DSGVO für Vereine

Einführung in die datenschutzrechtlichen Pflichten eines Vereins

Disclaimer

Der folgende Vortrag stellt KEINE Rechtsdienstleistung nach dem Rechtsdienstleistungsgesetz dar, da er sich mit dem Thema des Datenschutz nur auf allgemeiner Ebene befasst.

Sollten Sie Zweifel oder konkrete Datenschutzprobleme haben wenden Sie sich bitte an einen Rechtsanwalt.

Wir sind KEINE Juristen! Bloß Jurastudenten.

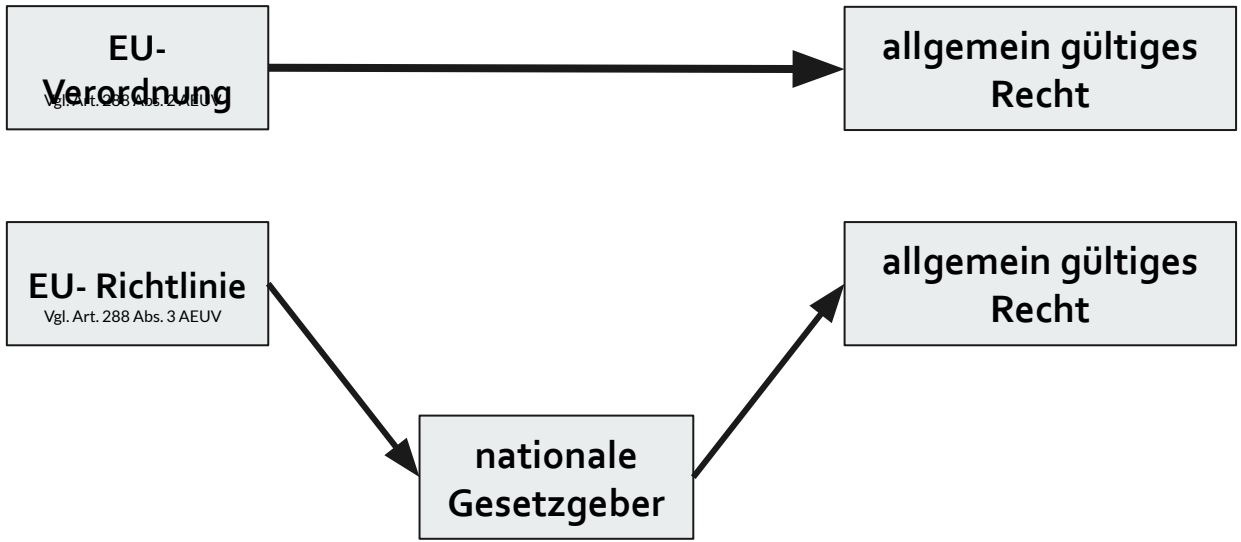
Eine (unentgeltliche, einzelfallbezogene) Rechtsdienstleistung wäre uns als Studierenden nach § 6 RDG untersagt.

Zudem garantieren wir nicht die Vollständigkeit oder Richtigkeit der Angaben. Trotzdem wurde der Vortrag nach bestem Wissen und Gewissen erstellt.

Überblick

Überblick: Grundlegendes

Was ist eine Verordnung?



Ab wann gilt die Verordnung?

Art. 99 DSGVO: Inkrafttreten und Anwendung

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

(2) Sie gilt ab dem 25. Mai 2018.

Anwendungsbereich: Vereine betroffen?

Art. 2 DSGVO: Sachlicher Anwendungsbereich

(1) Diese Verordnung gilt für die ganz oder teilweise **automatisierte Verarbeitung personenbezogener Daten** sowie für die **nichtautomatisierte Verarbeitung personenbezogener Daten**, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

DSGVO greift bei automatisierter Verarbeitung personenbezogener Daten ohne Einschränkungen!

➔ Für die Automatisierung reicht es, wenn auch nur eine Funktion des Verarbeitungsvorgangs durch Informationstechnik ohne menschliches Zutun unterstützt wird!

Beispiele:

- Digital gespeichertes Mitgliederverzeichnis (Suche erfolgt automatisch!)
- Automatisiertes Inhaltsverzeichnis für Papierakten

Anwendungsbereich: Vereine betroffen?

Art. 2 DSGVO: Sachlicher Anwendungsbereich

(1) Diese Verordnung gilt für die ganz oder teilweise **automatisierte Verarbeitung personenbezogener Daten** sowie für die **nichtautomatisierte Verarbeitung personenbezogener Daten**, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

DSGVO greift bei nichtautomatisierter Verarbeitung personenbezogener Daten NUR, wenn die personenbezogenen Daten in einem Dateiensystem gespeichert werden sollen.

➔ **Definiert in Art. 4 Nr. 6 DSGVO:** Strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind.

Beispiele:

- Papierakten in einem schriftlich geführten Register
- NICHT: Papierakten ohne jegliche Sortierung / System

Anwendungsbereich: Vereine betroffen?

Merken Sie sich also:

➔ Die DSGVO findet Anwendung **bei jeglicher Verarbeitung von personenbezogenen Daten**, außer bei Papierakten ohne jegliche Struktur und System.

Anwendungsbereich: Personenbezogene Daten

Art. 4 Nr. 1 DSGVO: Begriffsbestimmung

Nr.1 „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

Personenbezogene Daten = Alle Informationen, die sich auf eine identifizierbare Person beziehen

Beispiele:

- Name
- Anschrift
- Telefonnummer
- E-Mail
- Foto
- Personenbeschreibung
- Mitgliedsnummer

➔ Eine direkte Identifizierbarkeit ist nicht nötig. Es reicht aus, wenn die Informationen erst mit dem Wissen Dritter auf eine Person zurückzuführen sind und der Verein dieses Drittwissen vernünftigerweise einsetzen kann.

Anwendungsbereich: Verarbeiten

Art. 4 Nr. 2 DSGVO: Begriffsbestimmung

Nr.2 „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung

Verarbeiten = Im Grunde ALLES was man mit personenbezogenen Daten machen kann.

Beispiele im Vereinsleben:

- Lohnabrechnung
- Mitgliederverwaltung
- Betrieb der Webseite des Sportvereins
- Veröffentlichung von Mitgliederfotos auf der eigenen Webseite
- Beitragsverwaltung

Anwendungsbereich: Vereine betroffen?

Merken Sie sich also:

➔ Die DSGVO findet Anwendung bei jeglicher **Verarbeitung von personenbezogenen Daten**, außer bei Papierakten, ohne jegliche Struktur und System.

- ➔ Personenbezogene Daten sind alle Informationen, die auf eine identifizierbare Person beziehen
- ➔ Verarbeiten ist alles, was man mit Daten so macht

} **Anwendungsbereich riesig!**

Überblick: Rechtmäßigkeit einer Verarbeitung personenbezogener Daten

Worauf?

Rechtsgrundlage (vgl. Art. 6 DSGVO)

Wie?

- Verarbeitung nach Treu und Glauben und Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit der Daten
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

(vgl. Art. 5 DSGVO)

Rechtsgrundlage

4 Alternativen:

1. **Einwilligung** der betroffenen Person

   oder

2. Verarbeitung ist für die **Erfüllung eines Vertrages** oder einer rechtlichen Verpflichtung erforderlich

   oder

3. Wahrung **lebenswichtiger Interessen** des Betroffenen oder eines Dritten

   oder

4. Verarbeitung ist zur **Wahrung der berechtigten Interessen** des Verantwortlichen oder eines Dritten erforderlich UND Interessen der betroffenen Person überwiegen nicht

Rechtsgrundlage

1. Alternative: Einwilligung (Art. 6 Abs. 1 lit. a DSGVO)

➔ Einwilligung nur dann wirksam, wenn..

- sie **freiwillig** abgegeben wird (Art. 4 Nr. 11, 7 Abs. 4 DSGVO)
- sie für einen **bestimmten Fall** abgegeben wird (Art. 4 Nr. 11 DSGVO)
- der Betroffene **über die wesentlichen Umstände verständlich informiert** wurde (Art. 4 Nr. 11 DSGVO)
  - ➔ Identität des Verantwortlichen (Erwägungsgrund 42 DSGVO)
  - ➔ Zweck der Datenverarbeitung (Erwägungsgrund 42 DSGVO)
- der Betroffene über die ständige **Möglichkeit zum Widerruf seiner Erklärung informiert** wurde (Art. 7 Abs. 3 S. 3 DSGVO)
- sie durch eine **eindeutig bestätigende Handlung** erfolgt ist (Art. 4 Nr. 11 DSGVO)
  - ➔ schriftliche Erklärung; Ankreuzen einer Erklärung im Internet (opt-in); NICHT ABER "Stehenlassen" eines bereits angekreuzten Kästchens (opt-out)

Achtung!
Bei Personen **unter 16 Jahren** muss eine Zustimmung eines Erziehungsberechtigten erfolgen! (vgl. Art. 8 DSGVO)

Rechtsgrundlage

2. Alternative: Erfüllung eines Vertrages / einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. b und lit. c DSGVO)

➔ Personenbezogene Daten, die zur Erfüllung eines Vertrages notwendig sind, dürfen verarbeitet werden!

Beispiele:
- Verkäufer und Käufer dürfen Name, Kontaktdaten und Bankverbindung erheben
- Bankier darf vor Kreditvergabe Bonitätsdaten abfragen
- Hauspflegerin darf Medikamentendaten der Patienten speichern

➔ Personenbezogene Daten, die zur Erfüllung einer rechtlichen Verpflichtung notwendig sind, dürfen verarbeitet werden!

Rechtsgrundlage

3. Alternative: Wahrung lebenswichtiger Interessen (Art. 6 Abs. 1 lit. d DSGVO)

➔ Personenbezogene Daten, die zur Wahrung lebenswichtiger Interessen notwendig sind, dürfen verarbeitet werden!

- Kaum Anwendung im Vereinsleben!
- Schwelle sehr hoch!

Ein **"lebenswichtiges Interesse"** besteht regelmäßig nur in Notfällen, in denen der Einzelne nicht mehr selbst in die Verarbeitung einwilligen kann.

Rechtsgrundlage

4. Alternative: Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO)

➔ Personenbezogene Daten, die zur Wahrung berechtigter Interessen notwendig sind, dürfen verarbeitet werden, **sofern nicht** die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen!

- Vorsicht! Bis jetzt noch teils unklare Definition. Gesetzgeber lässt viel offen!
- Es ist **IMMER** eine Interessenabwägung vorzunehmen. Das kann schnell schiefgehen.
- Beachte Widerspruchsrecht (Art. 21 DSGVO; dazu später)

Beispiele für ein berechtigtes Interesse: Betrugsprävention, teilweise Direktwerbung, die Übermittlung von Kunden- und Beschäftigtendaten innerhalb einer Unternehmensgruppe sowie die Gewährleistung der Netz- und Informationssicherheit (vgl. Erwägungsgrund 47 S.6 u. 7, 48 S. 1, 49 S. 2)

Exkurs: Rechtsgrundlage bei Datenerhebung durch Covid-19

Durch Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO) und Wahrung lebenswichtiger Interessen (Art. 6 Abs. 1 lit. d DSGVO) legitimiert:

- Verarbeitung personenbezogener Daten **von Beschäftigten** um eine Ausbreitung zu verhindern, insb.
  - Informationen zu Fällen, bei denen eine Infektion festgestellt wurde oder Kontakt zu nachweislich Infizierten bestand
  - Informationen zu Fällen, bei denen in relevanten Zeitraum ein Aufenthalt in einem Risikogebiet stattgefunden hat
- Verarbeitung personenbezogener Daten **von Gästen und Besuchern**, um festzustellen, ob diese
  - selbst infiziert sind oder in Kontakt mit einer nachweislich infizierten Person standen
  - sich im relevanten Zeitraum in einem Risikogebiet aufgehalten haben

Durch Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c DSGVO) legitimiert:

- Pflicht zur Erhebung von Kontaktdaten der **Gäste in der Gastronomie**
  - ergibt sich aus: § 13 Abs. 4 Satz 3 der Fünften Bay. Infektionsschutzmaßnahmenverordnung und mit Ziff. 3.2.3 und Ziff. 3.2.9 des Hygienekonzepts Gastronomie

Exkurs: Rechtsgrundlage bei Datenerhebung durch Covid-19

Durch Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO) und Wahrung lebens Interessen (Art. 6 Abs. 1 lit. d DSGVO) legitimiert:

- Verarbeitung personenbezogener Daten **von Beschäftigten** um eine Ausbreitung zu verhindern, insb.:
  - Informationen zu Fällen, bei denen eine Infektion festgestellt wurde oder Kontakt zu nachweislich Infizierten bestand
  - Informationen zu Fällen, bei denen in relevanten Zeitraum ein Aufenthalt in einem Risikogebiet stattgefunden hat
- Verarbeitung personenbezogener Daten **von Gästen und Besuchern**, um festzustellen, ob diese
  - selbst infiziert sind oder in Kontakt mit einer nachweislich infizierten Person standen
  - sich im relevanten Zeitraum in einem Risikogebiet aufgehalten haben

Das Verbot der Verarbeitung von Gesundheitsdaten, gilt aufgrund von Art. 9 Abs. 2 lit. i DSGVO **nicht**!

Durch Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c DSGVO) legitimiert:

- Pflicht zur Erhebung von Kontaktdaten der **Gäste in der Gastronomie**
  - ergibt sich aus: § 13 Abs. 4 Satz 3 der Fünften Bay. Infektionsschutzmaßnahmenverordnung u Ziff. 3.2.9 des Hygienekonzepts Gastronomie

Das Verbot der Verarbeitung von Gesundheitsdaten, gilt aufgrund von Art. 9 Abs. 2 lit. i DSGVO **nicht**!

Beschäftigtendatenschutz

➔ Hier wird mangels Regelung in der DSGVO auf das BDSG zurückgegriffen.

Beschäftigte:
legaldefiniert in **Art. 26 Abs. 8 BDSG**
→ insb. Arbeitnehmer, Leiharbeiter, Auszubildende, Beamte, Freiwillige im Bundesfreiwilligendienst

Erlaubnistatbestände für eine Datenverarbeitung:

➔ **Datenverarbeitung erforderlich**: ...um Arbeitsverhältnis zu begründen, durchzuführen oder zu beenden,
...um Pflichten aus Gesetzen oder Betriebsvereinbarungen zu erfüllen

➔ **Einwilligung:**
- Informationspflicht über Datenverarbeitung!
- Einwilligung muss freiwillig sein.
- Aus Ablehnung darf dem Betroffenen kein Nachteil entstehen.

➔ **Verfolgung einer Straftat:**
- Verdacht einer bereits begangenen Straftat muss begründet vorliegen

Überblick: Rechtmäßigkeit einer Verarbeitung personenbezogener Daten

Worauf?

Rechtsgrundlage (vgl. Art. 6 DSGVO)

Wie?

- Verarbeitung nach Treu und Glauben und Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit der Daten
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

(vgl. Art. 5 DSGVO)

Verarbeitung nach Treu und Glauben und Transparenz

Art. 5 Abs. 1 lit. a DSGVO: Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a) 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“);

➔ Grundsatz von Treu und Glauben schwer positiv zu umschreiben. Daher Bildung von Negativfallgruppen, die den Grundsatz verletzen.

- Verwendung **verborgener Techniken** (zB heimliche Videoüberwachung, Spyware etc.) treuwidrig
- **unverhältnismäßig** sollte die Datenverarbeitung nicht sein

➔ Transparenz umfasst vor allem **Informationspflichten** (Art. 13 und 14 DSGVO) und **Auskunftsansprüche** (Art. 15 DSGVO)

Verarbeitung nach Treu und Glauben und Transparenz

➔ Vor der Verarbeitung von persönlichen Daten eines Betroffenen ist dieser nach **Art. 13 DSGVO** oder **Art. 14 DSGVO** zu informieren.

- **Art. 13 DSGVO:** Wenn man direkt vom Betroffenen die Daten erhebt.
- **Art. 14 DSVO:** Wenn die Daten des Betroffenen bei einem Dritten eingeholt werden.

Datenschutzerklärung nach Art. 13 DSGVO

Art. 13 DSGVO: Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a) den Namen und die **Kontaktdaten des Verantwortlichen** sowie gegebenenfalls seines **Vertreters**;
b) gegebenenfalls die **Kontaktdaten des Datenschutzbeauftragten**;
c) die **Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die **Rechtsgrundlage für die Verarbeitung**;
d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, **die berechtigten Interessen,** die von dem Verantwortlichen oder einem Dritten verfolgt werden;
e) gegebenenfalls die **Empfänger oder Kategorien von Empfängern** der personenbezogenen Daten und
f) gegebenenfalls die **Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln**, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a) die **Dauer**, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
b) das **Bestehen eines Rechts auf Auskunft** seitens des Verantwortlichen über die betreffenden personenbezogenen Daten **sowie auf Berichtigung** oder **Löschung** oder **auf Einschränkung der Verarbeitung** oder **eines Widerspruchsrechts gegen die Verarbeitung** sowie des **Rechts auf Datenübertragbarkeit**;
c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das **Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen**, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
d) das **Bestehen eines Beschwerderechts** bei einer Aufsichtsbehörde;
e) **ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist**, ob die **betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte** und
f) das **Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling** gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Überblick: Rechtmäßigkeit einer Verarbeitung personenbezogener Daten

Worauf?

Rechtsgrundlage (vgl. Art. 6 DSGVO)

Wie?

- Verarbeitung nach Treu und Glauben und Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit der Daten
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

(vgl. Art. 5 DSGVO)

Zweckbindung

Art. 5 Abs. 1 lit. b DSGVO: Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

b) 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 Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

➔ Daten dürfen nur für festgelegte Zwecke erhoben werden.

- Im Umkehrschluss scheidet eine Verarbeitung zu noch unbekannten Zwecken aus.

➔ Festlegung der Verarbeitungszwecke muss eindeutig sein.

- Keine vagen Umschreibungen der Verarbeitungszwecke!
- Mitteilung erfolgt über die Datenschutzerklärung nach Art. 13 DSGVO.

➔ Zwecke müssen auch legitim sein.

- allgemeinen Rechtsprinzipien und sonstiges einschlägiges Recht außerhalb des Datenschutzes muss entsprochen werden, insbesondere dem Diskriminierungsverbot und einschlägigen Anforderungen des Arbeitsrechts, Vertragsrechts und Verbraucherschutzrechts

Überblick: Rechtmäßigkeit einer Verarbeitung personenbezogener Daten

Worauf?

Rechtsgrundlage (vgl. Art. 6 DSGVO)

Wie?

- Verarbeitung nach Treu und Glauben und Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit der Daten
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

(vgl. Art. 5 DSGVO)

Datenminimierung

Art. 5 Abs. 1 lit. c DSGVO: Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung");

3 Stufen der Datenminimierung

Angemessenheit → Ist die Verarbeitung noch verhältnismäßig?

Erforderlichkeit → Ist die Verarbeitung auf das Nötigste begrenzt?

Erheblichkeit → Hilft die Verarbeitung überhaupt dem Zweck?

Überblick: Rechtmäßigkeit einer Verarbeitung personenbezogener Daten

Worauf?

Rechtsgrundlage (vgl. Art. 6 DSGVO)

Wie?

- Verarbeitung nach Treu und Glauben und Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit der Daten
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

(vgl. Art. 5 DSGVO)

Richtigkeit der Daten

Art. 5 Abs. 1 lit. c DSGVO: Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

d) 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");

➔ Daten müssen sachlich richtig und ggf. auf dem neusten Stand sein.

➔ Pflicht des Verantwortlichen, die Daten zu überprüfen (auch ohne Verlangen des Betroffenen) und alle vertretbaren Schritte einzuleiten, damit unrichtige Daten unverzüglich gelöscht o. berichtigt werden.

Überblick: Rechtmäßigkeit einer Verarbeitung personenbezogener Daten

Worauf?

Rechtsgrundlage (vgl. Art. 6 DSGVO)

Wie?

- Verarbeitung nach Treu und Glauben und Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit der Daten
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

(vgl. Art. 5 DSGVO)

Speicherbegrenzung

Art. 5 Abs. 1 lit. e DSGVO: Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

e) 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 Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung");

➔ **Speicherdauer** auf das **„unbedingt erforderliche Mindestmaß"** zu beschränken.
(vgl. Erwägungsgrund 39)

- Also nur solange wie es für die Zweckerreichung nötig ist

Überblick: Rechtmäßigkeit einer Verarbeitung personenbezogener Daten

Worauf?

Rechtsgrundlage (vgl. Art. 6 DSGVO)

Wie?

- Verarbeitung nach Treu und Glauben und Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit der Daten
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

(vgl. Art. 5 DSGVO)

Integrität und Vertraulichkeit

Art. 5 Abs. 1 lit. f DSGVO: Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

f) 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");

➔ Vertraulichkeit

- Schutz vor **unbefugter Kenntnisnahme**
- Schutz vor **unbefugter Verarbeitung**

➔ Integrität

- Schutz vor **Löschung** oder anderweitige **Vernichtung** der Daten
- Schutz vor **unbefugter Veränderung**

Konkretisierte Schutzmaßnahmen in **Art. 32 DSGVO**

Datensicherheit nach Art. 32 DSGVO

➔ Schutzmaßnahmen sind nach einem **dem Risiko angemessenen Schutzniveau** vorzunehmen.

Art

Stand der Technik

Umfang

Implementierungskosten

Umstände und Zwecke der Verarbeitung

Eintrittswahrscheinlichkeit

Schwere des Risikos für Rechte und Freiheiten

Datensicherheit nach Art. 32 DSGVO

➔ Konkrete Schutzmaßnahmen

- **Pseudonymisierung:** Aufteilen und gesonderte Aufbewahrung personenbezogener Daten, sodass sie einzeln nicht mehr auf eine spezifische Person zurückzuführen sind.

  → *In kleineren Vereinen selten nötig.*

- **Verschlüsselungen:**

- E-Mail-Server: Einstellung STARTTLS und Perfect Forward Secrecy
- Website: HTTPS als Transportverschlüsselung
- Datein, Dokumente: Zip-Verschlüsselung, bspw. AES-256 durch 7-ZIP oder WinZIP
- E-Mail: Zip-Verschlüsselung, PGP, S/MIME
- Cloud: Dateien vor dem senden an die Cloud verschlüsseln
- WLAN: WPA2 und 20-stelliges Passwort; voreingestellte Passwörter ändern
- Heimzugriff: per VPN
- Datenträger: VeraCrypt
- Endgeräte: Passwort

Datensicherheit nach Art. 32 DSGVO

➔ Konkrete Schutzmaßnahmen

- **Berechtigungsmanagement:** Nicht jeder Mitarbeiter braucht vollen Zugriff auf die gesamten Vereinsdaten.
  - → Teilen Sie hierzu die Mitarbeiter in Beschäftigungsbereiche ein und gewähren Sie nur Datenzugriff innerhalb des bearbeiteten Wirkungskreises.
- **Aktualisierung:**
  - → Installieren Sie stets die aktuellste Version der Programme, die mit der Verarbeitung personenbezogener Daten zu tun haben.
  - → Ganz veraltete Hardware mit bekannten Sicherheitslücken sollte ggf. aufgegeben werden.

Datensicherheit nach Art. 32 DSGVO

➔ Konkrete Schutzmaßnahmen

- **E-Mail:**
  - → E-Mail-Adressen, die nicht für die Weitergabe an Leute aus dem Mailverteiler bestimmt sind stets in die Empfängerzeile BCC setzen.
- **Backups:**
  - → regelmäßige, längerfristige Backups
  - → auf externen Datenträger, der NICHT mit ihrem Firmennetzwerk verbunden ist
  - → Backup in der Cloud reicht regelmäßig NICHT aus

Datensicherheit nach Art. 32 DSGVO

➔ Konkrete Schutzmaßnahmen

- **physischen Zugang erschweren:**

  → Nachts: Abschließen.

  → Tagsüber: Räume, von denen aus auf personenbezogene Daten zugegriffen werden können verschließen, solange diese unbeaufsichtigt sind.

Überblick: Rechtmäßigkeit einer Verarbeitung personenbezogener Daten

Worauf?

Rechtsgrundlage (vgl. Art. 6 DSGVO)

Wie?

- Verarbeitung nach Treu und Glauben und Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit der Daten
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

(vgl. Art. 5 DSGVO)

Rechenschaftspflicht

Art. 5 Abs. 2 DSGVO: Grundsätze für die Verarbeitung personenbezogener Daten

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

➔ *Konkretisiert in Art. 24 Abs. 1 DSGVO*

➔ Die Grundsätze aus Art. 5 Abs. 1 DSGVO müssen eingehalten werden.

NEU in der DSGVO:

➔ Die Einhaltung der Grundsätze muss zusätzlich vom Verarbeitenden nachgewiesen werden!

- **Konsequenz hieraus:** Verzeichnis von Verarbeitungstätigkeiten

Überblick: Verzeichnis von Verarbeitungstätigkeiten

- Allgemeines zum Verzeichnis
- Wer muss ein solches Verzeichnis führen?
- Wer ist eventuell davon befreit?
- Was muss ein solches Verzeichnis beinhalten?
- Vorlegen des Verzeichnisses
- Form des Verzeichnisses

Allgemeines: Verzeichnis von Verarbeitungstätigkeiten

Pflicht zum Führen eines solchen Verzeichnisses! (Art. 30 Abs. 1 S. 1 DSGVO)

- ➔ Dokumentation aller Verarbeitungen personenbezogener Daten
- ➔ wesentliche Angaben zur Datenverarbeitung müssen aufgeführt werden
  - z.B.: Datenkategorien, Kreis der betroffenen Personen, Zweck der Verarbeitung, Datenempfänger
- ➔ trägt zur Erfüllung der Rechenschaftspflichten bei

Anforderungen auf Inhalt dieses Verzeichnisses: verankert in Art. 30 Abs. 1 DSGVO

Wer muss ein solches Verzeichnis führen?

Wer ist vom Führen eines solchen Verzeichnisses befreit?

Was muss dieses Verzeichnis beinhalten?

Wer muss ein solches Verzeichnis führen?

Art. 30 Abs. 1 S. 1 DSGVO: Verzeichnis von Verarbeitungstätigkeiten

(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten.

Verantwortlicher:

Diejenige Person bzw. Einrichtung, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet

➔ **ergo:** der, der mit den Daten umgeht

Das betrifft auch:

Auftragsverarbeiter! → derjenige, der Daten im Auftrag des Verantwortlichen verarbeitet

Wer ist vom Verzeichnis befreit?

➔ Unternehmen/Einrichtungen mit weniger als 250 Mitarbeitern

- **ABER:** praktisch keine Bedeutung
  - Freistellung gilt nur dann, wenn Verarbeitung nur **gelegentlich** erfolgt,
  - und **keine besonderen Datenkategorien** nach Art. 9 Abs. 1 DS-GVO (Gesundheitsdaten, Religionsdaten) verwendet werden.
- **Somit bereits nicht umfasst von dieser Befreiung:** Jedes Unternehmen/jeder Verein, welches kontinuierlich für seine Beschäftigten Lohnabrechnungen durchführt.

Was muss das Verzeichnis beinhalten?

Festgelegt in Art. 30 Abs. 1 DSGVO

- Namen, Kontaktdaten des Verantwortlichen (oder der Verantwortlichen, sowie deren Vertreter)
- Zwecke der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und der Daten
- Kategorien von Empfängern, ggü. denen die Daten offengelegt werden
- ggf. Übermittlungen von Daten an internationale Organisation
- vorgesehene Fristen für Löschung der verschiedenen Datenkategorien
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 I DSGVO

Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten" gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf abrufbar.

Bayerisches Landesamt für Datenschutzaufsicht

Muster 1: Verein – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
TSV Waldermühl e.V.
Steinbauerstr. 45a
98123 Sonsthausen

Tel. 0981/123456-0
E-Mail: team@waldermuehler-tsv.de
Web: www.waldermuehler-tsv.de

Vorstand: Dieter Eckbauer-Düppels, geb. 03.12.1952

Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbez. Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über externen Dienstleister)	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	02.03.2018	• Auszahlung der Löhne/Gehälter • Abfuhr Sozialabgaben u. Steuern	Beschäftigte	• Name und Adressen der Beschäftigten • ggf. Religions-zugehörigkeit • Eindeutige Kennzahlen zur Steuer/ Sozialabgaben ...	Externer Dienstleister	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Mitgliederverwaltung	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	02.03.2018	Verwaltung der Vereinstätigkeiten	Mitglieder	• Name und Adressen • Eintrittsdatum • Sportbereiche ...	Keine	Keine	2 Jahre nach Beendigung der Vereinsmitgliedschaft	Siehe IT-Sicherheitskonzept
Betrieb der Webseite des Sportvereins (über Hosting-Dienstleister)	Max Meier 0981/123456-0 max@ waldmuehler-tsv.de	28.02.2018	Außendarstellung	• Mitglieder • Webseitenbesucher	IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept + HTTPS-Verschlüsselung
Veröffentlichung von Fotos der Mitglieder auf der Webseite	Max Meier 0981/123456-0 max@ waldmuehler-tsv.de	20.02.2018	Außendarstellung	Mitglieder	Fotos von Vereinstätigkeiten	Keine	Keine	Wenn Einwilligung widerrufen - unverzüglich	Siehe IT-Sicherheitskonzept
Beitragsverwaltung	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	22.02.2018	Vereinsfinanzierung	Mitglieder	Bankverbindung	Steuerberater	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
...	...	...	...	...	...	...	...	...	...

Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Automatische Updates im Betriebssystem aktivieren
- ✓ Standard-Gruppenverwaltung (z. B. in Windows)
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Aktueller Virenscanner/Sicherheitssoftware
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Standard-Shredder

Vorlegen des Verzeichnisses

Das Verzeichnis ist nicht öffentlich!

➔ Verlangt eine betroffene Person Einblick in die Verarbeitung der sie selbst betreffenden personenbezogenen Daten, müssen diese ihm **nicht** offengelegt werden!

Betroffene Person:
Jeder Mensch, der durch die personenbezogenen Daten identifiziert werden kann.

Denn: Das Verzeichnis dient ausschließlich dem Nachweis der Aufsichtsbehörde, in welchem Verfahren jeweils mit den Daten umgegangen wird

ABER: Art 15 DSGVO: Auskunftspflicht!

Form des Verzeichnisses

- ➔ in deutscher Sprache
- ➔ schriftlich, elektronisch
- ➔ auch Änderungen/Aktualisierungen sollen verzeichnet werden!
  - nicht einfach überschreiben oder alte Eintragungen löschen, sondern die unterschiedlichen Versionen mind. 1 Jahr aufheben

Überblick: Datenschutzbeauftragter

- Datenschutzbeauftragter: Grundlagen
- Checkliste – Pflicht zur Benennung eines Datenschutzbeauftragten
- Benennung des Datenschutzbeauftragten
  - Grundlagen
  - formale Vorgaben
- Meldung an die Aufsichtsbehörde
- Veröffentlichung der Kontaktdaten
- Aufgaben des Datenschutzbeauftragten

Datenschutzbeauftragter

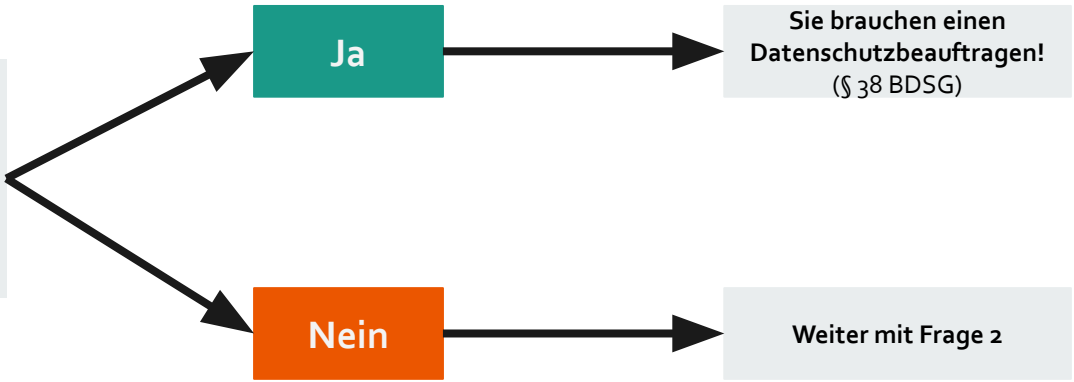
- ➔ Fachliche Unterstützung des Vereinsvorstandes
- ➔ Kontaktdaten des Datenschutzbeauftragten müssen an die Aufsichtsbehörde weitergeleitet werden
- ➔ Kontaktdaten des Datenschutzbeauftragten müssen veröffentlicht werden (Website, Datenschutzerklärung)

Achtung!
Die Verantwortlichkeit dafür, dass Datenschutz eingehalten wird **verbleibt rechtlich trotzdem beim Vereinsvorstand**!

Checkliste – Pflicht zur Benennung eines Datenschutzbeauftragten

Frage 1

Sind in ihrem Verein **mindestens 20 Personen** damit beschäftigt, personenbezogene Daten automatisiert zu verarbeiten?

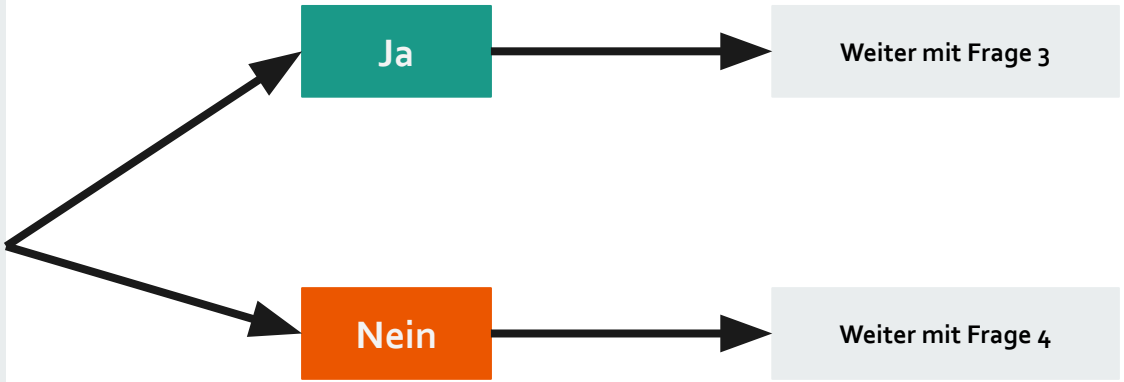


Checkliste – Pflicht zur Benennung eines Datenschutzbeauftragten

Frage 2

Verarbeiten Sie in Ihrem Verein Daten folgender Art?

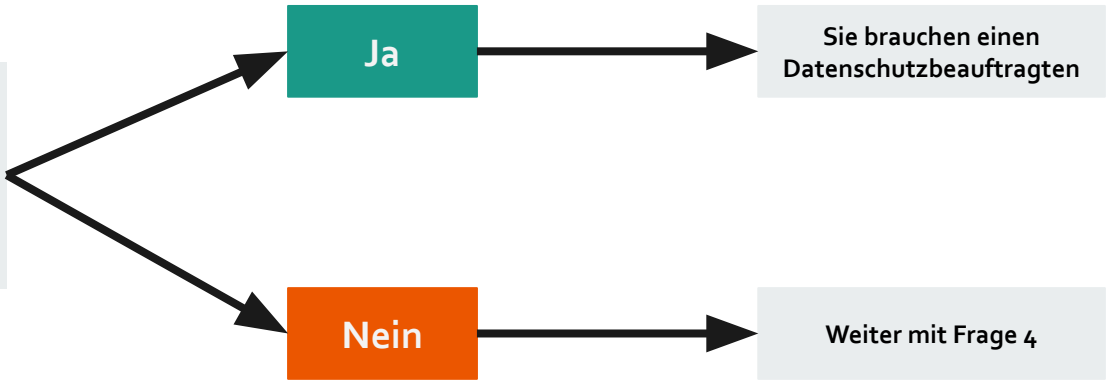
- Gesundheit
- Sexualleben oder zur sexuellen Orientierung
- rassische oder ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugung
- Gewerkschaftszugehörigkeit
- strafrechtliche Verurteilungen



Checkliste – Pflicht zur Benennung eines Datenschutzbeauftragten

Frage 3

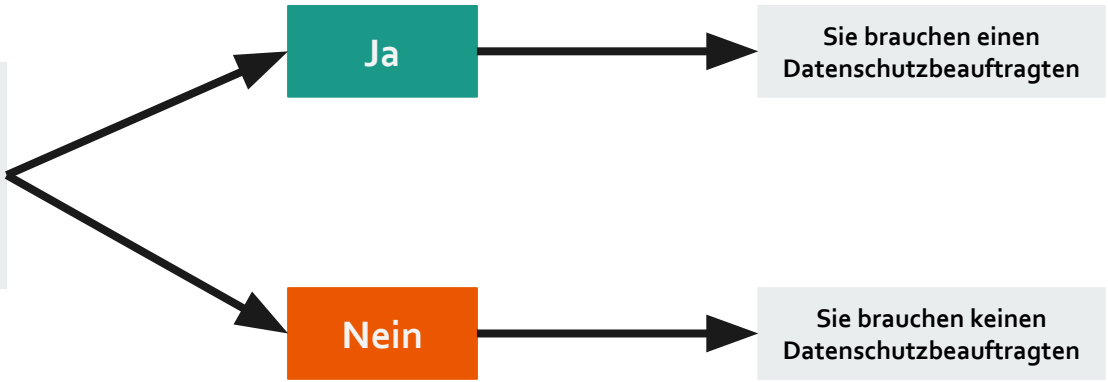
Ist die Verarbeitung von Daten, die in Frage 2 genannt worden sind, eine **Kerntätigkeit** des Vereins?



Checkliste – Pflicht zur Benennung eines Datenschutzbeauftragten

Frage 4

Gehört es zur Kerntätigkeit Ihres Vereins, Personen in umfangreicher Weise regelmäßig **systematisch zu überwachen**?



Benennung des Datenschutzbeauftragten

➔ Kann auch freiwillig benannt werden.

- zu empfehlen; Datenschutz auch ohne Pflicht eines Datenschutzbeauftragten zu achten

2 Varianten (Art. 37 Abs. 6 DSGVO)**:**

1) Benennung eines **eigenen Mitarbeiters**

   ➔ auch neben anderen Aufgaben und Pflichten möglich

   - Dabei darf **kein Interessenkonflikt** entstehen!

2) Benennung eines **externen Dienstleisters**

Benennung – formale Vorgaben

➔ Schriftliche Form ist nicht explizit vorgeschrieben.

- ABER dringendst empfohlen, da sonst schwierig ggü. Aufsichtsbehörde nachzuweisen.

Mustervorlagen werden gesondert zur Verfügung gestellt.

Muster 2: Benennung eines Mitarbeiters, der neben dieser Funktion noch andere Aufgaben wahrnimmt, zum Datenschutzbeauftragten in einem Unternehmen

Bestellung zum Datenschutzbeauftragten

……
(Bezeichnung und Anschrift des Unternehmens)

vertreten durch ……
(Name dessen, der für das Unternehmen handelt, z. B. des alleinigen Geschäftsführers)
benennt hiermit

……
(Name und Vorname des künftigen DSB)

zum Datenschutzbeauftragten.

Der Datenschutzbeauftragte nimmt in dieser Funktion mit Wirkung ab heute die in Art. 39 Abs. 1 DS-GVO ausdrücklich benannten Aufgaben wahr. Außerdem hat er in jedem Halbjahr eine Datenschutzschulung von mindestens 2 Stunden für die Mitarbeiterinnen und Mitarbeiter des Unternehmens durchzuführen.

Der Datenschutzbeauftragte ist mit (*Anteil einsetzen*) … % seiner gemäß Arbeitsvertrag vom (*Datum einsetzen*) festgelegten Arbeitszeit als Datenschutzbeauftragter tätig. Mit (*Anteil einsetzen*) … % seiner Arbeitszeit arbeitet er in der Abteilung (*Abteilungsname einsetzen*) des Unternehmens. Wann der Datenschutzbeauftragte im Rahmen seiner Arbeitszeit diese Funktion wahrnimmt, entscheidet er in eigener Verantwortung.

……
(Ort, Datum)

……
(Unterschrift, Funktion dessen, der für den Verantwortlichen unterzeichnet)

……
(Sinnvoll, aber nicht vorgeschrieben: Empfangsbestätigung durch den Datenschutzbeauftragten mit Ort, Datum und Unterschrift zum Nachweis des Zugangs der Benennung)

Muster 3: Benennung eines ehrenamtlich tätigen Datenschutzbeauftragten in einem Verein

Bestellung zum Datenschutzbeauftragten

……
(Bezeichnung des Vereins)

vertreten durch ……
(Name des Vorsitzenden bzw. des oder der Vertretungsberechtigten für den Verein)
benennt hiermit aufgrund des Vorstandsbeschlusses, der am (*Datum einsetzen*) gefasst wurde

……
(Name und Vorname des künftigen DSB)

zum Datenschutzbeauftragten.

Der Datenschutzbeauftragte ist ehrenamtlich tätig und nimmt in dieser Funktion die in Art. 39 Abs. 1 DS-GVO ausdrücklich benannten Aufgaben wahr. Außerdem hat er in jedem Halbjahr eine Datenschutzschulung von mindestens 2 Stunden für die Mitglieder des Vereins durchzuführen.

……
(Ort, Datum)

……
(Unterschrift des Vorsitzenden bzw. des oder der Vertretungsberechtigten für den Verein)

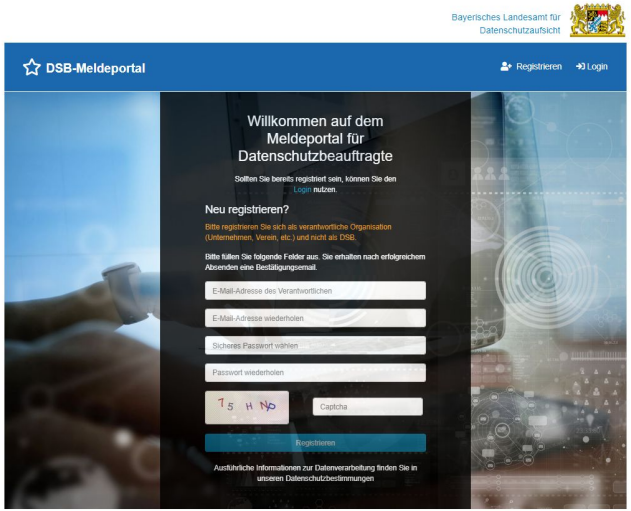
……
(Sinnvoll, aber nicht vorgeschrieben: Empfangsbestätigung durch den Datenschutzbeauftragten mit Ort, Datum und Unterschrift zum Nachweis des Zugangs der Benennung)

Meldung an die Aufsichtsbehörde

➔ Verantwortliche muss die Kontaktdaten des Datenschutzbeauftragten an die Aufsichtsbehörde *(Bayerisches Landesamt für Datenschutzaufsicht)* melden (Art. 37 Abs. 7 DSGVO)

Hierzu hat das BayLDA ein **Meldeportal** auf folgender Website eingerichtet:

https://lda.dsb-meldung.de/



Veröffentlichung der Kontaktdaten des Datenschutzbeauftragten

➔ Die Kontaktdaten des DSB müssen veröffentlicht werden, Art. 37 Abs. 7 DSGVO.

- zusätzlich zur **Veröffentlichung in der Datenschutzerklärung** auch **Veröffentlichung auf der Vereinswebsite**

➔ Name muss nicht angegeben werden.

➔ Ausreichend sind Informationen unter denen der DSB tatsächlich kontaktiert werden kann.

- E-Mail ODER
- Postanschrift ODER
- Telefonnummer

Aufgaben des Datenschutzbeauftragten

Art. 39 DSGVO

1. **Unterrichtung und Beratung** des Verantwortlichen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Datenschutzpflichten
2. **Überwachung der Einhaltung** der Datenschutzvorschriften
3. **Überwachung der Strategien** des Verantwortlichen für den Schutz personenbezogener Daten
4. **Zusammenarbeit mit der Aufsichtsbehörde**
5. **Anlaufstelle** der Aufsichtsbehörde bei Nachfragen
6. **Beratung** betroffener Personen gemäß Art. 38 Abs. 4 DSGVO

Überblick: Rechte des Betroffenen

- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung und Einschränkung
- Recht auf Datenübertragbarkeit
- Recht auf Widerspruch gegen die Verarbeitung
- Recht keiner automatischen Entscheidung unterworfen zu werden

Rechte von Betroffenen

Recht auf **Auskunft** *(Art. 15 DSGVO)*

➔ Betroffener kann auf Antrag eine zusammenfassende Abschrift (auch elektronisch) seiner gespeicherten Daten (kostenlos!) verlangen.

- Der Abschrift ist noch hinzuzufügen:
  - Zweck der Verarbeitung
  - Kategorie personenbezogener Daten
  - Empfänger der Daten
  - geplante Speicherdauer
  - Hinweis auf sonstige Betroffenenrechte und Beschwerdemöglichkeiten bei der Aufsichtsbehörde

Wichtig!
Es muss vor der Herausgabe der Daten sorgfältig sichergestellt sein, dass es sich um die Betroffene Person handelt. Im Zweifel ist ein Identitätsnachweis zu fordern!

Rechte von Betroffenen

Recht auf **Berichtigung** *(Art. 16 DSGVO)*

➔ Betroffener kann auf Antrag die Korrektur falscher Daten einfordern!

Rechte von Betroffenen

Recht auf **Löschung und Einschränkung** *(Art. 17, 18 DSGVO)*

➔ Betroffener kann auf Antrag die **Löschung** von Daten einfordern, sofern…

- die Daten für die Erfüllung des ursprünglichen Zwecks nicht mehr erforderlich sind.
- der Betroffene seine Einwilligung widerrufen hat und es keine andere Rechtsgrundlage gibt.
- es nie eine Rechtsgrundlage gegeben hat.

➔ Sollte Uneinigkeit über die Rechtmäßigkeit d. Datenverarbeitung bestehen hat der Betroffene das Recht die V**erarbeitung einzuschränken**.

Rechte von Betroffenen

Recht auf **Datenübertragbarkeit** *(Art. 20 DSGVO)*

neu in der DSGVO

- ➔ Betroffener kann verlangen, dass Sie ihm die Daten herausgeben, die der Betroffene mitgeteilt hatte.
- ➔ Bzgl. dieser Daten kann der Betroffene auch verlangen, dass Sie diese Daten an dritte Verantwortliche weiterleiten.

Rechte von Betroffenen

Recht auf **Widerspruch gegen die Verarbeitung** *(Art. 21 DSGVO)*

➔ Nur bei Rechtsgrundlage des berechtigten Interesses, die eine Interessenabwägung voraussetzt!

- Betroffener kann Datenverarbeitung widersprechen, sofern er plausible Gründe nennt und diese eine neue Interessenabwägung erfordern.

➔ Bei Werbemaßnahmen Widerspruch immer möglich.

Rechte von Betroffenen

Recht **keiner automatischen Entscheidung** unterworfen zu werden *(Art. 22 DSGVO)*

➔ Betroffener hat Anspruch darauf, dass nicht ein Computer alleine darüber entscheiden darf, wie mit personenbezogenen Daten einer betroffenen Person umgegangen wird.

- in kleineren Vereinen im Grunde **irrelevant**

Exkurs: Direktwerbung

➔ Auch Direktwerbung stellt eine Verarbeitung personenbezogener Daten dar!

Bedarf also einer **Rechtsgrundlage:**

- Einwilligung
  - **Opt-in**
- Wahrung berechtigter Interessen
  - **Opt-out**: es bedarf keiner aktiven Zustimmung des Beworbenen, sondern es genügt, wenn der Betroffene über die werbliche Nutzung und sein Widerspruchsrecht informiert wurde und nicht widersprochen hat

Exkurs: Direktwerbung

Kanal	Verbraucher (B2C)	Unternehmen (B2B)
E-Mail SMS Messenger	**Opt-in** *Wenn Bestandskundenprivileg greift:* Opt-out	**Opt-in** *Wenn Bestandskundenprivileg greift:* Opt-out
Telefon	**Opt-in**	**Opt-in** **Erleichterung:** mutmaßliche Einwilligung genügt
Post	**Opt-out**	**Opt-out**

Überblick: Auftragsverarbeitung

- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung und Einschränkung
- Recht auf Datenübertragbarkeit
- Recht auf Widerspruch gegen die Verarbeitung
- Recht keiner automatischen Entscheidung unterworfen zu werden

Auftragsverarbeitung:
Eine natürliche/ juristische Person, Behörde, Einrichtung etc. verarbeitet **im Auftrag** eines Verantwortlichen personenbezogene Daten.

Varianten der Auftragsverarbeitung:

- ➔ Verantwortlicher gibt, festgelegt durch einen Vertrag, personenbezogene Daten an jemanden außerhalb seines Unternehmens/Verein
  - *z.B. an Mitarbeiter einer externen Buchhaltung*
- ➔ Verantwortlicher ermöglicht Einblick in die eigene Datenhaltung
  - *z.B. Wartung der eigenen IT durch externe Firmen*

Pflichten bei der Auftragsverarbeitung

- ➔ Verantwortlicher muss sich **sicher sein, dass Auftragsverarbeiter im Einklang mit den datenschutzrechtlichen Vorschriften** arbeitet!
- ➔ **Verantwortlicher haftet** für Fehlverhalten der Auftragsverarbeitung!
- ➔ Verantwortlicher muss sich umfangreiche **Kontrollrechte** einräumen lassen.
- ➔ Verantwortlicher darf **ohne Ankündigung vor Ort Kontrollen etc durchführen oder durch externen Sachverständigen durchführen lassen**.
- ➔ Bei Auftragsvergabe muss auch an das **Ende der Vertragsbeziehung** gedacht werden (was muss wann zurückgegeben werden, was muss gelöscht werden etc).

“Richtige Auftragsverarbeitung”

Es liegt **“richtige Auftragsverarbeitung”** vor, wenn der Beauftragte **weisungsabhängig** vom Verantwortlichen ist.

➔ liegt vor bei:

- Datenverarbeitung für Lohn- und Gehaltsabrechnungen
- Werbeadressenverarbeitung in einem Lettershop
- Auslagerung eines Teils des eigenen Telekommunikationsbetriebs

➔ liegt **nicht** vor bei:

- Inanspruchnahme externer Fachleistungen (Personenverwaltung, Mitarbeiterekrutierung, Vertragskundenbetreuung, Finanzberatung…)

FOLGE: Gewisse Privilegierung für Unternehmen

➔ Sie dürfen personenbezogene Daten ihrer Kunden weitergeben, ohne dass dafür eine ausdrückliche Einwilligung vorliegen muss

Überblick: Sanktionen und Haftungen

- Zuständigkeit: Aufsichtsbehörde
- Untersuchungs- und Abhilfebefugnisse
- Geldbußen
- Schadensersatz

Zuständigkeit: Aufsichtsbehörden

➔ Unabhängige Datenschutzbeauftragte der Länder, Beauftragter für den Datenschutz und die Informationsfreiheit

Bei grenzüberschreitenden Datenverarbeitungen: Behörde desjenigen Landes, in dem Hauptniederlassung liegt. (‘federführend’)

Untersuchungs-und Abhilfebefugnisse

Katalog der Befugnisse in **Art. 58 DSGVO**

Untersuchungsbefunisse:

- Aufforderung des Verantwortlichen über Bereitstellung aller für ihre Arbeit notwendigen Informationen
- Datenschutzüberprüfung
- Hinweis auf Verstöße gegen Verordnung
- Zugang zu allen Räumlichkeiten, einschließlich aller Datenverarbeitungsanlagen und -geräte

Abhilfebefugisse:

- Warnung vor voraussichtlichen Verstößen
- Verwarnung von Verstößen
- Anweisung auf bestimmte Weise und bis zu einer bestimmten Zeit im Einklang mit Verordnung zu sein
- Anordnung von Berichtigung oder Löschung falscher personenbezogener Daten
- Anordnung der Aussetzung von Übermittlung personenbezogener Daten in ein Ausland

Geldbußen

Art. 83 Abs.1 DSVGO: Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gem. diesem Artikel für Verstöße gegen diese Verordnung gem. den Absätzen 4, 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

Gravierende Verstöße, Art. 83 Abs. 5 DSGVO:

- gegen Grundsätze der Verarbeitung gem. Art 5, 6, 7, 9 DSGVO
- gegen Rechte der betroffenen Person gem. Art 12-20 DSGVO
- Übermittlung personenbezogener Daten an ein Drittland/internationale Organisation gem. Art. 44-49 DSGVO
- Nichtbefolgung einer Anweisung/Beschränkung/Aussetzung durch Aufsichtsbehörde gem. Art. 58 DSGVO

Folge: bis zu 20.000.000 € Strafe, bei Unternehmen 4% ihres weltweiten Jahresumsatzes

Geldbußen

Verstöße mit geringerem Ausmaß, Art. 83 Abs. 4 DSGVO:

- gegen die Bestimmungen der Einwilligung eines Kindes gem. Art 8 DSGVO
- gegen Anforderungen des Datenschutzes durch Technikgestaltung
- gegen die Anforderungen der Zertifizierung gem. Art 42, 43 DSGVO
- gegen die Pflichten der Überwachungsstelle gem. Art 42 Abs. 1 DSGVO

Folge: Geldbußen bis zu 10.000.000 € bzw 2% des gesamten weltweiten Jahresumsatzes eines Unternehmens

Geldbußen

Genaue Höhe des Bußgelds wird durch Aufsichtsbehörde bestimmt

➔ Rahmen stark gestiegen!

mehrstufige Berechnungsmethode:
Größe des Unternehmens, Vorsatz, rechtzeitige Maßnahmen zur Schadensminimierung, Schwere des Verstoßes etc. werden in Betracht gezogen

Schadensersatz

Art. 82 Abs. 1 DSGVO: Haftung und Recht auf Schadensersatz

(1) Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter

Materiell: jeder Schaden, der in Geld zu messen ist, bei Verstößen gegen den Datenschutz eher selten

Immateriell: Schäden, die sich nicht in Geld messen lassen, z.B. Rufverletzung

Überblick: Umgang mit Fotos im Internet

- Technische Hintergründe
- Rechtliche Hintergründe
- Das Kunsturhebergesetz (KUG)
- Bilder auf Internetseiten von Unternehmen
- Widerruf der Einwilligung
- Bilder auf Internetseiten von Vereinen

Technische Hintergründe

- Fotos lassen sich ohne Qualitätsverlust beliebig oft kopieren
- Fotos lassen sich mühelos im Internet hochladen
- Fotos im Umlauf im Internet lassen sich nicht mehr ‘einfangen’, ein Internetnutzer, der die Bilder runtergeladen hat, kann sie problemlos wieder hochladen

Effektive technische Schutzmaßnahmen, die Verletzungen des Persönlichkeitsrecht bei Fotos effektiv verhindern gibt es - trotz aller Versicherungen - nicht!

Vorgeschlagene Maßnahmen zum Schutz:

- Reduzierung der Bildqualität vor dem Hochladen.
    - Wirkung gleich null! Unterschied kaum merkbar, sogar mit Verringerung der Bildauflösung um 50%
- Anbringen von Logos/Wasserzeichen auf Fotos:
    - Wirkung gleich null! keine Abschreckung, kopieren etc weiterhin möglich
- Sperren der Kopierfunktion: ‘speichern unter’ erscheint nicht
    - Wirkung fast gleich null, zwar sind Laien vom Kopieren abgehalten, im Internet jedoch genug Anleitungen., diese Sperre zu umgehen

Die Maßnahmen reichen in keinem Fall aus, um das Persönlichkeitsrecht an Bildern auch nur halbwegs zu schützen!

Rechtliche Hintergründe

- Fotos, die Personen abbilden, enthalten personenbezogene Daten
    - **Auch ohne den Namen** der Person, da diese dennoch identifizierbar ist
    - **Auch mit Verpixelung**, da diese für Verwandte etc dennoch erkennbar ist (Kopfform, Haltung etc)
- Bei Filmen: egal, wie kurz die Person zu sehen ist!

DSGVO selbst enthält **keine speziellen** Regelungen zu Umgang mit Fotos von Personen

➔ umfasst von Regelungen zu personenbezogenen Daten!

➔ Beachte aber: Kunsturhebergesetz!

Das Kunsturhebergesetz (KUG)

§ 22 KUG: Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie

Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden.
Die Einwilligung gilt im Zweifel als erteilt, wenn der Abgebildete dafür, dass er sich abbilden ließ, eine Entlohnung erhielt.

Einwilligung: vorherige Zustimmung zur Verbreitung des Bildes!
Bei Versäumnis: Rechtsverletzung! Jedoch nachträgliche Zustimmung möglich.

Verbreitung: nicht nur im Internet, es reicht schon, wenn **eine einzige weitere Person** Zugriff zu dem Bild hat

§ 23 KUG

(1) Ohne die nach § 22 erforderliche Einwilligung dürfen verbreitet und zur Schau gestellt werden:

1. Bildnisse aus dem Bereiche der Zeitgeschichte;
2. Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;
3. Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben;
4. Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient.

(2) Die Befugnis erstreckt sich jedoch nicht auf eine Verbreitung und Schaustellung, durch die ein berechtigtes Interesse des Abgebildeten oder, falls dieser verstorben ist, seiner Angehörigen verletzt wird.

Bereiche der Zeitgeschichte: Aktuelles und Vergangenes von allgemeinem und gesellschaftlichem Interesse.

Höheres Interesse der Kunst: Nicht Bildnis selber steht im Mittelpunkt, sondern die Aussage des Künstlers.

Berechtigtes Interesse: Intimsphäre der Person, Bereiche aus dem Privatleben, von denen man nicht ausgehen kann, dass andere ein Interesse daran haben sollten.

Bilder auf Internetseiten von Unternehmen

- möchte man Bilder von Mitarbeitern veröffentlichen, braucht es eine ausdrückliche, schriftliche Einwilligung (BVerfG)
- Einwilligung muss immer individuell erscheinen
  - → nicht in Form einer Betriebsvereinbarung!
- auch als ‘Sammeleinwilligung’ möglich: Einzelne Unterschrift aller Mitarbeiter auf einer Liste.
- empfehlenswert: Verwendungszweck der Bilder möglichst genau angeben!

Widerruf der Einwilligung

- Wird grds. von den Gerichten zugelassen, wenn ein wichtiger Grund vorliegt
    - Wichtiger Grund kann sein: Unternehmenswechsel mit jeweils tragender Funktion
- Bei Minderjährigen rasch gegeben, da besonderer Schutz von Minderjährigen gegeben sein soll.

Auch ein **rechtlich zulässiger Widerruf wirkt immer nur für die Zukunft!**
➔ führt nicht dazu, dass ein veröffentlichtes Foto rückwirkend als unzulässig anzusehen ist!

Bilder auf Internetseiten von Vereinen

- Hier kommen oft die Ausnahmen aus § 23 KUG zur Anwendung
    - besonders bei Veranstaltungen!
- Auch wenn Person individuell erkennbar ist
- Solange sie als Vereinsmitglied erkennbar ist, im Bezug zur Veranstaltung!
- Also nicht, wenn gezielt nur ein einziger Teilnehmer fotografiert wird!
- **Zuschauer:** Veröffentlichung zulässig, Argument: sind nur “Beiwerk”
  nicht zulässig: heranzoomen an einzelne Personen

Grenze auch hier: berechtigtes Interesse der Betroffenen!

Besonderheiten bei Minderjährigen

hier liegt oft das ‘berechtigte Interesse’ aus **§ 23 II KUG** vor → besonderer Schutz von Minderjährigen

➔ keine Spielszenen bei Mannschaftsspielen ohne Einwilligung der Sorgeberechtigten

➔ keine Gruppenfotos aller Art ohne Einwilligung

➔ **Aber:** Kinder im Zusammenhang mit **Zeitgeschehen** sind abbildbar ohne Erlaubnis!

Hinweise zur Einwilligung

- Am besten mit konkreten, schriftlichen Einwilligungen arbeiten
- Das Bauchgefühl hat meistens recht! ‘
  → wenn man sich nicht komplett sicher ist, ob Veröffentlichung legitim wäre, gibt es dafür einen guten Grund
- Hinweise auf Beabsichtigung einer Veröffentlichung ersetzen keine individuelle Einwilligung!
- Gibt es für einen Minderjährigen mehrere Sorgeberechtigte, müssen ALLE Sorgeberechtigten einwilligen!

Vertiefende Hinweise

Hierzu hat das BayLDA eine **Übersicht mit weiteren, vertiefenden Links** auf folgender Website eingerichtet:

https://www.lda.bayern.de/media/muster_1_verein.pdf

➔ Bezüglich **Direktwerbung** stellen wir einen vertiefenden Leitfaden als PDF zur Verfügung!

Link zur Präsentation:

(ohne Anspruch auf Vollständigkeit)

https://docs.google.com/presentation/d/1KNy5kE0hZd0zfvJKh66MhZoOyGrGl_oNMMNaXwrO3kM/edit?usp=sharing

Anfragen zu vertiefenden Musterformularen an:

sgerhold@outlook.de