetische Daten sind personenbezogene Daten, zu den vererbten oder erworbenen, genetischen Eigenschaften einer natürlichen Person, die eindeutig Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden, natürlichen Person gewonnen wurde.
<i>Gesundheitsdaten</i>	Gesundheitsdaten sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

*grenzüberschreitende
Verarbeitung*

Eine grenzüberschreitenden Verarbeitung ist entweder

- a) eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiters in der Union in mehr als einem Mitgliedstaat erfolgt, wenn der Verantwortliche oder Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist oder
- b) eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, die jedoch erhebliche Auswirkungen auf betroffenen Personen in mehr als einem Mitgliedstaat hat oder haben kann.

Hauptniederlassung

Hauptniederlassung bedeutet im Fall eines Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der EU, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen. In diesem Fall gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung.

Hauptniederlassung ist im Fall eines Auftragsverarbeiters mit Niederlassungen in mehr als einem Mitgliedstaat der Ort seiner Hauptverwaltung in der Union oder - sofern der Auftragsverarbeiter keine Hauptverwaltung in der Union hat - die Niederlassung des Auftragsverarbeiters in der Union, in der die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters hauptsächlich stattfinden, soweit der Auftragsverarbeiter spezifischen Pflichten aus dieser Verordnung unterliegt.

*internationale
Organisation*

Eine internationale Organisation ist eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder

mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

*maßgeblicher und
begründeter Einspruch*

Unter einem maßgeblichen und begründeten Einspruch ist ein Einspruch im Hinblick darauf zu verstehen, ob ein Verstoß gegen die DSGVO vorliegt oder nicht oder ob die beabsichtigte Maßnahme gegen den Verantwortlichen oder den Auftragsverarbeiter im Einklang mit der DSGVO steht, wobei aus diesem Einspruch die Tragweite der Risiken klar hervorgeht, die von dem Beschlussentwurf in Bezug auf die Grundrechte und -freiheiten der betroffenen Personen und ggfs. den freien Verkehr personenbezogener Daten in der Union ausgehen.

*personenbezogene
Daten*

Darunter sind alle Informationen zu verstehen, die sich auf identifizierte oder identifizierbare Personen beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, vor allem durch Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer (zB Sozialversicherungsnummer), zu Standortdaten, zu einer Online-Kennung (zB IP-Adresse) 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.

Profiling

Unter Profiling ist jede Art der automatisierten Verarbeitung personenbezogener Daten zu verstehen, 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 bzgl. Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

Pseudonymisierung

Unter Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise zu verstehen, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen,

betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren, natürlichen Person zugewiesen werden.

Unternehmen

Unternehmen ist eine natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen.

Unternehmensgruppe

Unternehmensgruppe ist eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht.

Verantwortlicher

Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sofern die Zwecke und Mittel der Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben sind, so kann der Verantwortliche bzw. können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgeesehen werden.

Verarbeitung

Verarbeitung bedeutet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solcher Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verarbeitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

*verbindliche, interne
Datenschutzvorschriften*

Unter verbindlichen, internen Datenschutzvorschriften sind Maßnahmen zum Schutz personenbezogener Daten zu verstehen, zu deren Einhaltung sich ein im Hoheits-

gebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter verpflichtet, im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter der selben Unternehmensgruppe oder der selben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern.

Verletzung des Schutzes personenbezogener Daten

Unter einer Verletzung des Schutzes personenbezogener Daten ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Vertreter

Vertreter ist eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 DSGVO bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach der DSGVO obliegenden Pflichten vertritt.

III. ANWENDUNGSBEREICH DER DSGVO

1. sachlicher Anwendungsbereich

Die DSGVO findet Anwendung auf die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie auf die nicht automatisierte Verarbeitung von personenbezogenen Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Keine Anwendung findet die DSGVO beispielsweise im Rahmen ausschließlich persönlicher oder familiärer Tätigkeiten. Die DSGVO findet auch nur auf die Verarbeitung von Daten natürlicher Personen Anwendung. Das Datenschutz-Anpassungsgesetz, das für Österreich Begleit- und Ausführungsregelungen enthält, kommt derzeit auch noch auf juristische Personen zur Anwendung. Es ist aber wohl davon auszugehen, dass es diesbezüglich noch zu einer Einschränkung kommen wird.

2. räumlicher Anwendungsbereich

Räumlich gesehen knüpft die DSGVO an die Datenverwendung im Rahmen einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters an, wobei die DSGVO nur dann anwendbar ist, wenn sich diese Niederlassung im Gebiet der EU befindet. Allerdings findet die DSGVO auch dann Anwendung, wenn die Datenverarbeitung durch einen nicht im Unionsgebiet niedergelassenen Verantwortlichen oder Auftragsverarbeiter erfolgt und die Datenverarbeitung im Zusammenhang damit steht, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten oder das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

IV. GRUNDSÄTZE DER DATENVERARBEITUNG

1. Übersicht

Die Verarbeitung personenbezogener Daten hat gemäß Artikel 5 DSGVO folgenden Grundsätzen zu entsprechen:

*** Rechtmäßigkeit**

Die Daten müssen auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

*** Zweckbindung**

Die personenbezogenen Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden.

*** Datenminimierung**

Die personenbezogenen Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

*** Richtigkeit**

Die personenbezogenen Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf den Zweck ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

*** Speicherbegrenzung**

Die personenbezogenen Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

*** Integrität und Vertraulichkeit**

Die personenbezogenen Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete, technische und organisatorische Maßnahmen.

Der Verantwortliche ist für die Einhaltung der soeben genannten Grundsätze verantwortlich und muss deren Einhaltung nachweisen können. Den Verantwortlichen trifft daher eine Rechenschaftspflicht.

2. Rechtmäßigkeit der Verarbeitung

2.1 Voraussetzungen

Gemäß Artikel 6 DSGVO ist die Verarbeitung nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- * Die betroffene Person hat ihre Einwilligung (siehe Muster 4 *Einwilligungserklärung*) zu der Verarbeitung ihrer personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben.
- * Die Verarbeitung ist für die Erfüllung eines Vertrags (zB Kaufvertrag) - dessen Vertragspartei die betroffene Person ist - oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen.
- * Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt.
- * Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.
- * Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.
- * Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und -freiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

2.2 Verarbeitung zu einem anderen Zweck

Wenn die Verarbeitung zu einem anderen als zu dem Zweck, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift beruht, so hat der Verantwortliche - um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist - u.a. folgendes zu berücksichtigen:

- * jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden und den Zwecken der beabsichtigten Weiterverarbeitung;
- * den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen;
- * die Art der personenbezogenen Daten, insbesondere, ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 DSGVO (zB politische Meinung, religiöse und weltanschauliche Überzeugung) verarbeitet werden;
- * die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen;
- * das Vorhandensein geeigneter Garantien, wozu Verschlüsselungen oder Pseudonymisierung gehören können.

3. Bedingungen für die Einwilligung

3.1 bereits vorhandene Einwilligung

Sofern bereits eine Einwilligung vorliegt, die den Voraussetzungen des Artikels 7 DSGVO entspricht, muss nicht nochmals eine Einwilligung eingeholt werden. Vorhandene Einwilligungen sollten daher geprüft werden.

3.2 Form

Wenn die Verarbeitung auf einer Einwilligung beruht, so muss der Verantwortliche gemäß Artikel 7 DSGVO nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. Die Einwilligung kann dabei sowohl mündlich als auch schriftlich erfolgen, wobei aus Gründen der Nachweisbarkeit die Schriftform zu bevorzugen ist.

Wenn die Einwilligung der betroffenen Person durch eine schriftliche Erklärung erfolgt, die auch noch andere Sachverhalte betrifft, so muss das Ersuchen um

Einwilligung gemäß Artikel 7 Abs. 2 DSGVO in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen die DSGVO darstellen.

3.3 Freiwilligkeit

Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand im größtmöglichen Umfang Rechnung getragen werden, ob u.a. die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, bei Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

3.4 Widerrufungsmöglichkeit

Auch wenn eine ordnungsgemäße Einwilligung vorliegt, muss beachtet werden, dass die betroffene Person das Recht hat, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung aber nicht berührt. Die betroffene Person muss vor Abgabe der Einwilligung darüber in Kenntnis gesetzt werden. Es bedarf daher einer Belehrung über das Recht zum Widerruf. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein, d.h., er darf nicht unnötig durch Formerfordernisse erschwert werden.

4. Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft

Bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, ist die Verarbeitung der personenbezogenen Daten rechtmäßig, wenn das Kind das 14. Lebensjahr vollendet hat. Hat das Kind noch nicht das 14. Lebensjahr vollendet, so ist diese Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird. Es bedarf daher einer Vorsorge, dass eine gewissenhafte Alterskontrolle erfolgt.

Gemäß Artikel 8 Abs. 2 DSGVO übernimmt der Verantwortliche unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen, um sich in solchen Fällen zu vergewissern, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung auch erteilt wurde.

5. Verarbeitung besonderer Kategorien personenbezogener Daten

5.1 Verbot der Verarbeitung

Die Verarbeitung personenbezogener Daten, aus denen die

- * rassistische und ethnische Herkunft
- * politische Meinung
- * religiöse oder weltanschauliche Überzeugung
- * oder die Gewerkschaftszugehörigkeit

hervorgehen sowie die Verarbeitung von

- * genetischen Daten
- * biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person
- * Gesundheitsdaten oder Daten zum Sexualleben
- * oder der sexuellen Orientierung

einer natürlichen Person ist gemäß Artikel 9 Abs. 1 DSGVO untersagt.

5.2 Ausnahmen vom Verbot der Verarbeitung

Das Verbot der Verarbeitung der zuvor genannten Daten gilt gemäß Artikel 9 Abs. 2 DSGVO nicht, wenn die betroffene Person in die Verarbeitung der genannten, personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt hat, es sei denn, dies wäre nach Unionsrecht oder dem Recht der Mitgliedstaaten nicht zulässig.

Weiters ist die Verarbeitung zulässig, wenn sie erforderlich ist, damit der Verantwortliche oder die betroffene Person die ihm / ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen / ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist.

Außerdem ist die Verarbeitung zulässig, wenn sie zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person aus körperlichen oder rechtlichen Gründen außer Stande ist, ihre Einwilligung zu geben.

Schließlich ist die Verarbeitung noch zulässig, wenn sie auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der

Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden.

Darüber hinaus ist die Verarbeitung zulässig, wenn sie sich auf personenbezogene Daten bezieht, die die betroffene Person öffentlich gemacht hat sowie wenn die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich ist.

6. Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist

Wenn für die Zwecke, für die ein Verantwortlicher personenbezogene Daten verarbeitet, die Identifizierung der betroffenen Person durch den Verantwortlichen nicht oder nicht mehr erforderlich ist, so ist dieser gemäß Artikel 11 Abs. 1 DSGVO nicht verpflichtet, zur bloßen Einhaltung der DSGVO zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren. Wenn der Verantwortliche nachweisen kann, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, so hat er - sofern möglich - die betroffene Person darüber zu informieren.

In diesen Fällen finden die Artikel 15 bis 20¹ DSGVO keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Artikel niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen.

¹ Auskunftspflicht; Recht auf Berichtigung; Recht auf Löschung; Recht auf Einschränkung der Verarbeitung; Mitteilungspflicht iZm Berichtigung oder Löschung oder der Einschränkung der Verarbeitung; Recht auf Datenübertragbarkeit

V. RECHTE DER BETROFFENEN PERSONEN

1. Transparenz und Modalitäten

1.1 Maßnahmen zur Information

Gemäß Artikel 12 Abs. 1 DSGVO hat der Verantwortliche geeignete Maßnahmen zu treffen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14² DSGVO und alle Mitteilungen gemäß den Artikeln 15 bis 22 und 34³ DSGVO, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Informationen hat schriftlich oder in anderer Form, ggfs. auch elektronisch zu erfolgen. Die betroffene Person kann verlangen, dass die Information mündlich erteilt wird, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

1.2 Erleichterung der Ausübung der Rechte der betroffenen Person

Gemäß Artikel 12 Abs. 2 DSGVO hat der Verantwortliche der betroffenen Person die Ausübung ihrer Rechte gemäß den Artikel 15 bis 22⁴ DSGVO zu erleichtern. In den in Artikel 11 Abs. 2 DSGVO genannten Fällen darf sich der Verantwortliche nur dann weigern, aufgrund des Antrags der betroffenen Personen auf Wahrnehmung ihrer Rechte gemäß den Artikeln 15 bis 22⁵ DSGVO, tätig zu werden, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren.

1.3 Informationspflicht über ergriffene Maßnahmen

In Artikel 12 Abs. 3 DSGVO ist festgelegt, dass der Verantwortliche der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22⁶ DSGVO,

² Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person; Informationspflicht, wenn die Daten nicht bei der betroffenen Person erhoben werden

³ Auskunftsrecht; Recht auf Berichtigung und Löschung; Recht auf Einschränkung der Verarbeitung; Mitteilungspflicht iZm der Berichtigung oder Löschung; Recht auf Datenübertragbarkeit; Widerspruchsrecht; automatisierte Entscheidungen im Einzelfall einschl. Profiling; Benachrichtigung der Verletzung des Schutzes personenbezogener Daten der betroffenen Person

⁴ Auskunftsrecht; Recht auf Berichtigung und Löschung; Recht auf Einschränkung der Verarbeitung; Mitteilungspflicht iZm der Berichtigung oder Löschung; Recht auf Datenübertragbarkeit; Widerspruchsrecht; automatisierte Entscheidungen im Einzelfall einschl. Profiling; Benachrichtigung der Verletzung des Schutzes personenbezogener Daten der betroffenen Person

⁵ Auskunftsrecht; Recht auf Berichtigung und Löschung; Recht auf Einschränkung der Verarbeitung; Mitteilungspflicht iZm der Berichtigung oder Löschung; Recht auf Datenübertragbarkeit; Widerspruchsrecht; automatisierte Entscheidungen im Einzelfall einschl. Profiling; Benachrichtigung der Verletzung des Schutzes personenbezogener Daten der betroffenen Person

⁶ Auskunftsrecht; Recht auf Berichtigung und Löschung; Recht auf Einschränkung der Verarbeitung; Mitteilungspflicht iZm der Berichtigung oder Löschung; Recht auf Datenübertragbarkeit; Widerspruchsrecht;

ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung stellt. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Wenn die betroffene Person den Antrag elektronisch stellt, so ist sie nach Möglichkeit auch auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

1.4 Information über Gründe für Untätigkeit

Wenn der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig wird, so ist er verpflichtet, die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit zu informieren, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

1.5 Unentgeltlichkeit der Information

Die Informationen gemäß den Artikeln 13 und 14⁷ DSGVO sowie alle Mitteilungen und Maßnahmen gemäß den Artikeln 15 bis 22⁸ DSGVO und Artikel 34⁹ DSGVO, werden unentgeltlich zur Verfügung gestellt.

1.6 Ausnahmen von der Unentgeltlichkeit

Bei offenkundig unbegründeten oder - insbesondere im Fall von häufiger Wiederholung - exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder

- * ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahmen berücksichtigt werden oder
- * sich weigern, aufgrund des Antrags tätig zu werden

Den Verantwortlichen trifft die Nachweispflicht, dass es sich um einen offenkundig unbegründeten oder exzessiven Antrag handelt. Artikel 12 Abs. 6 DSGVO bestimmt, dass der Verantwortliche im Fall von begründeten Zweifeln an der Identität der

automatisierte Entscheidungen im Einzelfall einschl. Profiling; Benachrichtigung der Verletzung des Schutzes personenbezogener Daten der betroffenen Person

⁷ Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person; Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

⁸ Auskunftrecht; Recht auf Berichtigung und Löschung; Recht auf Einschränkung der Verarbeitung; Mitteilungspflicht iZm der Berichtigung oder Löschung; Recht auf Datenübertragbarkeit; Widerspruchsrecht; automatisierte Entscheidungen im Einzelfall einschl. Profiling; Benachrichtigung der Verletzung des Schutzes personenbezogener Daten der betroffenen Person

⁹ Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

natürlichen Person berechtigt ist, zusätzliche Informationen anzufordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

2. Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

Wenn personenbezogene Daten bei der betroffenen Person erhoben werden, so hat der Verantwortliche gemäß Artikel 13 DSGVO der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgendes mitzuteilen.

- * Namen und Kontaktdaten des Verantwortlichen sowie ggfs. eines Vertreters
- * ggfs. Kontaktdaten des Datenschutzbeauftragten
- * Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen sowie die Rechtsgrundlage für die Verarbeitung
- * allenfalls die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden
- * ggfs. die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
- * ggfs. die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln sowie in diesem Zusammenhang weitere Informationen gemäß Artikel 13 Abs. 1 lit. f DSGVO

Um eine faire und transparente Verarbeitung zu gewährleisten, hat der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung der Daten folgende weitere Informationen gemäß Artikel 13 Abs. 2 DSGVO zur Verfügung zu stellen:

- * Dauer, für die personenbezogenen Daten gespeichert werden oder - falls dies nicht möglich ist - die Kriterien für die Festlegung dieser Dauer
- * das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die sie betreffenden, personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit
- * wenn die Verarbeitung auf Artikel 6 Abs. 1 lit. a DSGVO (*Einwilligung*) oder Artikel 9 Abs. 2 lit. a DSGVO (*Einwilligung bei besonderer Kategorien von Daten*) beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen,

ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird

- * das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde
- * ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist
- * ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen und welche möglichen Folgen die Nichtbereitstellung hätte und
- * das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Wenn der Verantwortliche beabsichtigt, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als für den, für den die personenbezogenen Daten erhoben wurden, so hat er der betroffenen Person vor dieser Weitergabe Informationen über diesen anderen Zweck und alle anderen, maßgeblichen Informationen gemäß der o.g. Punktreihe zur Verfügung zu stellen.

3. Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

3.1 Umfang der Informationspflicht

Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so hat der Verantwortliche der betroffenen Person gemäß Artikel 14 Abs. 1 DSGVO folgendes mitzuteilen:

- * Namen und Kontaktdaten des Verantwortlichen sowie ggfs. seines Vertreters
- * zusätzlich die Kontaktdaten des Datenschutzbeauftragten
- * die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen sowie die Rechtsgrundlage für die Verarbeitung
- * die Kategorien personenbezogener Daten, die verarbeitet werden
- * ggfs. die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten

- * ggfs. die Absicht des Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem Drittland oder eine internationale Organisation zu übermitteln

Darüber hinaus hat der Verantwortliche gemäß Artikel 14 Abs. 2 DSGVO der betroffenen Person die folgenden Informationen zur Verfügung zu stellen, die erforderlich sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten:

- * die Dauer, für die die personenbezogenen Daten gespeichert werden oder - falls dies nicht möglich ist - die Kriterien für die Festlegung dieser Dauer
- * ggfs. die berechtigten Interessen, die vom Verantwortlichen oder von einem Dritten verfolgt werden
- * das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden, personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung und eines Widerspruchsrechts gegen die Verarbeitung sowie das Recht auf Datenübertragbarkeit.
- * wenn die Verarbeitung auf Artikel 6 Abs. 1 lit. a oder Artikel 9 Abs. 2 lit. a DSGVO (*Einwilligung*) beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird
- * das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- * aus welcher Quelle die personenbezogenen Daten stammen und ggfs. ob sie aus öffentlich zugänglichen Quellen stammen
- * das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und aussagekräftige Information über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

3.2 Frist für die Information

Gemäß Artikel 14 Abs. 3 DSGVO hat der Verantwortliche die oben angeführten Informationen unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats, zu erteilen. Falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, hat die Mitteilung spätestens zum Zeitpunkt der ersten Mitteilung an sie zu erfolgen. Falls die Offenlegung an einen anderen

Empfänger beabsichtigt ist, hat die Mitteilung spätestens zum Zeitpunkt der ersten Offenlegung zu erfolgen.

3.3 Information bei der Verarbeitung für andere Zwecke

Wenn der Verantwortliche beabsichtigt, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als für den, für den die personenbezogenen Daten erlangt wurden, so hat er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diese und alle anderen maßgeblichen Informationen gemäß der zweiten, in diesem Kapitel enthaltenen Punktereihe zur Verfügung zu stellen.

3.4 Unterbleiben der Informationspflicht

Die in diesem Kapitel dargestellten Mitteilungen müssen nicht erfolgen, wenn und soweit die betroffene Person bereits über die Informationen verfügt oder die Erteilung dieser Informationen sich als unmöglich erweist oder ihr einen unverhältnismäßigen Aufwand erfordern würde oder die Erlangung oder Offenlegung durch Rechtsvorschriften, denen der Verantwortliche unterliegt, ausdrücklich geregelt ist oder die personenbezogenen Daten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen.

4. Auskunftsrecht der betroffenen Person

Gemäß Artikel 15 Abs. 1 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende, personenbezogene Daten verarbeitet werden. Wenn dies der Fall ist, so hat die betroffene Person ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

- * die Verarbeitungszwecke
- * die Kategorien personenbezogener Daten, die verarbeitet werden
- * die Empfänger oder die Kategorien von Empfängern gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen
- * falls möglich, die geplante Dauer, für die die personenbezogenen Daten gespeichert werden oder - falls dies nicht möglich ist - die Kriterien für die Festlegung dieser Dauer

- * das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden, personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung
- * das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- * wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten
- * das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und aussagekräftige Information über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person; der Verantwortliche hat auch eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen. Für alle weiteren Kopien, die die betroffene Person verlangt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Wenn die betroffene Person den Antrag elektronisch stellt, so sind diese Informationen in einem gängigen, elektronischen Format zur Verfügung zu stellen, sofern die betroffene Person nichts anderes verlangt.

5. Recht auf Berichtigung

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung von sie betreffenden, unrichtigen personenbezogenen Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten zu verlangen.

6. Recht auf Löschung („Recht auf Vergessenwerden“)

Gemäß Artikel 17 Abs. 1 DSGVO hat die betroffene Person das Recht, vom Verantwortlichen zu verlangen, dass sie betreffende, personenbezogene Daten unverzüglich gelöscht werden und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

- * die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig

- * die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung stützte und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung
- * die betroffene Person legt gemäß Artikel 21 Abs. 1 DSGVO Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen, berechtigten Gründe für die Verarbeitung vor oder die betroffene Person legt gemäß Artikel 21 Abs. 2 DSGVO Widerspruch gegen die Verarbeitung ein
- * die personenbezogenen Daten wurden unrechtmäßig verarbeitet
- * die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten erforderlich, dem der Verantwortliche unterliegt
- * die personenbezogenen Daten wurden im Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Abs. 1 DSGVO erhoben

Wenn der Verantwortliche die personenbezogenen Daten öffentlich gemacht hat und gemäß Artikel 17 Abs. 1 DSGVO zu deren Löschung verpflichtet ist, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahme, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat. Das Recht auf Löschung gilt gemäß Artikel 17 Abs. 3 DSGVO u.a. dann nicht, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (zB Führung des Mitgliederregisters).

7. Recht auf Einschränkung der Verarbeitung

Die betroffene Person hat gemäß Artikel 18 Abs. 1 DSGVO das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

- * die Richtigkeit der personenbezogenen Daten wird von der betroffenen Person bestritten und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen

- * die Verarbeitung ist unrechtmäßig und die betroffene Person lehnt die Löschung der personenbezogenen Daten ab und verlangt stattdessen die Einschränkung der Nutzung der personenbezogenen Daten
- * der Verantwortliche benötigt die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger, die betroffene Person benötigt sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
- * oder die betroffene Person hat Widerspruch gegen die Verarbeitung eingelegt, so lange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen

Wenn die Verarbeitung gemäß Artikel 18 Abs. 1 DSGVO eingeschränkt wurde, so dürfen diese personenbezogenen Daten gemäß Abs. 2 - von ihrer Speicherung abgesehen - nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen, natürlichen oder juristischen Person oder aus Gründen eines wichtigen, öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden.

8. Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung

Der Verantwortliche ist gemäß Artikel 19 DSGVO verpflichtet, allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung mitzuteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der Verantwortliche hat die betroffene Person über diese Empfänger zu unterrichten, wenn die betroffene Person dies verlangt.

9. Recht auf Datenübertragbarkeit

Die betroffene Person hat gemäß Artikel 20 DSGVO das Recht, die sie betreffenden, personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln. Dies gilt unter folgenden Voraussetzungen:

- * die Verarbeitung beruht auf einer Einwilligung oder auf einem Vertrag und
- * die Verarbeitung erfolgte mit Hilfe automatisierter Verfahren

Bei der Ausübung des Rechts auf Datenübertragbarkeit hat die betroffene Person das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.

10. Widerspruchsrecht

Die betroffene Person hat gemäß Artikel 21 DSGVO das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender, personenbezogener Daten, die aufgrund von Artikel 6 Abs. 1 lit. e (*öffentliches Interesse, Ausübung öffentlicher Gewalt*) oder f (*berechtigte Interessen des Verantwortlichen oder eines Dritten*) DSGVO erfolgt, Widerspruch einzulegen. Dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Der Verantwortliche darf dann die personenbezogenen Daten nicht mehr verarbeiten, es sei denn, er kann zwingende, schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender, personenbezogener Daten zum Zweck derartiger Werbung einzulegen, dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.

Wenn die betroffene Person der Verarbeitung für Zwecke der Direktwerbung widerspricht, so dürfen die personenbezogenen Daten nicht mehr für diese Zwecke ver-

arbeitet werden (Artikel 21 Abs. 3 DSGVO). Die betroffene Person muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf ihr Recht auf Widerspruch hingewiesen werden. Dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

11. automatisierte Entscheidung im Einzelfall einschließlich Profiling

Gemäß Artikel 22 Abs. 1 DSGVO hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung - einschließlich Profiling - beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkungen entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Dies gilt dann nicht, wenn die Entscheidung

- * für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist
- * aufgrund von Rechtsvorschriften der EU oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
- * mit ausdrücklicher Einwilligung der betroffenen Person erfolgt

Im Zusammenhang mit dem ersten und dritten Punkt o.g. Aufzählung trifft der Verantwortliche angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu zumindest das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.

VI. FÜR DIE DATENVERARBEITUNG VERANTWORTLICHE UND AUFTRAGSVERARBEITER

1. Verantwortung des für die Verarbeitung Verantwortlichen

Gemäß Artikel 24 DSGVO hat der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DSGVO erfolgt. Diese Maßnahmen müssen erforderlichenfalls überprüft und aktualisiert werden.

Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen die Anwendung der Datenschutzvorkehrungen durch den Verantwortlichen umfassen.

Gemäß Artikel 24 Abs. 3 DSGVO kann auf die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 DSGVO oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 DSGVO verwiesen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.

2. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

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 mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche gemäß Artikel 25 Abs. 1 DSGVO sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete, technische und organisatorische Maßnahmen - wie beispielsweise Pseudonymisierung - die dafür ausgelegt sind, die Datenschutzgrundsätze - etwa Datenminimierung - wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Personen zu schützen.

Weiters hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen, bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihrer Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

So kann beispielsweise ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 DSGVO zum Nachweis der Erfüllung der hier genannten Anforderungen dienen.

3. gemeinsam für die Verarbeitung Verantwortliche

Wenn zwei oder mehrere Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen, so sind sie gemeinsam Verantwortliche. Gemäß Artikel 26 Abs. 1 DSGVO haben sie in einer Vereinbarung in transparenter Form festzulegen, wer von ihnen welche Verpflichtung gemäß der DSGVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 DSGVO nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann auch eine Anlaufstelle für die betroffene Person angegeben werden.

Gemäß Artikel 26 Abs. 2 DSGVO muss die Vereinbarung die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das wesentliche der Vereinbarung muss der betroffenen Person zur Verfügung gestellt werden.

4. Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern

In den Fällen gemäß Artikel 3 Abs. 2 DSGVO hat der Verantwortliche oder der Auftragsverarbeiter schriftlich einen Vertreter in der Union zu nennen. Diese Pflicht gilt gemäß Artikel 27 Abs. 2 DSGVO nicht für

- * eine Verarbeitung, die nur gelegentlich erfolgt, nicht die umfangreiche Verarbeitung besonderer Datenkategorien iSd Artikel 9 Abs. 1 DSGVO einschließt

und unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt oder

- * Behörden oder öffentliche Stellen

Der Vertreter muss gemäß Artikel 27 Abs. 3 DSGVO in einem der Mitgliedstaaten niedergelassen sein, in denen die betroffenen Personen sich befinden, deren personenbezogene Daten im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen verarbeitet werden oder deren Verhalten beobachtet wird.

5. Auftragsverarbeiter

5.1 Auswahl

Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser gemäß Artikel 28 Abs. 1 DSGVO nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete, technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

5.2 Sub-Auftragsverarbeiter

Gemäß Artikel 28 Abs. 2 DSGVO darf der Auftragsverarbeiter keinen weiteren Auftragsverarbeiter ohne vorherige, gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch nehmen. Im Fall einer allgemeinen, schriftlichen Genehmigung hat der Auftragsverarbeiter den Verantwortlichen immer zu informieren, über jede beabsichtigte Änderung im Bezug auf die Hinzuziehung oder die Einsetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

5.3 Grundlage für die Auftragsverarbeitung

Die Verarbeitung durch einen Auftragsverarbeiter hat auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Recht der EU oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter im Bezug auf den Verantwortlichen bindet und in dem

- * Gegenstand und Dauer der Verarbeitung
- * Art und Zweck der Verarbeitung
- * die Art der personenbezogenen Daten
- * die Kategorie betroffener Personen und
- * die Pflichten und Rechte des Verantwortlichen

festgelegt sind. Dieser Vertrag (Muster 11 *Vereinbarung über Auftragsverarbeitung*) bzw. dieses andere Rechtsinstrument hat insbesondere vorzusehen, dass der Auftragsverarbeiter

- * die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen - auch im Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation - verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall hat der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mitzuteilen, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen, öffentlichen Interesses verbietet
- * gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen, gesetzlichen Verschwiegenheitspflicht unterliegen
- * alle gemäß Artikel 32 DSGVO (*Sicherheit der Verarbeitung*) (siehe Kapitel VI Punkt 10.) erforderlichen Maßnahmen ergreift
- * die Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält (siehe dazu im Anschluss an diese Aufzählung)
- * angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten, technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträge auf Wahrnehmung der in Kapitel III. genannten Rechte der betroffenen Person nachzukommen
- * unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikel 32 bis 36¹⁰ DSGVO genannten Pflichten unterstützt
- * nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Recht der EU oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht
- * dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt

¹⁰ *Sicherheit der Verarbeitung; Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und die betroffene Person; Datenschutz-Folgenabschätzung; vorherige Konsultation*

und Überprüfungen - einschließlich Inspektionen - die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt; im Hinblick darauf informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder Mitgliedstaaten verstößt

5.4 Sub-Auftragsverarbeitung

Wenn der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch nimmt, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so müssen diesem weiteren Auftragsverarbeiter im Wege eines Vertrag oder eines anderen Rechtsinstruments der EU oder dem Recht des betreffenden Mitgliedsstaats die selben Datenschutzpflichten auferlegt werden, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten, technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jedes anderen Auftragsverarbeiters. Als Nachweis der Einhaltung der hinreichenden Garantien kann die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 DSGVO oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 DSGVO durch einen Auftragsverarbeiter als Faktor herangezogen werden.

5.5 Standardvertragsklauseln und Form

Sowohl die Kommission als auch eine Aufsichtsbehörde kann Standardvertragsklauseln zur Einhaltung der Regelungen des Artikels 28 DSGVO festlegen.

Der Vertrag oder das andere Rechtsinstrument im vorgenannten Sinn ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

6. Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten gemäß Artikel 29 DSGVO ausschließlich auf Weisung des Verant-

wortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

7. Verzeichnis von Verarbeitungstätigkeiten

7.1 Inhalt für Verantwortliche

Gemäß Artikel 30 Abs. 1 DSGVO führen jeder Verantwortliche und ggfs. sein Vertreter ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis muss alle nachstehenden Angaben enthalten:

- * Namen und Kontaktdaten des Verantwortlichen und ggfs. des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten
- * Zwecke der Verarbeitung
- * Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- * Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen
- * ggfs. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation sowie bei dem in Artikel 49 Abs. 1, Unterabsatz 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien
- * wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- * wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DSGVO

7.2 Inhalt für Auftragsverarbeiter

Jeder Auftragsverarbeiter und ggfs. sein Vertreter haben ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung zu führen, die gemäß Artikel 30 Abs. 2 DSGVO folgende Angaben enthalten muss:

- * Namen und Kontaktdaten des Auftragsverarbeiter oder der Auftragsverarbeiter und jedes Verantwortlichen in dessen Auftrag der Auftragsverarbeiter tätig ist sowie ggfs. des Vertreter des Verantwortlichen oder des Auftragsverarbeiter und eines etwaigen Datenschutzbeauftragten
- * Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden
- * ggfs. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation sowie bei den in Artikel 49 Abs. 1 Unterabsatz 2 DSGVO genannten Datenübermittlungen, die Dokumentierung geeigneter Garantien
- * wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DSGVO

7.3 Form

Die beiden genannten Verzeichnisse sind schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann. Der Verantwortliche oder der Auftragsverarbeiter sowie ggfs. der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

7.4 Entfall der Verpflichtung

Die Verpflichtung zur Führung der genannten Verzeichnisse gilt nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn,

- * die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Person
- * die Verarbeitung erfolgt nicht nur gelegentlich oder
- * es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Abs. 1 DSGVO

8. Zusammenarbeit mit der Aufsichtsbehörde

Gemäß Artikel 31 DSGVO haben sowohl der Verantwortlich als auch der Auftragsverarbeiter und ggfs. deren Vertreter auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenzuarbeiten.

9. Sicherheit der Verarbeitung

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 des Risikos für die Rechte und Freiheiten natürlicher Personen haben der Verantwortliche und der Auftragsverarbeiter gemäß Artikel 32 Abs. 1 DSGVO geeignete, technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen u.a. folgendes ein:

- * die Pseudonymisierung und Verschlüsselung personenbezogener Daten
- * Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der System und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- * Fähigkeit, Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- * ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmäßig - Vernichtung, Verlust, Veränderung oder befugte Offenlegung von bzw. unbefugtem Zugang von personenbezogenen Daten, übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 DSGVO oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 DSGVO kann als Faktor herangezogen werden, um die Erfüllung der in diesem Kapitel genannten Anforderungen nachzuweisen.

Der Verantwortliche und der Auftragsverarbeiter haben gemäß Artikel 32 Abs. 4 DSGVO Schritte zu unternehmen, um sicherzustellen, dass ihnen unterstellte, natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

10. Datensicherheitsmaßnahmen nach dem Datenschutzanpassungsgesetz

Der Verantwortliche und der Auftragsverarbeiter haben im Hinblick auf die automatisierte Verarbeitung nach einer Risikobewertung Maßnahmen zu ergreifen, um folgende Zwecke zu erreichen:

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (**Zugangskontrolle**);
2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (**Datenträgerkontrolle**);
3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (**Speicherkontrolle**);
4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (**Benutzerkontrolle**);
5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (**Zugriffskontrolle**);
6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (**Übertragungskontrolle**);
7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (**Eingabekontrolle**);

8. Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (**Transportkontrolle**);
9. Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können (**Wiederherstellung**);
10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (**Datenintegrität**).

11. Meldung von Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde

11.1 Frist

Im Fall einer Verletzung des Schutzes personenbezogener Daten hat der Verantwortliche gemäß Artikel 33 Abs. 1 DSGVO unverzüglich und binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde zu melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen der genannten Frist, so ist ihr eine Begründung für die Verzögerung beizufügen.

Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, hat er diese dem Verantwortlichen gemäß § 33 Abs. 2 DSGVO unverzüglich zu melden (Muster 10 *Benachrichtigung von der Verletzung des Schutzes personenbezogener Daten*).

11.2 Inhalt der Meldung

Die Meldung des Verantwortlichen an die Aufsichtsbehörde hat zumindest folgende Informationen zu enthalten:

- * eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der personenbezogenen Datensätze
- * den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen

- * eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
- * eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und ggfs. Maßnahmen zur Abmilderung ihrer möglichen, nachteiligen Auswirkungen

Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung auch schrittweise zur Verfügung stellen.

Der Verantwortliche hat gemäß Artikel 33 Abs. 5 DSGVO Verletzung des Schutzes personenbezogener Daten einschließlich im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten zu dokumentieren, ebenso deren Auswirkungen und die ergriffenen Abhilfemaßnahmen. Diese Dokumentation ermöglicht der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen des Artikel 33 DSGVO.

12. Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

12.1 Voraussetzung für das Erfordernis

Wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat, so hat der Verantwortliche gemäß Artikel 34 Abs. 1 DSGVO die betroffene Person unverzüglich von der Verletzung zu benachrichtigen (Muster 9 *Benachrichtigung von der Verletzung des Schutzes personenbezogener Daten*). Die Benachrichtigung hat in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten zu beschreiben und zumindest die in Artikel 33 Abs. 3 lit. b, c und d DSGVO genannten Informationen und Empfehlungen zu enthalten.

12.2 Entfall des Erfordernisses

Gemäß Artikel 34 Abs. 3 DSGVO ist die Benachrichtigung der betroffenen Person nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

- * der Verantwortliche hat geeignete, technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen wurden auf die von der Verletzung betroffenen, personenbezogenen Daten angewandt, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht

zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung

- * der Verantwortliche hat durch nachfolgende Maßnahmen sichergestellt, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Person aller Wahrscheinlichkeit nach nicht mehr besteht
- * die Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden; in diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden

Wenn der Verantwortliche die betroffene Person nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann die Aufsichtsbehörde unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen oder sie kann mit einem Beschluss feststellen, dass bestimmte der in der o.g. Punktreihe genannten Voraussetzungen erfüllt sind.

13. Datenschutz-Folgenabschätzung

13.1 Voraussetzungen

Die Datenschutz-Folgenabschätzung ist in Artikel 35 DSGVO geregelt. Wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, so hat der Verantwortliche gemäß Artikel 35 Abs. 1 DSGVO vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen. Für die Untersuchung mehrerer, ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

Der Verantwortliche hat bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten einzuholen, sofern ein solcher benannt wurde. Eine Datenschutz-Folgenabschätzung ist gemäß Artikel 35 Abs. 3 DSGVO insbesondere in folgenden Fällen erforderlich:

- * systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechts-

wirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen

- * umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Abs. 1 DSGVO (*Einwilligung*) oder
- * systematische, umfangreiche Überwachung öffentlich zugänglicher Bereiche

Gemäß Artikel 35 Abs. 4 DSGVO erstellt die Aufsichtsbehörde eine Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist und veröffentlicht diese. Diese Liste wird als Anlage angeschlossen, sobald sie vorliegt.

Weiters kann die Aufsichtsbehörde eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Diese von der Datenschutzbehörde zu veröffentlichende Liste wird als Anlage angeschlossen, sobald sie vorliegt.

13.2 Inhalt / Umfang

Gemäß Artikel 35 Abs. 7 DSGVO hat die Folgenabschätzung zumindest folgendes zu enthalten:

- * eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und die Zwecke der Verarbeitung, ggfs. einschließlich der von dem Verantwortlichen verfolgten, berechtigten Interessen
- * eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- * eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und
- * die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die DSGVO eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen werden muss.

Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 DSGVO durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgängen, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung,

gebührend zu berücksichtigen. Der Verantwortliche hat ggfs. den Standpunkt der betroffenen Person oder ihrer Vertreter zur beabsichtigten Verarbeitung einzuholen.

Erforderlichenfalls hat der Verantwortliche eine Überprüfung durchzuführen, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird. Dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

13.3 Vorgehensweise für bereits existierende Verarbeitungsvorgänge

Für die existierenden Verarbeitungsvorgänge ist grundsätzlich keine Datenschutz-Folgenabschätzung durchzuführen, wenn für diese Verarbeitungsvorgänge durch die Datenschutzbehörde bereits zu einem früheren Zeitpunkt im Zuge einer DVR-Registrierung im Rahmen eines Vorabkontrollverfahrens gemäß § 18 Datenschutzgesetz 2000 (DSG 2000) genehmigt wurde. Bei der automatischen Registrierung über DVR-Online oder in Fällen, in denen die Datenschutzbehörde eine Datenanwendung registriert hat, jedoch kein Fall der Vorabkontrolle vorgelegen ist (das betrifft nichtvorabkontrollpflichtige Meldungen vor dem 01.09.2012), kommt dies hingegen nicht in Betracht.

Kommt es jedoch zu einer Änderung bestehender Verarbeitungsvorgänge, ist sehr wohl eine Datenschutz-Folgenabschätzung durchzuführen, wenn die Voraussetzungen des Artikel 35 Abs. 1 DSGVO zutreffen. Generell wird empfohlen, bereits existierende Datenverarbeitungsvorgänge einer regelmäßigen Evaluierung zu unterziehen, ob sich Voraussetzungen geändert haben. Bejahendenfalls wäre - bei Vorliegen aller Voraussetzungen - eine Datenschutz-Folgenabschätzung durchzuführen. Überdies wird empfohlen, auch zu dokumentieren, aus welchen Gründen keine Datenschutz-Folgenabschätzung durchgeführt wurde.

14. vorherige Konsultation

Der Verantwortliche hat gemäß Artikel 36 Abs. 1 DSGVO vor der Verarbeitung die Aufsichtsbehörde zu konsultieren, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

Falls die Aufsichtsbehörde der Auffassung ist, dass die geplante Verarbeitung nicht im Einklang mit der DSGVO stünde, insbesondere, weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, hat sie dem Verantwortlichen gemäß Artikel 36 Abs. 2 DSGVO und ggfs. dem Auftragsverarbeiter innerhalb eines Zeitraums von bis zu acht Wochen nach Erhalt des Ersuchens um Konsultation entsprechende, schriftliche Empfehlungen zu geben und

kann ihre in Artikel 58 DSGVO genannten Befugnisse ausüben, darunter erforderlichenfalls die Befugnis, ein Verbot der Datenverarbeitung auszusprechen. Diese Frist kann unter Berücksichtigung der Komplexität der geplanten Verarbeitung um sechs Wochen verlängert werden. Die Aufsichtsbehörde hat den Verantwortlichen oder ggfs. den Auftragsverarbeiter über eine solche Fristverlängerung binnen eines Monats nach Eingang des Antrags auf Konsultation zusammen mit den Gründen für die Verzögerung zu unterrichten. Diese Fristen können ausgesetzt werden, bis die Aufsichtsbehörde die für die Zwecke der Konsultation angeforderten Informationen erhalten hat.

Gemäß Artikel 36 Abs. 3 DSGVO hat der Verantwortliche der Aufsichtsbehörde bei einer Konsultation folgende Informationen zur Verfügung zu stellen:

- * ggfs. Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unternehmen
- * die Zwecke und Mittel der beabsichtigten Verarbeitung
- * die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß der DSGVO vorgesehenen Maßnahmen und Garantien
- * ggfs. die Kontaktdaten des Datenschutzbeauftragten
- * die Datenschutz-Folgenabschätzung und
- * alle sonstigen, von der Aufsichtsbehörde geforderten Informationen

15. Benennung eines Datenschutzbeauftragten

Der Verantwortliche und der Auftragsverarbeiter haben gemäß Artikel 37 DSGVO auf jeden Fall einen Datenschutzbeauftragten zu benennen, wenn

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

- * die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiter in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 DSGVO besteht

Eine Unternehmensgruppe darf gemäß Artikel 37 Abs. 2 DSGVO einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.

Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt sowie auf der Grundlage seiner Fähigkeiten zur Erfüllung der in Artikel 39 DSGVO genannten Aufgaben. Der Datenschutzbeauftragte kann auch Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgabe auf der Grundlage eines Dienstleistungsvertrags erfüllen. Der Verantwortliche oder der Auftragsverarbeiter haben die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen und diese Daten der Aufsichtsbehörde mitzuteilen.

16. Stellung des Datenschutzbeauftragten

Der Verantwortliche und der Auftragsverarbeiter haben gemäß Artikel 38 Abs. 1 DSGVO sicherzustellen, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird. Der Verantwortliche und der Auftragsverarbeiter haben den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 39 DSGVO zu unterstützen, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung zu stellen.

Weiters haben der Verantwortliche und der Auftragsverarbeiter sicherzustellen, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bzgl. der Ausübung dieser Aufgaben erhält. Der Datenschutzbeauftragte darf vom Verantwortlichen oder Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Der Datenschutzbeauftragte hat unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters zu berichten.

Betroffene Personen können den Datenschutzbeauftragten gemäß Artikel 38 Abs. 4 DSGVO zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der

Wahrnehmung ihrer Rechte gemäß der DSGVO im Zusammenhang stehenden Fragen zu Rate ziehen.

Der Datenschutzbeauftragte ist nach dem Recht der EU oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden. Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter haben aber sicherzustellen, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

17. Aufgaben des Datenschutzbeauftragten

Dem Datenschutzbeauftragten obliegen gemäß Artikel 39 Abs. 1 DSGVO zumindest die folgenden Aufgaben:

- * Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiter und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach der DSGVO sowie nach sonstigen Datenschutzvorschriften
- * Überwachung der Einhaltung der DSGVO, anderer Datenschutzvorschriften sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen
- * Beratung - auf Anfrage - im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung
- * Zusammenarbeit mit der Aufsichtsbehörde
- * Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen einschließlich der vorherigen Konsultation gemäß Artikel 36 DSGVO und ggfs. Beratung zu allen sonstigen Fragen

Gemäß Artikel 39 Abs. 2 DSGVO trägt der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung zu berücksichtigen hat.

18. Zertifizierung

Die Mitgliedstaaten, Aufsichtsbehörden, der Ausschuss und die Kommission haben insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen zu fördern, die dazu dienen, nachzuweisen, dass die Bestimmungen der DSGVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten werden. Den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen ist dabei Rechnung zu tragen.

Zusätzlich zur Einhaltung durch die unter die DSGVO fallenden Verantwortlichen oder Auftragsverarbeiter können auch datenschutzspezifische Zertifizierungsverfahren, Siegel oder Prüfzeichen, die gemäß Artikel 42 Abs. 5 DSGVO genehmigt worden sind, vorgesehen werden, um nachzuweisen, dass die Verantwortlichen oder Auftragsverarbeiter, die gemäß Artikel 3 DSGVO nicht unter die DSGVO fallen, im Rahmen personenbezogener Daten an Drittländer oder internationale Organisationen nach Maßgabe von Artikel 46 Abs. 2 lit. f DSGVO geeignete Garantien bieten. Diese Verantwortlichen oder Auftragsverarbeiter gehen mittels vertraglicher oder sonstiger, rechtlicher bindender Instrumente die verbindliche und durchsetzbare Verpflichtung ein, diese geeigneten Garantien anzuwenden, auch im Hinblick auf die Rechte der betroffenen Personen.

Gemäß Artikel 42 Abs. 3 DSGVO muss die Zertifizierung freiwillig und über ein transparentes Verfahren zugänglich sein. Eine Zertifizierung gemäß Artikel 42 DSGVO mindert nicht die Verantwortung des Verantwortlichen oder des Auftragsverarbeiters für die Einhaltung der DSGVO und berührt nicht die Aufgaben und Befugnisse der Aufsichtsbehörden.

Die Zertifizierung wird einem Verantwortlichen oder einem Auftragsverarbeiter gemäß Artikel 42 Abs. 7 DSGVO für eine Höchstdauer von drei Jahren erteilt und kann unter den selben Bedingungen verlängert werden, sofern die einschlägigen Voraussetzungen weiterhin erfüllt werden. Die Zertifizierung wird ggfs. durch die Zertifizierungsstelle nach Artikel 43 DSGVO oder durch die zuständige Aufsichtsbehörde widerrufen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden. Der Ausschuss hat alle Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen in ein Register aufzunehmen und in geeigneter Weise zu veröffentlichen.

VII. ÜBERMITTLUNG PERSONENBEZOGENER DATEN AN DRITTLÄNDER ODER AN INTERNATIONALE ORGANISATIONEN

1. allgemeine Grundsätze der Datenübermittlung

Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet wurden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist gemäß Artikel 44 DSGVO nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in der DSGVO niedergelegten Bedingungen einhalten. Dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende, internationale Organisation an ein anderes Drittland oder eine andere, internationale Organisation. Damit soll sichergestellt werden, dass das durch die DSGVO gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

2. Datenübermittlung auf Grundlage eines Angemessenheitsbeschlusses

Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf gemäß Artikel 45 Abs. 1 DSGVO vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende, internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung. Es muss allerdings beachtet werden, dass die Kommission den Angemessenheitsbeschluss auch wieder widerrufen kann.

3. Datenübermittlung vorbehaltlich geeigneter Garantien

Falls kein Angemessenheitsbeschluss vorliegt, darf ein Verantwortlicher oder ein Auftragsverarbeiter gemäß Artikel 46 Abs. 1 DSGVO personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

Diese geeigneten Garantien können, ohne dass dazu eine besondere Genehmigung einer Aufsichtsbehörde erforderlich wäre, in folgenden bestehen:

- * einem rechtlich bindenden und durchsetzbaren Dokument zwischen den Behörden oder öffentlichen Stellen
- * verbindlichen, internen Datenschutzvorschriften gemäß Artikel 47 DSGVO
- * Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Abs. 2 DSGVO erlassen werden
- * vor einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Abs. 2 DSGVO genehmigt wurden
- * genehmigten Verhaltensregeln gemäß Artikel 40 DSGVO zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtung des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich im Bezug auf die Rechte der betroffenen Personen oder
- * einem genehmigten Zertifizierungsmechanismus gemäß Artikel 42 DSGVO zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen

Vorbehaltlich der Genehmigung durch die zuständige Aufsichtsbehörde können die geeigneten Garantien gemäß Artikel 46 Abs. 3 DSGVO auch insbesondere bestehen in:

- * Vertragsklauseln, die zwischen dem Verantwortlichen oder dem Auftragsverarbeiter und dem Verantwortlichen, dem Auftragsverarbeiter oder dem Empfänger der personenbezogenen Daten im Drittland oder der internationalen Organisation vereinbart wurden, oder
- * Bestimmungen, die in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen aufzunehmen sind und durchsetzbare und wirksame Rechte für die betroffenen Personen einschließen

4. nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung

Jegliches Urteil eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird, dürfen gemäß Artikel 48 DSGVO nur dann anerkannt oder vollstreckt werden, wenn sie auf eine in Kraft befindliche, internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der EU oder einem Mitgliedstaat gestützt sind.

5. Ausnahme für bestimmte Fälle

Falls weder ein Angemessenheitsbeschluss nach Artikel 45 Abs. 3 DSGVO vorliegt, noch eine geeignete Garantie nach Artikel 46 DSGVO, einschließlich verbindlicher, interner Datenschutzvorschriften, bestehen, ist gemäß Artikel 49 DSGVO eine Übermittlung oder eine Reihe von Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur gemäß den folgenden Bedingungen zulässig:

- * die betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die für sie bestehenden, möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde
- * die Übermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich
- * die Übermittlung ist zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich
- * die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig
- * die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich

- * die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen außer Stande ist, ihre Einwilligung zu geben
- * die Übermittlung erfolgt aus einem Register, das gemäß dem Recht der EU oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht aber nur soweit die im Recht der Union oder der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

Falls die Übermittlung nicht auf eine Bestimmung der Artikel 45 oder 46 DSGVO - einschließlich der verbindlichen, internen Datenschutzvorschriften - gestützt werden könnte und keine der soeben genannten Ausnahmen anwendbar ist, darf eine Übermittlung an ein Drittland oder eine internationale Organisation nur dann erfolgen, wenn

- * die Übermittlung nicht wiederholt erfolgt
- * nur eine begrenzte Zahl von betroffenen Personen betrifft
- * für die Wahrung der zwingenden, berechtigten Interessen des Verantwortlichen erforderlich ist
- * sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen
- * und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung angemessene Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat

Der Verantwortliche hat die Aufsichtsbehörde von der Übermittlung in Kenntnis zu setzen. Weiters hat der Verantwortliche die betroffene Person über die Übermittlung und seine zwingenden, berechtigten Interessen zu unterrichten.

VIII. BILDVERARBEITUNG GEMÄß § 12 DATENSCHUTZ-ANPASSUNGSGESETZ

Eine Bildaufnahme iSd § 12 Datenschutz-Anpassungsgesetz ist unter Berücksichtigung der Vorgaben gemäß § 13 Datenschutz-Anpassungsgesetz zulässig, wenn

- * sie im lebenswichtigen Interesse einer Person erforderlich ist
- * die betroffene Person zur Verarbeitung ihrer personenbezogenen Daten eingewilligt hat
- * sie durch besondere, gesetzliche Bestimmungen angeordnet oder erlaubt ist oder
- * im Einzelfall überwiegende, berechtigte Interessen des Verantwortlichen oder eines Dritten bestehen und die Verhältnismäßigkeit gegeben ist, in diesem Fall ist eine Bildaufnahme insbesondere dann zulässig, wenn
 - sie dem vorbeugenden Schutz von Personen oder Sachen auf privaten Liegenschaften, die ausschließlich vom Verantwortlichen genutzt werden, dient und räumlich nicht über die Liegenschaft hinausreicht, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen
 - sie für den vorbeugenden Schutz von Personen oder Sachen an öffentlich zugänglichen Orten, die dem Hausrecht des Verantwortlichen unterliegen, aufgrund bereits erfolgter Rechtsverletzungen oder eines in der Natur des Orts liegenden, besonderen Gefährdungspotentials erforderlich ist und kein gelinderes, geeignetes Mittel zur Verfügung steht oder
 - sie ein privates Dokumentationsinteresse verfolgt, das nicht auf die identifizierende Erfassung unbeteiligter Personen oder die gezielte Erfassung von Objekten, die sich zur mittelbaren Identifizierung einer solchen Person eignen, gerichtet ist.

Gemäß § 12 Abs. 4 Datenschutz-Anpassungsgesetz ist unzulässig:

- * eine Bildaufnahme ohne ausdrückliche Einwilligung der betroffenen Person in deren höchstpersönlichem Lebensbereich

- * eine Bildaufnahme zum Zweck der Kontrolle von Arbeitnehmern
- * der automationsunterstützte Abgleich von mittels Bildaufnahmen gewonnenen, personenbezogenen Daten mit anderen personenbezogenen Daten oder
- * die Auswertung von mittels Bildaufnahmen gewonnenen, personenbezogenen Daten anhand von besonderen Kategorien personenbezogener Daten als Auswahlkriterium

Gemäß § 13 Abs. 1 Datenschutz-Anpassungsgesetz hat der Verantwortliche dem Risiko des Eingriffs angepasste, geeignete Datensicherheitsmaßnahmen zu ergreifen und dafür zu sorgen, dass der Zugang zur Bildaufnahme und eine nachträgliche Veränderung derselben durch Unbefugte ausgeschlossen ist. Der Verantwortliche hat - außer in den Fällen einer Echtzeitüberwachung - jeden Verarbeitungsvorgang zu protokollieren. Gemäß § 13 Abs. 3 Datenschutz-Anpassungsgesetz sind vom Verantwortlichen aufgenommene, personenbezogenen Daten zu löschen, wenn sie für den Zweck, für den sie ermittelt wurden, nicht mehr benötigt werden und keine andere, gesetzlich vorgesehene Aufbewahrungsfrist besteht. Eine länger als 72 Stunden andauernde Aufbewahrung muss verhältnismäßig sein und ist gesondert zu protokollieren und zu begründen. Dies gilt nicht für nur im privaten Dokumentationsinteresse erfolgte Bildaufnahmen.

Gemäß § 13 Abs. 5 Datenschutz-Anpassungsgesetz hat der Verantwortliche einer Bildaufnahme diese geeignet zu kennzeichnen. Aus der Kennzeichnung hat jedenfalls der Verantwortliche eindeutig hervorzugehen, es sei denn, diese ist den betroffenen Personen nach den Umständen des Falls bereits bekannt. Dies gilt nicht für ausschließlich mit privatem Dokumentationsinteresse erstellte Bildaufnahmen.

Werden keine ausreichenden Informationen bereitgestellt, kann jeder von einer Verarbeitung potentiell betroffene gemäß § 13 Abs. 7 Datenschutz-Anpassungsgesetz vom Eigentümer oder Nutzungsberechtigten einer Liegenschaft oder eines Gebäudes oder sonstigen Objekts, von dem aus eine solche Verarbeitung augenscheinlich ausgeht, Auskunft über die Identität des Verantwortlichen begehren.

IX. RECHTSBEHELFE, HAFTUNG UND SANKTIONEN

1. Recht auf Beschwerde bei einer Aufsichtsbehörde

Gemäß Artikel 73 Abs. 1 DSGVO hat jede betroffene Person unbeschadet eines anderweitigen, verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei der Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres Aufenthaltsort, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden, personenbezogenen Daten gegen die DSGVO verstößt. Die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, hat den Beschwerdeführer über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach Artikel 78 DSGVO zu unterrichten.

Gemäß § 24 Abs. 2 Datenschutz-Anpassungsgesetz hat die Beschwerde zu enthalten:

- * die Bezeichnung des als verletzt erachteten Rechts
- * soweit dies zumutbar ist, die Bezeichnung des Rechtsträgers oder Organs, dem die behauptete Rechtsverletzung zugerechnet wird, der sogenannte Beschwerdegegner
- * den Sachverhalt, aus dem die Rechtsverletzung abgeleitet wird
- * die Gründe, auf die sich die Behauptung der Rechtswidrigkeit stützt
- * das Begehen, die behauptete Rechtsverletzung festzustellen und
- * die Angaben, die erforderlich sind, um zu beurteilen, ob die Beschwerde rechtzeitig eingebracht ist

Einer Beschwerde sind ggfs. der zugrundeliegende Antrag und eine allfällige Antwort des Beschwerdegegners anzuschließen.

Gemäß § 4 Datenschutz-Anpassungsgesetz erlischt der Anspruch auf Behandlung einer Beschwerde, wenn der Einschreiter sie nicht binnen eines Jahres, nachdem er Kenntnis von dem beschwerenden Ereignis erlangt hat, längstens aber binnen drei Jahren, nachdem das Ereignis behauptetermaßen stattgefunden hat, einbringt. Verspätete Beschwerden sind zurückzuweisen.

Gemäß § 24 Abs. 6 Datenschutz-Anpassungsgesetz kann ein Beschwerdegegner bis zum Abschluss des Verfahrens vor der Datenschutzbehörde die behauptete Rechtsverletzung nachträglich beseitigen, in dem er den Anträgen des Beschwerdeführers entspricht. Erscheint der Datenschutzbehörde die Beschwerde insofern als gegenstandslos, so hat sie den Beschwerdeführer dazu zu hören. Gleichzeitig ist darauf aufmerksam zu machen, dass die Datenschutzbehörde das Verfahren formlos einstellen wird, wenn er nicht innerhalb einer angemessenen Frist begründet, warum er die ursprünglich behauptete Rechtsverletzung zumindest teilweise nach wie vor als nicht beseitigt erachtet.

2. Recht auf wirksamen, gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde

Jede natürliche oder juristische Person hat gemäß Artikel 78 DSGVO - unbeschadet eines anderweitigen, verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs - das Recht auf einen wirksamen, gerichtlichen Rechtsbehelf gegen einen sie betreffenden, rechtsverbindlichen Beschluss einer Aufsichtsbehörde.

Gemäß § 24 Abs. 8 Datenschutz-Anpassungsgesetz hat jede betroffene Person das Recht, das Bundesverwaltungsgericht zu befassen, wenn sich die Datenschutzbehörde nicht mit der Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der erhobenen Beschwerde in Kenntnis gesetzt hat.

Weiters hat jede betroffene Person gemäß Artikel 78 Abs. 2 DSGVO unbeschadet eines anderweitigen, verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen, gerichtlichen Rechtsbehelf, wenn die zuständige Aufsichtsbehörde sich nicht mit einer Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der erhobenen Beschwerde in Kenntnis gesetzt hat.

3. Recht auf wirksamen, gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter

Jede betroffene Person hat - unbeschadet eines verfügbaren, verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde - das Recht auf einen wirksamen, gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund der DSGVO zustehenden Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogener Daten verletzt wurden. Gemäß Artikel 79 Abs. 2 DSGVO sind

für Klagen gegen einen Verantwortlichen oder einen Auftragsverarbeiter die Gerichte des Mitgliedstaats zuständig, in dem der Verantwortliche oder Auftragsverarbeiter eine Niederlassung hat. Wahlweise können solche Klagen auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren Aufenthaltsort hat.

Gemäß § 29 Abs. 1 Datenschutz-Anpassungsgesetz hat jede Person, der wegen eines Verstoßes gegen die DSGVO oder gegen § 1 oder Artikel 2, erstes Hauptstück Datenschutz-Anpassungsgesetz ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Für Klagen auf Schadenersatz ist gemäß § 29 Abs. 2 Datenschutz-Anpassungsgesetz in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel der Kläger (Antragsteller) seinen gewöhnlichen Aufenthalt oder Sitz hat. Klagen (Anträge) können aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Beklagte seinen gewöhnlichen Aufenthalt oder Sitz oder eine Niederlassung hat.

4. Vertretung von betroffenen Personen

Die betroffene Person hat gemäß Artikel 80 Abs. 1 DSGVO das Recht, eine Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht, die ordnungsgemäß nach dem Recht eines Mitgliedstaats gegründet ist, deren satzungsgemäße Ziele im öffentlichen Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen im Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist, zu beauftragen, in ihrem Namen eine Beschwerde einzureichen, in ihrem Namen die in den Artikeln 77, 78 und 79 DSGVO genannten Rechte wahrzunehmen und das Recht auf Schadenersatz gemäß Artikel 82 DSGVO in Anspruch zu nehmen, sofern dieses im Recht der Mitgliedstaaten vorgesehen ist. In Österreich kann sohin beispielsweise eine Vertretung durch die *Arbeiterkammer* oder den *VKI* erfolgen.

5. Haftung und Recht auf Schadenersatz

Jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, hat gemäß Artikel 82 Abs. 1 DSGVO Anspruch auf Schadenersatz gegen den Verantwortlichen oder den Auftragsverarbeiter. Jeder an einer Verarbeitung beteiligte Verantwortliche haftet gemäß Artikel 82 Abs. 2 DSGVO für den Schaden, der durch eine nicht der DSGVO entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine

Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat. Der Verantwortliche oder der Auftragsverarbeiter wird allerdings von seiner Haftung befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

Wenn mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter oder sowohl ein Auftragsverarbeiter als auch ein Verantwortlicher an der selben Verarbeitung beteiligt sind und sie für einen durch die Verarbeitung verursachten Schaden verantwortlich sind, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadenersatz für die Betroffenen sichergestellt ist. Hat ein Verantwortlicher oder Auftragsverarbeiter vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so hat dieser Verantwortliche oder Auftragsverarbeiter das Recht, von den übrigen, an der selben Verarbeitung für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der ihrem Anteil an der Verantwortung für den Schaden entspricht.

6. allgemeine Bedingungen für die Verhängung von Geldbußen

Gemäß Artikel 83 Abs. 1 DSGVO hat jede Aufsichtsbehörde sicherzustellen, dass die Verhängung von Geldbußen für Verstöße gegen die DSGVO in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist. Gemäß Artikel 83 Abs. 2 DSGVO werden Geldbußen nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Abs. 2 lit. a-h und i DSGVO verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall folgendes berücksichtigt:

- * Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens
- * Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes
- * jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens

- * Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen getroffenen, technischen und organisatorischen Maßnahmen
- * etwaige, einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters
- * Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelpen und seine möglichen, nachteiligen Auswirkungen zu mindern
- * Kategorie personenbezogener Daten, die von dem Verstoß betroffen sind
- * Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und ggfs. in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat
- * Einhaltung der früher gegen den für den betreffenden Verantwortlichen dem Auftragsverarbeiter im Bezug auf den selben Gegenstand angeordneten Maßnahme, wenn solche Maßnahmen angeordnet wurden
- * Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 DSGVO oder genehmigten Zertifizierungsverfahren nach Artikel 42 DSGVO und
- * jegliche anderen, erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste

Wenn ein Verantwortlicher oder Auftragsverarbeiter bei gleichen oder miteinander verbundene Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen der DSGVO verstößt, so darf der Gesamtbetrag der Geldbußen gemäß Artikel 83 Abs. 3 DSGVO nicht den Betrag für den schwerwiegendsten Verstoß übersteigen.

Artikel 83 Abs. 4 DSGVO ordnet an, dass bei Verstößen gegen die folgenden Bestimmungen Geldbußen von bis zu € 10 Mio. oder im Fall eines Unternehmens von bis zu 2% seines gesamten, weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden dürfen, je nachdem, welcher der Beträge höher ist:

- * die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8¹¹, 11¹², 25-39¹³, 42¹⁴ und 43¹⁵ DSGVO
- * die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43 DSGVO
- * die Pflichten der Überwachungsstelle gemäß Artikel 41 Abs. 4 DSGVO

Bei Verstößen gegen die folgenden Bestimmungen werden gemäß Artikel 83 Abs. 5 DSGVO Geldbußen von bis zu € 20 Mio. oder im Fall eines Unternehmens von bis zu 4% seines gesamten, weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welche der Beträge höher ist:

- * die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung gemäß den Artikeln 5, 6, 7 und 9¹⁶ DSGVO
- * die Rechte der betroffenen Personen gemäß den Artikeln 12-22¹⁷ DSGVO
- * die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44-49¹⁸ DSGVO

¹¹ Bedingungen für die Einwilligung eines Kindes

¹² Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist

¹³ 25-39: Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen; gemeinsam für die Verarbeitung Verantwortliche; Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern; Auftragsverarbeiter; Verarbeitung unter Aufsicht des Verantwortlichen oder des Auftragsverarbeiters; Verzeichnis von Verarbeitungstätigkeiten; Zusammenarbeit mit der Aufsichtsbehörde; Sicherheit der Verarbeitung; Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde; Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen; Datenschutz-Folgenabschätzung; vorherige Konsultation; Benennung, Stellung und Aufgaben des Datenschutzbeauftragten

¹⁴ Zertifizierung

¹⁵ Zertifizierungsstellen

¹⁶ Grundsätze für die Verarbeitung personenbezogener Daten; Rechtmäßigkeit der Verarbeitung; Bedingungen für die Einwilligung; Verarbeitung besonderer Kategorien personenbezogener Daten

¹⁷ Recht auf Löschung und Einschränkung der Verarbeitung; Mitteilungspflicht iZm der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung; Recht auf Datenübertragbarkeit; Widerspruchsrecht; automatisierte Entscheidungen im Einzelfall einschl. Profiling

¹⁸ allgemeine Grundsätze der Datenübermittlung; Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses und vorbehaltlich geeigneter Garantien; verbindliche, interne Datenschutzvorschriften; nach dem Unionsrecht nicht zulässige Übermittlung der Offenlegung; Ausnahmen für bestimmte Fälle

- * alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitel IX. erlassen wurden
- * Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Abs. 2 DSGVO oder Nichtgewährung des Zugangs und der Verstoß gegen Artikel 58 Abs. 1 DSGVO

Gemäß Artikel 83 Abs. 6 DSGVO werden bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Abs. 2 DSGVO Geldbußen von bis zu € 20 Mio. oder im Falle eines Unternehmens von bis zu 4% seines gesamten, weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

7. Verwaltungsstrafbestimmungen nach dem Datenschutz-Anpassungsgesetz

§ 62 Abs. 1 Datenschutz-Anpassungsgesetz bestimmt, dass - sofern die Tat nicht einen Tatbestand nach Artikel 83 DSGVO verwirklicht oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist - eine Verwaltungsübertretung begeht, die mit Geldstrafen von bis zu € 50.000 zu ahnden ist, wer

- * sich vorsätzlich widerrechtlichen Zugang zu einer Datenverarbeitung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrecht erhält
- * Daten vorsätzlich in Verletzung des Datengeheimnisses übermittelt, insbesondere Daten, die ihm gemäß den §§ 7 oder 8 Datenschutz-Anpassungsgesetz anvertraut wurden, vorsätzlich für andere unzulässige Zwecke verarbeitet
- * sich unter Vortäuschung falscher Tatsachen vorsätzlich personenbezogene Daten gemäß § 10 Datenschutz-Anpassungsgesetz verschafft
- * eine Bildverarbeitung entgegen den Bestimmungen des Datenschutz-Anpassungsgesetzes betreibt oder
- * die Einschau gemäß § 22 Abs. 2 Datenschutz-Anpassungsgesetz verweigert

Gegen juristische Personen können bei solchen Verwaltungsübertretungen Geldbußen nach Maßgabe des § 30 Datenschutz-Anpassungsgesetz verhängt werden.

Wer mit dem Vorsatz, sich oder einen Dritten dadurch unrechtmäßig zu bereichern oder mit der Absicht, einen anderen dadurch in seinem von § 1 Abs. 1 Datenschutz-Anpassungsgesetz gewährleisteten Anspruch zu schädigen, personenbezogene Daten, die ihm ausschließlich aufgrund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich gemacht worden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem Anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, gemäß § 63 Datenschutz-Anpassungsgesetz vom Gericht mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe von bis zu 720 Tagessätzen zu bestrafen.

X. ANLAGE

CHECKLISTE - Status Quo und Anpassungsbedarf

	JA	NEIN (keine)	Erhebung erl.	Anmerkung
Status Quo - Erhebung (Analyse des Ist-Zustands) und Anpassungsbedarf (Soll-Zustand)				
Welche personenbezogenen Daten werden verarbeitet? zB Name Adresse Geb.Datum ...				
Welche Datenanwendungen bestehen? zB Personalverwaltung				
Welche Standardanwendungen liegen derzeit vor?				
Welche Datenanwendungen sind derzeit im DVR registriert?				
Überprüfen Sie Ihre AGB, Datenschutzerklärungen, Impressum, laufende Verträge, Website-Einstellungen, etc.				
Was sind Zwecke meiner Datenverarbeitung?				
Was ist die Rechtsgrundlage der Datenverarbeitung?				
zB Liegt eine Einwilligung vor? Liegt ein Vertrag vor?				
Welche sensiblen Daten werden verarbeitet?				
Werden Kindern Dienste der Informationsgesellschaft angeboten?				
Erfolgt Profiling?				

CHECKLISTE - Status Quo und Anpassungsbedarf

	JA	NEIN (keine)	Erhebung erl.	Anmerkung
Werden Auftragsverarbeitern (derzeit „Dienstleister“) heran- gezogen? zB Steuerberater Lohnverrechner				
Gibt es schriftliche Vereinbarungen für die Auftragsver- arbeitung?				
Weist der Auftragsverarbeiter die erforderliche Zuverlässigkeit auf?				
Wie werden die Informationspflichten (nach DSGVO) erfüllt?				
Wie werden die Betroffenenrechte (nach DSGVO) erfüllt?				
An wen in meinem Unternehmen können sich betroffene Personen für die Ausübung ihrer Betroffenenrechte wenden?				
Welche Datensicherheitsmaßnahmen sind vorhanden?				
Wie ist privacy by design (Datenschutz durch Technik) / privacy by default (datenschutzfreundliche Voreinstellungen) implementiert?				
Besteht für meine Datenverarbeitung Dokumentationspflicht?				
Wie wird die Dokumentationspflicht erfüllt?				
Welche Vorkehrungen gegen Datenschutzverletzungen existieren schon in meinem Unternehmen?				
Ist für meine Datenverarbeitung eine Datenschutz-Folgenab- schätzung durchzuführen?				

CHECKLISTE - Status Quo und Anpassungsbedarf

	JA	NEIN (keine)	Erhebung erl.	Anmerkung
Welche Risiken aus der Datenverarbeitung ergeben sich für die Rechte und Freiheiten der Betroffenen?				
Wie kann ich den Risikoeintritt verhindern oder zumindest minimieren?				
Ist eine vorherige Konsultation bei der Aufsichtsbehörde notwendig?				
Brauche ich einen Datenschutzbeauftragten?				
Welcher Datenverkehr mit dem EU Ausland besteht und auf welcher Rechtsgrundlage?				
Besonderheiten Arbeitnehmerdatenschutz				
Überprüfung von Dienstverträgen, Betriebsvereinbarungen, Dienstordnungen, etc.				
Rechtzeitige Kommunikation mit dem Betriebsrat.				
Wie weise ich nach, dass meine Datenverarbeitungen DSGVO konform erfolgen? zB Dokumentation der Einwilligungserklärungen, Verarbeitungsverzeichnis, Dokumentation der ergriffenen Sicherheitsmaßnahmen, Dokumentation der Risikoabschätzung, Protokollierung oder Dokumentation der Weisungen an dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Personen, Dokumentation der Verpflichtung der Mitarbeiter des Auftragsverarbeiters zur Vertraulichkeit, etc.				

CHECKLISTE - Status Quo und Anpassungsbedarf

	JA	NEIN (keine)	Erhebung erl.	Anmerkung
Rechtsdurchsetzung und Strafen: Rechtsbehelfe, Haftungen und Sanktionen				
Maßnahmenplan (für identifizierten Anpassungsbedarf)				
zeitliche und budgetäre Planung (Priorisierung der Ziele)				
Maßnahmen festlegen				
Maßnahmen umsetzen				

soweit vorhanden

..... [E-Mail]

[illegible]

..... [E-Mail]

[illegible]

EINWILLIGUNGSERKLÄRUNG

entweder als gesondertes Dokument oder durch
Kennzeichnung abgehobener Text

Tipp

Vorher prüfen, ob nicht bereits eine ausreichende Einwilligungserklärung vorliegt oder ob nicht eine andere Rechtsgrundlage für die Datenverarbeitung vorliegt, dann bedarf es keiner (weiteren) Einwilligung.

Der Vertragspartner stimmt zu, dass seine persönlichen Daten (nämlich Name / Firma, Geburtsdatum / Firmenbuchnummer, Adresse) zum Zwecke der **[zB Zusendung des regelmäßig erscheinenden Newsletters bei dem Unternehmen]** gespeichert werden. Diese Einwilligung kann jederzeit bei **[genaue Kontaktdaten]** widerrufen werden.

.....,

[Ort, Datum]

.....

[Name und Unterschrift]

NN

.....

.....

.....

..... (Ort),

Auskunftserteilung gemäß Artikel 15 DSGVO
keine Daten werden verarbeitet (Negativauskunft)

Sehr geehrte Damen und Herren !

Wir haben Ihr Ansuchen vom auf Auskunftserteilung nach Artikel 15 DSGVO am erhalten und können Sie fristgemäß wie folgt informieren:

In unserem Unternehmen werden **keine Daten** zu Ihrer Person verarbeitet. Wenn Sie glauben, dass Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Datenschutzbehörde beschweren.

Wir ersuchen um Kenntnisnahme und verbleiben

mit freundlichen Grüßen

NN

NN

.....

.....

.....

..... (Ort),

Auskunftserteilung gemäß Artikel 15 DSGVO fristgerechte Auskunftserteilung

Sehr geehrte Damen und Herren !

Wir haben Ihr Ansuchen vom auf Auskunftserteilung nach Artikel 15 DSGVO am erhalten und können Sie fristgemäß wie folgt informieren:

In unserem Unternehmen werden nachstehende Daten zu Ihrer Person verarbeitet:

..... **[zB Name, Adresse, ...]**

Diese Daten werden zu folgenden Zwecken verarbeitet:

..... **[zB aufgrund Ihrer Einwilligungserklärung für die Übermittlung unseres Newsletters und aufgrund von § 15 GenG für die Erstellung des Mitgliederregisters]**

Ihre Daten werden an folgende Empfänger übermittelt:

..... **[zB Steuerberater, ...]**

Wir speichern Ihre Daten für die Übermittlung des Newsletters bis zum Widerruf Ihrer Einwilligungserklärung und für die Zwecke der Führung des Mitgliederregisters aufgrund der gesetzlichen Bestimmungen derzeit unbegrenzt. Sie können uns gegenüber - soweit gesetzlich zulässig - die Rechte auf Berichtigung und Löschung Ihrer Daten, auf Einschränkung und Widerruf zur Datenverarbeitung geltend machen. Sofern Sie der Ansicht sein sollten, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt, oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich an die Datenschutzbehörde wenden.

NN

.....

.....

Wir ersuchen um Kenntnisnahme und verbleiben

mit freundlichen Grüßen

NN

NN

.....

.....

.....

..... (Ort),

Auskunftserteilung gemäß Artikel 15 DSGVO
fristgerechte Auskunftserteilung - mit Fristverlängerung

Sehr geehrte Damen und Herren !

Wir haben Ihr Ansuchen vom und vom sowie vom und vom auf Auskunftserteilung nach Artikel 15 DSGVO am,, und erhalten. Wie wir Ihnen mit Schreiben vom mitgeteilt haben, haben wir aufgrund der Anzahl Ihrer Anträge bei unterschiedlichen Abteilungen unseres Unternehmens die Möglichkeit zur Fristverlängerung [Variante: aufgrund der Komplexität der Anfrage → **nähere Begründung notwendig**] in Anspruch genommen.

In unserem Unternehmen werden nachstehende Daten zu Ihrer Person verarbeitet:

..... [**zB Name, Adresse, ...**]

Diese Daten werden zu folgenden Zwecken verarbeitet:

..... [**zB aufgrund Ihrer Einwilligungserklärung für die Übermittlung unseres Newsletters und aufgrund von § 15 GenG für die Erstellung des Mitgliederregisters**]

Ihre Daten werden an folgende Empfänger übermittelt:

..... [**zB Steuerberater, ...**]

Wir speichern Ihre Daten für die Übermittlung des Newsletters bis zum Widerruf Ihrer Einwilligungserklärung und für die Zwecke der Führung des Mitgliederregisters aufgrund der gesetzlichen Bestimmungen derzeit unbegrenzt. Sie können uns gegenüber - soweit gesetzlich zulässig - die Rechte auf Berichtigung und Löschung Ihrer Daten, auf Einschränkung und Widerruf zur Datenverarbeitung geltend machen. Sofern Sie der Ansicht sein sollten, das die Verarbeitung Ihrer Daten gegen das

NN

.....

.....

Datenschutzrecht verstößt, oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich an die Datenschutzbehörde wenden.

Wir ersuchen um Kenntnisnahme und verbleiben

mit freundlichen Grüßen

NN

NN

.....

.....

.....

..... (Ort),

Auskunftserteilung gemäß Artikel 15 DSGVO
fristgerechte Auskunftserteilung - Übermittlung Drittland

Sehr geehrte Damen und Herren !

Wir haben Ihr Ansuchen vom auf Auskunftserteilung nach Artikel 15 DSGVO am erhalten und können Sie fristgemäß wie folgt informieren:

In unserem Unternehmen werden nachstehende Daten zu Ihrer Person verarbeitet:

..... ***[zB Name, Adresse, ...]***

Diese Daten werden zu folgenden Zwecken verarbeitet:

..... ***[zB aufgrund Ihrer Einwilligungserklärung für die Übermittlung unseres Newsletters und aufgrund von § 15 GenG für die Erstellung des Mitgliederregisters]***

Die Übermittlung der Daten an jene Empfänger, die sich in einem Drittland befinden, basiert auf dem Angemessenheitsbeschluss der Kommission / vorbildlicher, interner Datenschutzvorschriften / Standardschutzklauseln / genehmigten Verhaltensregeln / einem genehmigten Zertifizierungsmechanismus / genehmigten Vertragsklauseln / Ihrer ausdrücklichen Zustimmung / in Erfüllung des zwischen uns geschlossenen Vertrags / zur Geltendmachung, Ausübung von der Verteidigung von Rechtsansprüchen ***[Unzutreffendes nicht verwenden]***

Wir speichern Ihre Daten für die Übermittlung des Newsletters bis zum Widerruf Ihrer Einwilligungserklärung und für die Zwecke der Führung des Mitgliederregisters aufgrund der gesetzlichen Bestimmungen derzeit unbegrenzt. Sie können uns gegenüber - soweit gesetzlich zulässig - die Rechte auf Berichtigung und Löschung Ihrer Daten, auf Einschränkung und Widerruf zur Datenverarbeitung geltend machen. Sofern Sie der Ansicht sein sollten, dass die Verarbeitung Ihrer Daten gegen das

NN

.....

.....

Datenschutzrecht verstößt, oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich an die Datenschutzbehörde wenden.

Wir ersuchen um Kenntnisnahme und verbleiben

mit freundlichen Grüßen

NN

Auskunftserteilung gemäß Artikel 15 DSGVO
weitere mögliche Zusätze

- * Wir haben Ihre Daten von erhalten *[sofern nicht bei der betroffenen Person erhoben]*
- * Wir setzen ein Verfahren zur automatisierten Entscheidungsfindung / Profiling *[Unzutreffendes nicht verwenden]* ein, die Ihnen gegenüber eine rechtliche Wirkung haben oder Sie in ähnlicher Weise erheblich beeinträchtigen *[Details über involvierte Logik → Tragweite und Auswirkungen sind anzuführen]*.

BESTELLUNG ZUM DATENSCHUTZBEAUFTRAGTEN

Wir,

.....

..... **[Adresse]**

....., bestellen hiermit

....., **geb.**

wohnhaft in **[Adresse]**

zum Datenschutzbeauftragten iSd DSGVO 2018. hat mit seiner / ihrer Bestellung jedenfalls folgende Aufgaben zu erfüllen:

- * Übermittlung und Beratung der Geschäftsführung und der Mitarbeiter hinsichtlich ihrer Pflichten nach dem Datenschutzrecht.
- * Überwachung und Überprüfung der Einhaltung der Datenschutzvorschriften und Strategien für den Schutz personenbezogener Daten, einschließlich der Zuweisung von Zuständigkeiten, Sensibilisierung und Schulung der Mitarbeiter.
- * Beratungen im Zusammenhang mit der Datenschutz-Folgenabschätzung und der Überwachung der Durchführung.
- * Zusammenarbeit mit der Aufsichtsbehörde und Anlaufstelle für diese.

Mit der Bestellung einverstanden:

.....

[Ort, Datum]

.....

[Ort, Datum]

.....
[Name und Unterschrift Verantwortlicher]

.....
**[Name und Unterschrift
Datenschutzbeauftragter]**

NN

.....

.....

An die Datenschutzbehörde
Hohenstaufengasse 3
1010 Wien

..... (Ort),

Meldung Datenschutzbeauftragter

Sehr geehrte Damen und Herren !

Wir geben hiermit bekannt, dass wir, geb. am, wohnhaft in, zum Datenschutzbeauftragten für unser Unternehmen bestellt haben.

..... ist unter folgenden Kontaktdaten erreichbar:

Adresse

Telefonnummer

E-Mail Adresse

Wir ersuchen um Kenntnisnahme und verbleiben

mit freundlichen Grüßen

NN

NN

.....

.....

An die Datenschutzbehörde
Hohenstaufengasse 3
1010 Wien

..... (Ort),

Meldung Data Breach

Sehr geehrte Damen und Herren !

Am fand um Uhr *[allenfalls Begründung, falls die Meldung später als 72 Stunden erfolgt]* eine Verletzung des Schutzes personenbezogener Daten in der Form *[zB Diebstahl PC]* statt. Dadurch sind folgende Kategorien von etwa betroffenen Personen betroffen *[zB Kundendaten]* und (- soweit möglich -) folgende Kategorien von etwa personenbezogenen Datensätzen *[zB Name, Adresse, E-Mail Adressen]*. Es ist davon auszugehen, dass die Verletzung des Schutzes der personenbezogenen Daten folgende Folgen haben wird: *[Beschreibung der wahrscheinlichen Folgen; zB Kontaktaufnahme durch Unbefugte; Weitergabe der Kundendaten]*.

Wir haben folgende Maßnahmen zur Behebung der Verletzung ergriffen: *[zB Diebstahlanzeige und Zurücksetzung der Passwörter ; ggfs. auch Angabe von Maßnahmen zur Abmilderung der Auswirkungen der Verletzung]*.

[Falls vorhanden: wurde zum Datenschutzbeauftragten bestellt; die Kontaktdaten lauten wie folgt]

Mit freundlichen Grüßen

NN

NN

.....

.....

[Benachrichtigung ist nicht erforderlich, wenn auf die von der Verletzung betroffenen, personenbezogenen Daten geeignete technische und organisatorische Sicherheitsvorkehrungen angewandt wurden (zB Verschlüsselung), der Verantwortliche nachträglich Maßnahmen gesetzt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Person aller Wahrscheinlichkeit nach nicht besteht oder die Benachrichtigung mit einem unverhältnismäßigem Aufwand verbunden wäre.]

Herrn/Frau

Adresse

...

..... (Ort),

Benachrichtigung von der Verletzung des Schutzes personenbezogener Daten - Meldung an betroffene Person

Sehr geehrte/r !

Am fand um ca. Uhr ***[zB Einbruchdiebstahl]*** statt, bei dem es zu folgender Verletzung des Schutzes personenbezogener Daten kam ***[zB Diebstahl PC]*** statt. Dadurch kam es zu folgenden, wahrscheinlichen Folgen des Schutzes personenbezogener Daten kommen: ***[zB Weitergabe Ihrer Kundendaten und Kontaktaufnahme durch Unbefugte]***.

Wir haben bereits folgende Maßnahmen zur Behebung der Verletzung ergriffen: ***[zB Zurücksetzen der Passwörter und Diebstahlanzeige]***.

[Falls vorhanden: Für weitere Informationen steht Ihnen auch unser Datenschutzbeauftragter unter ***[Kontaktdaten]*** zur Verfügung.

Wir bedauern den Vorfall und verbleiben

mit freundlichen Grüßen

NN

NN

.....

.....

Herrn/Frau/Firma

Adresse

...

..... (Ort),

Benachrichtigung von der Verletzung des Schutzes personenbezogener Daten - Meldung Auftraggeber an Verantwortlichen

Sehr geehrte/r !

Am fand um ca. Uhr **[zB Einbruchdiebstahl]** statt, bei dem es zu folgender Verletzung des Schutzes personenbezogener Daten kam **[zB Diebstahl PC]** statt. Dadurch kam es zu folgenden, wahrscheinlichen Folgen des Schutzes personenbezogener Daten kommen; **[zB Weitergabe der Lohnverrechnungsdaten und allenfalls Kontaktaufnahme durch Unbefugte oder Veröffentlichung der Daten]**.

Wir haben bereits folgende Maßnahmen zur Behebung der Verletzung ergriffen: **[zB Zurücksetzen der Passwörter und Diebstahlanzeige]**. Wir ersuchen Sie, die allenfalls erforderlichen Benachrichtigungen der betroffenen Personen vorzunehmen.

Wir bedauern den Vorfall und verbleiben

mit freundlichen Grüßen

NN

VEREINBARUNG ÜBER AUFTRAGSVERARBEITUNG

(kann auch eine Ergänzung zu einem Werk- / Rahmenvertrag sein)

abgeschlossen zwischen

.....

..... **[Adresse]**

(in Folge kurz „der Auftraggeber“ genannt)

einerseits und

.....

..... **[Adresse]**

(in Folge kurz „Auftragnehmer“ genannt)

andererseits, wie folgt:

1. Vertragsgegenstand

- 1.1 Der Auftraggeber beauftragt hiermit den Auftragnehmer mit der Durchführung folgender Tätigkeiten [zB Lohnverrechnung] und der Auftraggeber nimmt diese Beauftragung an.
- 1.2 Der Auftragnehmer übernimmt dabei die Verarbeitung folgender Kategorien von Daten [zB Personaldaten, Lohnzettel] von folgenden Kategorien von Personen [zB Dienstnehmer].

2. Pflichten des Auftragnehmers

- 2.1 Der Auftragnehmer verpflichtet sich hiermit, die Daten und die Ergebnisse der Datenverarbeitung ausschließlich auf Basis der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers ist untersagt, sofern der Auftraggeber nicht im Einzelfall im Vorhinein sein Einverständnis schriftlich erklärt.
- 2.2 Sollte der Auftragnehmer von einem Gericht oder einer Behörde aufgefordert werden, Daten des Auftraggebers offenzulegen oder herauszugeben, so hat der Auftragnehmer - sofern dies nicht gesetzlich verboten ist - den Auftraggeber

unverzüglich darüber zu informieren und das Gericht oder die Behörde an den Auftraggeber zu verweisen.

- 2.3 Der Auftragnehmer ist weiters verpflichtet, alle Personen, die er mit der Datenverarbeitung beauftragt oder bei der Datenverarbeitung einsetzt, vor der Aufnahme der Tätigkeit zur Vertraulichkeit zu verpflichten, sofern diese nicht ohnedies einer gesetzlichen Verschwiegenheitsverpflichtung unterliegen.
- 2.4 Außerdem ist der Auftragnehmer verpflichtet, alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Artikel 32 DSGVO zu ergreifen.
- 2.5 Der Auftragnehmer hat die technischen und organisatorischen Maßnahmen zu ergreifen, damit der Auftraggeber seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person fristgerecht nachkommen kann, das sind das Recht auf Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch sowie automatisierte Entscheidungsfindung im Einzelfall. Sollte der Auftragnehmer einen entsprechenden Antrag einer betroffenen Person erhalten, so hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und den Antragsteller darüber zu informieren.
- 2.6 Darüber hinaus hat der Auftragnehmer den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zu unterstützen (d.h. bei Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Datenschutzbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgenabschätzung, vorherige Konsultation).
- 2.7 Nach Abschluss der Erbringung der vertragsgegenständlichen Leistungen ist der Auftragnehmer verpflichtet, alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben, sofern nicht eine gesetzliche Verpflichtung zur Speicherung besteht.
- 2.8 Der Auftraggeber ist berechtigt, jederzeit im Zusammenhang mit der Verarbeitung der von ihm überlassenen Daten Einsicht zu nehmen und die Datenverarbeitungseinrichtungen zu kontrollieren, dies auch unter Beiziehung von von ihm beauftragter Dritter. Der Auftragnehmer ist verpflichtet, dem Auftraggeber alle Informationen zu geben, die zur Kontrolle der Einhaltung der in dieser Vereinbarung festgelegten Pflichten erforderlich sind.

- 2.9 Schließlich ist der Auftragnehmer verpflichtet, den Auftraggeber zu informieren, wenn er der Ansicht ist, dass eine Weisung des Auftraggebers gegen Datenschutzbestimmungen der EU oder von Österreich verstößt.

3. Ort der Vertragserfüllung

Der Auftragnehmer ist verpflichtet, alle Datenverarbeitungstätigkeiten, die dieser Vereinbarung unterliegen, ausschließlich innerhalb der EU und des EWR durchzuführen.

4. Weitergabe von Vertragsleistungen an Dritte

Variante 1

Der Auftragnehmer ist nicht berechtigt, einen Sub-Auftragsverarbeiter heranzuziehen und einzelne Vertragsleistungen durch Beiziehung Dritter zu erbringen.

Variante 2

Der Auftragnehmer ist mit vorheriger, schriftlicher Zustimmung des Auftraggebers berechtigt, Sub-Auftragsverarbeiter zur Erfüllung der vertraglichen Pflichten heranzuziehen. Diesfalls ist der Auftragnehmer verpflichtet, die erforderlichen Vereinbarungen gemäß Artikel 28 Abs. 4 DSGVO mit dem Sub-Auftragsverarbeiter abzuschließen und der Auftragnehmer hat dabei sicherzustellen, dass der Sub-Auftragsverarbeiter die selben Pflichten übernimmt, die der Auftragnehmer gemäß dieser Vereinbarung übernommen hat. Verletzt der Sub-Auftragsverarbeiter seine Datenschutzpflichten, so haftet der Auftragnehmer dem Auftraggeber dafür.

5. Dauer der Vereinbarung

Variante 1

Diese Vereinbarung wird auf unbestimmte Zeit geschlossen und kann von jeder Partei unter Einhaltung einer Kündigungsfrist [zB ein Monat] zum [zB Ende des Kalenderjahrs] schriftlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt davon unberührt.

Variante 2

Diese Vereinbarung wird für einen Zeitraum von / bis geschlossen und endet nach Ablauf dieser Dauer, ohne dass es einer gesonderten Kündigung bedarf.

6. Schlussbestimmungen

- 6.1 Der Auftragnehmer hat den Auftraggeber über wesentliche Änderungen der wirtschaftlichen und rechtlichen Verhältnisse unverzüglich zu informieren.
- 6.2 Sollte eine Bestimmung dieser Vereinbarung rechtsunwirksam oder undurchsetzbar sein oder werden, so wird dadurch die Wirksamkeit und Durchsetzbarkeit der übrigen Bestimmungen nicht berührt. Die Vertragsparteien verpflichten sich diesfalls, eine wirksame und durchsetzbare Bestimmung zu vereinbaren, die dem wirtschaftlichen Zweck der zur ersetzenden Bestimmung bestmöglich entspricht. Diese Regelungen gelten für allfällige Lücken sinngemäß.
- 6.3 Für allfällige Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung und ihrer Erfüllung, Wirksamkeit, Nichtigkeit und Anfechtbarkeit wird die ausschließliche Zuständigkeit des sachlich für **[Ort]** zuständigen Gerichts vereinbart.
- 6.4 Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform; ebenso ein Abgehen vom Erfordernis der Schriftlichkeit.
- 6.5 Diese Vereinbarung wird in zwei Ausfertigungen errichtet, von denen jede Vertragspartei eine erhält.

.....
[Ort, Datum]

.....
[Ort, Datum]

.....
...

.....
...

VORGEHENSWEISE BEI DATENSCHUTZ-FOLGENABSCHÄTZUNG

- 1. Feststellung, ob eine Datenschutz-Folgenabschätzung überhaupt notwendig ist - wenn eine der folgenden Fragen mit JA beantwortet wird, bedarf es einer Datenschutz-Folgenabschätzung.**

	JA	NEIN
Wird bei der beabsichtigten Datenverarbeitung neue Technologie verwendet oder besteht aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person?		
Werden Daten zum Zweck des Profiling oder in Scoringverfahren verarbeitet?		
Werden besonders schützenswerte, personenbezogene Daten gespeichert, verarbeitet oder genutzt?		
Findet die systematische Überwachung (zB Videoüberwachung) im öffentlichen Raum statt?		
Ist die Prüfung der Negativ- und Positivlisten der Datenschutzbehörde erfolgt?		
Gibt es besondere Vorgaben?		

2. Erhebung der zu verarbeitenden, personenbezogenen Daten

allgemeine Prüfung

	JA	NEIN
Welche Daten werden verarbeitet? <i>sensibel?</i> <i>nicht sensibel?</i>		
Liegt eine Einwilligungserklärung der betroffenen Person vor?		
Ist die Datenverarbeitung für eine Vertragserfüllung oder die Durchführung vorvertraglicher Maßnahmen erforderlich?		
Ist die Datenverarbeitung für die Erfüllung einer rechtlichen Verpflichtung notwendig?		
Ist die Datenverarbeitung notwendig, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen?		
Besteht auf Seiten des Verantwortlichen oder eines Dritten ein berechtigtes Interesse an der Datenverarbeitung und überwiegen nicht die Interessen oder Grundfreiheiten der betroffenen Person?		

VORGEHENSWEISE BEI DATENSCHUTZ-FOLGENABSCHÄTZUNG

Prüfung bei sensiblen Daten

	JA	NEIN
Liegt eine ausdrückliche Einwilligung vor?		
Ist die Datenverarbeitung erforderlich, um lebenswichtige Interessen des Betroffenen oder einer anderen natürlichen Person zu schützen und ist der Betroffene aus körperlichen oder rechtlichen Gründen außerstande, die Einwilligung zu geben?		
Wurden die „sensiblen Daten“ offensichtlich von der betroffenen Person öffentlich zugänglich gemacht?		
Ist die Verarbeitung „sensibler Daten“ zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich?		
Erfolgt die Verarbeitung der „sensiblen Daten“ auf Grundlage geeigneter Garantien (zB verbindliche, interne Datenschutzvorschriften, Zertifizierungen) durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemaligen Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakt mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Person nach außen offengelegt werden?		
Ist die Verarbeitung „sensibler Daten“ auf Grundlage gesetzlicher Vorgaben aus Gründen eines erheblichen, öffentlichen Interesses erforderlich?		
Ist die Verarbeitung für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich auf Grundlage von Gesetzen oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs erforderlich?		
Ist die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden, grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsvorsorge und bei Arzneimitteln und Medizinprodukten, auf der Grundlage von europarechtlichen oder nationalen Gesetzen erforderlich?		
Ist die Verarbeitung auf gesetzlicher Grundlage für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erforderlich?		

VORGEHENSWEISE BEI DATENSCHUTZ-FOLGENABSCHÄTZUNG

3. Prüfung der Datenschutzkonformität - werden folgende Grundsätze berücksichtigt?

	JA	NEIN
Notwendigkeit		
Verhältnismäßigkeit		
Zweckgebundenheit		
Datensparsamkeit		
Integrität		
Nichtverkettbarkeit		
Vertraulichkeit		
Intervenierbarkeit		
Transparenz		
Wird sichergestellt, dass die Daten richtig und auf dem neuesten Stand sind?		
Gibt es Strategien zur Wahrung der Rechte der betroffenen Person? (zB Recht auf Löschung, etc.)		
Kann bei Anfragen der Datenschutzbehörde die Einhaltung der datenschutzrechtlichen Prinzipien nachgewiesen werden? (zB Vorlage von Einwilligungserklärungen)		

4. Darlegung der Gründe, warum eine Datenschutz-Folgenabschätzung nicht für erforderlich erachtet wird

5. Beschreibung der geplanten Verarbeitungsvorgänge

VORGEHENSWEISE BEI DATENSCHUTZ-FOLGENABSCHÄTZUNG

6. Risikobewertung und Maßnahmen zur Risikovermeidung

	JA	NEIN
Besteht bei der Datenverarbeitung oder bei einzelnen Schritten vermutlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen? (zB Rufschädigung, materieller Schaden)		
Wenn ja, welche?		
Wurden jedem einzelnen Risiko Abhilfemaßnahmen zugeordnet? (zB Einsatz von Verschlüsselungstechnologien, Garantien, Schutzverfahren, etc.)		
Sind die Abhilfemaßnahmen für alle Zuständigen dokumentiert?		

7. Maßnahmenplan auf Basis der getroffenen Feststellungen (beispielsweise)

	JA	NEIN
Netzwerksicherheit durch Firewalls		
bauliche Maßnahmen (zB Zutrittskontrollen)		
Passwortschutz und regelmäßige Änderungen		
PC Benutzungsregelungen		
Verpflichtungserklärungen der Mitarbeiter im Bezug auf Einhaltung des Daten- geheimnisses		

8. Dokumentation

	JA	NEIN
Wurde die Datenschutz-Folgenabschätzung umfassend, systematisch und belastbar dokumentiert?		

