Handreichung zur Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten, vereinfachtes Modell

1. Vorbemerkungen

Personenbezogene Daten sind ein schützenswertes Gut. Ihre Verwendung unterliegt den Grundsätzen der Transparenz, der Rechtmäßigkeit, der Zweckbindung, der Verhältnismäßigkeit, der Richtigkeit und der Vertraulichkeit. Die EU- Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), kurz „DSGVO", präzisiert diese Grundsätze (Art. 5 der DSGVO) und erinnert an die Rechte, die jeder in Bezug auf seine Daten hat: insbesondere das Recht auf Auskunft, das Recht auf Berichtigung, das Recht auf Löschung, das Recht auf Einschränkung und das Recht auf Widerspruch in der Verarbeitung seiner personenbezogenen Daten (Art. 12 – 21 der DSGVO).

Neben diesen Grundprinzipien gibt die DSGVO einige Verfahren und Instrumente vor, zu denen das Verzeichnis der Verarbeitungstätigkeiten gehört (Art. 30 der DSGVO).

1.1. Was sind „personenbezogene Daten"?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (Art. 4 der DSGVO). Hierzu zählen beispielsweise Name, Adresse, Nationalregister-Nr., E-Mail-Adresse, IP-Adresse, Auto-Kennzeichen, Bilder,...

Als besonders schützenswert gelten „sensible Daten". Hierzu gehören u.a. Angaben zur ethnischen bzw. rassischen Herkunft einer Person, zur sexuellen Orientierung, zur Religionszugehörigkeit oder sonstigen ideologischen Überzeugung, Gesundheitsdaten, zu strafrechtlichen Verurteilungen und Straftaten, zur Gewerkschaftszugehörigkeit, biometrische und genetische Daten (Art. 9 und Art. 10 der DSGVO).

1.2. Was ist eine „Verarbeitung"?

Eine Verarbeitung im Sinne der DSGVO ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche 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, Verbreitung oder eine andere Form

der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (Art. 4 der DSGVO). Die Form, in der diese Daten zur Verfügung stehen, spielt dabei keine Rolle. Dies können also beispielsweise Exceltabellen, komplexe Datenbanken, aber auch Karteikarten, Ordner mit Einschreibeformularen, Fotosammlungen, … sein.

1.3. Wer muss ein solches Verzeichnis führen?

Grundsätzlich ist festzuhalten, dass ein solches Verzeichnis ein geeignetes Instrument ist, um eine Übersicht über die personenbezogenen Daten zu erhalten, die effektiv in der Einrichtung oder im Verein verwendet werden. Es dient der Datenpflege und damit der Qualitätssteigerung und es hilft, bei Anfragen um Auskunft zeitnah eine Antwort zu liefern und gegebenenfalls eine Berichtigung oder Löschung der Daten vorzunehmen.

Einrichtungen und Vereine, die (1) weniger als 250 Mitarbeiter beschäftigen und (2) deren Datenverarbeitung mit Sicherheit keinerlei Risiko für die Rechte und Freiheiten der betroffenen Personen birgt und (3) die sehr selten personenbezogene Daten und keinesfalls sensible Daten verarbeiten, müssen dieses Verzeichnis der Verarbeitungen jedoch nicht führen (vgl. Art. 30 der DSGVO). Für alle anderen Einrichtungen und Vereine ist es eine Pflicht.

Dieses Verzeichnis beinhaltet selber keine personenbezogene Daten, sondern nur die Beschreibungen, also Typenbeschreibung der Daten.

1.4. Was geschieht mit dem Verzeichnis?

Das Verzeichnis mit den Beschreibungen der einzelnen Verarbeitungen bleibt am Sitz der Einrichtung oder des Vereins. Die Datenschutzbehörde (https://www.autoriteprotectiondonnees.be/) kann im Rahmen ihrer Funktion als Aufsichtsbehörde entweder vor Ort Einsicht in dieses Verzeichnis verlangen oder sich dieses zusenden lassen.

2. Das vereinfachte Modell eines Verzeichnisses von Verarbeitungstätigkeiten

Bitte beachten Sie, dass dieses vereinfachte Modell lediglich eine Arbeitshilfe für Ihre Vereinigung darstellt. Es ersetzt nicht die eigene Prüfung der Umsetzung der DSGVO in der Einrichtung oder im Verein. Das Modell hilft Ihnen aber, alle wichtigen Aspekte bei Ihrer eigenen Prüfung zu berücksichtigen.

Dieses Modell des Verzeichnisses besteht aus zwei Teilen:

- Ein Deckblatt, das alle Angaben des Verantwortlichen, dessen Vertreter sowie gegebenenfalls des Datenschutzbeauftragten beinhaltet, sowie die Übersicht der einzelnen Verarbeitungen.
- Pro Verarbeitung eine präzise Beschreibung.

Das Dokument wurde so gestaltet, dass es mit jeder Textverarbeitung verwendet werden kann. Bitte überschreiben Sie die gepunkteten Linien einfach mit Ihren Angaben.

2.1. Angaben zum Verantwortlichen

Als verantwortlich für die Verarbeitung gilt die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 der DSGVO). Dies kann bei Vereinen z.B. der Vorstand sein.

2.2. Angaben zum Vertreter des Verantwortlichen

Dies ist die Person, die formell die Einrichtung oder den Verein vertreten kann. Dies sind beispielsweise der Geschäftsführer oder der/die Präsidenten/in.

2.3. Angaben zum Datenschutzbeauftragten

Ein eigener oder ein geteilter Datenschutzbeauftragter ist erforderlich, wenn die Einrichtung oder der Verein eine Behörde oder öffentlichen Stelle ist, oder die Datenverarbeitung eine umfangreiche regelmäßige und systematische Kontrolle von betroffenen Personen erforderlich macht oder wenn sensible Daten regelmäßig verarbeitet werden (Art. 37 der DSGVO). Trifft eine dieser Bedingungen zu, muss ein Datenschutzbeauftragter bezeichnet werden. In allen anderen Fällen kann man auch einen Datenschutzbeauftragten bezeichnen. Diese Bezeichnung ist insbesondere in der Öffentlichkeitsarbeit von Vereinigungen stets ein Vorteil.

Die Kontaktdaten des Datenschutzbeauftragten werden der Datenschutzbehörde mitgeteilt. Da der Datenschutzbeauftragte der erste Ansprechpartner bei Nachfragen zum Datenschutz ist - sei es für Mitglieder, Kunden, Mitarbeiter, den Vorstand, ... - werden seine Kontaktdaten z.B. in der Vereinszeitschrift, im Newsletter, auf der Webseite usw. bekannt gemacht.

2.4. Die Liste der Verarbeitungen

Alle Verarbeitungen werden hier durchnummeriert und aufgelistet. Einige Beispiele: Verzeichnis der Kunden, Verzeichnis der Lieferanten, Personalregister, Lohn- oder Honorarabrechnung, Mitgliederverwaltung, Beitragsverwaltung, Verzeichnis der Förderer oder Sponsoren, Abonnentenverwaltung des Newsletters „XYZ“, Fotosammlung der Vereinsaktivitäten, ... Die Umschreibung soll auch für Außenstehende nachvollziehbar sein. Sie sollte nicht zu vage bleiben. Führt man z.B. mehrere Kundenlisten, dann sollte schon durch den Titel nachvollziehbar sein, um welche Liste es sich handelt. Nur intern bekannte Abkürzungen sind zu vermeiden.

Pro aufgelistete Verarbeitung ist jeweils eine gesonderte Beschreibung zu führen.

2.5. Benennung der Verarbeitung

Hier werden jeweils die laufende Nummer und die Bezeichnung vom Deckblatt übernommen. [Den Text in Klammern überschreiben].

Datum der Beschreibung: Das Datum, an dem zum ersten Mal die Verarbeitung beschrieben wurde.

Datum der letzten Anpassung: Sobald die Verarbeitung in irgendeiner Form angepasst oder erweitert wird, aktualisiert man dies in der Beschreibung. Damit man diese Aktualisierungen verfolgen kann, wird hier das Datum der letzten Anpassung festgehalten. Die vorherigen Beschreibungen werden archiviert, damit man alle Änderungen nachvollziehen kann.

Ansprechpartner für die konkrete Verarbeitung ist die Person, die regelmäßig mit diesen Daten arbeitet. Das kann z.B. der Kassierer für die Beitragsverwaltung sein, der Schriftführer für die Mitgliederverwaltung, Mitarbeiter der Geschäftsführung für das Personalregister, …

Eingesetzte Verfahren: beschreibt die physische Form, wie die Daten verwaltet werden. Dies kann eine bestimmte Standardsoftware sein, wie z.B. MS Excel, LibreOffice Writer, eine speziell entwickelte Software, aber auch sonstige Formate, wie Ordner mit Einschreibeformulare, Karteikasten, … Man sollte auch die Fachbereich oder die Person angeben, wo die Daten zu finden sind, falls es nicht der o.g. Ansprechpartner ist.

2.6. Zweckbestimmung der Verarbeitung

Hier wird angegeben, zu welchem Zweck die Verarbeitung angelegt wurde. Die Beschreibung sollte ausführlich und auch für Externe nachvollziehbar sein. Beispiele können sein: Auszahlung der Gehälter, Verwaltung der Vereinstätigkeiten (Einladungen, Mitteilungen, Organisation von Aktivitäten), Vereinsfinanzierung, Organisation von Weiterbildungen, Verwaltung von Sportergebnissen, …

Außerdem kann man hier die Rechtmäßigkeit angeben, mit der die Datenverarbeitung geschieht.

Für kleinere Einrichtungen und Vereine kommen im Wesentlichen drei Varianten in Frage:

- Erfüllung gesetzlicher Auflagen (z.B. Führung eines Mitgliederregisters, um Artikel 10 des Gesetzes vom 27. Juni 1921 über die Vereinigungen ohne Gewinnerzielungsabsicht zu entsprechen; Führung einer Teilnehmerliste aufgrund Art. XX des Dekretes vom xx.xx.xxxx zur Bezuschussung von Vereinen; Sozial- und Steuergesetze, …).
- Erfüllung eines Vertrags / einer Vereinbarung (z.B. Führung einer Personalliste für die Arbeitsunfallversicherung, Organisation eines öffentlichen Turniers,…). Zur Information: die Mitgliedschaft in einem Verein kann als Vertrag zwischen dem Mitglied und dem Verein betrachtet werden. Der Vorstand kann in diesem Zusammenhang die Daten für Aktivitäten verwenden, die vereinstypisch sind und von denen das Mitglied ausgehen kann (Organisation von Training oder Proben, Organisation von Auftritten oder Sportwettbewerbe,…).
- Für die Verarbeitung liegt eine Einverständniserklärung aller betroffenen Personen vor. Diese muss explizit und dokumentiert sein. Ein automatisches Einverständnis kann nicht vorausgesetzt werden. Ein einmal gegebenes Einverständnis kann jederzeit zurückgezogen werden.

2.7. Beschreibung der Kategorien betroffener Personen

Einige Beispiele: Mitglieder des Vereins, Besucher des Webportals, Beschäftigte der Einrichtung, Kursteilnehmer, ehemalige Mitglieder des Vereins, Ansprechpartner der Lieferanten,…

Auch hier sollte die Beschreibung so ausführlich sein.

2.8. Beschreibung der Kategorien personenbezogener Daten

Wie bereits angemerkt, werden keine individuelle personenbezogene Daten im Verzeichnis selber eingetragen, sondern nur die Art der Daten.

Es wird nach folgenden Rubriken unterschieden:

- **Primäre Identifikationsdaten**: Name, Vorname, Adresse, Geburtsdatum, Geburtsort, …
- **Personenbezogene Merkmale**: Gewichtsklasse, Körpergröße, …
- **Daten zu Privatleben und Freizeit**: Zivilstand, Hobbys, Eintritts- und eventuelles Austrittsdatum, Sportart, Musikinstrument, Stimmlage, …
- **Daten zur Ausbildung, Beruf und Arbeit**: Diplome, sonstige absolvierte Ausbildungen, Trainerzertifikaten, Sprachkenntnisse, Berufserfahrungen, aktuell ausgeübte Funktion, Statut, …
- **Wirtschaftliche und finanzielle Daten**: Bankverbindungen, wirtschaftliche Situation, Einkommen, …
- **Verbindungsdaten**: Festnetz- und Mobiltelefon-Nr., private und berufliche E-Mail-Adresse, IP-Adressen, Logdatei, Lokalisierungsdaten,…

2.9. Werden sensible Daten verarbeitet?

Zur Definition von sensiblen Daten, siehe Punkt 1.1, Seite 1.

Sensible Daten sind beispielsweise: Gesundheitsdaten der Sportler (z.B. Sportunfälle, Allergien, körperliche Einschränkungen), Gesundheitsdaten der Mitarbeiter, Leumundszeugnis der Mitarbeiter, Religionszugehörigkeit, Nationalregister-Nr., ethnische Herkunft, …

2.10. Sonstige personenbezogene Daten

Hier kann man weitere Datenkategorien angeben, die nicht den vorherigen Rubriken zugeordnet werden konnten.

2.11. Aufbewahrungsdauer und Löschung der Daten

Mögliche Varianten sind beispielsweise:

- gesetzliche Aufbewahrungsfrist von „x“ Jahren;
- Verbandsvorschrift von „y“ Jahre nach Beendigung der Mitgliedschaft;
- Vertragsvereinbarung mit dem Provider zur Löschung der IP-Adresse nach „z“ Tagen, …

Sollten Unterschiede in der Aufbewahrungsdauer verschiedener o.g. Datenkategorien bestehen, kann man dies hier differenzieren.

Falls es Vorgaben und Verfahren zur Löschung der Daten gibt, sollten diese angegeben werden: wie veranlasst wer die Löschung von Daten und wer führt sie durch? Werden Papierunterlagen z.B. im Shredder vernichtet? …

2.12. Datenweitergabe und deren Empfänger

Es wird unterschieden zwischen der internen Weitergabe innerhalb der Einrichtung/ des Vereins und externen Empfänger.

Beispiele für die interne Weitergabe: Weitergabe der Personaldaten vom Personaldienst an den Finanzdienst zwecks Auszahlung der Gehälter, Weitergabe der Liste der eingeschriebenen Mitglieder vom Schriftführer an den Kassierer zwecks Überprüfung der Mitgliedsbeiträge, …

Beispiele für die externe Weitergabe: Übermittlung der Mitgliederliste an die Gemeindeverwaltung zwecks Erhalt eines Vereinszuschusses, Übermittlung der Mitgliederliste nach Einwilligung an einen nationalen Dachverband, Übermittlung der Angaben der Beschäftigten in einer Arbeitsbeschaffungsmaßnahme an das Ministerium zwecks Erhalt der Lohnbeihilfe, … In diesen Fällen ist es hilfreich, die gesetzlichen Bestimmungen oder die Vertragssituation zu erwähnen, aus der sich die Verpflichtung der Datenweitergabe ergibt.

Sollte die Datenweitergabe an einen Dienstleister, wie z.B. an ein Sozialsekretariat, eine Versicherung, einen IT-Dienstleister, … gehen, ist dies an dieser Stelle zu dokumentieren. Die DSGVO sieht in Artikel 28 vor, dass in diesem Fall eine Vereinbarung mit dem „Auftragsverarbeiter“ abgeschlossen wird, in der dieser sich dazu verpflichtet, seinerseits die Datenschutzbestimmungen einzuhalten und anzugeben, wer der Ansprechpartner in seiner Einrichtung für Datenschutzfragen ist.

2.13. Datenübermittlung in Drittstaaten außerhalb der EU oder an internationale Organisationen

Falls personenbezogene Daten an Einrichtungen außerhalb der EU oder an internationale Organisationen (wie UNO, WHO, Internationales Rotes Kreuz, Greenpeace, Amnesty International,…) übermittelt werden, ist dies gesondert zu vermerken.
Außerdem sind in diesem Fall zusätzliche Garantien einzufordern, die in Art. 47 der DSGVO beschrieben werden.

2.14. Technische und organisatorische Sicherheitsmaßnahmen

Je nach Umfang und Sensibilität der personenbezogenen Daten, die in einer Einrichtung oder Verein verarbeitet werden, müssen organisatorische und technische Maßnahmen ergriffen werden, damit diese Daten sicher sind, d.h. nicht von unberechtigten Personen

eingesehen, manipuliert oder gelöscht werden können und zudem immer verfügbar bleiben.
Hier wird unterschieden zwischen folgenden Maßnahmen:

- **Zugangskontrollen und Protokollierung:** z.B. Passwort geschützte PC-Arbeitsplätze; Server in abschließbarem Raum, zu dem nur der IT-Administrator Zugang hat; Papierunterlagen in einem abgeschlossenen Schrank, zu dem beispielsweise nur der Präsident und Schriftführer Zugang haben; Protokollierung der Benutzerzugriffe mit User-ID und Uhrzeit in Logfiles; …
- **Softwaresicherheit**: z.B. Einrichtung einer Firewall, Installation eines Virenscanners, regelmäßige (automatische) Aktualisierung der Virensignaturen, automatische Updates des Betriebssystems, Aktualisierung des Internetbrowsers und der Softwareanwendungen, …
- **Sicherung der Daten**: z.B. regelmäßige, zeitnahe Backups, Sicherung der Daten auf externe Datenträger, ausgelagerte Sicherungskopien, Verschlüsselung der Daten, Belastungstests der IT-Infrastruktur, …
- **Sonstige Maßnahmen**: z.B. für Mitarbeiter oder Vorstandsmitglieder: Sensibilisierung und regelmäßige Schulung zu Datenschutz-Themen, Papieraktenvernichtung durch einen Shredder, Einführung einer Sicherheitspolitik für die Einrichtung, Einführung einer IKT-Benutzercharta; Bezeichnung eines Datenschutzbeauftragten mit Publikation der Kontaktdaten; Aktualisierung der Datenschutzerklärung auf der Webseite, …

Noch ein Tipp für Vereine zum Schluss:

Im Interesse des Vereins und im Sinne des „privacy by design“ ist anzuraten, dass bereits beim Antrag auf Mitgliedschaft das zukünftige Mitglied über die Gewährleistung des Datenschutzes informiert wird. Ein Antragsformular auf Mitgliedschaft sollte neben den Kontaktdaten auch das Einverständnis zur Verarbeitung personenbezogener Daten einholen.
Im Folgenden einige nützliche Textbausteine als Beispiele für Antragsformulare auf Mitgliedschaft:

- *Wir weisen gemäß Datenschutz-Grundverordnung vom 27. April 2016 darauf hin, dass zum Zweck der Mitgliederverwaltung und -betreuung folgende Daten verarbeitet werden: Namen, Adressen, Telefonnummern, E-Mailadresse, … [zu ergänzen]*
- ☐ *Ich bin mit der Erhebung, Verarbeitung und Nutzung folgender personenbezogener Daten durch den Verein zur Mitgliederverwaltung einverstanden: Name, Anschrift,*

Geburtsdatum, Telefonnummer, E-Mail-Adresse, Übungsleiterlizenz … [zu ergänzen]. Mir ist bekannt, dass dem Aufnahmeantrag ohne dieses Einverständnis nicht stattgegeben werden kann.

- ☐ *Unser Verein ist verpflichtet, folgende Daten an den Dachverband XY sowie an die uns bezuschussenden Institutionen XY zu übermitteln: Name, Geburtsdatum, Eintrittsdatum … [zu ergänzen]. Mit dieser Übermittlung im Rahmen des Vereinszwecks bin ich einverstanden.*
- ☐ *Ich bin damit einverstanden, dass zum Vereinszweck personenbezogene Daten und Fotos von mir in der Vereinszeitung und auf der Homepage des Vereins veröffentlicht und diese ggf. an Print und andere Medien übermittelt werden. Dieses Einverständnis betrifft insbesondere folgende Veröffentlichungen: Ergebnislisten, Mannschaftslisten, Berichte über Ehrungen, Veranstaltungsfotos, …[zu ergänzen]*