REHASPORTGRUPPE
anerkannt+zertifiziert DBS-GEPRÜFT

Deutscher Behindertensportverband e.V.
National Paralympic Committee Germany

Leitfaden – Datenschutz im Rehabilitationssport

Deutscher Behindertensportverband e.V.

– Im Hause der Gold-Kraemer-Stiftung –
Tulpenweg 2-4
50226 Frechen-Buschbell

Inhalt

Vorwort **3**
Haftungsausschluss **3**
Wie nähere ich mich dem Thema Datenschutz? **4**
Abschnitt 1: Grundsätzliches **5**
Gebot der Datensparsamkeit 5
Verzeichnis von Verarbeitungstätigkeiten 5
Brauche ich einen Datenschutzbeauftragten? 5
Wann ist eine Datenschutz-Folgenabschätzung notwendig? 6
Betroffenenrechte 7
Organisatorische und technische Maßnahmen zur Sicherung personenbezogener Daten 7
Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde 8
Abschnitt 2: Personenbezogene Daten im Anerkennungsverfahren zum Rehabilitationssport **9**
Einwilligungserklärungen Ansprechpartner, Mediziner und Übungsleitung 9
Mitarbeiter auf Verschwiegenheit verpflichten 9
Vertrag zur Auftragsverarbeitung 10
Abschnitt 3: Personenbezogene Daten bei der Durchführung des Rehabilitationssports **10**
Beratungsgespräch 10
Umgang mit der Anwesenheitsliste 12
Umgang mit der Teilnahmebestätigung 12
Verarbeitung von Daten für die Abrechnung 12
Aufbewahrung der Teilnehmerbezogenen Unterlagen 13
Abschnitt 4: Kommunikation mit Dritten zu Teilnehmerdaten **13**
Kommunikation mit dem DBS-Landesverband 13
Kommunikation mit dem Rehabilitationsträger und dem verordnenden Arzt 13

Vorwort

Der nachfolgende „Leitfaden – Datenschutz im Rehabilitationssport“ soll den Vereinen und Landesverbänden als Orientierung für den Datenschutz im Rehabilitationssport dienen.
Die hier zur Verfügung gestellten allgemeinen Hinweise können nicht jeden Einzelfall abdecken. Die EU-Datenschutzgrundverordnung (EU-DSGVO; Art. 4 Ziffer 7) und das Bundesdatenschutzgesetz (BDSG; §46, Abs. 7) erfordern es, dass sich jeder Verein und Landesverband – konkret der vertretungsberechtigte Vereinsvorstand nach §26 Bürgerliches Gesetzbuch (BGB) – eigenständig mit dem Thema Datenschutz für seinen Wirkungsbereich auseinandersetzt.
Die nachstehende Darstellung konzentriert sich auf den Datenschutz beim Rehabilitationssport, für darüberhinausgehende Vereinsmitgliedschaften sowie andere Vereinsleistungen und damit einhergehende Datenverarbeitung sind ggf. weiterführende Vorschriften zu beachten. In der Regel informieren die zuständigen Landesverbände oder der jeweilige Landessportbund über den Umgang mit Daten im Kontext einer Vereinsmitgliedschaft oder andere Vereinsleistungen. Weitere Informationen erhalten Sie auch bei der zuständigen Landesbehörde zum Datenschutz. Eine Auflistung der Kontaktdaten der jeweiligen Landesbehörden zum Datenschutz ist der Anlage 1 zu entnehmen.
Dieser Leitfaden soll Sie dabei unterstützen, sich die individuell notwendigen, datenschutzkonformen Lösungen erarbeiten zu können. Eine abschließende Rechtsberatung kann dieser Leitfaden jedoch nicht darstellen. Ein guter Indikator für die Praxis ist die Frage: „Wie würde ich wollen, dass mit meinen Daten umgegangen wird, wenn ich der Betroffene wäre?“

Aus Gründen der besseren Lesbarkeit wird nachfolgend nur eine Geschlechterform verwendet. Jede Geschlechterform ist stets mit angesprochen.

Haftungsausschluss

Alle Informationen sind nach bestem Wissen und Gewissen zusammengetragen sowie grundsätzlich durch Fachleute geprüft.

Es gelten die gesetzlichen Vorschriften gemäß EU-DSVGO und BDSG.

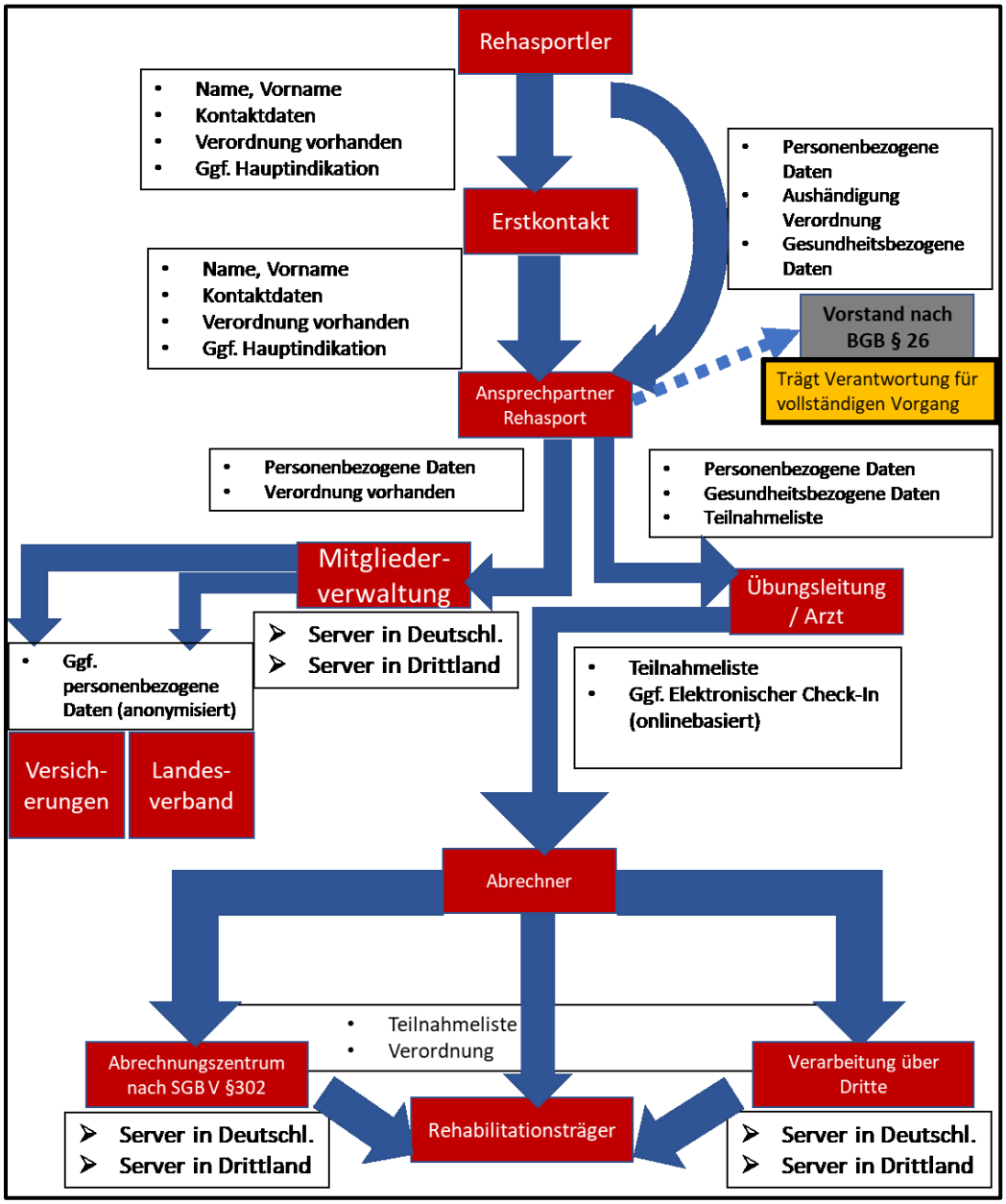
Der Deutsche Behindertensportverband (DBS) garantiert nicht für die Richtigkeit und Vollständigkeit der zur Verfügung gestellten Informationen und schließt insbesondere für die beigefügten, unverbindlichen Mustervordrucke die Haftung ausdrücklich aus.
Der Haftungsausschluss gilt nicht für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die auf einer fahrlässigen Pflichtverletzung beruhen.

Wie nähere ich mich dem Thema Datenschutz?

Bevor Sie überhaupt beurteilen können, wie sich die Regelungen zum Datenschutz auf Ihren Verein auswirken, ist es notwendig, zunächst eine Bestandsaufnahme durchzuführen. Hierzu ist es wichtig zu klären, welche Daten, von wem, wie erhoben, verarbeitet und weitergegeben werden.

Sobald Sie diese grundsätzlichen Fragen geklärt haben, können Sie mit der Beurteilung beginnen, welche Maßnahmen zum Datenschutz Sie ergreifen müssen.

Ein denkbarer Weg des Datenflusses zum Rehabilitationssport im Verein ist im Folgenden schematisch dargestellt:



Die Darstellung ist nur eine Möglichkeit, welchen Weg die Daten des Rehasportlers nehmen können und welche Aspekte bei der Bewertung hinsichtlich des Datenschutzes zu beachten sind. Bei der individuellen Bewertung Ihres Vereins können einzelne Aspekte wegfallen oder hinzukommen.

Abschnitt 1: Grundsätzliches

Gebot der Datensparsamkeit

Grundsätzlich gilt das Gebot der Datenminimierung oder Datensparsamkeit (Art. 5 Abs. 1 c EU-DSGVO). D.h. es sollen nur Daten verarbeitet und gespeichert werden, die für den jeweiligen Zweck auch tatsächlich benötigt werden.
Bezogen auf den Rehabilitationssport, ergeben sich diese Daten grundsätzlich aus der ärztlichen Verordnung. Lediglich Kontaktmöglichkeiten, wie Telefonnummer und/oder Email-Adresse, sollten hier zusätzlich herangezogen werden, um z.B. bei kurzfristiger Krankheit der Übungsleitung die Teilnehmer rechtzeitig über eine Verschiebung oder den Ausfall der Übungsstunde informieren zu können.

Verzeichnis von Verarbeitungstätigkeiten

Jeder Verantwortliche hat gemäß Art. 30 EU-DSGVO ein Verzeichnis von Verarbeitungstätigkeiten zu führen, sofern das Unternehmen mehr als 250 Mitarbeiter beschäftigt, die von Ihnen vorgenommene Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder eine Verarbeitung von besonderen Kategorien von Daten gemäß Art. 9 Abs. 1 EU-DSGVO (z.B. Gesundheitsdaten) erfolgt.

Dieses Verzeichnis enthält jegliche Verarbeitungstätigkeiten, die in der Zuständigkeit des Verantwortlichen liegen und muss in schriftlicher Form geführt werden. Auf Anfrage ist dieses Verzeichnis der zuständigen Aufsichtsbehörde zur Verfügung zu stellen.

Ein unverbindliches Muster einer Checkliste für ein Verzeichnis der Verarbeitungstätigkeiten ist in Anlage 2 beigefügt.

Was muss ich tun?
Wird im Verein Rehabilitationssport angeboten, so ist aufgrund der hierzu notwendigen Verarbeitung von Gesundheitsdaten verpflichtend ein Verzeichnis der Verarbeitungstätigkeiten zu führen.

Brauche ich einen Datenschutzbeauftragten?

Ob ein Datenschutzbeauftragter bestellt werden muss, kommt auf den jeweiligen Einzelfall bzw. die Gegebenheiten des Vereins an. Die Prüfung und Bewertung, ob ein Datenschutzbeauftragter bestellt werden muss, kann nur durch den Verein selbst erfolgen. Im Zweifel empfiehlt sich eine rechtliche Absicherung über den Landesdatenschutzbeauftragten.

Verpflichtend ist die Bestellung eines Datenschutzbeauftragten jedoch, insofern in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (vgl. § 38 Abs. 1 BDSG) bzw. die Kerntätigkeit des Vereins (vgl. Art. 37 Abs. 1 c EU-DSGVO) in der umfangreichen Verarbeitung von besonderen Kategorien personenbezogener Daten liegt.

Nach Einschätzung der Landesbeauftragten für den Datenschutz Nordrhein-Westfalen (LDI NRW) ist die Datenverarbeitung eines Vereins jedenfalls dann als Kerntätigkeit anzusehen, wenn die satzungsmäßigen Zwecke des Vereins ohne die Datenverarbeitung nicht erreicht werden können. Im Falle des beispielhaften Vereinszwecks der „Förderung von Gesundheits- und Rehabilitationssport" kann die Datenverarbeitung von Gesundheitsdaten als Kerntätigkeit des Vereins bewertet werden. Die LDI NRW führt aus, dass ferner von einer umfangreichen Datenverarbeitung auszugehen ist, wenn 10 oder mehr Personen mit der Datenverarbeitung beschäftigt sind.

Die Klarstellungen durch den Beschluss der Datenschutzkonferenz zu Ärzten, Apothekern und sonstigen Gesundheitsberufen (Anlage 3, zweiter Beschluss) sind diesbezüglich analog anzuwenden.

Laut der LDI NRW spielt die Art des Beschäftigungsverhältnisses bei der Frage, welche Personen für die Datenverarbeitung zu zählen sind, keine Rolle. Entscheidend sei, dass die Verarbeitung von personenbezogenen Daten im Aufgabenbereich der Person eingeschlossen ist. Von einer ständigen Verarbeitung ist außerdem auch auszugehen, wenn die Tätigkeit nur in zeitlichen Abständen (z.B. monatlich) anfällt.

Außerdem ist die Bestellung eines Datenschutzbeauftragten notwendig, wenn die Verarbeitungen des Verantwortlichen einer Datenschutz-Folgenabschätzung unterliegen.

Ein Muster einer Bestellungsurkunde zum Datenschutzbeauftragten ist als Anlage 4 beigefügt. Dieses Muster stammt von der Führungsakademie des Deutschen Olympischen Sportbundes. Die Kontaktdaten des Datenschutzbeauftragten müssen veröffentlicht (z.B. auf der Internetseite) und der Aufsichtsbehörde (Anlage 1) mitgeteilt werden (Art. 37, 7 EU-DSGVO).

Ein mögliches Schema vom Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW) zur Prüfung, ob ein Datenschutzbeauftragter berufen werden muss, ist in Anlage 5 hinterlegt.

Was muss ich tun?
Es muss geprüft werden, ob die Kriterien zur verpflichtenden Bestellung eines Datenschutzbeauftragten durch den Verein erfüllt werden.
Ggf. Kontaktdaten des Datenschutzbeauftragten veröffentlichen und der Aufsichtsbehörde mitteilen.

Wann ist eine Datenschutz-Folgenabschätzung notwendig?

Die Datenschutz-Folgenabschätzung ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Ihr Ziel besteht darin, Kriterien für den Schutz der betroffenen Personen zu definieren und die Folgen der Datenverarbeitung möglichst umfassend zu erfassen.

Eine Datenschutz-Folgenabschätzung ist insbesondere dann notwendig, wenn eine Form der Datenverarbeitung aufgrund ihrer Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat (Art.

35 Abs. 1 EU-DSGVO). Hierunter zählt unter anderem eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 EU-DSGVO (z.B. Gesundheitsdaten).

Die Datenschutzkonferenz hat hierzu eine sogenannte „Positiv-Liste“ herausgegeben (siehe Anlage 6), die u.a. als Beispiel auch Telemedizin enthält. Dienstleistungen, die z.B. mit einer digitalen Unterschrift arbeiten, können hiervon betroffen sein.

Eine Datenschutz-Folgenabschätzung sollte gemäß Art. 35 Abs. 7 EU-DSGVO zumindest folgende Inhalte enthalten:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls 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 gemäß Art. 35 Absatz 1 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 diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstigen Betroffenen Rechnung getragen wird.

Betroffenenrechte

Jeder Person, über die personenbezogene Daten erhoben werden, stehen bestimmte Rechte zu. Folgende Rechte hat die betroffene Person gem. Art. 13 II lit. b DSGVO:

- Auskunftsrecht – Art. 15 DSGVO
- Berichtigung – Art. 16 DSGVO
- Löschung – Art. 17 DSGVO
- Einschränkung – Art. 18 DSGVO
- Datenübertragbarkeit – Art. 20 DSGVO
- Widerruf – Art. 21 DSGVO

Organisatorische und technische Maßnahmen zur Sicherung personenbezogener Daten

Grundsätzlich gilt, dass der Verantwortliche ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu gewährleisten hat, indem geeignete technische und organisatorische Maßnahmen ergriffen werden. Hierbei sollen u.a. der Stand der Technik, der Umfang, sowie Umstände und Zwecke der Verarbeitungen berücksichtigt werden (Art. 32 Abs. 1 EU-DSGVO).

Geeignete Maßnahmen sind u.a. die Pseudonymisierung oder Verschlüsselung personenbezogener Daten und die Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und

Dienste, die im Zusammenhang mit der Verarbeitung personenbezogener Daten genutzt werden, sicherzustellen.

Darüber hinaus gilt es auch, die Fähigkeit, Verfügbarkeit sowie den Zugang der personenbezogenen Daten nach einem technischen oder physischen Zwischenfall rasch wiederherstellen zu können. Fortlaufend sollte außerdem ein Verfahren zur regelmäßigen Überprüfung und Bewertung der ergriffenen technischen und organisatorischen Maßnahmen eingeführt werden.

Gemeint sind hierbei z.B. die Lagerung von entsprechenden Daten in verschließbaren Schränken oder auch die Verschlüsselung von digitalen Daten bzw. den verwendeten Endgeräten.

Hinsichtlich des Serverstandortes bei der elektronischen Datenverarbeitung verweisen wir auf Artikel 44ff. EU-DSGVO. Sollten betroffene Server sich nicht innerhalb der Europäischen Union befinden, so sind entsprechende Vorkehrungen zum Datenschutz zu treffen.

Was muss ich tun?
Die aktuellen technischen und organisatorischen Maßnahmen zur Wahrung des Datenschutzes müssen (fortlaufend) auf Angemessenheit geprüft und ggf. ergänzt bzw. aktualisiert werden.

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

Im Falle der Verletzung des Schutzes von personenbezogenen Daten hat der Verantwortliche grundsätzlich binnen 72 Stunden nach Bekanntwerden der Verletzung die zuständige Aufsichtsbehörde (bei Vereinen die Landesdatenschutzbehörde, siehe Anlage 1) zu informieren. Erfolgt die Meldung nicht innerhalb von 72 Stunden, so ist eine Begründung für die Verzögerung beizufügen. Bei der Behebung der Datenpanne ist der Datenschutzbeauftragte hinzuziehen, sofern vorhanden. Weiterhin ist es sinnvoll, eine Anleitung „Wie verhalte ich mich bei einer Datenpanne?“ an die Mitarbeiter herauszugeben (Anlage 7).

Gleichzeitig sind grundsätzlich auch die betroffenen Personen unverzüglich über die Datenschutzverletzung zu informieren.

Die Aufsichtsbehörden sind dazu angehalten, dass verhängte Geldbußen für Verstöße in jedem Einzelfall wirksam, **verhältnismäßig,** aber auch abschreckend wirken sollen. Je nach Umstand des Einzelfalls werden Maßnahmen nach Art. 58 Abs. 2 a-h bzw. j EU-DSGVO und/oder Geldbußen verhängt (Art. 83 Abs. 2 EU-DSGVO).

Was muss ich tun?
Bei Datenschutzverletzungen muss die zuständige Aufsichtsbehörde innerhalb von 72 Stunden informiert werden. Ebenso muss die betroffene Person unverzüglich informiert werden.

Abschnitt 2: Personenbezogene Daten im Anerkennungsverfahren zum Rehabilitationssport

Laut Rahmenvereinbarung über den „Rehabilitationssport und das Funktionstraining vom 01.01.2011“ (Rahmenvereinbarung) Ziffer 8.1, bedürfen Rehabilitationssportgruppen der Anerkennung. Die Anerkennung orientiert sich an der Anlage der Rahmenvereinbarung und ist innerhalb des DBS durch das bundeseinheitliche Anerkennungsverfahren verbindlich geregelt. Die „Richtlinie zur Durchführung des Rehabilitationssports im DBS“ (Richtlinie) gibt weitere Handlungsempfehlungen.

Für die Anerkennung von Gruppen auf Grundlage der Rahmenvereinbarung und der nachgeordneten vertraglichen Regelungen sind personenbezogene Daten von mindestens einer Person als Ansprechpartner, Mediziner und Übungsleitung erforderlich.

Einwilligungserklärungen Ansprechpartner, Mediziner und Übungsleitung

Damit der Verein die personenbezogenen Daten vom Ansprechpartner, Mediziner und Übungsleiter an den zuständigen Landesverband als anerkennende Stelle für den Rehabilitationssport weitergeben darf, ist eine Einwilligungserklärung zur Datenerhebung, -verarbeitung und -weitergabe erforderlich. Der zuständige Landesverband ist als anerkennende Stelle vertraglich verpflichtet, den Rehabilitationsträgern auf Bundes- und Landesebene nach § 6 Sozialgesetzbuch (SGB) IX regelmäßig ein Verzeichnis der anerkannten Rehabilitationsgruppen zur Verfügung zu stellen, landesspezifische Regelungen sind hierbei zu beachten. Die in diesem Verzeichnis geführten Rehabilitationssport-gruppen sind, bei Vorliegen einer genehmigten Verordnung, zur Abrechnung ihrer Leistung gegenüber dem jeweiligen Rehabilitationsträger berechtigt. Die Übermittlung erfolgt also aufgrund der Erfüllung eines Vertrages.
Dabei wird den Rehabilitationsträgern regelmäßig der Name und Vorname des Ansprechpartners zur Verfügung gestellt.
Darüber hinaus sind die Rehabilitationsträger gemäß Vertrag dazu berechtigt, beim jeweiligen zuständigen Landesverband vorliegende Unterlagen zur Anerkennung einzusehen, also auch die personenbezogenen Daten von Übungsleitungen und Medizinern.

Entsprechende unverbindliche Muster für Einwilligungserklärungen können Sie beim zuständigen Landesverband als anerkennende Stelle erfragen.

Was muss ich tun?
Jeweils von Ansprechpartner, Mediziner und Übungsleitung des Vereins müssen Einwilligungserklärungen zu Datenerhebung, -verarbeitung und -weitergabe vorliegen, damit diese Daten dem DBS-Landesverband und den Rehabilitationsträgern übermittelt werden dürfen.

Mitarbeiter auf Verschwiegenheit verpflichten

Grundsätzlich gilt nach § 35 Abs. 1 SGB I, dass jeder den Anspruch hat, dass seine Sozialdaten nicht unbefugt von Leistungsträgern (z.B. Krankenkassen) verarbeitet werden. Um dem Gerecht werden zu können, erfordert die Verwendung von Sozialdaten nach SGB X, die Verpflichtung auf

Verschwiegenheit der Personen, die mit Daten zum Rehabilitationssport in Kontakt kommen. Dies ist in den einschlägigen Vereinbarungen auf Bundes- und Landesebene ebenso geregelt (vgl. z.B. §11 der „Durchführungs- und Finanzierungsvereinbarung vom 01.01.2012 vdek/DBS/DOSB).

Eine unverbindliche Checkliste, anhand der eine Verpflichtung auf Verschwiegenheit erstellt werden kann, ist in der Anlage 8 beigefügt.

Grundsätzlich unterliegen die betreuenden Mediziner des Vereins aufgrund ihrer beruflichen Stellung einer besonderen Geheimhaltungspflicht (bspw. § 203 Abs. 1 S. 1 StGB). Auf den Abschluss einer gesonderten Verschwiegenheitserklärung mit ihnen kann daher in der Regel verzichtet werden. Wir empfehlen jedoch, sich vom Arzt die schriftliche Bestätigung geben zu lassen, dass er der ärztlichen Schweigepflicht unterliegt und alle gesetzlichen Anforderungen hinsichtlich des Datenschutzes erfüllt.

Was muss ich tun?
Alle Mitarbeiter des Vereins, die mit personenbezogenen Daten des Rehabilitationssports in Kontakt kommen, müssen auf Verschwiegenheit verpflichtet werden.

Vertrag zur Auftragsverarbeitung

Werden personenbezogenen Daten nicht durch den Verein selbst verarbeitet, sondern wird hierfür eine andere Stelle in Anspruch genommen, sind laut EU-DSGVO gesonderte Regelungen und Maßnahmen zu ergreifen.

In Anlage 9 ist ein Kurzpapier der Datenschutzkonferenz hinterlegt, in dem erläutert wird, in welchen Fällen ein Auftragsverarbeitungsvertrag erforderlich ist.

Was muss ich tun?
Prüfen, ob für die delegierte Datenverarbeitung (z.B. im Rahmen der Abrechnung) ein Vertrag zur Auftragsverarbeitung erforderlich ist.

Abschnitt 3: Personenbezogene Daten bei der Durchführung des Rehabilitationssports

Beratungsgespräch

In der Regel erfolgt vor Beginn des ärztlich verordneten Rehabilitationssports ein Beratungsgespräch durch den Verein. Der DBS empfiehlt hierbei ein Beratungsprotokoll zu führen, insbesondere um nachweisen zu können, dass hinsichtlich einer zuzahlungsfreien Teilnahme bzw. der Freiwilligkeit einer etwaigen zusätzlichen Leistung des Vereins, ordnungsgemäß beraten wurde. Weitere Ausführungen hierzu finden sich in der Richtlinie unter Ziffer 3.

Im Beratungsgespräch werden personenbezogene Daten, darunter in der Regel auch besondere Kategorien (Art. 9 EU-DSGVO) von Daten, wie Gesundheitsdaten des Rehabilitationssport-

interessenten erhoben und zumeist auch verarbeitet. Bleibt es bei der Erstkontaktaufnahme und werden die Daten nicht weiterverarbeitet, ist eine Einwilligungserklärung des Rehabilitationssports-interessenten nicht erforderlich.

Bei der Durchführung des Rehabilitationssports ist eine Datenverarbeitung zwingend erforderlich, sodass eine Nichtbereitstellung von Daten im Regelfall dazu führt, dass der Rehabilitationssport nicht durchgeführt werden kann. Dies bezieht sich auch auf weitere Gesundheitsdaten (z.B. Eingangsfragebogen zum Gesundheitszustand – Anamnese), die für die Durchführung des Rehabilitationssports relevant sind.

Verarbeitung kann im konkreten Falle z.B. heißen: Mitteilung an die betreuende Übungsleitung, Rückfrage an betreuenden Mediziner des Vereins oder elektronische Verarbeitung in der Mitglieder/Teilnehmer-Verwaltungssoftware. Außerdem werden die erhobenen Daten im Rahmen des Abrechnungsverfahrens weiterverarbeitet und ggf. an Abrechnungszentren bzw. den Rehabilitationsträger übermittelt.

Für die Beachtung folgender Punkte im Rahmen des Beratungsgesprächs empfiehlt der DBS die Verwendung des Beiblattes zum Datenschutz, welches im Rahmen des Beratungsprozesses ausgegeben werden sollte und ggf. auf den Einzelfall angepasst werden muss. Ein Beiblatt zum Datenschutz für den Beratungsprozess erhalten Sie bei Ihrem zuständigen Landesverband als anerkennende Stelle.

Die Grundlage hierzu bildet Art. 13 Abs. 1 + 2 der EU-DSGVO (siehe Anlage 10).

Gemäß Artikel 9 EU-DSGVO ist die Verarbeitung von Gesundheitsdaten zunächst untersagt und ist entweder erst nach Einwilligung der betroffenen Person erlaubt bzw. wenn die Verarbeitung für die Erfüllung eines Vertrages notwendig ist oder nach §22 Absatz 1 b BDSG NEU zum Zwecke der Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich verarbeitet werden.

- Da für den Rehabilitationssport § 22 Absatz 1 b BDSG sowie, die jeweiligen Spezialgesetze (§§67ff.) Anwendung finden, ist eine explizite Einwilligungserklärung zur Datenverarbeitung von den Teilnehmenden grundsätzlich nicht verpflichtend einzuholen.
- Verpflichtend ist jedoch die Information zu erteilen, dass Daten erhoben und verarbeitet werden, zu welchem Zweck diese verarbeitet werden und an wen diese übermittelt werden.

Werden über den Rehabilitationssport hinaus freiwillig zusätzliche Leistungen und/oder eine Vereinsmitgliedschaft in Anspruch genommen, so müssen für diese weiteren Zwecke Einwilligungserklärungen über die Verarbeitung der personenbezogenen Daten und besonderen Kategorien von Daten eingeholt werden. Aus diesen Einwilligungserklärungen (siehe Anlage 11) muss eindeutig und leicht verständlich hervorgehen, zu welchen Zwecken welche Daten verarbeitet werden (Art. 7 Abs. 2 EU-DSGVO). Ebenso muss deutlich sein, an wen diese Daten übermittelt werden.

Was muss ich tun?
Einsatz des Beratungsprotokolls im Beratungsgespräch prüfen sowie die rechtmäßige Weitergabe der verpflichtenden Information zur Datenerhebung und -verarbeitung sicherstellen. Außerdem sind Einwilligungserklärungen für z.B. zusätzliche Leistungen hinsichtlich der Konformität mit der EU-DSGVO zu prüfen.

Umgang mit der Anwesenheitsliste

Die Übungsleitung hat nach Ziffer 10 der Richtlinie eine Anwesenheitsliste je Gruppe zu führen. Es ist darauf zu achten, dass nur die Übungsleitung Einsicht in diese Anwesenheitslisteliste hat und diese separat von den Teilnahmebestätigungen aufbewahrt wird. Auch im Rahmen von Audits darf diese Liste nicht eingesehen werden ohne, dass eine entsprechende Einwilligung aller Teilnehmer der Gruppe vorliegt.

Umgang mit der Teilnahmebestätigung

Für die Teilnahmebestätigungen sollte je Gruppe ein Ordner geführt werden, um den Zugriff auf die besonderen Kategorien von personenbezogenen Daten (z.B. Rehabilitationsträger, Versicherten-Nr.) zu verhindern.

Da die Teilnahmebestätigung in der Regel auch durch andere Rehabilitationssportler eingesehen werden kann, wird empfohlen für die Zeit der Durchführung des Rehabilitationssports, nur den Namen sowie die Gruppe in die Teilnahmebestätigung einzutragen. Erst wenn die Abrechnung bzw. eine Zwischenabrechnung der Verordnung erfolgt und somit ein Zugriff durch Dritte nicht mehr zu erwarten ist, sollten die noch fehlenden personenbezogenen und ggf. besonderen Kategorie von Daten (z.B. Geburtsdatum, Krankenkasse, Versicherten-Nr.) in die Teilnahmebestätigung eingetragen werden.

Verarbeitung von Daten für die Abrechnung

Erfolgt die Abrechnung über ein Abrechnungszentrum, welches nicht nach § 302 SGB V abrechnet oder sind anderweitig Dritte beim Abrechnungsverfahren involviert, so ist die Einholung einer zusätzlichen Einwilligung von allen Rehabilitationssportlern erforderlich. Es gilt jedoch den Einzelfall zu prüfen.

Wird ein Abrechnungszentrum mit der Abrechnung beauftragt, so wird in der Regel ein Vertrag über eine Auftragsverarbeitung gemäß Art. 28 Abs. 3 EU-DSGVO notwendig. Verein und Abrechnungszentrum haben zu prüfen, inwiefern ein solcher Vertrag im konkreten Fall notwendig ist und den aktuellen Datenschutzregelungen entspricht.

Dieser Vertrag ist dem zuständigen Landesverband als anerkennende Stelle in Kopie zur Verfügung zu stellen (vgl. „Ergänzungsvereinbarung Elektronisches Abrechnungsverfahren mit dem vdek §2, Ziff. 15“).

In der Anlage 12 finden Sie eine Liste der Abrechnungszentren, von denen bereits bekannt ist, dass sie nach den Vorgaben des §302 SGB V arbeiten. Sollte Ihr Abrechnungszentrum hier nicht aufgeführt sein, wenden Sie sich bitte unmittelbar an Ihr Abrechnungszentrum.

Was muss ich tun?
Beteiligte am Abrechnungsverfahren hinsichtlich Verarbeitung nach §302 SGB V prüfen und ggf. notwendige Maßnahmen einleiten.

Aufbewahrung der Teilnehmerbezogenen Unterlagen

Die Teilnahmebestätigungen und Unterlagen mit besonderen Kategorien von Daten (z.B. Verordnungen, weiterführende medizinische Informationen) müssen getrennt voneinander und für Dritte unzugänglich aufbewahrt werden. Hinsichtlich der Aufbewahrungsfrist von Unterlagen vgl. Ziffer 19 der Richtlinie.

Abschnitt 4: Kommunikation mit Dritten zu Teilnehmerdaten

Kommunikation mit dem DBS-Landesverband

Bei konkreten Fragestellungen in Bezug auf Teilnehmende oder Interessenten am Rehabilitationssport dürfen keine personenbezogenen Daten oder Dokumente, die solche enthalten, übermittelt werden, solange keine entsprechende Einverständniserklärung des Betroffenen vorliegt.

Eine Übermittlung anonymisierter Dokumente ist möglich. Sollten Rückfragen zur indikationsgerechten Zuordnung eines Interessenten bestehen, so empfiehlt sich die Schwärzung der personenbezogenen Daten (Name, Vorname, Adresse, Geb.-Datum, Versicherten-Nr.) auf der Kopie/ dem Scan der Verordnung.

Bei Audits dürfen keine Teilnehmerunterlagen eingesehen werden. Dies bezieht sich auf jegliche Unterlagen, aus denen bereits zu schließen ist, dass bzw. wann eine bestimmbare Person am Rehabilitationssport teilnimmt. Der Grund hierfür ist, dass schon die Information, dass eine Person am ärztlich verordneten Rehabilitationssport überhaupt teilnimmt als Information der besonderen Kategorie gemäß Art. 9 EU-DSGVO gilt.

Kommunikation mit dem Rehabilitationsträger und dem verordnenden Arzt

Es ist empfehlenswert, dass Rückfragen zur Genehmigung einer Verordnung oder der Abrechnungsfähigkeit bei Zuordnung zu einer bestimmten Gruppe sowie bei Rückfragen an den verordnenden Arzt, aufgrund seiner besonderen Stellung hinsichtlich der Verschwiegenheit, über den betreuenden Mediziner des Vereins erfolgen.

Liste der zuständigen Landesdatenschutz-Aufsichtsbehörden

Baden-Württemberg

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg
Postfach 10 29 32
70025 Stuttgart

Telefon: 07 11/61 55 41-0
Telefax: 07 11/61 55 41-15
E-Mail: poststelle@lfdi.bwl.de
http://www.baden-wuerttemberg.datenschutz.de

Bayern

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27 (Schloss)
91522 Ansbach

Telefon: 0981/53-1300
Telefax: 0981/53-5300
E-Mail: poststelle@lda.bayern.de
http://www.lda.bayern.de

Berlin

Berliner Beauftragte für Datenschutz und Informationsfreiheit
Friedrichstraße 219
10969 Berlin

Telefon: 030/13 889-0
Telefax: 030/215-5050
E-Mail: mailbox@datenschutz-berlin.de
http://www.datenschutz-berlin.de

Brandenburg

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht
Stahnsdorfer Damm 77
14532 Kleinmachnow

Telefon: 03 32 03/356-0
Telefax: 03 32 03/356-49
E-Mail: poststelle@lda.brandenburg.de
http://www.lda.brandenburg.de

Stand: 26.10.2018

Bremen

Die Landesbeauftragte für Datenschutz und Informationsfreiheit
der Freien Hansestadt Bremen
Postfach 10 03 80
27503 Bremerhaven

Telefon: 0421/361-2010
Telefax: 0421/496-18495
E-Mail: office@datenschutz.bremen.de
http://www.datenschutz.bremen.de

Hamburg

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Klosterwall 6 (Block C)
20095 Hamburg

Telefon: 040/42854-4040
Telefax: 040/42854-4000
E-Mail: mailbox@datenschutz.hamburg.de
http://www.datenschutz.hamburg.de

Hessen

Der Hessische Datenschutzbeauftragte
Gustav-Stresemann-Ring 1
65189 Wiesbaden

Telefon: 06 11/140 80
Telefax: 06 11/14 08-900
E-Mail: poststelle@datenschutz.hessen.de
http://www.datenschutz.hessen.de

Mecklenburg-Vorpommern

Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern
Lennéstraße 1, Schloss Schwerin
19053 Schwerin

Telefon: 0385/59494-0
Telefax: 0385/59494-58
E-Mail: info@datenschutz-mv.de
http://www.lfd.m-v.de

Niedersachsen

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstr. 5
30159 Hannover

Telefon: 05 11/120-45 00
Telefax: 05 11/120-45 99

E-Mail: poststelle@lfd.niedersachsen.de
http://www.lfd.niedersachsen.de

Nordrhein-Westfalen

Landesbeauftragte für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen
Kavalleriestraße 2-4
40213 Düsseldorf

Telefon: 0211/38424-0
Telefax: 0211/38424-10
E-Mail: poststelle@ldi.nrw.de
http://www.ldi.nrw.de

Rheinland-Pfalz

Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit Rheinland-Pfalz
Postfach 30 40
55020 Mainz

Telefon: 061 31/208-24 49
Telefax: 061 31/208-24 97
E-Mail: poststelle@datenschutz.rlp.de
http://www.datenschutz.rlp.de

Saarland

Unabhängiges Datenschutzzentrum Saarland
Fritz-Dobisch-Straße 12
66111 Saarbrücken

Telefon: 06 81/947 81-0
Telefax: 06 81/947 81-29
E-Mail: poststelle@datenschutz.saarland.de
http://www.datenschutz.saarland.de

Sachsen

Der Sächsische Datenschutzbeauftragte
Devrientstraße 1
01067 Dresden

Telefon: 03 51/49 3-5401
Telefax: 03 51/49 3-5490
E-Mail: saechsdsb@slt.sachsen.de
http://www.datenschutz.sachsen.de

Sachsen-Anhalt

Landesbeauftragter für den Datenschutz Sachsen-Anhalt
Postfach 19 47

39009 Magdeburg

Telefax: 03 91/818 03-33
E-Mail: poststelle@lfd.sachsen-anhalt.de
http://www.datenschutz.sachsen-anhalt.de

Schleswig-Holstein

Aufsichtsbehörde
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Postfach 71 16
24171 Kiel

Telefon: 0431/988-1200
Telefax: 0431/988-1223
E-Mail: mail@datenschutzzentrum.de
http://www.datenschutzzentrum.de

Thüringen

Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 90 04 55
99107 Erfurt

Telefon: 03 61/57 311 29 00
Telefax: 03 61/57 311 2904
E-Mail: poststelle@datenschutz.thueringen.de
http://www.tlfdi.de

Checkliste zum Verzeichnis der Verarbeitungstätigkeiten

Die folgende Checkliste soll bei der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten unterstützen und anhand der Beispiele darstellen, welche Daten konkret benötigt werden.

Zunächst dürfen im Verzeichnis der Verarbeitungstätigkeiten die Informationen zum Verantwortlichen und ggf. seiner Vertreter und des Datenschutzbeauftragten nicht fehlen. Ebenso sollte im allgemeinen Teil beschrieben werden, durch welche technischen und organisatorischen Maßnahmen ein angemessenes Schutzniveau erreicht werden soll.

Allgemeine Informationen

- ☐ Namen des Verantwortlichen / der gemeinsam Verantwortlichen
- ☐ Kontaktdaten des Verantwortlichen / der gemeinsam Verantwortlichen
- ☐ Ggf. Namen und Kontaktdaten des Vertreters des Verantwortlichen
- ☐ Ggf. Namen und Kontaktdaten des Datenschutzbeauftragten
- ☐ Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus nach Art. 32. Abs. 1 DSGVO (z.B. Verschlüsselungsverfahren, Verfahren zur regelmäßigen Überprüfung der Sicherheit des Systems, etc.)

Verarbeitungstätigkeiten

Bei der Auflistung der verschiedenen Tätigkeiten müssen jeweils die untenstehenden Punkte beantwortet werden:

- ☐ Tätigkeitsbezeichnung (z.B. Abrechnung Rehabilitationssport)
- ☐ Zwecke der Verarbeitung (z.B. Abrechnung von erfolgten Teilnahmen am Rehabilitationssport gegenüber den Rehabilitationsträgern)
- ☐ Betroffene Personengruppen (z.B. Teilnehmer am Rehabilitationssport)
- ☐ Kategorien der betroffenen personenbezogenen Daten (z.B. Name, Vorname, Geburtsdatum, KV-Nummer, Rehabilitationsträger, Teilnahmedaten, etc.)
- ☐ Empfänger, denen die personenbezogenen Daten offengelegt werden (z.B. Abrechnungszentrum, Rehabilitationsträger, etc.)
- ☐ Ggf. Übermittlung von personenbezogenen Daten in ein Drittland unter Angabe des Drittlands und die Dokumentation geeigneter Garantien nach Art. 49 Abs. 1 DSGVO (z.B. „keine Übermittlung personenbezogener Daten an Drittland“)
- ☐ Frist zur Löschung der verschiedenen Kategorien von Daten (z.B. Abrechnungsrelevante Unterlagen bzw. Buchungsbelege werden gemäß §147 AO zehn Jahre aufbewahrt)

Beschluss der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Düsseldorf, 26. April 2018

Datenschutzbeauftragten-Bestellpflicht nach Artikel 37 Abs. 1 lit. C Datenschutz-Grundverordnung bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs

1. Betreibt ein einzelner Arzt, Apotheker oder sonstiger Angehöriger eines Gesundheitsberufs eine Praxis, Apotheke oder ein Gesundheitsberufsunternehmen und sind dort einschließlich seiner Person in der Regel mindestens 10 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt, besteht eine gesetzliche Verpflichtung zur Benennung eines Datenschutzbeauftragten (DSB).

2. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) bzw. Gemeinschaftspraxis zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, ist in der Regel nicht von einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten im Sinne von Art. 37 Abs. 1 lit. c DS-GVO auszugehen – in diesen Fällen ist unter Berücksichtigung von Punkt 3 dann kein DSB zu benennen, wenn weniger als 10 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind.

3. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) bzw. Gemeinschaftspraxis zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, bei denen ein hohes Risiko für die Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten zu erwarten ist, ist eine Datenschutzfolgenabschätzung vorgeschrieben und damit zwingend ein Datenschutzbeauftragter zu benennen. Dies kann neben einer umfangreichen Verarbeitung (z.B. große Praxisgemeinschaften), die ohnehin nach Art. 37 Abs. 1 lit. c DS-GVO zu einer Benennungspflicht führt, beispielsweise beim Einsatz von neuen Technologien, die ein hohes Risiko mit sich bringen, der Fall sein. Der Datenschutzbeauftragte ist damit auch dann zu benennen,

wenn weniger als 10 Personen ständig mit der Verarbeitung personenbezogener Daten zu tun haben.

4. Der Begriff „Gesundheitsberuf“ ist im Sinne der Aufzählung nach § 203 Abs. 1 StGB auszulegen und umfasst die in § 203 Abs. 1 Nr. 1, 2, 4 und 5 StGB aufgezählten Berufsbilder.

Platzhalter
Ihr Logo

FA-DATENSCHUTZPLATTFORM

Ihr Vereins-/Verbandsname

Bestellungsurkunde zum Datenschutzbeauftragten

Die Verantwortliche Stelle – Klicken Sie hier, um Text einzugeben. – bestellt auf der Grundlage der beigefügten Arbeitsplatzbeschreibung mit sofortiger Wirkung.

Herrn/Frau: Klicken Sie hier, um Text einzugeben.

wohnhaft in Klicken Sie hier, um Text einzugeben.

geboren am: Klicken Sie hier, um Text einzugeben.

gemäß §38 BDSG(neu), Art.37 und Art. 39 – DSGVO zu ihrem / seinem Beauftragten für den Datenschutz.

Beide Parteien vereinbaren dazu folgende Regelungen:
Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:

(1) Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;

Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten 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 gemäß Artikel 35;

Zusammenarbeit mit der Aufsichtsbehörde;

Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen.

(2) Zu den Aufgaben gehört auch der Kontakt zum / zur Landesbeauftragen für den Datenschutz, zu Behörden und Verbänden zur Klärung datenschutzrechtlicher Problemstellungen mit Einverständnis der Klicken Sie hier, um Text einzugeben. oder in anonymisierter Form.

(3) Der Datenschutzbeauftragte informiert die Mitarbeiter(innen) der / des Klicken Sie hier, um Text einzugeben. über Gesetzesnovellen, EU-Richtlinien, Persönlichkeitsrechte und Rechtsprechung zu datenschutzrechtlich relevanten Themen.

(4) Der / Die Klicken Sie hier, um Text einzugeben. kann den Datenschutzbeauftragten auch zu Fragen der allgemeinen Datensicherung in Anspruch nehmen. Das betrifft insbesondere die Gestaltung der innerbetrieblichen Organisation im Sinne des Arte. 32 DSGVO, um den besonderen Anforderungen des Datenschutzes gerecht zu werden, z.B. bei

- der Zugriffskontrolle (Organisation des EDV-Zugriffs),
- der Eingabekontrolle (Protokollierung der Nutzer-Aktivitäten),
- der Verfügbarkeitskontrolle (Schutz gegen Zerstörung und Verlust).

© 2018 by SVBG MÜLOT GmbH

Platzhalter
Ihr Logo

FA-DATENSCHUTZPLATTFORM

Ihr Vereins-/Verbandsname

Bestellungsurkunde zum Datenschutzbeauftragten

Der Datenschutzbeauftragte ist ausschließlich gegenüber der Geschäftsführung berichtspflichtig. Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Von der besonderen Verschwiegenheitsverpflichtung über ihm zur Kenntnis gelangte Tatsachen, die Rückschlüsse auf eine bestimmte Person zulassen, kann er nur von dem / von der Betroffenen entbunden werden.

(5) Der Verantwortliche i.S.d. Art. 4 Abs. (7) DSGVO hat den Datenschutzbeauftragten bei der Erfüllung der hier fest gelegten Aufgaben zu unterstützen und ihm, soweit dies zur Erfüllung der Aufgabe erforderlich ist, auch Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen.

(6) Der Datenschutzbeauftragte darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden.

(7) Diese Bestellung kann nur in entsprechender Anwendung des § 626 BGB oder auf Verlangen der Aufsichtsbehörde widerrufen werden.

Ort, Datum

_____ _____

Unterschrift Verantwortliche Stelle *Unterschrift des Datenschutzbeauftragten*

© 2018 by SVBG MÜLOT GmbH

3. Benennung eines Datenschutzbeauftragten

Wann muss der Verein einen Datenschutzbeauftragten benennen?

Der Verein hat einen Datenschutzbeauftragen zu benennen, wenn mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind oder der Verein Verarbeitungen vornimmt, die einer Datenschutzfolgenabschätzung gemäß Art. 35 DS-GVO unterliegen.

Darüber hinaus muss ein Datenschutzbeauftragter benannt werden, wenn die Kerntätigkeit des Vereins in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Person erforderlich macht (z.B. Videoüberwachung im Stadion) oder die Kerntätigkeit in der Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 DS-GVO (z.B. Gesundheitsdaten in Selbsthilfegruppen) oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO besteht (Art. 37 Abs. 1 lit. b) und lit. c) DS-GVO).

Für die Frage, ob der Verein einen Datenschutzbeauftragten benennen muss, empfiehlt sich folgendes **Prüfschema**.

a) Sind mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt?

„Ständig" beschäftigt ist eine Person, wenn sie für diese Aufgabe auf längere Zeit vorgesehen ist und sie entsprechend wahrnimmt. Irrelevant ist, ob die Person beim Verein beschäftigt oder ehrenamtlich tätig ist. Die Aufgabe braucht auch nicht Hauptaufgabe der Person zu sein. Das Tatbestandsmerkmal „ständig" ist daher auch erfüllt, wenn die Aufgabe selbst nur gelegentlich anfällt, die betreffende Person sie aber stets wahrzunehmen hat. Nicht ständig beschäftigt ist hingegen, wer die eigentlich anderen obliegende Aufgabe gelegentlich mit übernimmt oder nur vorübergehend in diesem Bereich tätig ist. Ständig bedeutet daher, dass die Person immer dann mit der Verarbeitung personenbezogener Daten beschäftigt ist, wenn diese Tätigkeit anfällt.

✔ Ja: Datenschutzbeauftragter erforderlich

✘ Nein: weiterprüfen:

b) Nimmt der Verein Verarbeitungen vor, die einer Datenschutzfolgenabschätzung unterliegen?

Eine Datenschutzfolgeabschätzung ist nur dann erforderlich, wenn die Verarbeitung personenbezogener Daten ein hohes Risiko für die betroffenen Personen hat. Ein solch hohes Risiko ist jedoch die Ausnahme und besteht in aller Regel nicht. Mehr Informationen hierzu unten Nr. 5.

✔ Ja: Datenschutzbeauftragter erforderlich

✘ Nein: weiterprüfen:

c) Liegt die Kerntätigkeit des Vereins in Verarbeitungsprozessen, welche aufgrund ihrer Art, ihres Umfangs oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Person erforderlich macht?

Werden personenbezogene Daten nur als Nebentätigkeit und nicht als Haupttätigkeit verarbeitet, so liegt keine „Kerntätigkeit vor. Bei „klassischen" Vereinen erfolgt eine Verarbeitung personenbezogener Daten nur als notwendig anfallende Nebentätigkeit (Mitgliederverwaltung, Verarbeitung von Daten von Beschäftigten etc.). Vereine, deren Kerntätigkeit in Verarbeitungsprozessen liegt, welche eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Person erforderlich machen, sind kaum denkbar.

✔ Ja: Datenschutzbeauftragter erforderlich

✘ Nein: weiterprüfen:

d) Besteht die Kerntätigkeit in der Verarbeitung besonderer Kategorien von Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten?

Besondere Kategorien von Daten sind personenbezogene Daten, aus denen die rassische, ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen hervorgehen sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben und der sexuellen Orientierung. Als Beispiele kommen die Religionszugehörigkeit, Parteizugehörigkeit sowie Angaben über Krankheiten in Betracht. Hinzukommen muss jedoch auch hier, dass die Kerntätigkeit des Vereins in der Verarbeitung vorgenannter Daten liegt. Dies ist immer dann der Fall, wenn ohne die Verarbeitung dieser Daten der Zweck des Vereins nicht erreicht werden könnte. Denkbar ist dies etwa bei Selbsthilfegruppen oder Vereinen mit politischer Zielrichtung.

✔ Ja: Datenschutzbeauftragter erforderlich

✘ Nein: Kein Datenschutzbeauftragter erforderlich.

Der Verein hat die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen. Hierbei ist es ausreichend, wenn die E-Mail-Adresse des Datenschutzbeauftragten auf der Vereinshomepage frei zugänglich genannt wird.

Der Datenschutzbeauftragte ist der zuständigen Aufsichtsbehörde zu melden. Eine Meldung ist beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg ist über folgendes Online–Formular möglich:
https://www.baden-wuerttemberg.datenschutz.de/dsb-online-melden/

Welche fachlichen Qualifikationen ein Datenschutzbeauftragter erfüllen muss und was seine Aufgaben sind, siehe ab S. 31 Punkt 7.1 der Orientierungshilfe „Datenschutz im Verein nach der DS-GVO“ (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf) sowie in Kurzpapier Nr. 12 der Datenschutzkonferenz (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/01/DSK_KPNr_12_Datenschutzbeauftragter.pdf).

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
1	Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung natürlicher Personen, wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft: • Daten zu schutzbedürftigen Betroffenen • Systematische Überwachung • Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen • Bewerten oder Einstufen (Scoring) • Abgleichen oder Zusammenführen von Datensätzen • Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung • Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert	Verwendung von biometrischen Systemen zur Zutrittskontrolle oder für Abrechnungszwecke.	Ein Unternehmen setzt flächendeckend Fingerabdrucksensoren zur Zutrittskontrolle für bestimmte Bereiche ein. Eine Schulkantine bietet den Schülern das „Bezahlen per Fingerabdruck“ an.
2	Verarbeitung von genetischen Daten im Sinne von Artikel 4 Nr. 13 DSGVO, , wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft: • Daten zu schutzbedürftigen Betroffenen • Systematische Überwachung • Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen • Bewerten oder Einstufen (Scoring) • Abgleichen oder Zusammenführen von Datensätzen • Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung • Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert	Früherkennung von Erbkrankheiten Genetische Datenbanken zur Abstammungsforschung	Eine Klinik setzt DNA-Tests zur Früherkennung vererblicher Krankheiten bei Neugeborenen ein. Ein Unternehmen bietet einen Dienst an, über den Kunden die eigenen genetischen Daten mit denen Dritter abgleichen können, um mehr über die eigene Abstammung zu erfahren. Dazu pflegt das Unternehmen eine Datenbank mit genetischen Daten einer Vielzahl von Personen.
3	Umfangreiche Verarbeitung von Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen, auch wenn es sich nicht um Daten gemäß Art. 9 Abs. 1 und 10 DS-GVO handelt	Betrieb eines Insolvenzverzeichnisses Träger von großen sozialen Einrichtungen Große Anwaltssozietät	Ein Unternehmen bietet ein umfassendes Verzeichnis über Privatinsolvenzen an. Große Rechtsanwaltskanzlei, die im Schwerpunkt familienrechtliche Mandate betreut.
4	Umfangreiche Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen	Fahrzeugdatenverarbeitung – Car Sharing / Mobilitätsdienste	Ein Unternehmen bietet einen Car-Sharing-Dienst oder andere Mobilitätsdienstleistungen an und verarbeitet

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist			
Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
			hierfür insbesondere umfangreich Positions- und Abrechnungsdaten.
		Fahrzeugdatenverarbeitung – Zentralisierte Verarbeitung der Messwerte oder Bilderzeugnisse von Umgebungssensoren	Ein Unternehmen erhebt personenbezogene Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren.
		Offline-Tracking von Kundenbewegungen in Warenhäusern, Einkaufszentren o. ä. Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes	Ein Unternehmen verarbeitet die GPS-, Bluetooth- und/oder Mobilfunksignale von Passanten und Kunden, um die Laufwege und das Einkaufsverhalten nachverfolgen zu können.
5	Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Verarbeitung der so zusammengeführten Daten, sofern • die Zusammenführung oder Verarbeitung in großem Umfang vorgenommen werden, • für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den betroffenen Personen erhoben wurden, • die Anwendung von Algorithmen einschließen, die für die betroffenen Personen nicht nachvollziehbar sind, und der Erzeugung von Datengrundlagen dienen, die dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den betroffenen Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen können	Fraud-Prevention-Systeme	Zur Prävention von Betrugsfällen verarbeitet der Betreiber eines Online-Shops umfassende Datenmengen. Das Ergebnis der Prüfung ist ein Risikowert, der darüber entscheidet, ob einem Käufer der Rechnungskauf als Zahlungsart angeboten wird oder nicht.
		Scoring durch Auskunfteien, Banken oder Versicherungen	Eine Auskunftei führt ein Scoring im Hinblick auf die Vertrauenswürdigkeit von Personen durch. Eine Bank führt Scoring durch, um das Ausfallrisiko der Rückzahlungen von Personen zu bestimmen. Eine Versicherung führt ein Scoring durch, um das Risiko einer Person im Hinblick auf bestimmte Eigenschaften oder Aktivitäten der Person zur Bestimmung der Höhe einer Versicherungspolice zu bestimmen.
6	Mobile optisch-elektronische Erfassung personenbezogener Daten in öffentlichen Bereichen, sofern die Daten aus ein oder mehreren Erfassungssystemen in großem Umfang zentral zusammengeführt werden.	Fahrzeugdatenverarbeitung – Umgebungssensoren	Ein Unternehmen erhebt personenbezogene Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren.
7	Umfangreiche Erhebung und Veröffentlichung oder Übermittlung von personenbezogenen Daten, die zur Bewertung des Verhaltens und anderer persönlicher Aspekte von Personen dienen und von Dritten dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den bewerteten Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen	Betrieb von Bewertungsportalen	Ein Online-Portal bietet Nutzern die Möglichkeit an, Leistungen von Selbstständigen öffentlich feingranular zu bewerten. Online-Bewertungsportal bspw. für Ärzte, Selbstständige oder Lehrer.
		Inkassodienstleistungen – Forderungsmanagement	Ein Unternehmen verarbeitet für seine Kunden in großem Umfang personenbezogene Daten von Schuldnern, insbesondere Vertragsdaten, Rechnungsdaten und

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist			
Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
		Inkassodienstleistungen – Factoring	Daten über Vermögensverhältnisse von Schuldnern zur Geltendmachung von Forderungen. Ggf. werden Daten an Auskunfteien übermittelt. Ein Unternehmen lässt sich in großem Umfang Forderungen übertragen um diese auf eigenes Risiko geltend zu machen. Es verbarbeitet hierfür insbesondere Vertragsdaten, Rechnungsdaten, Scoringdaten und Informationen über Vermögensverhältnisse von Schuldnern. Ggf. werden Daten an Auskunfteien übermittelt.
8	Umfangreiche Verarbeitung von personenbezogenen Daten über das Verhalten von Beschäftigten, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben oder diese Betroffenen in anderer Weise erheblich beeinträchtigt werden	Einsatz von Data-Loss-Prevention Systemen, die systematische Profile der Mitarbeiter erzeugen Geolokalisierung von Beschäftigten	Zentrale Aufzeichnung der Aktivitäten (z.B. Internetverkehr, Mailverkehr und die Nutzung von Wechselmedien) am Arbeitsplatz mit dem Ziel, von Seiten des Verantwortlichen unerwünschtes Verhalten (z.B. Versand interner Dokumente) zu erkennen. Ein Unternehmen lässt Bewegungsprofile von Beschäftigen erstellen (per RFID, Handy-Ortung oder GPS) zur Sicherung des Personals (Wachpersonal, Feuerwehrleute), zum Schutz von wertvollem Eigentum des Arbeitgebers oder eines Dritten (LKW mit Ladung, Geldtransport) oder zur Koordination von Arbeitseinsätzen im Außendienst.
9	Erstellung umfassender Profile über die Interessen, das Netz persönlicher Beziehungen oder die Persönlichkeit der Betroffenen	Betrieb von Dating- und Kontaktportalen Betrieb von großen Sozialen Netzwerken	Ein Webportal erstellt Profile der Nutzer um möglichst passende Kontaktvorschläge zu generieren.
10	Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Verarbeitung der so zusammengeführten Daten, sofern • die Zusammenführung oder Verarbeitung in großem Umfang vorgenommen werden, • für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den betroffenen Personen erhoben wurden, • die Anwendung von Algorithmen einschließen, die für die betroffenen Personen nicht nachvollziehbar sind, und • der Entdeckung vorher unbekannter Zusammenhänge zwischen den Daten für nicht im Vorhinein bestimmte Zwecke dienen	Big-Data-Analyse von Kundendaten, die mit Angaben aus Drittquellen angereichert wurden	Eine Unternehmen mit umfangreichem Stamm an natürlichen Personen als Kunden, analysiert Daten über das Kaufverhalten der Kunden und die Nutzung der eigenen Webangebote einschließlich des eigenen Webshops, verknüpft mit Bonitätsdaten von dritter Seite und Daten aus der Werbeansprache über soziale Medien einschließlich der vom Betreiber des sozialen Medium bereitgestellten Daten über die angesprochenen Mitglieder, um Informationen zu gewinnen, die zur Steigerung des Umsatzes eingesetzt werden können.
11	Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der betroffenen Person	Kundensupport mittels künstlicher Intelligenz	Ein Callcenter wertet automatisiert die Stimmungslage der Anrufer aus. Ein Unternehmen setzt ein System ein, welches mit Kunden durch Konversation interagiert und für deren Beratung personenbezogene Daten durch eine künstliche Intelligenz verarbeitet werden

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist			
Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
12	Nicht bestimmungsgemäße Nutzung von Sensoren eines Mobilfunkgeräts im Besitz der betroffenen Personen oder von Funksignalen, die von solchen Geräten versandt werden, zur Bestimmung des Aufenthaltsorts oder der Bewegung von Personen über einen substantiellen Zeitraum	Offline-Tracking von Kundenbewegungen in Warenhäusern, Einkaufszentren o. ä. Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes	Ein Unternehmen verarbeitet die WLAN-, Bluetooth- oder Mobilfunksignale von Passanten und Kunden, um die Laufwege und das Einkaufsverhalten nachverfolgen zu können.
13	Automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung der Persönlichkeit der Betroffenen	Telefongespräch-Auswertung mittels Algorithmen	Ein Callcenter wertet automatisiert die Stimmungslage der Anrufer aus.
14	Erstellung umfassender Profile über die Bewegung und das Kaufverhalten von Betroffenen	Erfassung des Kaufverhaltens unterschiedlicher Personenkreise zur Profilbildung und Kundenbindung unter Zuhilfenahme von Preisen, Preisnachlässen und Rabatten.	Ein Unternehmen verwendet Kundenkarten, welche das Einkaufsverhalten der Kunden erfassen. Als Anreiz zur Verwendung der Kundenkarte erhält der Kunde mit jedem Einkauf Treuepunkte. Mithilfe der gewonnenen Daten erstellt der Anbieter umfassende Kundenprofile.
15	Anonymisierung von besonderen personenbezogenen Daten nach Artikel 9 DS-GVO nicht nur in Einzelfällen (in Bezug auf die Zahl der betroffenen Personen und die Angaben je betroffener Person) zum Zweck der Übermittlung an Dritte	Anonymisierung von besonderen Arten personenbezogener Daten nach Artikel 9	Umfangreiche besondere personenbezogene Daten werden durch ein Apothekenrechenzentrum oder eine Versicherung anonymisiert und zu anderen Zwecken selbst verarbeitet oder an Dritte weitergegeben.
16	Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO - auch wenn sie nicht als „umfangreich“ im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist - sofern eine nicht einmalige Datenerhebung mittels der innovativen Nutzung von Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden.	Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten	Ein Arzt nutzt ein Webportal oder setzt eine App an, um mit Patienten mittels Videotelefonie zu kommunizieren und Gesundheitsdaten durch Sensoren beim Patienten (z.B. Blutzucker, Sauerstoffmaske,…) detailliert und systematisch zu erheben und zu verarbeiten.
17	Verarbeitung von Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO - auch wenn sie nicht als „umfangreich“ im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist – sofern die Daten durch die Anbieter neuer Technologien dazu verwendet werden, die Leistungsfähigkeit der Personen zu bestimmen.	Zentrale Speicherung der Messdaten von Sensoren, die in Fitnessarmbändern oder Smartphones verbaut sind	Ein Unternehmen bietet einen Dienst an, mit dem Daten aus Fitnessarmbändern zur Verbesserung des Trainings verarbeitet werden.

Hinweise

1. Diese Liste ist nicht abschließend, sondern ergänzt die in den Absätzen 1 und 3 des Artikels 35 DSGVO enthaltenen allgemeinen Regelungen.

Allgemein gilt, dass für jede Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, die 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, vorab eine Datenschutz-Folgenabschätzung durchgeführt werden muss, insbesondere in den in Absatz 3 genannten Fällen.

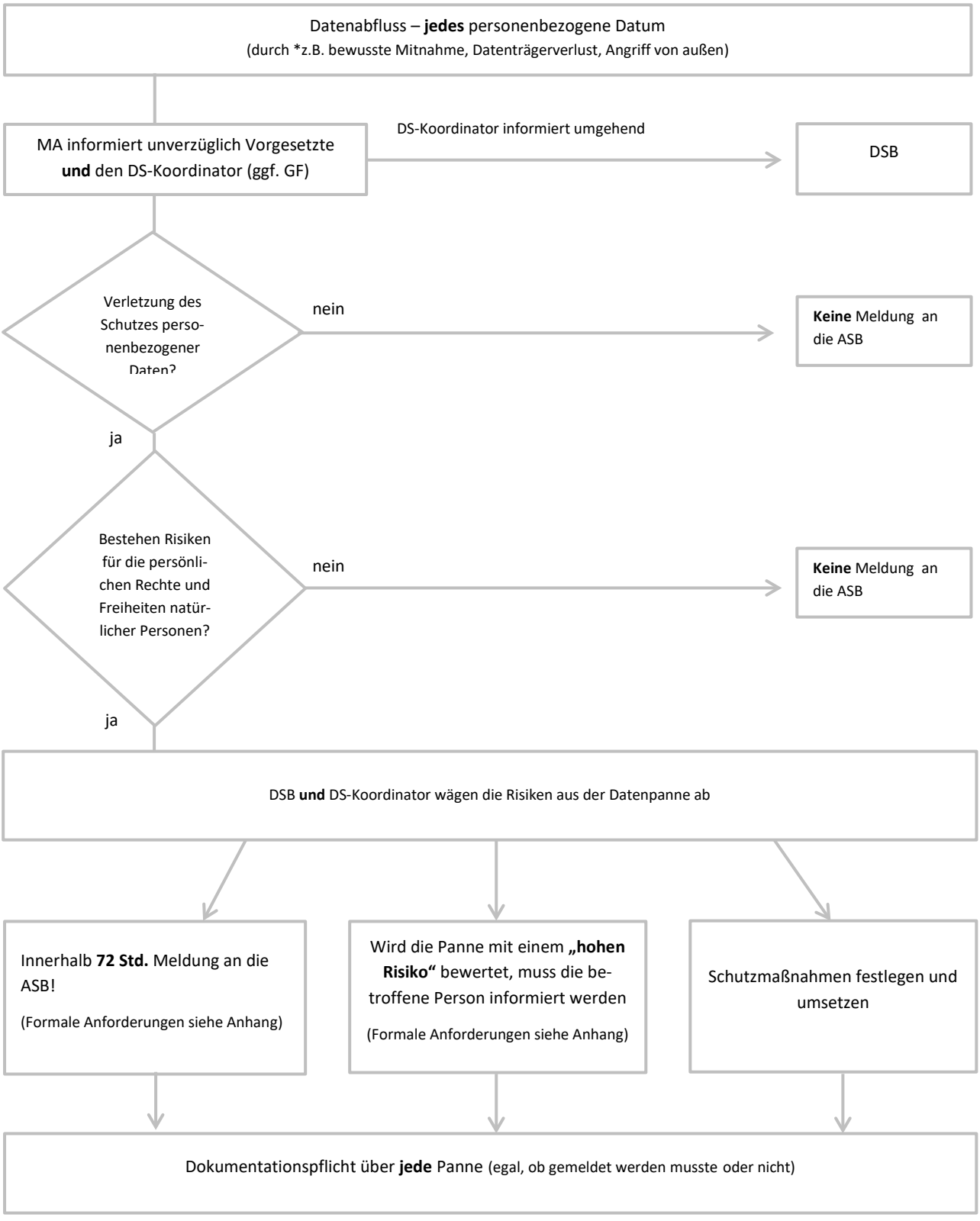
2. Diese Liste orientiert sich an der allgemeinen, im Arbeitspapier 248 Rev. 1 *Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“* beschriebenen Vorgehensweise. Sie ergänzt und konkretisiert diese allgemeine Vorgehensweise.

Der Leitlinie sind folgende neun maßgebliche Kriterien aus WP 248 Rev. 01 zur Einordnung von Verarbeitungsvorgängen zu entnehmen:

a) Vertrauliche oder höchst persönliche Daten
b) Daten zu schutzbedürftigen Betroffenen
c) Datenverarbeitung in großem Umfang
d) Systematische Überwachung
e) Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
f) Bewerten oder Einstufen (Scoring)
g) Abgleichen oder Zusammenführen von Datensätzen
h) Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
i) Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert

Version 1.1 vom 17.10.2018, ersetzt die Liste vom 18.07.2018

Platzhalter Ihr Logo	Datenschutzmanagement-Firmenname Merkblatt SACHVERSTÄNDIGENBÜRO MÜLOT GMBH Datenschutz | Datensicherheit | Forensische Informatik Risikomanagement | ISO27001	Version: 1.0 Status vom: 26.07.2018



*Bsp.: Fax an falsche Nummer; falsches Dokument verschickt; falsches oder anderes Dokument mitverschickt, welches ausversehen mit in die Unterlagen gelangt ist

Formale Anforderungen der Meldung an die ASB gem. Art. 33 DSGVO

- Beschreibung der Art der Verletzung des Schutzes pb Daten, wenn möglich mit Angabe:
  - der Kategorien,
  - ungefähre Zahl der betroffenen Personen,
  - der betroffenen Kategorien,
  - ungefähre Zahl der betroffenen personenbezogenen Datensätze.

- Namen und Kontaktdaten des Datenschutzbeauftragten oder eines Ansprechpartners für weitere Informationen

- Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten

- Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

Formale Anforderungen der Meldung an betroffene Personen gem. Art. 34 DSGVO:

- Meldung in einer angemessenen Frist (keine festen Vorgaben wie bei Meldungen an die Behörde)

- Die Meldung muss enthalten:
  - Eine Beschreibung der Art der Verletzung,
  - Namen und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle,
  - eine Beschreibung der wahrscheinlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

- Die Meldung muss klar und verständlich erfolgen

Checkliste zur Verpflichtung auf Verschwiegenheit

Verpflichtet werden müssen die „unterstellten natürlichen Personen“ des Verantwortlichen. Aufgrund der Bedeutung dieser Regelung ist dieser Personenkreis weit auszulegen und u.a. ehrenamtliche Träger mit einzubeziehen. Die Verpflichtung muss bei der Aufnahme der Tätigkeit erfolgen und sollte spätestens am ersten Arbeitstag vorgenommen werden.

Aus Nachweisgründen sollte die Verpflichtung auf Verschwiegenheit in schriftlicher Form oder elektronischer Form und in einem separaten Dokument erfolgen. Zur Verpflichtung gehört ebenso die Belehrung über die sich hieraus ergebenden Pflichten.

Die Verpflichtungserklärung sollte folgende Informationen enthalten:

- ☐ Verbot, personenbezogene Daten unbefugt zu verarbeiten
- ☐ Erlaubnis, personenbezogene Daten nur dann zu verarbeiten, wenn eine Einwilligung oder gesetzliche Regelung dies erlauben, eine Verarbeitung dieser Daten der Erfüllung oder Durchführung eines Vertrages dient oder die sonst in Art. 6 Abs. 2 EU-DGVO genannten Fälle vorliegen
- ☐ Ggf. individuelle Regelungen, je nach Tätigkeit
- ☐ Die Grundsätze für die Verarbeitung der personenbezogenen Daten nach Art. 5 Abs. 1 EU-DSGVO:
  - ☐ Rechtmäßigkeit
  - ☐ Verarbeitung nach Treu und Glauben
  - ☐ Transparenz
  - ☐ Zweckbindung
  - ☐ Datenminimierung
  - ☐ Richtigkeit
  - ☐ Speicherbegrenzung
  - ☐ Integrität und Vertraulichkeit
- ☐ Regelungen zu Verstößen gegen die Verpflichtung
- ☐ Information, dass die Verpflichtung auch nach Beendigung der Tätigkeit weiter gilt
- ☐ Unterschrift über die Bestätigung der Verpflichtung des Mitarbeiters
- ☐ Unterschrift des Verantwortlichen
- ☐ Aufführung der relevanten Vorschriften
- ☐ Dauer der Verpflichtung

Kurzpapier Nr. 13
Auftragsverarbeitung, Art. 28 DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Begriff des Auftragsverarbeiters

Auftragsverarbeiter ist nach Art. 4 Nr. 8 DS-GVO eine Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Der Begriff des Verantwortlichen und in der Folge die maßgebliche Unterscheidung zwischen Verantwortlichem und Auftragsverarbeiter ist in der DS-GVO nicht vollständig deckungsgleich mit dem Wortlaut des BDSG-alt. Verantwortlicher ist gemäß Art. 4 Nr. 7 DS-GVO die Stelle, die allein oder gemeinsam mit anderen über die Mittel und Zwecke der Verarbeitung personenbezogener Daten entscheidet. Hierbei kommt es maßgeblich auf die Entscheidung über die Verarbeitungszwecke an, während die Entscheidung über die technisch-organisatorischen Fragen der Verarbeitung auch auf den Auftragsverarbeiter delegiert werden kann (vgl. dazu schon WP 169 der Artikel-29-Gruppe, S. 17f. Dieses Arbeitsdokument bezieht sich zwar auf die Rechtslage unter der EU Datenschutzrichtlinie 95/46/EG [DS-RL], die grundsätzlichen Erwägungen zu diesen Fragestellungen sind aber auch für die Auslegung der DS-GVO heranziehbar[1]).

Unter BDSG-alt wurde häufig in Abgrenzung zur Auftrags(daten)verarbeitung die Figur der sog. Funktionsübertragung verwendet. Bei der Funktionsübertragung wurde anstelle einer Auftrags(daten)verarbeitung eine Übermittlung personenbezogener Daten an Dritte im Zuge des Outsourcings solcher „Funktionen"/Aufgaben angenommen, die über eine bloße Datenverarbeitung als solche hinausgehen und bei denen dem Empfänger zumindest gewisse Entscheidungsspielräume zur Aufgabenerfüllung übertragen wurden. Die Figur der Funktionsübertragung ist jedoch in der DS-GVO nicht vorgesehen. Dies ergibt sich aus der Gesamtsystematik, insbesondere aus der speziell geregelten Figur der gemeinsam Verantwortlichen (Art. 26 DS-GVO) sowie aus dem Umstand, dass gewisse Entscheidungsspielräume eines Beauftragten - innerhalb des durch den Verantwortlichen gesteckten Rahmens - bezüglich der Mittel der Verarbeitung hinsichtlich der technisch-organisatorischen Fragen die Auftragsverarbeitung nicht ausschließen (WP 169, S. 17f.).

Fortbestehende Sonderregelung für Verarbeitungen von personenbezogenen Daten im Auftrag

Wie schon bislang besteht auch unter der DS-GVO eine Sonderregelung für Verarbeitungen von personenbezogenen Daten im Auftrag. Allerdings legt die DS-GVO den Auftragsverarbeitern künftig mehr Verantwortung und mehr Pflichten auf.

Nach Art. 29 DS-GVO ist der aufgrund eines Auftrages tätige Dienstleister weisungsgebunden. Er führt daher die Verarbeitung für den Auftraggeber nicht als Dritter i. S. d. Art. 4 Nr. 10 DS-GVO durch. Es besteht vielmehr zwischen dem den Auftrag erteilenden Verantwortlichen und seinem Auftragsverarbeiter ein „Innenverhältnis". Die Verarbeitung durch den Auftragsverarbeiter wird deshalb grundsätzlich dem Verantwortlichen zugerechnet.

[1] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf

Zu beachten ist, dass die Datenverarbeitung im Auftrag auch künftig keine Erlaubnis darstellt, Daten dem Auftragsverarbeiter zu offenbaren, die aufgrund gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, vertraulich zu behandeln sind (vgl. § 1 Abs. 2 S. 3 BDSG-neu).

Mit dem „Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“ wurden jedoch verschiedene Gesetze zu Berufsgeheimnissen novelliert. So dürfen nunmehr u.a. die in § 203 Abs. 1 oder 2 StGB genannten Berufsgeheimnisträger zum Beispiel externen Dienstleistern, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, Geheimnisse unter den Voraussetzungen des § 203 Abs. 3 und 4 StGB offenbaren. Im Gegenzug unterliegt der Auftragsverarbeiter nach § 203 Abs. 4 StGB nunmehr ebenfalls einer auch strafrechtlich sanktionierten Verschwiegenheitspflicht.

Für die Weitergabe von personenbezogenen Daten an den Auftragsverarbeiter und die Verarbeitung durch den Auftragsverarbeiter bedarf es regelmäßig keiner weiteren Rechtsgrundlage im Sinne von Art. 6 bis 10 DS-GVO als derjenigen, auf die der Verantwortliche selbst die Verarbeitung stützt.

Möglich ist nach der DS-GVO auch eine Auftragsverarbeitung durch Dienstleister außerhalb des EU-/EWR-Raums, wenn die zusätzlichen Anforderungen der Art. 44 ff. DS-GVO für Verarbeitungen in Drittstaaten eingehalten werden (angemessenes Schutzniveau im Drittstaat, geeignete Garantien nach Art. 46 DS-GVO wie z.B. Standarddatenschutzklauseln, oder Ausnahmetatbestand nach Art. 49 DS-GVO).

Auftragsverarbeiter sind Empfänger im Sinne von Art. 4 Nr. 9 DS-GVO. Die Eigenschaft als Empfänger führt zu gesonderten Informations- (vgl. u. a. Art. 13 Abs. 1 lit. e DS-GVO) und Mitteilungspflichten (Art. 19 DS-GVO) des Verantwortlichen sowie zu Auskunftsrechten (Art. 15 DS-GVO) der betroffenen Person gegenüber dem Verantwortlichen. Empfänger von Daten müssen im Verzeichnis von Verarbeitungstätigkeiten (vgl. Art. 30 Abs. 1 lit. d DS-GVO) geführt werden.

Regelungen für Auftragsverarbeitung in Art. 28 DS-GVO

Die zentrale Vorschrift für Auftragsverarbeiter in der DS-GVO ist Art. 28, wonach dem Verantwortlichen gemäß Absatz 1 vor Auftragsvergabe zunächst eine Prüfung der Geeignetheit des Auftragsverarbeiters auferlegt wird. Der Verantwortliche darf sich danach nur solcher Auftragsverarbeiter bedienen, die hinreichende Garantien dafür bieten, dass sie geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz anwenden, so dass die Verarbeitung im Einklang mit der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet. Zum Beleg solcher Garantien können auch genehmigte Verhaltensregeln des Auftragsverarbeiters nach Art. 40 DS-GVO oder Zertifizierungen nach Art. 42 DS-GVO als Faktoren herangezogen werden.

Vertrag mit dem Auftragsverarbeiter

Wie nach der bisherigen Rechtslage muss der Verantwortliche mit dem Auftragsverarbeiter einen Vertrag über die weisungsgebundene Tätigkeit schließen, der schriftlich oder in einem elektronischen Format abgefasst sein kann. Hierfür können sowohl individuelle Regelungen getroffen, als auch von der EU-Kommission oder von der zuständigen Aufsichtsbehörde verabschiedete Standardvertragsklauseln verwendet werden. Für den notwendigen Inhalt des Vertrags gilt in großen Teilen das Gleiche wie bisher. Die bestehenden Verträge können daher fortgelten, wenn sie den Anforderungen der DS-GVO entsprechen oder darüber hinausgehen. Beispielsweise muss ein Vertrag zur Auftragsverarbeitung eine Regelung zur Bereitstellung der Daten beinhalten und die Einhaltung der besonderen Bedingungen für den Einsatz von Subunternehmern regeln. Unter anderem muss der Vertrag außerdem

vorsehen, dass der Auftragsverarbeiter die gemäß Art. 32 DS-GVO erforderlichen Maßnahmen ergreift. Da der Verantwortliche für die Rechtmäßigkeit der Verarbeitung insgesamt verantwortlich ist und bleibt (s. Art. 24 DS-GVO), ist weiterhin anzuraten, die mindestens erforderlichen technischen und organisatorischen Maßnahmen darzustellen.

Subunternehmer-Einsatz

Will sich der Auftragsverarbeiter zur Erbringung der vereinbarten Dienstleistung Subunternehmen als weiterer Auftragsverarbeiter bedienen, so bedarf dies der vorherigen (schriftlichen oder elektronischen) Genehmigung durch den Verantwortlichen (Art. 28 Abs. 2 DS-GVO). Später beabsichtigte Änderungen bei den eingesetzten Subunternehmen muss der Auftragsverarbeiter dem Auftraggeber als Verantwortlichem vorher mitteilen, wobei es dem Verantwortlichen vorbehalten bleibt, gegen die geplante Einbeziehung eines Subunternehmens Einspruch zu erheben. Kann nach dem Einspruch keine Einigung zwischen dem Verantwortlichen und dem Auftragsverarbeiter erreicht werden, hat der Verantwortliche die Unterbeauftragung per Weisung zu unterbinden oder die Auftragsverarbeitung zu beenden.

Der Vertrag zwischen dem Auftragsverarbeiter und dem Subunternehmer muss die gleichen vertraglichen Verpflichtungen enthalten, die der Auftragnehmer zugunsten des Auftraggebers übernommen hat.

Neue Verantwortlichkeiten und Pflichten für Auftragsverarbeiter sind insbesondere:

Die Gesamtverantwortung für die Datenverarbeitung und Nachweispflicht des Verantwortlichen nach Art. 5 Abs. 2 DS-GVO umfasst auch die Verarbeitung durch den Auftragsverarbeiter. Hiervon kann sich der Verantwortliche nicht durch die Beauftragung eines Auftragsverarbeiters befreien.

Verstößt ein Auftragsverarbeiter gegen die Pflicht zur weisungsgebundenen Verarbeitung, indem er die Daten des Auftraggebers verordnungswidrig für eigene Zwecke oder Zwecke Dritter verarbeitet, gilt er nach Art. 28 Abs. 10 DS-GVO insoweit selbst als Verantwortlicher – mit allen rechtlichen Folgen, z. B. auch der Pflicht zur Erfüllung der Betroffenenrechte. Neu hinzugekommen sind in Art. 82 DS-GVO auch spezielle Haftungsregelungen für Auftragsverarbeiter bei Datenschutzverletzungen. Demnach drohen nun Auftragsverarbeitern bei Verstößen gegen die in der DS-GVO speziell den Auftragsverarbeitern auferlegten Pflichten Schadensersatzforderungen von betroffenen Personen.

Des Weiteren besteht für Auftragsverarbeiter die neue Pflicht, künftig auch ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO für alle Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung zu führen. Das Verzeichnis muss der Aufsichtsbehörde auf Anfrage nach Art. 30 Abs. 4 DS-GVO, z. B. bei Kontrollen, zur Verfügung gestellt werden.

Nach Art. 33 Abs. 2 DS-GVO muss ein Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten nach Bekanntwerden unverzüglich dem Verantwortlichen melden.

Wartung und Fernzugriffe

Ist Gegenstand des Vertrages zwischen Verantwortlichem und Auftragsverarbeiter die IT-Wartung oder Fernwartung (z. B. Fehleranalysen, Support-Arbeiten in Systemen des Auftraggebers) und besteht in diesem Rahmen für den Auftragsverarbeiter die Notwendigkeit oder Möglichkeit des Zugriffs auf personenbezogene Daten, so handelt es sich im Hinblick auf die weite Definition einer Verarbeitung in Art. 4 Nr. 2 DS-GVO (z. B. Auslesen, Abfragen, Verwenden) ebenfalls um eine Form oder Teiltätigkeit einer Auftragsverarbeitung und die Anforderungen des Art. 28 DS-GVO – wie etwa der Abschluss eines Vertrages zur Auftragsverarbeitung – sind umzusetzen. Anders ist dies bei einer rein technischen Wartung der Infrastruktur einer IT durch Dienstleister (z. B. Arbeiten an Stromzufuhr, Kühlung, Hei-

zung), die nicht zu einer Qualifikation des Dienstleisters als Auftragsverarbeiter und einer Anwendung von Art. 28 DS-GVO führen.

Folgen bei Verstößen

Ebenso sind die umfassenden Vorschriften über Geldbußen in Art. 83 Abs. 4, 5 und 6 DS-GVO zu berücksichtigen (bei Verstößen gegen die Vorgaben des Art. 28 DS-GVO können Geldbußen von bis zu 10.000.000,- Euro oder bis zu 2% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres eines Unternehmens verhängt werden). Diese Sanktionen können bei Verstößen nicht nur den Verantwortlichen selbst, sondern auch den Auftragsverarbeiter treffen, z. B. bei Verstößen des Auftragsverarbeiters gegen seine Verpflichtungen aus Art. 28 Abs. 2 bis 4 DS-GVO.

Anhang:

Anhang A

Auftragsverarbeitung können regelmäßig z. B. folgende Dienstleistungen sein:

- DV-technische Arbeiten für die Lohn- und Gehaltsabrechnung oder die Finanzbuchhaltung durch Rechenzentren,
- Outsourcing personenbezogener Datenverarbeitung im Rahmen von Cloud-Computing, ohne dass ein inhaltlicher Datenzugriff des Cloud-Betreibers erforderlich ist,
- Werbeadressenverarbeitung in einem Lettershop,
- Verarbeitung von Kundendaten durch ein Callcenter ohne wesentliche eigene Entscheidungsspielräume dort,
- Auslagerung der E-Mail-Verwaltung oder von sonstigen Datendiensten zu Webseiten (z. B. Betreuung von Kontaktformularen oder Nutzeranfragen),
- Datenerfassung, Datenkonvertierung oder Einscannen von Dokumenten,
- Auslagerung der Backup-Sicherheitsspeicherung und anderer Archivierungen,
- Datenträgerentsorgung durch Dienstleister,
- Prüfung oder Wartung (z. B. Fernwartung, externer Support) automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.
- Zentralisierung bestimmter „Shared Services-Dienstleistungen“ innerhalb eines Konzerns, wie Dienstreisen-Planungen oder Reisekostenabrechnungen (jedenfalls sofern kein Fall gemeinsamer Verantwortlichkeit nach Art. 26 DS-GVO vorliegt)

Anhang B

Keine Auftragsverarbeitung, sondern die Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen, für die bei der Verarbeitung (einschließlich Übermittlung) personenbezogener Daten eine Rechtsgrundlage gemäß Art. 6 DS-GVO gegeben sein muss, sind beispielsweise in der Regel die Einbeziehung eines

- Berufsgeheimnisträgers (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer),
- Inkassobüros mit Forderungsübertragung,
- Bankinstituts für den Geldtransfer,
- Postdienstes für den Brieftransport,

und vieles mehr.

Anhang C

Keine Auftragsverarbeitung liegt ferner vor, wenn gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO gegeben ist, d.h. wenn mehrere Verantwortliche gemeinsam über die Verarbeitungszwecke und -mittel entscheiden. Hierunter können je nach Gestaltung eine Reihe von Verarbeitungen fallen, die bisweilen unter BDSG-alt als sog. Funktionsübertragung eingestuft wurden, etwa

- klinische Arzneimittelstudien, wenn mehrere Mitwirkende (z. B. Sponsor, Studienzentren/

Ärzte) jeweils in Teilbereichen Entscheidungen über die Verarbeitung treffen,

- gemeinsame Verwaltung bestimmter Datenkategorien (z.B. „Stammdaten“) für bestimmte gleichlaufende Geschäftszwecke mehrerer Konzernunternehmen.

Gemäß Art. 13 Abs. 1 EU-DSGVO muss dem Interessenten zum Zeitpunkt der Erhebung über die Erhebung der personenbezogenen folgendes mitgeteilt werden:

- den Namen und die Kontaktdaten des Verantwortlichen für Datenerhebung (Vereinsvertreter nach BGB §26 und Kontaktdaten) sowie ggf. seines Vertreters
- Kontaktdaten des Datenschutzbeauftragten (wenn vorhanden; aufgrund der medizinischen Daten muss ggf. ein DSB berufen werden)
- der Zweck für die die personenbezogenen Daten verarbeitet werden sollen (z.B. Verfolgung des Vereinszwecks, Erfüllung von Vereinbarung zur Durchführung von Rehabilitationssport, Meldung an Versicherung und/oder Verbände)
- die Rechtsgrundlage der Verarbeitung (nach EU-DSGVO)
- Empfänger bzw. Kategorien von Empfängern der personenbezogenen Daten (z.B. Übungsleitung, Abrechnungszentrum nach § 302 SGB IV, Rehabilitationsträger)
- ggf. Absicht zur internationalen Übermittlung (z.B. Mitgliederverwaltung in der Cloud)

Gemäß Art. 13 Abs. 2 EU-DSGVO muss dem Interessenten außerdem die Möglichkeit zur Information über folgendes ermöglicht werden (z.B. über Verweis auf Internetseite, Informationsblatt)

- die Dauer bzw. die Kriterien für die Festlegung der Dauer der Speicherung der personenbezogenen Daten (z.B. bis Abschluss der Abrechnung einer ärztlichen Verordnung, gesetzliche Fristen zur Aufbewahrung von Rechnungsbelegen)
- das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit
- wenn die Grundlage der Verarbeitung auf der Einwilligung der Person 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, in der Regel bei dem Landesdatenschutzbeauftragten (siehe Anlage 1)
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte (z.B. ohne personenbezogene Daten ist die Durchführung des ärztlich verordneten Rehabilitationssports nicht möglich)
- wenn eine automatisierte Entscheidungsfindung besteht

Checkliste zur Erstellung einer Einwilligungserklärung über die Datenverarbeitung

Eine Einwilligungserklärung ist grundsätzlich immer erforderlich, sofern es für die beabsichtigte Datenverarbeitung keine gesetzliche Grundlage gibt. Folgende Anforderungen werden grundsätzlich an eine Einwilligungserklärung über die Datenverarbeitung gestellt:

- ☐ Nachweispflicht des Verantwortlichen (Schriftform wird empfohlen ist jedoch nicht zwingend notwendig)
- ☐ ausführliche und schriftliche Information der betroffenen Personen über Art, Umfang und Zweck der Erhebung, Verarbeitung und Speicherung der Daten
- ☐ deutlicher Hinweis, ob Daten an Dritte und an wen diese übermittelt werden
- ☐ verständliche, leicht zugängliche Form sowie klare und einfache Sprache
- ☐ Klare Abgrenzbarkeit von anderen Sachverhalten der schriftlichen Erklärung
- ☐ Einwilligung muss aktiv erfolgen (z.B. keine vorausgefüllten Kästchen)
- ☐ die betroffene Person muss mindestens 16 Jahre alt sein (Für Kinder/Jugendliche müssen bis zum vollendeten 16. Lebensjahr die Eltern/gesetzlichen Vertreter einwilligen)
- ☐ Hinweis auf die Möglichkeit zum Widerruf der Einwilligung für die Zukunft
- ☐ Gewährleistung der Freiwilligkeit der Einwilligungserklärung (die betroffene Person muss in der Lage sein, die Einwilligung verweigern oder zurückziehen zu können, ohne Nachteile zu erleiden)

Im Rahmen der Informationspflicht nach Art. 13 EU-DSGVO ist darauf zu achten, dass der betroffenen Person darüber hinaus noch folgende Informationen mitgeteilt werden, wenn personenbezogene Daten erhoben werden:

- ☐ Name und die Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
- ☐ ggf. die Kontaktdaten des Datenschutzbeauftragten
- ☐ ggf. die Absicht, die Daten in ein Drittland oder an eine internationale Organisation zu übermitteln (vgl. Art. 13 Abs. 1 f)
- ☐ die Dauer, für die die personenbezogenen Daten gespeichert werden sollen
- ☐ Bestehen des Rechts der betroffenen Person auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, das Recht auf Datenübertragbarkeit, Widerspruch und Widerruf der Einwilligung für die Zukunft und das Recht, nicht einer automatisierten Einzelentscheidung unterworfen zu werden
- ☐ Bestehen eines Beschwerderechts bei einer 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 mögliche Folgen die Nichtbereitstellung hätte
- ☐ Bestehen einer automatisierten Entscheidungsfindung (vgl. Art. 22 Abs. 1 u. 4 EU-DSGVO)

Liste der bekannten Abrechnungszentren, die nach § 302 SGB V verfahren

Von folgenden Abrechnungszentren liegt dem DBS eine schriftliche Bestätigung vor, dass das Abrechnungsverfahren nach § 302 SGB V erfolgt. Eine Einwilligungserklärung der Rehasportler über die Übermittlung der Daten an diese Abrechnungszentren ist grundsätzlich nicht notwendig. Die Liste wird fortlaufend aktualisiert.

- ADH – Abrechnungszentrum für Heilmittelerbringer
- ARNI – Abrechnungsstelle Niedersachsen
- AS Bremen AG
- AZH
- DMRZ
- Herbst EDV Beratung GmbH
- Opta data
- Optica Abrechnungszentrum
- PVS Mosel-Saar
- PVS Sachsen
- RZH
- Schweriner Rechenzentrum
- Severins GmbH
- Styra + Partner