

Kontakt und Herausgeber:

Unabhängiges Datenschutzzentrum Saarland

Die Landesbeauftragte für Datenschutz und
Informationsfreiheit

Postfach 10 26 31
66026 Saarbrücken

Fritz-Dobisch-Straße 12
66111 Saarbrücken

Telefon 0681 94781 0

Telefax 0681 94781 29

E-Mail poststelle@datenschutz.saarland.de

Internet www.datenschutz.saarland.de



Inhalt

Datenschutz im Verein.....	4
1. Was ändert sich für Vereine?.....	5
2. Was sind personenbezogene Daten und was ist unter Datenverarbeitung zu verstehen?	6
3. Was haben Vereine im Umgang mit personenbezogenen Daten künftig zu beachten?.....	7
3.1 Datenschutzrechtliche Grundsätze bei der Verarbeitung personenbezogener Daten, Art. 5 DS-GVO ..	7
3.2 Transparenzpflichten	9
3.3 Technisch-organisatorischer Datenschutz	10
4. Wie sollten Vereine vorgehen?.....	12
4.1 Ist-Analyse.....	12
4.2 Informationspflichten nach Art. 13 und 14 DS-GVO	12
4.3 Bearbeitung von Auskunftersuchen.....	13
4.4 Erstellung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DS-GVO	13
4.5 Aufnahme datenschutzspezifischer Regelungen in die Vereinssatzung oder Erstellung einer Datenschutzordnung	14
5. Was ist darüber hinaus noch zu berücksichtigen?.....	15
5.1 Meldung von Datenschutzpannen	15
5.2 Datenschutz-Folgenabschätzung in Sonderfällen	15
5.3 Bestellung eines Datenschutzbeauftragten	15
5.4 Auftragsverarbeitungsverträge.....	16
5.5 Haftung und Sanktionen.....	16
Weitere Informationen.....	17

Datenschutz im Verein

Am 25. Mai 2018 löst die Europäische Datenschutz-Grundverordnung (DS-GVO) das Bundesdatenschutzgesetz (BDSG) in der bis dahin geltenden Fassung ab, mit der Konsequenz, dass auch Vereine die Prozesse der Verarbeitung personenbezogener Daten an die Vorgaben der DS-GVO und der ergänzend dazu erlassenen Vorschriften der ab Mai 2018 gültigen Fassung des BDSG (2018) anpassen müssen.

Aus diesem Grund möchten wir Ihnen die wesentlichen Neuregelungen zusammengefasst darstellen, damit Sie deren Vorgaben in Ihrem Verein zeitnah umsetzen können. Es soll zum einen aufgezeigt werden, welche personenbezogenen Daten Sie für vereinspezifische Zwecke verarbeiten dürfen, und zum anderen, welche formalen Anforderungen nunmehr zu erfüllen sind.

Unabhängiges Datenschutzzentrum Saarland

Saarbrücken, im März 2018

1. Was ändert sich für Vereine?

Auch wenn vieles aus dem bisher geltenden BDSG übernommen wurde, wird es mit der DS-GVO einige Änderungen geben, die die Vereine als sog. nicht-öffentliche Stellen umsetzen müssen. Als für die Vereine wesentliche Änderung ist die Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO zu nennen. Danach sind die datenverarbeitenden Stellen insbesondere verpflichtet, die Rechtmäßigkeit der Datenverarbeitung und die Einhaltung der datenschutzrechtlichen Grundsätze nachweisen zu können. Dies erfordert nicht nur eine grundlegende Überprüfung der bisherigen Datenverarbeitungsprozesse, sondern bringt vor allem umfangreichere Dokumentationspflichten mit sich. Mit der DS-GVO werden außerdem die Rechte der von der Datenverarbeitung Betroffenen (insbes. Mitglieder) gestärkt, indem u.a. die Informationspflichten der datenverarbeitenden Stellen ausgeweitet werden.

Neuerungen in der Übersicht:

- *Neuer Rechtsrahmen mit Wirksamwerden der DS-GVO*
- *Rechenschaftspflicht*
- *Umfangreichere Dokumentationspflichten*
- *Ausweitung der Informationspflichten*
- *Höhere Bußgelder*

2. Was sind personenbezogene Daten und was ist unter Datenverarbeitung zu verstehen?

Personenbezogene Daten sind neben den identifizierenden Angaben einer Person wie Name und Anschrift auch sämtliche Informationen, die etwas über die persönlichen oder sachlichen Verhältnisse eines Betroffenen aussagen, beispielsweise Kontodaten, Funktion im Verein etc.

Unter Datenverarbeitung ist jeder Umgang mit personenbezogenen Daten, wie z.B. das Erheben, die Speicherung, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung sowie das Löschen gemeint (Art. 4 Abs. 2 DS-GVO). Vereine verarbeiten regelmäßig personenbezogene Daten ihrer Mitglieder und ggf. auch sonstiger Personen.

Beispiele für die Verarbeitung personenbezogener Daten durch Vereine:

- *Abbuchung von Mitgliedsbeiträgen*
- *Einladung zur Mitgliederversammlung*
- *Veröffentlichung von Wettkampfergebnissen*
- *Weitergabe von Mitgliedsdaten an übergeordnete Verbände*
- *Zusammenarbeit mit Sponsoren*

3. Was haben Vereine im Umgang mit personenbezogenen Daten künftig zu beachten?

3.1 Datenschutzrechtliche Grundsätze bei der Verarbeitung personenbezogener Daten, Art. 5 DS-GVO

Die DS-GVO schreibt im Wesentlichen die bisherigen Grundprinzipien des Datenschutzes fort und entwickelt sie weiter.

Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 DS-GVO:

- *Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz ✓*
- *Zweckbindung ✓*
- *Datenminimierung ✓*
- *Richtigkeit ✓*
- *Speicherbegrenzung ✓*
- *Integrität und Vertraulichkeit ✓*

Jede Datenverarbeitung bedarf entweder der Einwilligung der betroffenen Person oder einer sonstigen gesetzlichen Ermächtigungsgrundlage (**Rechtmäßigkeit der Datenverarbeitung**, Art. 6 DS-GVO).

Die im unmittelbaren Zusammenhang mit einer Vereinsmitgliedschaft stehende Verarbeitung personenbezogener Daten wird regelmäßig auch ohne die ausdrückliche Einwilligungserklärung der Betroffenen auf Grundlage des **Mitgliedschaftsverhältnisses** und damit aufgrund eines vertragsähnlichen Verhältnisses nach Art. 6 Abs. 1 Buchst. b DS-GVO rechtmäßig erfolgen können.

Zulässig ist beispielsweise die Verarbeitung von Vor- und Zuname, Anschrift und Kontodaten für die Mitgliederverwaltung und für die Abbuchung der Mitgliedsbeiträge.

Erfolgt die Datenverarbeitung außerhalb des mitgliedschaftlichen Verhältnisses, ist zu prüfen, ob die Verarbeitung zur Erfüllung einer **rechtlichen Verpflichtung**, der der Verein unterliegt, erforderlich ist (Art. 6 Abs. 1 Buchst. c DS-GVO, beispielsweise Aufbewahrungsfristen nach Handels- und Steuerrecht).

Die Verarbeitung kann gegebenenfalls auch im **berechtigten Interesse** des Vereins oder eines Dritten nach Art. 6 Abs. 1 Buchst. f DS-GVO erforderlich sein. In diesem Zusammenhang sind die Interessen des Vereins gegen die schutzwürdigen Interessen der Betroffenen abzuwägen, wobei insbesondere auf die vernünftigen Erwartungen der betroffenen Personen abzustellen ist.

Beispielsweise ist vor einer beabsichtigten Weitergabe von Daten eines Vereinsmitglieds an einen übergeordneten Verband im Rahmen der Interessenabwägung zu berücksichtigen, ob eine solche Datenübermittlung beim Vereinseintritt bereits absehbar war (gegebenenfalls durch einen Hinweis in der Vereinssatzung o.ä.).

Die Datenverarbeitung ist grundsätzlich auch dann datenschutzrechtlich zulässig, wenn der Betroffene seine **Einwilligung** hierzu wirksam erteilt hat (Art. 7 DS-GVO), das bedeutet, die Erklärung muss ohne Zwang abgegeben werden und der Betroffene muss über den Zweck der Datenverarbeitung und über die Möglichkeit, die Einwilligung jederzeit widerrufen zu können, informiert werden. Die datenverarbeitende Stelle muss den Nachweis einer wirksam abgegebenen Einwilligung im Rahmen ihrer Dokumentationspflichten sicherstellen, weshalb die Einholung einer schriftlichen oder elektronischen Erklärung empfehlenswert ist.

Besondere Kategorien personenbezogener Daten - wie beispielsweise Gesundheitsdaten, politische Meinungen etc. - dürfen grundsätzlich nur aufgrund einer Einwilligung oder aufgrund einer ausdrücklichen gesetzlichen Befugnis verarbeitet werden (Art. 9 Abs. 1 und 2 DS-GVO, § 22 BDSG (2018)).

Erfolgt eine Datenverarbeitung im Rahmen eines **Beschäftigungsverhältnisses** (z.B. Vertragsamateure im sportlichen Bereich, Verwaltungsmitarbeiter), dürfen auf der Grundlage von § 26 BDSG (2018) die zur Begründung, Durchführung und Beendigung des Arbeitsverhältnisses erforderlichen personenbezogenen Daten des Beschäftigten verarbeitet werden.

Darüber hinaus sind bei jeder Datenverarbeitung weitere datenschutzrechtliche Grundsätze zu beachten. So dürfen Daten grundsätzlich nur zu dem Zweck verarbeitet werden, zu dem sie erhoben worden sind (**Zweckbindungsgrundsatz**). Die Zwecke der Datenverarbeitung sind dabei im Vorfeld der Verarbeitung konkret in einem **Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO)** zu dokumentieren, um eine objektive Überprüfung der Datenverarbeitung zu ermöglichen. Personenbezogene Daten sind außerdem auf das für die Zweckerreichung erforderliche Maß zu beschränken (**Datenminimierung**).

3.2 Transparenzpflichten

Ein weiterer zentraler Aspekt der DS-GVO sind die in Art. 12 ff. DS-GVO aufgeführten **Informations- und Auskunftspflichten** der datenverarbeitenden Stelle. Der Umfang der Informationspflicht bei der Erhebung personenbezogener Daten unmittelbar bei der betroffenen Person richtet sich nach Art. 13 DS-GVO. Wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben worden sind, richtet sich die Informationspflicht nach Art. 14 DS-GVO.

Informationspflichten nach Art. 13 DS-GVO

- *Name und Kontaktdaten des Verantwortlichen und des Vertreters*
- *Ggf. Kontaktdaten des Datenschutzbeauftragten*
- *Zwecke der Datenverarbeitung und Rechtsgrundlage*
- *Berechtigte Interessen nach Art. 6 Abs. 1 Satz 1 Buchst. f*
- *Empfänger oder Kategorien von Empfängern*
- *Drittstaatstransfer*
- *Speicherdauer*
- *Auskunftsanspruch (Art. 15), Berichtigung (Art. 16), Löschung (Art. 17 Abs. 1), Einschränkung der Verarbeitung (Art. 18), Widerspruch (Art. 21), Datenübertragbarkeit (Art. 20)*
- *Widerruf der Einwilligung*
- *Beschwerderecht*
- *Pflicht zur Bereitstellung der Daten*
- *Automatisierte Entscheidungsfindung*

Darüber hinaus haben die Vereinsmitglieder und sonstigen Betroffenen nach Art. 15 DS-GVO einen Auskunftsanspruch gegenüber dem Verein hinsichtlich des Umgangs mit ihren personenbezogenen Daten.

Dabei sieht Art. 12 Abs. 1 DS-GVO vor, dass alle Informationen und Mitteilungen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung zu stellen sind.

3.3 Technisch-organisatorischer Datenschutz

Um sicherstellen und nachweisen zu können, dass die Datenverarbeitung rechtmäßig erfolgt, muss der Verein nach Art. 24 DS-

GVO unter Berücksichtigung der Art, des Umfangs, der Umstände, der Zwecke der Verarbeitung, der Eintrittswahrscheinlichkeit und der Risiken für die Betroffenenrechte **technische und organisatorische Maßnahmen** umsetzen. Daneben sind die in Art. 32 Abs. 1 DS-GVO aufgezählten Maßnahmen zu ergreifen, um ein angemessenes Schutzniveau zu gewährleisten. Zugriff auf die einzelnen Datenkategorien darf außerdem nur denjenigen Vereinsmitgliedern eingeräumt werden, die die jeweiligen Daten zur Erledigung der ihnen übertragenen Aufgaben benötigen (z.B. sollte Zugriff auf Kontendaten lediglich der Kassenwart haben).

Maßnahmen nach Art. 32 Abs. 1 DS-GVO

- *Pseudonymisierung und Verschlüsselung personenbezogener Daten*
- *Dauerhafte Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit*
- *Wiederherstellung von Verfügbarkeit bei Zwischenfall*
- *Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen*

4. Wie sollten Vereine vorgehen?

4.1 Ist-Analyse

Zuerst sollten Sie sich im Rahmen einer **Bestandsaufnahme** einen Überblick verschaffen, welche Daten von welchen Personenkategorien Sie mit welcher Zwecksetzung verarbeiten und an welche (dritten) Stellen Sie diese Daten mit welcher Zielsetzung übermitteln.

Da auch nach der DS-GVO für die Verarbeitung personenbezogener Daten eine Rechtsgrundlage erforderlich ist, ist zu prüfen, ob alle (bisherigen) Datenverarbeitungsprozesse von einer Ermächtigungsgrundlage abgedeckt sind oder ob Sie für die einzelnen Verarbeitungsvorgänge die Einwilligung der Betroffenen benötigen.

Hierbei ist es keinesfalls ratsam, für sämtliche Verarbeitungsvorgänge vorsorglich Einwilligungserklärungen einzuholen, da die Einwilligungen jederzeit widerrufen werden können. Die Verarbeitung personenbezogener Daten zur Mitgliederverwaltung und -betreuung wird überwiegend auf Grundlage des Art. 6 Abs. 1 Buchst. b DS-GVO zulässig sein. Bei der Datenübermittlung an Dritte werden Sie jedoch regelmäßig dann eine Einwilligung benötigen, wenn dies mit den eigentlichen Zwecken der Datenverarbeitung des Vereins nicht in Einklang gebracht werden kann (beispielsweise Weitergabe für Werbezwecke).

4.2 Informationspflichten nach Art. 13 und 14 DS-GVO

Um den Informationspflichten nach Art. 13 DS-GVO nachzukommen, sollten die **Aufnahmeanträge** des Vereins für Neumitglieder entsprechend angepasst werden. Vor dem Hintergrund, dass sich die Informationspflichten im Vergleich zur noch geltenden Rechtslage erweitert haben (insbesondere die Angaben nach Art. 13 Abs. 2 DS-GVO treten nunmehr hinzu), sollten die Bestandsmitglieder vor Wirksamwerden der DS-GVO

ebenfalls informiert werden, wobei sich hier auch eine entsprechende Veröffentlichung auf der vereinseigenen **Webseite** bzw. eine Information per E-Mail oder auf dem Schriftweg empfiehlt. Verarbeitet der Verein Daten, die er nicht bei den Mitgliedern selbst, sondern bei Dritten erhoben hat, sind darüber hinaus die **erweiterten Informationspflichten nach Art. 14 DS-GVO** zu beachten.

4.3 Bearbeitung von Auskunftersuchen

Ebenso sollten organisatorische Vorkehrungen getroffen werden, um entsprechenden Auskunftersuchen von Vereinsmitgliedern und sonstigen Betroffenen nach Art. 15 DS-GVO in einer angemessenen Bearbeitungszeit gerecht werden zu können. Dies betrifft u.a. die Festlegung von Zuständigkeiten für die Bearbeitung sowie die Erstellung von Mustervorlagen.

4.4 Erstellung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DS-GVO

In dem Verzeichnis von Verarbeitungstätigkeiten sind insbesondere die Zwecke der Verarbeitung und eine Beschreibung der Kategorien der verarbeiteten personenbezogenen Daten, der betroffenen Personen und der Empfänger aufzunehmen. Dabei sind sämtliche Verarbeitungstätigkeiten getrennt voneinander zu betrachten. Beispielsweise stellen die Mitgliederverwaltung, der Wettkampfbetrieb oder die Pressearbeit jeweils eigene Verarbeitungstätigkeiten dar. So kann für die Mitgliederverwaltung die Verarbeitung von Name, Anschrift und Kontodaten des Mitglieds erforderlich sein, wohingegen es bei der Veröffentlichung von Wettkampfergebnissen regelmäßig ausreichend sein kann, den Namen sowie das erzielte Ergebnis zu verarbeiten.

Da die meisten Vereine regelmäßig personenbezogene Daten verarbeiten (z.B. Abbuchung der Mitgliedsbeiträge, Einladung zur Mitgliederversammlung etc.), ist die Führung eines Ver-

zeichnisses von Verarbeitungstätigkeiten im Regelfall verpflichtend (Art. 30 Abs. 5 DS-GVO). Das Verzeichnis muss intern vorgehalten und der Aufsichtsbehörde auf Verlangen vorlegt werden können.

Eine **Mustervorlage** kann auf unserer Internetseite heruntergeladen werden.

4.5 Aufnahme datenschutzspezifischer Regelungen in die Vereinssatzung oder Erstellung einer Datenschutzordnung

Daneben ist es zweckdienlich, die datenschutzrechtlich relevanten Datenverarbeitungsvorgänge des Vereins in textlicher Form in der **Vereinssatzung** oder in einer separaten **Datenschutzordnung** präzise festzuhalten. So sollte dargestellt werden, welche Daten zu welchem Zweck von wem an welche (dritte) Stellen übermittelt werden dürfen, welche Personen auf welche Datenkategorien Zugriff haben und unter welchen Voraussetzungen eine Datenverarbeitung zulässig erfolgen kann.

5. Was ist darüber hinaus noch zu berücksichtigen?

5.1 Meldung von Datenschutzpannen

Datenschutzpannen wie Datenlecks, Hacking, gestohlene oder verlorengegangene Datenträger sind unverzüglich und möglichst innerhalb von 72 Stunden nach Bekanntwerden der Aufsichtsbehörde, im Saarland also dem Unabhängigen Datenschutzzentrum Saarland, zu melden (Art. 33 Abs. 1 DS-GVO). Eine entsprechende Mustervorlage, welche den inhaltlichen Vorgaben des Abs. 3 Rechnung trägt, sollte vereinsintern abgestimmt werden, ebenso der Prozess der Meldung sowie die dafür verantwortliche Person im Verein. Die hierbei bestehenden Dokumentationspflichten nach Abs. 5 sind ebenfalls zu beachten. Art. 34 DS-GVO legt fest, unter welchen Voraussetzungen darüber hinaus die Betroffenen zu benachrichtigen sind.

5.2 Datenschutz-Folgenabschätzung in Sonderfällen

Sind besonders risikoreiche Datenverarbeitungen durch den Verein vorgesehen, ist im Vorfeld eine sog. Datenschutzfolgenabschätzung nach Art. 35 DS-GVO durchführen. Dies ist u.a. bei einer umfangreichen Verarbeitung von besonderen Kategorien personenbezogener Daten (Gesundheitsdaten, politische Meinungen, religiöse Überzeugungen oder die Gewerkschaftszugehörigkeit) der Fall.

5.3 Bestellung eines Datenschutzbeauftragten

Besteht die Kerntätigkeit des Vereins in der umfangreichen Verarbeitung besonders sensibler Daten (beispielsweise Selbsthilfvereine) oder sind zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt, so

ist die Bestellung eines (internen oder externen) Datenschutzbeauftragten (Art. 37 DS-GVO, § 38 BDSG (2018)) verpflichtend. Der Datenschutzbeauftragte handelt im Rahmen seiner Zuständigkeiten weisungsfrei und ist unmittelbar dem Vorstand zugeordnet. Die Kontaktdaten des Datenschutzbeauftragten sind zu veröffentlichen und dem Unabhängigen Datenschutzzentrum Saarland mitzuteilen.

Ein entsprechendes Online-Meldeformular wird ab Geltung der DS-GVO auf unserer Internetseite zur Verfügung stehen.

5.4 Auftragsverarbeitungsverträge

Sofern der Verein personenbezogene Daten im Auftrag durch Dritte verarbeiten lässt (beispielsweise Mitgliederverwaltung unter Nutzung einer Cloud-Lösung), muss zwischen dem Verein und dem Dritten als Auftragnehmer ein Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO geschlossen werden. Besonderheiten können gelten, wenn der Auftragnehmer seinen Sitz außerhalb der Europäischen Union hat.

5.5 Haftung und Sanktionen

Da Verstöße gegen die Bestimmungen der DS-GVO, seien es nun unrechtmäßige Datenverarbeitungen oder die Nichtbeachtung der Dokumentations- oder Informationspflichten, Schadensersatzansprüche von Betroffenen nach sich ziehen und mit Bußgeldern geahndet werden können (Art. 82 und 83 DS-GVO), sollten die Prozesse in den Vereinen bis zum 25. Mai 2018 an die neuen gesetzlichen Vorgaben angepasst werden.

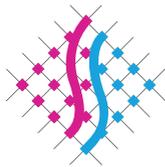
Weitere Informationen

Die Aufsichtsbehörden befassen sich aktuell mit den neuen Rechtsgrundlagen und stimmen eine einheitliche Sichtweise ab. Daraus resultierend veröffentlicht die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) abgestimmte Mustervorlagen sowie Kurzpapiere mit Auslegungshilfen zur DS-GVO, die neben sonstigen weiterführenden Informationen auf unserer Internetseite unter:

→ <https://datenschutz.saarland.de>

unter den Rubriken „Themen > Vereine“ sowie im Bereich „DS-Grundverordnung“ abgerufen werden können.

Kontakt und Herausgeber:



UNABHÄNGIGES DATENSCHUTZ ZENTRUM SAARLAND

Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Fritz-Dobisch-Straße 12
66111 Saarbrücken

Telefon 0681 94781 0
Telefax 0681 94781 29
E-Mail poststelle@datenschutz.saarland.de
Internet www.datenschutz.saarland.de

