Die Datenschutz-Grundverordnung

Praxisratgeber für Vereine

Inhalt

Vorwort

Die Datenschutz-Grundverordnung[1] (nachfolgend: die „DSGVO“) gilt seit dem 25. Mai 2018 in allen Mitgliedstaaten der europäischen Union. Wenn Sie personenbezogene Daten erheben und verarbeiten und sich in der Union niedergelassen haben, unterliegen Sie der DSGVO, unabhängig von Ihrer Größe, Ihrer Rechtsform, Ihren Aktivitäten oder Ihrem Gesellschaftszweck.

Die DSGVO sieht also den neuen europäischen Rechtsrahmen im Bereich des Datenschutzes vor und ersetzt in Luxemburg das abgeänderte Gesetz vom 2. August 2002 zum Schutz personenbezogener Daten bei der Datenverarbeitung.

Das im genannten Gesetz vom 2. August 2002 vorgesehene System der Vorabgenehmigungen und Vorabmeldungen bei der Nationalen Datenschutzkommission (nachfolgend: die „CNPD“) existiert somit nicht mehr. Alle auf dem luxemburgischen Hoheitsgebiet niedergelassenen Akteure müssen selbst ihre Konformität mit der DSGVO nachweisen können.

Dieser Ratgeber soll gemeinnützigen Vereinen (nachfolgend „Sie“ oder „die Vereine“) einen allgemeinen Überblick im Bereich Datenschutz verschaffen. Er richtet sich hauptsächlich an sogenannte „klassische“ oder „traditionelle“ Vereine, deren Tätigkeiten sich auf die Datenverarbeitungen beschränken, die üblich und notwendig für die Verwaltung eines Vereins sind. Er ist nicht geeignet, um Vereine umfassend zu leiten, deren Aktivitäten Datenverarbeitungen beinhalten (in Bezug auf den Volumen, die Sensibilität, usw.), deren Zwecke über diesen üblichen Rahmen hinausgehen (z.B. gemeinnützige Vereine, die dem Gesetz « ASFT »[2] unterliegen und die im sozialen, familiären und therapeutischen Bereich tätig sind).

[1] 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).

[2] Abgeänderte Gesetz vom 8. September 1998 über die Regelung der Beziehungen zwischen dem Staat und Organisationen aus dem sozialen, familiären und therapeutischen Bereich.

Begriffsbestimmungen

- Der Verantwortliche ist 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; der also bestimmt „warum“ und „wie“ personenbezogene Daten erhoben und verarbeitet werden.

Die einzelnen Einrichtungen, lokalen Gruppierungen, Vorstandsmitglieder, sowie Mitarbeiter eines Vereins sind als ein und derselbe für die Verarbeitung Verantwortliche anzusehen, solange sie in der Ausübung der Missionen des Vereins aktiv sind. Die Mitglieder und Dachverbände sind hingegen prinzipiell in Bezug auf den Verein als Dritte anzusehen.

- Der Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag und auf Anweisung des Verantwortlichen verarbeitet.

- Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Eine Person kann:

- direkt (z.B. durch ihren Namen, Vornamen, ihre Adresse oder eine namentliche E-Mail-Adresse); oder
- indirekt identifiziert werden (z.B. mittels Zuordnung zu einem Benutzernamen (Mitgliedsnummer), zu einer Kennnummer (Telefonnummer), zu biometrischen Daten (Fingerabdrücke) oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck seiner physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind).

Eine Person kann identifiziert werden auf Grund von:

- nur einer einzigen Information (z.B.: der Name, Vorname oder eine namentliche E-Mail-Adresse);
- einer Kombination von mehreren Daten, ohne den Vornamen und Namen der betroffenen Person zu erwähnen (z.B.: ein Sportler, geboren an jenem Datum, der während einem bestimmten Wettkampf an diesem Tag und Ort einen nationalen Rekord über die 100 Meter erzielt hat).

Bei anonymen oder anonymisierten Daten (Informationen, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr vom Verantwortlichen oder einem Dritten identifiziert werden kann) appliziert sich die DSGVO nicht. Das vorherige Beispiel des Sportlers, der einen nationalen Rekord aufgestellt hat, zeigt jedoch, dass das Löschen des Namens, Vornamens und der Adresse nicht ausreichend ist, um einen ganzen Datensatz zu anonymisieren. In diesem Fall ist von pseudonymisierten Daten die Rede, welche in den Anwendungsbereich der DSGVO fallen.

- Eine Verarbeitung von personenbezogenen Daten ist jeder ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, ganz gleich welches Verfahren benutzt wurde. Die DSGVO zählt eine ganze Reihe von verschiedenen Verarbeitungsarten auf, wie zum Beispiel das Erheben, die Speicherung, die Anpassung oder Veränderung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, oder auch das Löschen oder die Vernichtung.

Eine Datenverarbeitung muss nicht automatisiert sein: geordnete Papierakten (z.B: alphabetisch oder chronologisch) sind ebenfalls betroffen und müssen auf die gleiche Art und Weise geschützt werden.

Hinzu kommt, dass die DSGVO nicht für personenbezogene Daten Verstorbener gilt, wie zum Beispiel im Falle einer Veröffentlichung in einer Vereinszeitung eines Nachrufes betreffend ein ehemaliges Mitglied, unter der Bedingung, dass die Würde und das Privatleben der Familienangehörigen des Verstorbenen respektiert werden.

Zusammenfassend finden Sie nachfolgend ein Beispiel, das die verschiedenen Begriffe beinhaltet: Ein Sportsverein, der durch seinen Präsidenten und die anderen Mitglieder des Vorstandes (Entscheidungsorgan) vertreten wird, ist insgesamt als ein und derselbe für die Verarbeitung Verantwortliche anzusehen, in dem er das „warum“ und „wie“ der Datenverarbeitungen entscheidet. Der Verein entschließt sich, eine Excel-Tabelle auszuarbeiten, die eine Liste mit den aktiven und nicht-aktiven Mitgliedern beinhaltet. Diese Liste enthält folgende Informationen: Namen, Vornamen, Postadressen und E-Mail-Adressen. Diese Datei dient zur Verschickung von Newsletter und zur Einberufung der Generalversammlungen. Der Sportsverein hat eine Firma WWW damit beauftragt, eine Internetseite zu erstellen, damit Personen sich informieren und dem Verein beitreten können.

Die erhobenen Daten sind als personenbezogene Daten einzustufen, da die Mitglieder eindeutig identifiziert werden können. Die Daten werden für eindeutige Zwecke erhoben: die administrative Verwaltung der Mitglieder, das Verschicken von Newsletter und die Einberufung der Generalversammlungen. Die einzelnen Vorgänge, wie das Erfassen und Verschicken von Informationen, sind als verschiedene Verarbeitungen anzusehen. Schlussendlich ist die Firma WWW als Auftragsverarbeiter des Sportsvereins zu betrachten, indem sie nur im Auftrag und auf Anweisung des Vereins handelt.

➔ **Siehe Artikel 4 der DSGVO bezüglich der Definitionen der einzelnen Begriffe.**

Errichtung eines Verzeichnisses von Verarbeitungstätigkeiten

Zu den Verpflichtungen des Verantwortlichen zählt als Erstes das Verfassen eines Verzeichnisses von Verarbeitungstätigkeiten. Der erste Schritt besteht also darin, die verschiedenen Verarbeitungstätigkeiten von personenbezogenen Daten zu identifizieren und zu erfassen. Die Ausarbeitung eines Verzeichnisses erlaubt es Ihnen, eine Bestandsaufnahme der Verarbeitungen zu vollziehen. Prinzipiell müssen alle Vereine ein solches Verzeichnis für sich wiederholende Verarbeitungen erstellen (wie zum Beispiel die Aktualisierung der Mitgliedslisten, die Verwaltung der Mitgliedsbeiträge, die Erneuerung der Internetseite, gegebenenfalls die Einschreibung zu Wettkämpfen, usw.). Es ist nicht notwendig, die gelegentlichen Verarbeitungstätigkeiten zu erwähnen.

Identifizieren Sie also jene Aktivitäten, die das Erheben und Verarbeiten von personenbezogenen Daten benötigen und erstellen Sie je nach Zweck eine Liste mit allen Aktivitäten. Generell werden Daten von Vereinen für folgende Zwecke erhoben: administrative Verwaltung der Mitglieder, Verwaltung der Internetseite, Verschicken von Newsletter, Verwaltung der Lieferanten, Verwaltung der Beiträge, Buchführung, Verwaltung der „VIP“ Kontaktlisten um Einladungen zu Veranstaltungen zu verschicken. Sollte ein Verein zusätzlichen Aktivitäten nachgehen, so können Daten für andere Zwecke erfasst werden, wie zum Beispiel die Verwaltung im Personalbereich, die Dopingbekämpfung oder die Verwaltung der sportmedizinischen Betreuung.

Jedes Arbeitsblatt (oder eine Zeile pro Verarbeitung und pro Zweckbestimmung) sollte vor allem Folgendes spezifizieren:

- das verfolgte Ziel (der Zweck der Verarbeitung – siehe die obenstehenden Beispiele);
- die Kategorien betroffener Personen (z.B.: alle Lizenzinhaber);
- die Kategorien personenbezogener Daten (z.B. für die Lizenzinhaber: Name, Vorname, Postadresse, E-Mail-Adresse und Geburtsdatum; aufgepasst: das Verzeichnis soll nur Kategorien von Daten enthalten und auf keinen Fall die Daten selbst);
- die Kategorien von Empfängern (ein Buchhalter, ein Ministerium, der Veranstalter eines Sportturniers, usw.);
- die Aufbewahrungsdauer der Daten (Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; dies muss von Fall zu Fall analysiert werden);
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation.

Ein Muster eines Verzeichnisses mit konkreten Beispielen befindet sich im Anhang. Dieses Muster muss an die Aktivitäten und Zweckbestimmungen der Datenverarbeitungen eines Vereins angepasst werden.

➔ **Siehe Artikel 30 der DSGVO bezüglich des Verzeichnisses von Verarbeitungstätigkeiten.**

Die Rechtmäßigkeit der Datenverarbeitung

Personenbezogene Daten müssen auf Basis von nur einer der sechs in der DSGVO vorgesehenen Rechtsgrundlagen verarbeitet werden: die Einwilligung, die Erfüllung eines Vertrags, eine rechtliche Verpflichtung, die Bewahrung lebenswichtiger Interessen, eine Aufgabe die im öffentlichen Interesse liegt oder das berechtigte Interesse.

➔ **Siehe Artikel 6 der DSGVO bezüglich der Rechtmäßigkeit der Datenverarbeitung.**

Gesetzestexte können in speziellen Bereichen Datenverarbeitungen durch einen Verein vorschreiben, die seine Aktivitäten beeinflussen können (Arbeitsgesetzbuch, das abgeänderte Gesetz vom 21. April 1928 über Vereine und Stiftungen ohne Erwerbszwecke, Vorschriften im Steuer - und Sozialbereich, im Rahmen der Dopingbekämpfung, usw.). Der Anti-Dopingkodex der nationalen Anti-Doping-Agentur, der die Regeln und Prinzipien des internationalen Anti-Dopingkodexes umsetzt, sieht zum Beispiel vor, dass genannte Agentur nach einer Anti-Doping-Untersuchung verschiedene Daten publizieren muss. Hierbei handelt es sich unter anderem um den Namen des Sportlers oder einer dritten Person, die einen Verstoß begangen hat.

Generell kommen aber nur drei Grundlagen in Frage, um die Verarbeitungen durch einen Verein zu legitimieren:

1. Die Einwilligung der betroffenen Person

Vorsicht: Die Einwilligung muss auf der freien Entscheidung der Person beruhen und diese muss zuvor über die auf Seite 11 aufgeführten Informationen verfügen. Bei verschiedenen anzukreuzenden Kästchen muss die Person die Möglichkeit haben, einer Verarbeitung zuzustimmen (z.B.: Erhalt der Newsletter) und eine andere abzulehnen (z.B.: Weitergabe der Daten zu Marketingzwecken). Bereits angekreuzte Kästchen sind verboten.

Untenstehend finden Sie einige Beispiele, bei denen die Zustimmung der betroffenen Personen als notwendig und angemessen anzusehen ist:

- Veröffentlichung auf einer Internetseite der privaten Kontaktdaten der Mitglieder des Vorstandes;
- Veröffentlichung in einem Informationsblatt der Geburtsdaten der Neugeborenen der Mitglieder, sowie ihre Hochzeitsdaten;
- Eintragung in eine Newsletter-Liste;
- Übermittlung der Kontaktdaten der Lizenzinhaber eines Sportvereins an ein Kleidergeschäft;
- Übermittlung der Kontaktdaten der in einer Selbsthilfegruppe eingeschriebenen Personen an einen anderen Verein;
- Veröffentlichung der Namen der externen Sponsoren (physische Personen) eines Vereins, sowie des Betrages der Spende;
- Einrichtung einer „What's App" Gruppe durch einen Trainer, um mit den Spielern und ihren Eltern in Kontakt zu bleiben, vorausgesetzt er bietet eine Alternative im Falle einer Weigerung an.

Aufgepasst: Bei Minderjährigen ist die Zustimmung der gesetzlichen Vertreter erforderlich. Hat ein Minderjähriger ein urteilsfähiges Alter erreicht („âge de raison"), das sich nach der aktuellen Rechtsprechung zwischen 12 und 14 Jahren befindet, so müssen sowohl das Kind, als auch die Eltern ihre Zustimmung geben, damit der Wille des Kindes berücksichtigt wird.

Die Einwilligung muss nicht in Schriftform erfolgen, sondern kann auch aus einer sonstigen eindeutigen bestätigenden Handlung hervorgehen, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Durch die Zahlung der Beiträge für eine Mitgliedskarte stimmt eine Person zum Beispiel zu, auf der Mitgliedsliste des betroffenen Vereins zu stehen und jedes Jahr eine Anfrage zur Erneuerung seiner Mitgliedschaft zu erhalten. Nichtdestotrotz wird aus Beweismittelzwecken (gegenüber Ihren Mitgliedern und im Falle einer Untersuchung durch die CNPD) empfohlen zu dokumentieren, auf welche Art und Weise die Einwilligung erfolgt ist. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person stellen aber keine Einwilligung dar.

2. Die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist. Um zum Beispiel den Arbeitsvertrag eines Arbeitnehmers zu erfüllen, muss der Arbeitgeber verschiedene Daten erfassen. Prinzipiell handelt es sich hierbei um Namen, Vornamen, Adresse, Geburtsdatum, Sozialversicherungsnummer und Kontonummer. In diesem Fall ist die Einwilligung des Arbeitnehmers nicht die treffende Rechtgrundlage für die Verarbeitung.

   Hinzu kommt, dass die Zugehörigkeit zu einem Verein in verschiedenen Fällen und abhängig von der Vereinssatzung, sowie den Vereinsaktivitäten (die angebotenen Dienstleitungen) als Vertragsverhältnis zwischen den Mitgliedern und dem Verein anzusehen ist. Die Verarbeitung der personenbezogenen Daten der Mitglieder darf aber nicht über das hinausgehen, was notwendig ist um diesen Vertrag zu erfüllen (prinzipiell nur den Namen, Vornamen, Adresse, Geburtsdatum und Kontonummer).

3. Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Vereins erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Nachfolgend einige Beispiele:
   - Veröffentlich auf der Internetseite eines Sportsvereines einer Liste mit den Namen, Vornamen und Geburtsjahren der Spieler;
   - Versand einer Liste mit den Namen der Spender und die Höhe ihrer jeweiligen Beiträge an die Hinterbliebenen einer verstorbenen Person;
   - Veröffentlichung auf der Internetseite der Namen, Vornamen und professionellen E-Mail-Adressen der Mitglieder des Vorstandes;
   - Vorübergehende Veröffentlichung der Namen, Vornamen und Geburtsjahren der Spieler, die für einen Wettkampf selektioniert worden sind, sowie die Resultate;
   - Übermittlung der Daten der Spieler an den Veranstalter eines Turniers;
   - Übermittlung der Daten der Spieler an einen Sportsverband um eine Lizenz zu erhalten.

Aufgepasst! Die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person, sowie der Grundsatz der Datenminimierung sind zu beachten. Erheben und verarbeiten Sie nur Daten, die auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind. Zum Beispiel: Sofern Sie nicht über die Zustimmung der Personen verfügen, würde die Veröffentlichung auf der Internetseite eines Sportsvereins des genauen Geburtsdatums und der Nationalität der Spieler, sowie der Privatadressen der Mitglieder des Vorstandes das notwendige Maß überschreiten und einen Eingriff in die Privatsphäre der betroffenen Personen darstellen.

Aufgepasst! Ein Verein darf Daten nicht in einer mit den ursprünglichen Zwecken nicht zu vereinbarenden Weise weiterverarbeiten. So dürfen Daten der Mitglieder nicht an ein Kleidergeschäft übermittelt werden, damit dieses ihnen Werbung zukommen lassen kann, außer die Mitglieder haben dieser Weiterverarbeitung zugestimmt.

Verarbeitung besonderer Kategorien von personenbezogenen Daten („sensible Daten")

Eine erhöhte Wachsamkeit ist notwendig bei der Verarbeitung von sensiblen Daten (z.B. die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung). Grundsätzlich ist die Verarbeitung sensibler Daten untersagt, außer eine der zehn in der DSGVO vorgesehenen Bedingungen ist erfüllt, wie zum Beispiel:

- die ausdrückliche Einwilligung der betroffenen Personen;
- eine arbeitsrechtliche Verpflichtung;
- die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden;
- offensichtlich öffentlich gemachte Daten;
- …

➔ **Siehe Artikel 9 der DSGVO bezüglich der Verarbeitung von „sensiblen" Daten.**

Das Recht am eigenen Bild

Das Recht am eigenen Bild bedeutet, dass jede Person das Exklusivrecht an seinem eigenen Bild und seiner Nutzung besitzt und sich einer nicht autorisierten Verbreitung widersetzen kann. Auch wenn es in Luxemburg keinen speziellen Gesetzestext über das Recht am eigenen Bild gibt, so hat die Rechtsprechung dies jedoch klar vorgesehen. In der Tat basieren sich die meisten Gerichtsentscheidungen auf Artikel 1 des Gesetzes vom 11. August 1982 über den Schutz des Privatlebens, welcher vorsieht, dass jeder das Recht auf Achtung seines Privatlebens hat (« *chacun a droit au respect de sa vie privée* »).

Prinzipiell kann ein Foto nur aufgenommen und veröffentlicht werden, wenn die betroffene Person seine vorherige Zustimmung dafür erteilt hat. Für die Aufnahme und Veröffentlichung von Fotos von Minderjährigen ist die Zustimmung der gesetzlichen Vertreter erforderlich und hat der Minderjährige ein urteilsfähiges Alter erreicht, so muss auch er seine Zustimmung geben. Die CNPD empfiehlt Vereinen, die im Zuge ihrer Aktivitäten Fotos von Minderjährigen aufnehmen und publizieren, den gesetzlichen Vertreter jährlich eine Einwilligungserklärung vorzulegen und gegebenenfalls auch den Minderjährigen. Diese Erklärung sollte klar definieren, für welche Zwecke Fotos aufgenommen und wie sie veröffentlicht werden können (Internet, Intranet, Zeitschrift eines Vereins, soziale Medien, usw.). Die Möglichkeit muss bestehen, die Veröffentlichung mittels bestimmter Medien zu akzeptieren oder abzulehnen.

Die Einwilligung zur Aufnahme eines Fotos kann auch durch eine eindeutige bestätigende Handlung erfolgen, zum Beispiel in dem man auf einer Jahresabschlussfeier eines Vereins für ein Foto posiert, das von einem Mitglied des Vereins aufgenommen wird. Nimmt ein Mitglied an einer Informationsveranstaltung über ein bestimmtes Thema teil und wird durch ein Schild an der Eingangstür darauf hingewiesen, dass Fotos aufgenommen und auf der Internetseite des Vereins veröffentlicht werden, so hat dieses Mitglied durch seine Teilnahme an der Veranstaltung seine Zustimmung erteilt. Es ist aber wichtig zu erwähnen, dass eine Person das Recht hat seine Einwilligung jederzeit zu widerrufen indem sie den Fotografen bittet, seine Fotos auf dem Fotoapparat zu löschen oder sie von einer bestimmten Internetseite zu entfernen im Falle einer Publikation.

Wie beinahe jedes Recht kennt das Recht am eigenen Bild auch Ausnahmen, zum Beispiel, wenn das Recht der freien Meinungsäußerung überwiegt, welches die Redefreiheit sowie die Freiheit Informationen zu empfangen und weiterzugeben beinhaltet (zum Beispiel die Darstellung einer bestimmten Vereinsaktivität auf seiner Internetseite oder die Veröffentlichung eines Presseartikels über eine Veranstaltung eines Vereins). Organisiert ein Verein eine öffentliche Veranstaltung, so können Fotos aufgenommen und über verschiedene Medien veröffentlicht werden, ohne Zustimmung der betroffenen Personen. Sollte jemand sich der Veröffentlichung widersetzen, so sollte der Verein versuchen, diese Widersetzung zu respektieren in dem er zum Beispiel ein individuelles Foto entfernt oder die betroffene Person unkenntlich macht.

In jedem Fall muss das Recht auf Information der betroffenen Personen respektiert werden, wie nachfolgend beschrieben.

Sie können in diesem Kontext unseren speziellen Leitfaden betreffend das Recht am eigenen Bild auf unserer Internetseite konsultieren.

Die Informationspflicht des für die Verarbeitung Verantwortlichen

Erfolgt eine Erhebung personenbezogener Daten direkt bei der betroffenen Person, so muss der Verein aus Gründen der Transparenz der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten verschiedene Informationen mitteilen, unabhängig welche von den vorhergenannten Rechtsgrundlagen anwendbar ist.

Diese Information muss Folgendes enthalten:

- Ihre Identität und Kontaktdaten;
- wieso Sie Daten erheben („die Zweckbestimmung“; z.B.: um die Liste Ihrer Mitglieder zu verwalten);
- wieso Sie diese Daten erheben dürfen („die Rechtsgrundlage“: einer der sechs vorhergenannten Kriterien);
- die Empfänger der Daten (z.B.: ein Sportsverband, die Verwaltung der sportmedizinischen Betreuung, der Veranstalter eines Turniers, usw.);
- gegebenenfalls die Absicht personenbezogene Daten an ein Drittland oder eine internationale Organisation zu übermitteln (präzisieren Sie das Land und stellen Sie sicher, dass angemessene Garantien vorhanden sind, zum Beispiel, wenn Sie auf eine Cloud-Plattform zurückgreifen, die in den USA beherbergt ist);
- wie lange Sie die Daten aufbewahren (z.B.: so lange wie eine Person Mitglied Ihres Vereins ist);
- die Rechte der betroffenen Personen wie untenstehend erläutert;
- das Bestehen eines Beschwerderechts bei der CNPD.

Um zu lange Angaben auf einem elektronischen oder Papierformular zu vermeiden, können Sie zum Beispiel am Schluss eines Formulars erste Informationen angeben und dann auf Ihre Datenschutzbestimmungen oder auf einen speziellen Link betreffend die Privatsphäre auf Ihrer Internetseite hinweisen, die dann alle obenstehenden Informationen beinhalten muss. In diesem Fall sind Sie Ihrer Verpflichtung, die betroffenen Personen auf eine transparente Art und Weise zu informieren, nachgekommen.

Ein Muster eines Informationsblattes befindet sich im Anhang. Dieses Muster muss an die Aktivitäten und Zweckbestimmungen der Datenverarbeitungen eines Vereins angepasst werden.

➔ **Siehe Artikel 12 und 13 der DSGVO bezüglich der Informationspflicht des Verantwortlichen.**

Die Achtung der Rechte der betroffenen Personen

Die Personen, von denen Sie Daten erheben, haben bestimmte Rechte, die übrigens mit der DSGVO verstärkt worden sind. Es handelt sich insbesondere um folgende Rechte:

- das Recht auf Information wie oben beschrieben;
- das Auskunftsrecht: das Recht auf Auskunft über seine Daten sowie das Recht, eine Kopie davon zu erhalten;
- das Recht auf Berichtigung: das Recht, die Berichtigung unrichtiger Daten zu verlangen;
- das Recht auf Löschung (das sogenannte „Recht auf Vergessenwerden"): das Recht, unter verschiedenen Umständen vom Verantwortlichen zu verlangen, dass personenbezogene Daten unverzüglich gelöscht werden (z.B. wenn die betroffene Person ihre Einwilligung widerruft, auf die sich die Verarbeitung stützt). Es handelt sich hier aber nicht um ein absolutes Recht. Müssen Daten zum Beispiel aufbewahrt werden, um eine rechtliche Verpflichtung zu erfüllen, so findet das Recht auf Löschung keine Anwendung;
- das Widerspruchsrecht: das Recht, aus Gründen, die sich aus der besonderen Situation der betroffenen Person ergeben, jederzeit gegen die Verarbeitung personenbezogener Daten Widerspruch einzulegen, außer der Verantwortliche kann überwiegende, zwingende und schutzwürdige Gründe für die Verarbeitung nachweisen oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, muss man zwei Arten des Versands voneinander unterscheiden.

Wird die Werbung mit der regulären Post verschickt, so sieht die DSGVO vor, dass die betroffene Person jederzeit Widerspruch gegen die Verarbeitung einlegen kann („opt-out"), aber ihre vorherige Zustimmung ist nicht notwendig. Ein Verein kann also Informationsblätter oder Anfragen zu Spenden an seine eigenen Mitglieder per Brief verschicken, sofern die angeschriebenen Personen sich widersetzen können (zum Beispiel indem Sie ihnen einen Antwortschein beilegen oder eine spezielle E-Mail-Adresse, die es ihnen ermöglicht ihr Widerspruchsrecht geltend zu machen).

Sollte die Werbung per E-Mail versandt werden, so appliziert sich weiterhin das abgeänderte luxemburgische Gesetz vom 30. Mai 2005[3] im Bereich der elektronischen Kommunikation. Zwei verschiedene Hypothesen sind dann möglich:

1. Hat ein Verein eine E-Mail-Adresse im Rahmen einer bestehenden Beziehung erhalten (z.B. durch den Verkauf einer Mitgliedskarte), so kann diese Adresse zu Werbezwecken benutzt werden ohne vorherige Genehmigung. Im Gegenzug müssen die betroffenen Personen sich jederzeit widersetzen können (und zum Zeitpunkt der Erhebung und bei jeder weiteren Mitteilung über dieses Recht informiert werden);

2. Besteht keine Verbindung zwischen dem Verein und einer Person, so muss die Einwilligung vor dem Verschicken der E-Mail eingenommen werden („opt-in").

[3] Abgeändertes Gesetz vom 30. Mai 2005 betreffend die spezifischen Bestimmungen bezüglich des Schutzes der Person bei der Datenverarbeitung auf dem Gebiet der elektronischen Kommunikation und betreffend die Abänderung der Artikel 88-2 und 88-4 der Strafprozessordnung.

Ein Verein muss den betroffenen Personen die Mittel zur Verfügung stellen, um ihre Rechte geltend zu machen. Sollten Sie eine Internetseite haben, so sehen Sie ein spezielles Kontaktformular, eine Telefonnummer oder eine E-Mail-Adresse vor. Bieten Sie ein Online-Konto an, dann geben Sie Ihren Mitgliedern die Möglichkeit, ihre Rechte über ihr Konto auszuüben. Richten Sie interne Prozeduren ein, die es Ihnen erlauben, die Identifikation und Verarbeitung der einzelnen Anfragen in kurz festgelegten Fristen (prinzipiell ein Monat) zu garantieren.

Stellen Sie sicher, dass Sie die Daten nicht länger als nötig aufbewahren. Sollte zum Beispiel ein Mitglied eines Vereins zurücktreten, so sind diese Daten prinzipiell zu löschen.

Die CNPD kann von jeder Person kontaktiert werden, die den Eindruck hat, dass Sie ihre Rechte nicht respektieren.

➔ **Siehe Artikel 13 bis 21 der DSGVO bezüglich der Rechte der betroffenen Personen.**

Der Datenschutzbeauftragte

Der Datenschutzbeauftragte (auf Englisch „Data Protection Officer“ oder „DPO“) nimmt einen wichtigen Platz in dem neuen, durch die DSGVO geschaffenen, Rechtsrahmen ein. Er hat die Aufgabe, die Organisation, die ihn benannt hat, in Datenschutzfragen zu unterrichten und zu beraten sowie die Einhaltung der Datenschutzvorschriften zu überwachen. Hinzu kommt, dass der DPO die erste Anlaufstelle für die CNPD ist.

Prinzipiell gehören Datenverarbeitungen nicht zu den alltäglichen Kernaktivitäten eines Vereins. Es handelt sich eher um eine nebensächliche Aktivität, die unumgänglich für seine Funktionsweise und seine Verwaltung ist. Die Benennung eines DPO ist in diesem Bereich selten erforderlich.

Die Benennung eines DPO ist in den folgenden drei Fällen vorgeschrieben:

1. Sie sind eine Behörde oder öffentliche Stelle (nicht anwendbar);
2. Ihre Kerntätigkeit besteht in der Durchführung von Verarbeitungsvorgängen, welche eine umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen (prinzipiell nicht anwendbar);
3. Ihre Kerntätigkeit besteht in der umfangreichen Verarbeitung sensibler Daten oder Daten über strafrechtliche Verurteilungen und Straftaten (selten anwendbar).

Für einen Verein kommt generell nur der letztgenannte Fall in Frage, zum Beispiel bei einem nationalen Hilfsnetz für häusliche Pflege, welches eine umfangreiche Verarbeitung von Gesundheitsdaten vornimmt. Verschiedene Vereine können auch einen gemeinsamen DPO ernennen, der entweder ein Mitglied des Personals (interner DPO) ist oder seine Aufgaben auf Basis von einem Dienstleistungsvertrag ausführt (externer DPO).

Seine Kontaktdaten müssen veröffentlicht (die Angabe auf Ihrer Internetseite einer speziellen E-Mail-Adresse genügt) und der CNPD über ein auf unserer Internetseite verfügbares Formular mitgeteilt werden.

➔ **Siehe Artikel 37 bis 39 der DSGVO bezüglich des DPO.**

Die Auftragsverarbeitung

Sie können in Ihrer Funktion als für die Verarbeitung Verantwortlicher die Verwaltung von verschiedenen Datenverarbeitungen an externe Dienstanbieter übertragen (z.B. für die Einrichtung und die technische Verwaltung Ihrer Internetseite, für die Abspeicherung von Daten auf Servern von Dritten, für die Benutzung eines Cloud-Service, für die administrative Verwaltung Ihrer Mitglieder, ein Buchhalter, der die Löhne ausrechnet, usw.).

Sie dürfen nur auf Auftragsverarbeiter zurückgreifen, die hinreichend Garantien dafür bieten, dass die Verarbeitung im Einklang mit den Datenschutzvorschriften erfolgt (Sie müssen dies überprüfen und beweisen können).

Die Verarbeitung durch einen Auftragsverarbeiter muss auf der Grundlage eines Vertrags erfolgen, der unter anderem vorsehen muss, dass der Auftragsverarbeiter die Daten nicht für seine eigenen Zwecke verarbeiten darf, sondern nur auf dokumentierte Weisung des Verantwortlichen. Standardklauseln bezüglich der Vorschriften der DSGVO müssen sich in diesem Vertrag befinden.

Die DSGVO verstärkt die Pflichten des Auftragsverarbeiters. So muss er zum Beispiel ebenfalls ein Verzeichnis von Verarbeitungstätigkeiten erstellen, er muss den Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten melden und er muss auch gegebenenfalls einen DPO benennen.

➔ **Siehe Artikel 28 der DSGVO bezüglich der Auftragsverarbeitung.**

Andere spezifische Pflichten

Hat eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so muss der Verantwortliche vorab eine Datenschutz-Folgenabschätzung durchführen (Artikel 35 und 36 der DSGVO). Vereine unterliegen dieser Verpflichtung sehr selten.

Verletzungen des Schutzes personenbezogener Daten (Artikel 33 und 34 der DSGVO) können nie zu 100% ausgeschlossen werden (Angriffe durch Hacker, Verlust einer Mitgliedsliste, Abhandenkommen eines Laptops oder eines USB-Sticks, usw.). Eine solche Verletzung muss als Erstes in einem internen Verzeichnis festgehalten werden (dieses Verzeichnis unterscheidet sich vom Verzeichnis von Verarbeitungstätigkeiten). Danach müssen Sie die Verletzung binnen 72 Stunden, nachdem sie Ihnen bekannt wurde, der CNPD melden und in einigen Fällen auch den betroffenen Personen. Ein Formular zur Meldung von Verletzungen des Schutzes personenbezogener Daten befindet sich auf der Internetseite der CNPD.

Die DSGVO sieht spezifische Regeln im Falle von möglichen Übermittlungen von Daten an ein Drittland (außerhalb der europäischen Union) oder eine internationale Organisation vor (Artikel 44 bis 49 der DSGVO). Die betroffenen Personen müssen im Voraus über diese Übermittlungen informiert werden. Dies trifft zum Beispiel zu, wenn Sie zum Verschicken Ihrer Newsletter einen Dienstanbieter aussuchen, der seine Dienste zwar in Europa anbietet, die Daten aber in ein Land außerhalb der europäischen Union übermittelt (z.B. die USA, China, Indien, usw.). Generell empfiehlt die CNPD von Anfang an zu überprüfen, ob es keine Dienstleister gibt, die ihren Sitz in der europäischen Union haben und die gleichen Dienste anbieten, da diese dieselben Datenschutzvorschriften respektieren müssen.

Sie müssen geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Artikel 32 der DSGVO). Die Prinzipien des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sind äußerst wichtig. Solche Maßnahmen müssen zum Beispiel sicherstellen, dass innerhalb eines Vereins personenbezogene Daten nur den Personen zugänglich gemacht werden, die diesen Zugang benötigen, um ihre Aufgaben zu erfüllen. So muss der Vorstand eines Vereins zum Beispiel Zugang zu den Daten der Mitglieder haben um seinen Missionen zu erfüllen. Der Schatzmeister eines Vereins muss hingegen nicht zwingend einen Zugang zu allen Daten der verschiedenen Verarbeitungen haben, sondern nur jene, die notwendig sind, um seine Aufgaben zu erfüllen, wie zum Beispiel die Verwaltung der Beiträge, die Finanzbuchhaltung und um Finanzüberweisungen zu tätigen.

Sie können auch unsere Broschüren bezüglich der Rechte der betroffenen Personen (auf Deutsch und Französisch) und die Pflichten des Verantwortlichen (auf Französisch und Englisch) konsultieren, sowie unsere speziell der DSGVO gewidmeten Internetseite.

Anhang 1: Muster eines Informationsblattes

Aufgepasst: Dieses Dokument stellt nur ein Muster eines Informationsblattes dar, welches die obligatorischen Informationen aus Artikel 13 der DSGVO enthält. Die Punkte 1 bis 4 müssen ergänzt und von Fall zu Fall an die Aktivitäten und Zwecke der Verarbeitungen eines Vereins angepasst werden. Dieses Informationsblatt muss mindestens auf der Internetseite des Vereins publiziert werden und gegebenenfalls auch in den Dokumenten und Korrespondenzen, die an die betroffenen Personen gerichtet sind.

1. Namen und Kontaktdaten des für die Verarbeitung Verantwortlichen

Name des Vereins, Postanschrift, Telefonnummer, E-Mail-Adresse, Internetseite und eventuell die Namen der Vorstandsmitglieder.

2. Zwecke, Rechtsgrundlage und Kategorien von verarbeiteten personenbezogenen Daten

Ein Verein verarbeitet Daten für folgende Zwecke:

- Für die administrative Verwaltung der Mitglieder (auf Basis der Zustimmung / eines Vertrags): Name, Vorname, Postanschrift, E-Mail-Adresse, Datum des Beitritts;
- Für das Verschicken von Newsletter (auf Basis der Zustimmung): Name, Vorname, Postanschrift, E-Mail-Adresse;
- Für die Verwaltung der Lieferanten (auf Basis eines Vertrags): Name und Vorname der Kontaktperson, Postanschrift, E-Mail-Adresse, Telefonnummer;
- Für die Verwaltung der Beiträge (auf Basis der Zustimmung / eines Vertrags): Name, Vorname, Postanschrift, E-Mail-Adresse, Bankkonto;
- Für die Verwaltung der „VIP“ Kontaktlisten (auf Basis der Zustimmung): Name, Vorname, Postanschrift, E-Mail-Adresse;
- Für die Verwaltung des Personals[4] (auf Basis eines Vertrags): Name, Vorname, CV, Postanschrift, E-Mail-Adresse, Sozialversicherungsnummer, Geburtstag, Steuerklasse, Strafregister, Lohn, ärztliche Atteste;
- Für die Verwaltung der lizensierten Spieler (auf Basis der Zustimmung / eines Vertrags): Name, Vorname, Postanschrift, E-Mail-Adresse, Geburtstag, Foto;
- …
- **(muss von Fall zu Fall angepasst werden)**

3. Kategorien von Empfängern der personenbezogenen Daten

- Im Rahmen der administrativen Verwaltung der Mitglieder werden Daten an interne Funktionsträger übermittelt (der Ausschuss, der Sekretär, der Schatzmeister, usw.);
- Um die Newsletter zu verschicken werden Daten an einen externen Dienstleister übermittelt;
- Die Daten des Personals werden an einen Buchhalter übermittelt, um die Gehaltsabrechnungen zu erstellen;

[4] Falls anwendbar müssen die Arbeitnehmer individuell informiert werden.

- Die Daten der lizensierten Spieler können an den Veranstalter eines Sportturniers oder an die Verwaltung der sportmedizinischen Betreuung übermittelt werden;
- Alle Daten werden durch einen in Luxemburg etablierten Auftragsverarbeiter abgespeichert;
- **(muss von Fall zu Fall angepasst werden)**

4. Aufbewahrungsdauer

- Daten der Mitglieder: 1 Jahr nach:
    - der Nicht-Bezahlung des jährlichen Beitrags
    - dem Austritt eines Mitglieds;
    - dem Ausschluss eines Mitglieds
    - …
    - **(muss von Fall zu Fall angepasst werden)**

- Daten, die im Rahmen der Verwaltung der Beiträge gesammelt werden: 2 Monate nach dem jährlichen Rechnungsabschluss;
- …
- **(muss von Fall zu Fall angepasst werden)**

5. Rechte der betroffenen Personen

Sie haben ein Recht auf Auskunft über Sie betreffende personenbezogene Daten und können eine Kopie davon verlangen (Artikel 15 der Datenschutz-Grundverordnung). Sie können außerdem die Berichtigung Sie betreffender unrichtiger personenbezogener Daten verlangen (Artikel 16 der Datenschutz-Grundverordnung) und gegen die Verarbeitung Sie betreffender personenbezogener Daten Widerspruch einlegen gemäß den Bedingungen des Artikels 21 der Datenschutz-Grundverordnung. Außerdem haben Sie das Recht, von dem Verantwortlichen zu verlangen, dass Sie betreffende personenbezogene Daten unverzüglich gelöscht werden gemäß den Bedingungen des Artikels 17 der Datenschutz-Grundverordnung, sowie das Recht auf Einschränkung der Verarbeitung gemäß Artikel 18 der Datenschutz-Grundverordnung.

6. Widerspruchsrecht

Sie können eine Beschwerde bei der CNPD einreichen, wenn Sie der Ansicht sind, dass die von uns vollzogene Verarbeitung Ihrer personenbezogenen Daten gegen die Datenschutz-Grundverordnung verstößt.

Anhang 2: Muster eines Verzeichnisses von Verarbeitungstätigkeiten auf Basis von Artikel 30 der Datenschutz-Grundverordnung

Aufgepasst: Dieses Dokument stellt nur ein Muster eines Verzeichnisses von Verarbeitungstätigkeiten dar, welches eine exemplarische und nicht vollständige Liste mit den üblichen Verarbeitungstätigkeiten eines Vereins enthält. Die einzelnen Rubriken müssen also ergänzt und von Fall zu Fall an die Aktivitäten und Zwecke der Verarbeitungen eines Vereins angepasst werden.

Name und Kontaktdaten des für die Verarbeitung Verantwortlichen: Name des Vereins, Namen der Vorstandsmitglieder, Postanschrift, Telefonnummer, E-Mail-Adresse, Internetseite, letzte Aktualisierung[5]

	Zwecke der Ver-arbeitung	Kategorien von betroffenen Personen	Kategorien von verarbeiteten Daten	Kategorien von Empfängern	Über-mittlung an ein Drittland	Löschfristen	Technische und organisatorische Sicherheits-maßnahmen
Verarbeitung n°1	Administrative Verwaltung der Mitglieder	Mitglieder	• Name • Vorname • Postanschrift • E-Mail-Adresse • Beitrittsdatum • usw.[6]	• Druckerei der Mitgliedskarten • Cloud-Anbieter • interne Funktionsträger (der Sekretär, usw.) • usw.	N/A[7]	1 Jahr nach: • der Nicht-Bezahlung des jährlichen Beitrags • dem Austritt eines Mitglieds • dem Ausschluss eines Mitglieds • usw.	• Zugangskontrolle zu den Dateien • Maßnahmen zur Rückverfolgbarkeit • Softwareschutz • etc.
Verarbeitung n°2	Verwaltung der Beiträge	Mitglieder	Zusätzlich zu der Verarbeitung n°1 : Bankkonto	interne Funktionsträger (der Schatzmeister, usw.)	N/A	2 Monate nach dem jährlichen Rechnungsabschluss	Idem

[5] Der Verein muss regelmäßig (+/- einmal im Jahr) sicherstellen, dass sein Verzeichnis auf dem neuesten Stand ist.
[6] Jedes Mal, wenn in diesem Dokument von « usw. » die Rede ist, bedeutet dies, dass der Verein den Inhalt dieser Rubrik ergänzen und an seine konkrete Situation anpassen muss.
[7] Prinzipiell nicht anwendbar.

Verarbeitung n°3	Newsletter	Alle, die zugestimmt haben	• Name • Vorname • Postanschrift • E-Mail-Adresse • usw.	Externe Dienstanbieter	N/A[8]	Bis zum Widerruf der Einwilligung	Idem
Verarbeitung n°4	Verwaltung der Internetseite	• Mitglieder • Besucher der Seite	• I.P. Adresse • Cookies • etc.	Externe Dienstanbieter	N/A	Muss von Fall zu Fall bestimmt werden	Idem
Verarbeitung n°5	Veröffentlichung von Fotos auf der Internetseite	• Mitglieder • Zuschauer • Dritte	Auf Veranstaltungen aufgenommene Fotos	Besucher der Seite	N/A	Bis zum Widerruf der Einwilligung	Idem
Verarbeitung n°6	Verwaltung der « VIP" Kontaktlisten	• Politiker • Kaufleute • Sponsoren • usw.	• Name • Vorname • Postanschrift • E-Mail-Adresse • usw.	N.A.	N/A	Bis zum Widerspruch der betroffenen Person	Idem
Verarbeitung n°7	Verwaltung der Lieferanten	Lieferanten	• Name und Vorname der Kontaktperson • Postanschrift • E-Mail-Adresse • Telefonnummer • usw.	• Buchhalter • Interne Funktionsträger (der Schatzmeister, usw.) • usw.	N/A	• 10 Jahre	Idem
Verarbeitung n°8	Verwaltung des Personals	Arbeitnehmer	Zusätzlich zu der Verarbeitung n°1: • CV • Sozialversicherungsnummer • Steuerklasse • Strafregister • Lohn • ärztliche Atteste • usw.	• Buchhalter • Interne Funktionsträger (der Vorstand, usw.) • Steuern • Sozialversicherung • usw.	N/A	• 3 Jahre nach Beendigung des Arbeitsvertrags • Strafregister: 1 Monat nach Vertragsabschluss • usw.	Idem

[8] Es muss aufgepasst werden, ob der Dienstleister, der seine Dienste in Europa anbietet, Daten nicht außerhalb der Union übermittelt.

Verarbeitung n°9	Videoüberwachung um die Waren zu schützen (Räume, Anlagen, Ausrüstungen, usw.)	Mitglieder und andere Nutzer der Räume	Bilder	• Interne Funktionsträger (der Vorstand, usw.) • Auftragsverarbeiter (eine Sicherheitsfirma) • Polizei • Justizbehörden • usw.	N/A	8 Tage	Idem
…							