Die Neuerungen der DS-GVO

Im Hinblick auf vereinsrelevante Themen

Dr. Lutz Hasse

Thüringer **L**andesbeauftragter für den **D**atenschutz und die **I**nformationsfreiheit (**TLfDI**)

Inhalt

- Rechtsgrundlagen des Datenschutzes
- Allgemeines zur DS-GVO
- Rechtsnatur der DS-GVO
- Definition personenbezogener Daten, Art.4 DS-GVO
- Grundsätze für die Verarbeitung Art. 5 DS-GVO
- Rechtmäßigkeit der Verarbeitung personenbezogener Daten , Art. 6 DS-GVO
- Rechtmäßigkeit der Verarbeitung personenbezogener Daten , Art. 9 DS-GVO
- Betroffenenrechte
- Pflichten des Verantwortlichen
- Effektive Durchsetzung
- Fazit

Rechtsgrundlagen des Datenschutzes

Grundrecht auf informationelle Selbstbestimmung:

Auszug aus dem sog. Volkszählungsurteil des BVerfG vom 15.12.1983:

„Mit dem Recht auf informationelle Selbstbestimmung wäre […] eine Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. ***Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.*** […] Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst.“ (…)

„Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“

Rechtsgrundlagen des Datenschutzes

Thüringer Verfassung (Art. 6)

...

(2) Jeder hat Anspruch auf Schutz seiner **personenbezogenen Daten**. Er ist berechtigt, über die Preisgabe und Verwendung solcher **Daten selbst zu bestimmen**.

...

3) Diese Rechte dürfen nur **auf Grund eines Gesetzes eingeschränkt** werden. Den Belangen historischer Forschung und geschichtlicher Aufarbeitung ist angemessen Rechnung zu tragen.

Allgemeines zur DS-GVO

- EU Datenschutz-Grundverordnung ist am 25.05.2016 in Kraft getreten
- sie gilt ab dem 25.05.2018 in allen europäischen Mitgliedstaaten
- Bis dahin gilt noch die EG – Datenschutzrichtlinie vom 24.10.1995
- deren Umsetzung in nationales Recht findet sich im Bundesdatenschutzgesetz (BDSG) wieder

Rechtsnatur der DS-GVO

- Da die Umsetzung der EU-Richtlinie in der Praxis nicht immer zufriedenstellend funktionierte, nun Regelung des EU Datenschutzes durch Verordnung (DS-GVO)
- Im Gegensatz zu Richtlinien sind Verordnungen allgemein und unmittelbar geltende und in allen Teilen verbindliche Rechtsakte
- DS-GVO hat sog. Öffnungsklauseln, die den Mitgliedstaaten einen Gesetzgebungsspielraum einräumen, insoweit das nationale Datenschutzrecht strenger oder liberaler als die DS-GVO auszugestalten

Rechtsnatur der DS-GVO

- Um diese Öffnungsklauseln mit Leben zu füllen, wurde das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom deutschen Bundestag mit Zustimmung des Bundesrates am 30.06.2017 verabschiedet

- kurz: Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU)

- In Art. 1 des DSAnpUG-EU findet sich das das neue Bundesdatenschutzgesetz (BDSG neu)

Definition personenbezogener Daten DS-GVO Art. 4

- “personenbezogene Daten” alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden “betroffene Person”) beziehen

- Eine identifizierte Person , ist eine Person, wenn das Datum selbst einen unmittelbaren Rückschluss auf die Identität des Betroffenen zulässt, z.B.:
  - Name
  - Telefonnummer

- Eine identifizierbare Person, wenn sie zwar durch das Datum selbst noch nicht allein bzw. eindeutig identifizierbar ist, aber mit Hilfe weiterer Informationen (Zusatzhinweise) der Bezug herstellbar ist, z.B.:

  - Smartphone-ID, Lokalisation

Grundprinzipien des Datenschutzes

- Die Datenschutz-Grundverordnung behält im Wesentlichen die bisherigen datenschutzrechtlichen Grundprinzipien bei und entwickelt sie weiter

- Die **Grundprinzipien**
  des „Verbots mit Erlaubnisvorbehalt“,
  der „Datenvermeidung und Datensparsamkeit“,
  der „Zweckbindung“ und
  der „Transparenz“

prägen auch die Datenschutz-Grundverordnung

Grundsätze für die Verarbeitung personenbezogener Daten, **Art. 5 DS-GVO**

- zentrale Norm ist **Art. 5 DS-GVO** in dem die Grundsätze zur Verarbeitung personenbezogener Daten geregelt werden

❖ Rechtmäßigkeit

❖ Verarbeitung nach Treu und Glauben

❖ Transparenz

❖ Zweckbindung

❖ Datenminimierung

❖ Richtigkeit

❖ Speicherbegrenzung

❖ Integrität und Vertraulichkeit

❖ Rechenschaftspflicht

Grundsätze für die Verarbeitung personenbezogener Daten, **Art. 5 DS-GVO**

(1) Personenbezogene Daten müssen

1. auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
2. für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Art. 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);
3. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
4. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

Grundsätze für die Verarbeitung personenbezogener Daten, **Art. 5 DS-GVO**

5. in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Art.89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);
6. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Grundsätze für die Verarbeitung personenbezogener Daten, **Art. 5 DS-GVO**

- Personenbezogene Daten dürfen nur auf **„rechtmäßige Weise“** verarbeitet werden

- Für die Verarbeitung personenbezogener Daten normiert Art. 5 Abs. 1 lit. a DS-GVO als allgemeinen Grundsatz ein sogenanntes Verbot mit Erlaubnisvorbehalt

- Die Rechtmäßigkeit der Verarbeitung ergibt sich dann unmittelbar aus Art. 6 DS-GVO

Grundsätze für die Verarbeitung personenbezogener Daten, **Art. 5 DS-GVO**

- Personenbezogene Daten müssen zudem nach „**Treu und Glauben**“ und in einer für den Betroffenen nachvollziehbaren Art und Weise, also transparent, verarbeitet werden

- Die Ausgestaltung dieser **Transparenz** findet in den umfangreichen Informationspflichten (Art.13) und Auskunftsansprüchen (Art.14) ihren Niederschlag, deren Erfüllung durch den Verantwortlichen ,also den Verein, ebenfalls umfangreich geregelt ist (Art.12)

Grundsätze für die Verarbeitung personenbezogener Daten, **Art. 5 DS-GVO**

- Ein weiterer zentraler Grundsatz ist die **Zweckbindung**

- Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden, Art. 5 Abs. 1 lit. b DS-GVO
- bei Vereinen ist das regelmäßig der in der Satzung festgelegte Vereinszweck

Grundsätze für die Verarbeitung personenbezogener Daten, **Art. 5 DS-GVO**

- die Verarbeitung personenbezogener Daten muss dem Zweck angemessen und sachlich relevant und auf das notwendige Maß beschränkt sein, Art. 5 Abs. 1 lit. c DS-GVO , d.h. der Verein darf nur die Daten verarbeiten, die für die Ausübung der Mitgliedschaft relevant sind und vom Zweck des Vereins und der Satzung gedeckt sind
- z.B. darf der Sportverein das Geburtsdatum eines Mitglieds erheben oder speichern weil er wissen muss, in welcher Altersklasse ein Spieler starten darf; ob er das Geburtsdatum jedoch an eine andere Stelle übermitteln darf, ist hängt wiederum vom Zweck ab. Ggf. darf er es an den Verband übermitteln, zwecks der Zuordnung zu Altersklassen, er darf es aber nicht an einen Sponsor, zwecks zielgerichteter Werbung übermitteln

Grundsätze für die Verarbeitung personenbezogener Daten, **Art. 5 DS-GVO**

- Das bereits im Bundesdatenschutzgesetz (BDSG) verankerte Prinzip der Datensparsamkeit oder **Datenminimierung** findet sich nunmehr auch als eines der zentralen Prinzipien der DS-GVO in Art.5 Abs. 1 lit. c wieder

- Die Erhebung der Daten muss auf das für den Zweck der Datenverarbeitung notwendige Maß beschränkt sein

Grundsätze für die Verarbeitung personenbezogener Daten, **Art. 5 DS-GVO**

- Das Prinzip der **Speicherbegrenzung** ergänzt die Datensparsamkeit in zeitlicher Hinsicht, Art.5 Abs. 1 lit. e
- Daten dürfen daher nur solange gespeichert werden wie es erforderlich ist, den Speicherzweck zu erfüllen
- d.h. bei Beendigung der Vereinsmitgliedschaft ist die weitere Speicherung der Daten grds. nicht mehr erforderlich
- aus der Umsetzung dieser Prinzipien folgt auch das „Recht auf Vergessenwerden“ des Betroffenen, Art. 17 DS-GVO

Grundsätze für die Verarbeitung personenbezogener Daten, **Art. 5 DS-GVO**

- Als zentrales Prinzip des Datenschutzes wurde auch die Gewährleistung von **Integrität und Vertraulichkeit**, also die Datensicherheit gesetzlich verankert (Art. 5 Abs. 1 lit. f und Art. 32 DS-GVO)

- Daten müssen dabei in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich dem Schutz durch geeignete **technische und organisatorische Maßnahmen**, Art. 24 Abs.1 DS-GVO

Grundsätze für die Verarbeitung personenbezogener Daten, **Art. 5 DS-GVO**

- Mit dem Grundsatz der **Rechenschaftspflicht** in Art. 5 Abs. 2 DS-GVO wird der Verantwortliche stärker in die Pflicht genommen

- Das bedeutet, dass der Verantwortliche die Grundsätze aus Art. 5 DS-GVO nicht nur einhalten muss, er muss auch deren Einhaltung **nachweisen** können

Grundsätze für die Verarbeitung personenbezogener Daten, **Art. 5 DS-GVO**

- damit tragen die Verantwortlichen die **Darlegungs- und Beweislast** dafür, dass die Betroffenen in die Datenverarbeitung eingewilligt haben

- die sorgfältige **Dokumentation und Protokollierung** der Abläufe ist daher für den Verantwortlichen (Verein) unverzichtbar!

Rechtmäßigkeit der Verarbeitung personenbezogener Daten, **Art. 6 DS-GVO**

- Die Verarbeitung von personenbezogenen Daten ist nur rechtmäßig, wenn dies mit einer **Einwilligung** oder aufgrund einer anderen, in der DS-GVO **normierten Rechtsgrundlage** erfolgt, Art. 6 Abs.1 DS-GVO

Rechtmäßigkeit der Verarbeitung personenbezogener Daten, **Art. 6 DS-GVO**

- Die Voraussetzungen für eine **Einwilligung** ergeben sich aus der Begriffsbestimmung in Art.4 Nr.11 DS-GVO
- sie sind weitestgehend identisch mit den bisherigen Anforderungen (**freiwillig, zweckbestimmt und informiert**)
- Weitere Bedingungen für die wirksame Erteilung der Einwilligung sind in Art.7 und 8 DS-GVO geregelt (Nachweis, schriftliche Erklärung, Widerruf)
- z.B. Einwilligung eines Kindes erst mit 16 Jahren rechtmäßig, Art. 8 Abs.1 DS-GVO

Rechtmäßigkeit der Verarbeitung personenbezogener Daten, **Art. 6 DS-GVO**

- Die gesetzlichen Erlaubnistatbestände werden von Art. 6 Abs.1 lit. b-f DS-GVO geregelt

- ohne eine Einwilligung ist eine Datenverarbeitung z.B. dann erlaubt, wenn sie zur **Erfüllung eines Vertrages** oder eines vorvertraglichen Schuldverhältnisses mit dem Betroffenen **erforderlich** ist, Art. 6 Abs.1 lit. b DS-GVO

  z.B. Erhebung von erforderlichen Daten für die reine Mitgliedschaft im Verein, wie bisher am Vereinszweck ausgerichtet

- Diese Regelung hat im wesentlichen den gleichen Regelungsinhalt wie der bisherige § 28 Abs.1 S.1 Nr.1 BDSG „alt“

Rechtmäßigkeit der Verarbeitung personenbezogener Daten, **Art. 6 DS-GVO**

- eine weitere Rechtsgrundlage für die Verarbeitung normiert Art.6 Abs. 1 lit. f DS-GVO

- Danach ist die Verarbeitung rechtmäßig, wenn sie zur **Wahrung der berechtigten Interessen des Verantwortlichen** oder eines Dritten erforderlich ist, sofern nicht die Interessen der betroffenen Person überwiegen

Rechtmäßigkeit der Verarbeitung personenbezogener Daten, **Art. 9 DS-GVO**

- Die allg. Erlaubnisgründe aus Art. 6 DS-GVO werden bezüglich der Verarbeitung von **besonderen Kategorien personenbezogener Daten** durch Art. 9 DS-GVO modifiziert

- Die **Verarbeitung** personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung **ist untersagt**

Rechtmäßigkeit der Verarbeitung personenbezogener Daten, **Art. 9 DS-GVO**

- In Art.9 Abs.2 DS-GVO werden spezielle Rechtsgrundlagen aufgeführt, aufgrund derer eine ausnahmsweise Verarbeitung sensibler Daten möglich sein soll.

- Auch hier wurden dem nationalen Gesetzgeber wieder Gestaltungsspielräume eingeräumt, die dieser mit § 22 BDSG neu auch umgesetzt hat

- So ist die Verarbeitung z.B. dann zulässig, wenn der Betroffene ausdrücklich eingewilligt hat

Rechtmäßigkeit der Verarbeitung personenbezogener Daten, **Art. 9 DS-GVO**

- Wenn die Verarbeitung erforderlich ist um Rechte aus dem Arbeitsrecht, dem Recht der Sozialen Sicherheit und dem Sozialschutz auszuüben

- Die Verarbeitung dem Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist und die betroffene Person körperlich oder rechtlich außerstande ist ihre Einwilligung zu geben

Rechtmäßigkeit der Verarbeitung personenbezogener Daten, **Art. 9 DS-GVO**

- Die Verarbeitung zum Zwecke der Gesundheitsvorsorge oder Arbeitsmedizin, für medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich erforderlich ist

Betroffenenrechte

- In der DS-GVO werden natürlich auch die **Rechte der Betroffenen** geregelt (Art. 12 ff. DS-GVO) und modernisiert:

- Art. 12 DS-GVO stellt Anforderungen an die **Transparenz** der Informationen, an die Kommunikation und die Modalitäten für die Ausübung der Rechte der betroffenen Person

- In Art.12 Abs.3 DS-GVO ist verankert, dass der Verantwortliche der betroffenen Person die Informationen über einen Antrag zu den Art. 12ff. (Ausübung der Betroffenenrechte) **unverzüglich, spätestens aber innerhalb eines Monats** nach Eingang des Antrags zur Verfügung stellen muss

Betroffenenrechte

- Art. 15 DS-GVO regelt das **Auskunftsrecht** der betroffenen Person

- Die betroffene Person hat das Recht, eine Bestätigung zu verlangen, ob personenbezogene Daten verarbeitet werden
- Ist das der Fall, hat sie ein Recht auf Auskunft über diese Daten sowie über Informationen unter anderem über die Verarbeitungszwecke, deren Herkunft, Empfänger, über die Dauer der Speicherung sowie über ihre Rechte
- Der Verantwortliche stellt eine Kopie der personen-bezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung, Art. 15 Abs. 3 DS-GVO

Betroffenenrechte

- Die betroffene Person hat zudem das Recht, die **Berichtigung** sie betreffender unrichtiger Daten sowie im Hinblick auf den Zweck die Vervollständigung unzutreffender personenbezogener Daten zu verlangen (Art. 16 DS-GVO)

Betroffenenrechte

- Daneben hat die betroffene Person nach Art. 17 DS-GVO (mit bestimmten Ausnahmen) das Recht, die **Löschung** ihrer Daten zu verlangen – zum Beispiel wenn diese zu dem Zweck, zu dem sie ursprünglich erhoben oder verarbeitet wurden, nicht mehr erforderlich sind oder die dazu erteilte Einwilligung widerrufen wurde

Betroffenenrechte

- Als besondere Ausformung des Löschungsanspruches besteht nun auch ein „**Recht auf Vergessenwerden**“ (Art. 17 Abs. 2 DS-GVO)

- wenn die verantwortliche Stelle die zu löschenden Daten öffentlich gemacht hat, muss sie vertretbare Schritte unternehmen, um die Stellen, die diese Daten verarbeiten, zu informieren, dass die betroffene Person von ihnen die Löschung aller Links zu diesen Daten oder von Kopien oder Replikationen verlangt.

Betroffenenrechte

- Der Verantwortliche hat eine **Mitteilungspflicht** und muss grundsätzlich allen Empfängern der Daten jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitteilen (Art. 19 DS-GVO)

- Ähnlich wie das Recht auf Vergessenwerden knüpft diese Verpflichtung an eine vorangegangene Übermittlungen an konkrete Empfänger an.

Betroffenenrechte

- Nach Art. 21 Abs. 1 DS-GVO hat jeder das Recht, aus Gründen, die sich aus seiner besonderen Situation ergeben, jederzeit gegen eine Verarbeitung seiner Daten oder Profilerstellung **Widerspruch** einzulegen (allgemeines Widerspruchsrecht)

- Diesem Widerspruch ist vom Verantwortlichen grundsätzlich nachzukommen

Pflichten des Verantwortlichen

- Adressat der Pflichten aus der DS-GVO ist der für die Verarbeitung **Verantwortliche**

- Eine Definition findet sich in Art. 4 Nr. 7 DS-GVO,

  „…natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle die …über die Zwecke und Mittel der Verarbeitung entscheidet“

Der Verein ist daher Verantwortlicher im Sinne der DS-GVO.

Pflichten des Verantwortlichen

- Die Datenschutz-Grundverordnung stellt insbesondere die Bedeutung des technischen und organisatorischen Datenschutzes heraus, dem der Verantwortliche nachkommen muss, hierzu zählen die Regelungen zu:

- Privacy by Design und Privacy by Default, also Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, (Art. 25 DS-GVO);

Pflichten des Verantwortlichen

- zur Auftragsverarbeitung, (Art. 28 DS-GVO);
- Zum Verzeichnis von Verarbeitungstätigkeiten, (Art.30 DS-GVO)
- Zur Sicherheit der Verarbeitung (Art.32 DS-GVO)
- zur Meldung über Datenschutzverletzungen,(Art. 33f. DS-GVO);
- zur Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) und
- zum betrieblichen Datenschutzbeauftragten (Art. 37 DS-GVO)

Pflichten des Verantwortlichen

insbesondere folgende Pflichten des Verantwortlichen sind in diesem Zusammenhang besonders zu beleuchten:

- Datenschutz durch Technikgestaltung und Voreinstellung,
- Dokumentationspflichten,
- Datensicherheitsmaßnahmen,
- Meldepflichten,
- die Datenschutzfolgeabschätzung und die
- Bestellung eines Datenschutzbeauftragten
- Auftragsdatenverarbeitung

Pflichten des Verantwortlichen

<u>Datenschutz durch Technikgestaltung:</u>

- Der Verantwortliche muss technische und organisatorische Schutzmaßnahmen treffen und damit sicherstellen, dass die personenbezogenen Daten rechtmäßig verarbeitet werden , Art.5 DS-GVO

Pflichten des Verantwortlichen

- Gemäß Art. 25 DS-GVO muss der Verantwortliche sicherstellen, dass Standardeinstellungen darauf ausgerichtet sind, nur personenbezogene Daten zu verarbeiten, die für den konkreten Zweck auch erforderlich sind (privacy by design and by default)

- Das betrifft den Umfang der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit

- Der Verein hat daher dafür zu sorgen, dass technische und organisatorische Maßnahmen ergriffen werden, z.B. Pseudonymisierung und Verschlüsselung, die geeignet sind die datenschutzrechtlichen Grundsätze umzusetzen (Art.32 DS-GVO)

Pflichten des Verantwortlichen

Dokumentationspflichten:

- Der Verantwortliche muss in einem Verzeichnis sämtliche seiner Verarbeitungstätigkeiten dokumentieren, Art.30 DS-GVO
- Dieses Verzeichnis muss er der Aufsichtsbehörde jederzeit auf deren Anfrage zur Verfügung stellen
- Um den jeweiligen Verantwortlichen diese Pflicht zu erleichtern, wird es dazu ein gemeinsames Formular und ein umfangreiches Hinweisblatt der Datenschutzbehörden geben

- Darüber hinaus bestehen allerdings weitere Pflichten, z.B. Dokumentation von Datenschutzverletzungen, Nachweis hinsichtlich der erteilten Einwilligungserklärungen usw.

Pflichten des Verantwortlichen

Datensicherheitsmaßnahmen

- Nach Art. 32 DS-GVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten

Diese Maßnahmen schließen unter anderem Folgendes ein:

- Die Pseudonymisierung und Verschlüsselung personenbezogener Daten,
- Die Fähigkeit , die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen,

Pflichten des Verantwortlichen

- Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen und technischen Zwischenfall rasch wiederherzustellen

- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Pflichten des Verantwortlichen

Meldungen über Datenschutzverletzungen, Art. 33f. DS-GVO:

- Gemäß Art. 33f. DS-GVO müssen Verletzungen des Schutzes personenbezogener Daten unverzüglich, nach Möglichkeit innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls, an die zuständige Aufsichtsbehörde gemeldet werden

- eine Ausnahme besteht, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten des Betroffenen führt. (vgl. Art. 33 Abs. 1 DS-GVO)

Pflichten des Verantwortlichen

- Weiterhin müssen die Betroffenen darüber informiert werden, Art. 34 DS-GVO, wenn ein hohes Risiko für die Verletzung ihrer persönlichen Rechte und Freiheiten besteht

- Die Benachrichtigungspflicht besteht auch dann, wenn bei sensiblen Daten (u.a. Gesundheitsdaten, Daten zur Religionszugehörigkeit) Datenschutzverletzungen begangen worden sind

- (hier z.B. Datenschutzverletzung bezüglich der immer wieder gerne angeforderten Geburtsurkunden von Spielern, aus denen auch die Religionszugehörigkeit hervorgeht)

- Der Verantwortliche muss die Datenschutzverletzungen, die Auswirkungen und die ergriffenen Maßnahmen **dokumentieren**, Art.33 Abs. 5 DS-GVO

Pflichten des Verantwortlichen

Datenschutzfolgeabschätzung, Art. 35 DS-GVO

- Diese ist stets erforderlich, wenn eine Form der Datenverarbeitung voraussichtlich zu einem hohen Risiko für den Betroffenen führt, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung

- Der Verantwortliche hat daher vorab eine Abschätzung der Folgen für den Schutz der personenbezogenen Daten durchzuführen

Pflichten des Verantwortlichen

- Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungs-vorgänge, für die gemäß Art. 35 Abs.1 DS-GVO eine Datenschutzfolgeabschätzung (DSFA) verpflichtend durchzuführen ist.

- Diese Liste wird derzeit gemeinsam durch die Datenschutzbehörden aller Bundesländer erstellt und rechtzeitig vor Geltung der DS-GVO veröffentlicht werden.

Pflichten des Verantwortlichen

<u>betrieblicher/behördlicher Datenschutzbeauftragter (Art. 37 DS-GVO):</u>

- Nach Art. 37 Abs. 1 DS-GVO müssen in drei Fällen interne Datenschutzbeauftragte bestellt werden

- öffentliche Stellen haben, sofern sie personenbezogene Daten verarbeiten, stets einen Datenschutzbeauftragten zu bestellen

Pflichten des Verantwortlichen

- Nicht-öffentliche Stellen (wozu auch Vereine gehören), haben einen Datenschutzbeauftragten zu bestellen, wenn:

- deren Kerntätigkeit in einer Datenverarbeitung besteht, die aufgrund ihres Zwecks oder ihres Umfangs eine umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen erfordert oder

- eine umfangreiche Verarbeitung von Daten, die nach Art. 9 oder 10 DS-GVO besonders schutzwürdig sind, umfasst (u.a. Gesundheitsdaten)

Pflichten des Verantwortlichen

- Die DS-GVO erlaubt zudem, dass die Mitgliedstaaten im nationalen Recht für weitere Fälle die Bestellung eines Datenschutzbeauftragten vorschreiben können
- Hiervon hat der Bundesgesetzgeber durch § 38 Abs. 1 BDSG neu Gebrauch gemacht
- Danach werden nichtöffentliche Stellen auch künftig einen Datenschutzbeauftragten zu bestellen haben, wenn in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind

Pflichten des Verantwortlichen

- Im Verein zählen zu diesen Personen grundsätzlich alle ehrenamtlich Tätigen, also Übungsleiter, Vorstände, Kassenwart usw. , die Zugriff auf personenbezogene Daten haben

- Kleine Vereine, die dieser Pflicht dann unterliegen, können daher auch einen gemeinsamen Datenschutzbeauftragten ernennen, d.h. sie teilen sich entweder einen Externen Beauftragten, der in keinem Verein tätig ist, oder der interne DSB eines Vereins wird für die anderen Vereine als deren externer DSB tätig.

Pflichten des Verantwortlichen

<u>Auftragsverarbeitung, Art. 28 DS-GVO:</u>

- Der Auftragsverarbeiter ist in Art.28 DS-GVO geregelt und wird gem. Art. 4 Nr. 8 DS-GVO definiert als:

„eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.“

- orientiert sich daher am bisherigen § 11 BDSG

- der Begriff des Auftragnehmers ist daher an den bisherigen Kriterien, Weisungsgebundenheit des Auftragnehmers und Entscheidungshoheit des Auftraggebers, zu beurteilen

Effektive Durchsetzung

- Effektiver Datenschutz erfordert auch die Möglichkeit einer effektiven Durchsetzung
- Die Datenschutz-Grundverordnung sieht im Vergleich zur Datenschutzrichtlinie umfangreichere Befugnisse für die Datenschutzaufsichtsbehörden vor
- Zudem werden die Sanktionsmöglichkeiten der Aufsichtsbehörden ausgedehnt

Effektive Durchsetzung

- die so erweiterten Befugnisse werden ebenfalls durch eine spürbare Ausweitung des Bußgeldrahmens begleitet (Art. 83 DS-GVO)

- So sind für bestimmte Rechtsverstöße Bußgelder bis zu 4 % des Jahresumsatzes eines Unternehmens, beziehungsweise 20 Mio. Euro, zulässig

Fazit

- Die DS-GVO behält viele Grundsätze des bisherigen BDSG bei

- Für den Verantwortlichen bestehen aber erhöhte Informations- und Mitteilungspflichten gegenüber den Betroffenen, aus deren Nichtbeachtung eine rechtswidrige Datenverarbeitung resultieren kann und diese Verletzungen auch bußgeldbewehrt sind

- Weiterhin besteht eine Rechenschaftspflicht des Verantwortlichen, aufgrund derer er verpflichtet ist, verschiedene Nachweise und Dokumentationen zu erbringen, z.B. über erteilte Einwilligungen u.a.

Und das soll´s gewesen sein…

Leopoldina
Nationale Akademie
der Wissenschaften

Leopoldina-Symposium
Die Digitalisierung und ihre Auswirkungen
auf Mensch und Gesellschaft

Quelle: Leopoldina Nationale Akademie der Wissenschaften, Veranstaltung „Die Digitalisierung und ihre Auswirkungen auf Mensch und Gesellschaft“

Michal Kosinski - Schafft Digitalisierung eine eigene Dynamik in der Meinungsbildung?

Und das soll´s gewesen sein…

Ich bedanke mich für Ihre Aufmerksamkeit!