1.4. Datenschutzrechtliche Rechtsgrundlagen für Vereine

Neben dem Wirksamwerden der DSGVO im Jahr 2018 wurden ergänzende Datenschutzregelungen im Datenschutzgesetz (DSG) und in zahlreichen Materiengesetzen beschlossen, die ebenfalls seit dem 25. Mai 2018 gelten.

Die elektronische und telefonische (nicht jedoch die postalische) Kontaktaufnahme ist bis auf weiteres nach wie vor im Telekommunikationsgesetz geregelt. Ebenso gilt für den Einsatz von sogenannten Cookies in Österreich weiterhin das Telekommunikationsgesetz.

Somit lässt sich festhalten, dass der Kern des für Vereine derzeit unmittelbar anwendbaren Datenschutzrechts vorwiegend aus folgenden Rechtsquellen besteht:

- Der Datenschutz-Grundverordnung (DSGVO),
- dem Datenschutz-Gesetz (DSG) und
- dem Telekommunikationsgesetz (TKG) für den Bereich elektronische und telefonische Kontaktaufnahme sowie für den Bereich Cookies.

Zusätzlich dazu gibt es zahlreiche Stellungnahmen und Richtlinien, die von der Artikel-29-Datenschutzgruppe zu datenschutzrechtlichen Fragestellungen veröffentlicht worden sind. Die Artikel-29-Datenschutzgruppe war ein unabhängiges Gremium, das die EU-Kommission in Datenschutzfragen beraten hat. Sie wurde am 25. Mai 2018 vom Europäischen Datenschutzausschuss (EDSA) abgelöst. Viele der bisherigen Leitlinien der Artikel-29-Datenschutzgruppe wurden vom Europäischen Datenschutzausschuss bestätigt und können daher weiterhin zur Interpretation des Datenschutzrechts herangezogen werden.

1.5. Vereine als Verantwortliche des Datenschutzrechts

Grundsätzlich sieht die DSGVO keine datenschutzrechtlichen Erleichterungen für Vereine vor. Die DSGVO behandelt Vereine (egal ob gemeinnützig oder nicht) wie alle anderen datenschutzrechtlichen Akteure.

Viele Tätigkeiten, die im Rahmen von Vereinen erfolgen, werden ehrenamtlich geleistet und können somit eher dem „Hobbybereich“ zugerechnet werden. Die DSGVO sieht für gewisse private Tätigkeiten Ausnahmen vor. Nach der so genannten Haushaltsausnahme sind Verarbeitungen von personenbezogenen Daten, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen werden, von der DSGVO ausgenommen. Diese Einschränkung ist jedoch sehr eng zu interpretieren.

Als persönliche oder familiäre Tätigkeiten können nach der DSGVO zB das Führen eines Schriftverkehrs, von Anschriftenverzeichnissen oder die Nutzung sozialer Netze und Online-Aktivitäten gelten. Die ehrenamtlichen Tätigkeiten in einem

Verein und diejenigen eines Vereins gehen über diese Haushaltsausnahme hinaus und unterliegen der DSGVO.

Die DSGVO gilt somit für beinahe alle „Datenverarbeiter". Sie unterteilt diese Datenverarbeiter dabei in sogenannte „Verantwortliche" und „Auftragsverarbeiter". Dabei handelt es sich um Begriffe, deren Definitionen direkt in der DSGVO zu finden sind.

Verantwortliche gemäß der DSGVO sind dabei natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden.

Verantwortlich ist also, wer darüber entscheidet, dass Daten für einen oder mehrere Zwecke verarbeitet werden sollen. Dabei ist es nicht erforderlich, dass diese Daten vom Verantwortlichen selbst erhoben werden. Die Erhebung kann auch durch einen Dritten erfolgen.

Bereits hier ist ersichtlich, dass die Stellung als Verantwortlicher nicht an eine bestimmte Rechtsform gebunden ist. Ein Verantwortlicher im Sinne des Datenschutzrechts kann somit jede Rechtsform aufweisen, daher auch ein Verein sein oder etwa auch eine „Privatperson".

Der datenschutzrechtliche Verantwortliche ist hier, im Falle von Vereinen, in der Regel die juristische Person, also der Verein selbst. Ausnahmen sind für bestimmte Verarbeitungstätigkeiten vor allem dann denkbar, wenn Vereine nicht über die Zwecke und Mittel der personenbezogenen Daten entscheiden, sondern sich an strenge Vorgaben anderer Auftraggeber halten müssen. Dies kann etwa im geförderten Bereich der Fall sein bzw bei Projekten, bei denen öffentliche Auftraggeber im Fördervertrag auch über die Zwecke und Mittel der Verarbeitung entscheiden.

In der überwiegenden Zahl der Fälle ist jedoch der Verein selbst der Verantwortliche. Entscheidungsträger innerhalb eines Vereins (etwa Geschäftsführer eines Vereins) sind nur dann als datenschutzrechtliche Verantwortliche anzusehen, wenn sie als Privatpersonen und nicht in ihrer vereinsinternen Funktion Entscheidungen über die Zwecke und Mittel der Verarbeitung treffen. Sehr wohl kann den Entscheidungsträger aber im Innenverhältnis ein Regressanspruch des für die Datenschutzverletzung bestraften oder zivilrechtlich in Anspruch genommenen Vereins treffen. Dem Verein werden dabei Personen zugerechnet, die unter der Verantwortung des Vereins personenbezogene Daten verarbeiten.

Häufig setzt man für Verarbeitungstätigkeiten externe Dienstleister ein. Der Betrieb der eigenen Website wird etwa durch einen so genannten Host-Provider erfolgen. Für die Versendung von Newslettern kann ein Newsletter-Versanddienst (wie Mailchimp) herangezogen werden. Zur Anzeige von Benutzerstatistiken

können „fremde“ Analyse-Tools (wie Google Analytics) eingesetzt werden (Reichweitenmessung). Auch werden Druckereien beauftragt, die für die Versendung von Mailings Broschüren und das Adressmaterial von Vereinen übermittelt bekommen. Zudem werden oft auch Datenbanken von Externen auf Fremdservern zur Verfügung gestellt und von diesen gewartet, auf denen etwa die Mitgliederverwaltung oder Spenderverwaltung erfolgt. Regelmäßig wird auch die Lohnverrechnung an Externe ausgelagert.

Bei allen diesen Dienstleistern kann es sich um sogenannte datenschutzrechtliche Auftragsverarbeiter handeln. Der Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Wesentlich für die Einstufung als Auftragsverarbeiter ist hier, dass ein Weisungsverhältnis zwischen Verantwortlichen und Auftragsverarbeitern vorliegt. Der Verantwortliche entscheidet, was mit den personenbezogenen Daten geschehen soll, und auch, wie diese verarbeitet werden. Verantwortliche sind die „Herren“ der Daten. Wenn ein Auftragsverarbeiter die Daten für eigene Zwecke weiterverarbeitet, wird er selbst zum Verantwortlichen.

Die DSGVO gilt grundsätzlich sowohl für Verantwortliche als auch für Auftragsverarbeiter. Die Unterscheidung zwischen Verantwortlichen und Auftragsverarbeitern ist für die Zuordnung von datenschutzrechtlichen Verpflichtungen wesentlich. Den Löwenanteil der datenschutzrechtlichen Verpflichtungen hat dabei der Verantwortliche zu tragen.

Den Verantwortlichen treffen dabei insbesondere folgende Pflichten:

- Abschluss der erforderlichen Auftragsvertragsverarbeitervereinbarungen,
- Einhaltung der Betroffenenrechte,
- Sicherstellung von Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen,
- Meldung von allfälligen Datenschutzverletzungen und
- (ggf) Durchführung der Datenschutz-Folgenabschätzung.

Bei der Wahrnehmung seiner Pflichten muss der Verantwortliche jedoch in der Regel von seinen Auftragsverarbeitern unterstützt werden. Das muss er bei Abschluss der Auftragsverarbeitervereinbarung sicherstellen.

Folgende Pflichten können sowohl Verantwortliche als auch Auftragsverarbeiter treffen:

- Erstellung und Führung eines Verzeichnisses von Verarbeitungstätigkeiten,
- ggf Ernennung eines Datenschutzbeauftragten (bei Vorliegen der übrigen Kriterien) und
- Ergreifen von angemessenen Datensicherheitsmaßnahmen.

1.6. Ziele und Auswirkungen des neuen Datenschutzrechts

Warum ist es überhaupt zum Beschluss der Datenschutz-Grundverordnung gekommen?

In der Vergangenheit wurde das Datenschutzrecht häufig als „zahnlos" angesehen. Die Betroffenen kannten ihre Datenschutzrechte nicht und kümmerten sich folglich auch nicht um die Durchsetzung ihrer Rechte. Verstöße gegen das Datenschutzrecht wurden kaum geahndet, un, wenn doch, wurden Verantwortliche, wenn überhaupt, mit vernachlässigbaren Strafen belegt. Die Datenschutzbehörde hatte zudem keine Strafbefugnisse.

Vielerorts wurde die Verwendung von Daten hauptsächlich durch die technologischen Möglichkeiten bestimmt, über die rechtliche Zulässigkeit bzw die datenschutzrechtlichen Voraussetzungen machten sich Datenverarbeiter kaum Gedanken. Kurzum, das Datenschutzrecht wurde als „totes Recht" betrachtet und oft nicht ernst genommen.

Eine Zeit, in der den Daten immer mehr die Qualität als „neues Öl" zugeschrieben wird, erfordert für den Umgang mit diesem neuen Rohstoff ein adaptiertes Regelwerk, welches für einen fairen Interessenausgleich zwischen Betroffenen und Datenverarbeitern sorgt. Wer die Möglichkeiten dieses „neuen Öls" nutzen möchte, der soll das nach dem Willen des europäischen Gesetzgebers in vielen Fällen auch dürfen, jedoch auch die Verantwortung für die damit verbundenen Risiken übernehmen und hier wesentlich sorgfältiger agieren als bisher – und zwar dem jeweiligen Risiko angemessen.

Dieser risikobasierte Ansatz ist eine wesentliche Neuerung im Vergleich zur Rechtslage vor der DSGVO. Risiken sind fortan von Datenverarbeitern selbst einzustufen (höhere Eigenverantwortung durch Selbsteinschätzung) und es sind den Risiken entsprechende Schutzmaßnahmen zu treffen.

Sofern eine Datenverarbeitung für den Betroffenen mit hohen Risiken verbunden ist, treffen ihn höhere Anforderungen.

Nach langen Verhandlungen wurde die DSGVO letztlich ein Kompromiss zwischen den Interessen der Wirtschaft, Daten möglichst uneingeschränkt verarbeiten zu dürfen, und den Interessen der Verbraucherschützer bzw Menschenrechts-NGOs, natürliche Personen bestmöglich vor der missbräuchlichen Verwendung ihrer personenbezogenen Daten zu schützen.

Wie auch häufig als Regelungstechnik im Völkerrecht zu finden, wurden in Bereichen, in denen man sich während der Verhandlungen nicht auf eine bestimmte Regelung einigen konnte, offene bzw „schwammige" Formulierungen gewählt, Textpassagen, die als Regelungsinhalt gedacht waren, nur in die „Erläuterungen" (Erwägungsgründe) aufgenommen und somit die finale Entscheidung

für die Auslegung vieler Begriffe den jeweiligen nationalen Aufsichtsbehörden und in letzter Instanz dem Europäischen Gerichtshof überlassen.

Die wesentlichen Zielsetzungen bzw Auswirkungen der DSGVO sind unter anderem:

- die deutliche Stärkung der Betroffenenrechte,
- deutlich mehr Eigenverantwortung von Datenverarbeitern,
- größere Harmonisierung des Datenschutzrechts im europäischen Raum und somit ein erleichterter Datenaustausch innerhalb der europäischen Staaten,
- ein erweiterter Anwendungsbereich des Datenschutzrechts durch das so genannte Marktortprinzip. Erfasst werden auch nicht europäische Anbieter, die ihre Leistungen in der EU anbieten (zB Facebook, Google, Amazon), sowie
- deutlich höhere Strafdrohungen als bisher.

1.7. Der Begriff der personenbezogenen Daten

Der Schutzbereich der DSGVO umfasst nur personenbezogene Daten. Dabei handelt es sich um alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (den Betroffenen) beziehen.

Identifiziert ist eine Person, wenn der Datenverwender die jeweilige Person identifizieren kann, etwa mittels Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, Standortdaten oder zu einer Online-Kennung.

Identifizierbar ist eine Person, wenn sie zwar aktuell nicht identifiziert werden kann, aber dies anhand der vorhandenen Informationen mit zumutbarem Aufwand möglich ist oder mit der Identifizierung durch andere Personen ernsthaft gerechnet werden muss. Umstritten ist die Frage, ab wann es ausreichend ist, dass ein Personenbezug (theoretisch) hergestellt werden kann.

- Wenn etwa in einer Vereinszeitschrift Fotos mit Namen veröffentlicht werden, ist die Person jedenfalls identifiziert.
- Wird in einer Vereinszeitschrift ein Foto mit einer Funktionsbeschreibung („Kassier“) veröffentlicht, kann es sein, dass die Person einigen Vereinsmitgliedern unbekannt ist und nicht identifiziert werden kann, diese jedoch durch genauere Recherche erfahren können, um wen es sich handelt.
- Ähnlich verhält es sich mit Wettkampfergebnissen. Werden Listen von Namen mit Wettkampfergebnissen veröffentlicht, handelt es sich um identifizierte Personen.
- Wird in einem Internetforum unter einem Pseudonym das exakte Wettkampfdatum mit der genauen Zielzeit veröffentlicht, kann Identifizierbarkeit vorliegen.

Bei der Feststellung der Identifizierbarkeit sollten nach der DSGVO alle Mittel berücksichtigt werden, die vom Verantwortlichen oder einer anderen Person

nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten nach der DSGVO alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.

Häufig gibt es hinsichtlich der Verarbeitung (Speicherung) von IP-Adressen Diskussionen, ob hier personenbezogene Daten vorliegen.

Statische IP-Adressen werden als personenbezogenes Datum behandelt, da man die Anschlussinhaber über Datenbanken ermitteln kann, bei dynamischen IP-Adressen weiß zudem der Internetprovider für gewöhnlich, welcher Kunde zu welchem Zeitpunkt eine bestimmte IP-Adresse verwendet hat. Somit sind diese IP-Adressen für den Provider jedenfalls personenbezogen. Websitenbetreiber speichern regelmäßig die IP-Adressen, wissen aber ohne Zusatzinformationen nicht, wer der Besucher der Website ist. Auch beim Behavioural Advertising oder Device Fingerprinting weiß der Verantwortliche ohne Zusatzwissen nicht, wer der dahinterstehende Betroffene ist.

Insbesondere hinsichtlich der Einstufung von dynamischen IP-Adressen wird von manchen Aufsichtsbehörden vertreten, dass der Personenbezug auch dann gegeben ist, wenn irgendeine Person den Personenbezug herstellen kann und diese Möglichkeit nicht rein hypothetisch ist. Rein praktisch folgt daraus, dass der Personenbezug bei IP-Adressen im Zweifel „zur Sicherheit“ angenommen werden sollte und IP-Adressen generell als personenbezogenes Datum behandelt werden sollten.

In den Erwägungsgründen der DSGVO wird erstmals klargestellt, dass kein Recht auf Datenschutz für verstorbene Personen besteht.

Auch wenn hinsichtlich der primärrechtlichen Grundlagen umstritten ist, ob juristische Personen datenschutzrechtlich geschützt sind, beinhaltet die DSGVO kein Recht auf Datenschutz für diese. Somit sind etwa der Name, die Rechtsform oder die Kontaktdaten der juristischen Person nicht geschützt. Das trifft etwa jedenfalls auf die Office-Adresse, Office-Telefonnummer oder Office-E-Mail-Adresse datenschutzrechtlich (sehr wohl aber telekommunikationsrechtlich geschützt) zu. Daten von juristischen Personen sind nur dann geschützt, wenn sie sich auch auf natürliche Personen beziehen. Das kann etwa der Fall sein, wenn der Firmenname den Namen einer natürlichen Person aufweist.

Zu den personenbezogenen Daten zählen auch Kontaktdaten der Geschäftspartner, so etwa auch die Handynummern und E-Mail-Adressen von Geschäftskontakten, also die beruflichen personenbezogenen Kontaktdaten. Grundsätzlich