Datenschutz in der Europa-Union und ihren Untergliederungen unter Berücksichtigung der EU-Daten-schutz-Grundverordnung

-

Eine Übersicht

Stand: 16. Juni 2018

Inhaltsverzeichnis

Zu meiner Person

Ich bin Diplom-Verwaltungswirt (Ausbildung für den gehobenen nicht-technischen Verwaltungsdienst in Nordrhein-Westfalen) und war bis zum Eintritt in die Freizeitphase meiner Altersteilzeit über 20 Jahre lang Datenschutzbeauftragter der Stadt Bochum. Außerdem hatte ich über ein Jahrzehnt den Vorsitz des Arbeitskreis „Datenschutz“ beim Städtetag Nordrhein-.Westfalen inne. Ich bin seit 1993 Geschäftsführer des Bochumer Kreisverbandes der Europa-Union.

Kontakt

Für Fragen erreichen Sie mich per E-Mail unter:

rkarn@europa-union-bochum.de

Bitte kennzeichnen Sie Ihre Frage im Betreff als [Datenschutzfrage], damit ich die Übersicht behalte. Bitte haben Sie Verständnis dafür, dass ich Fragen ggf. in aller Kürze beantworte.

Haftungsausschluss

Die zu Rechtsvorschriften und zum Thema Datenschutz gemachten Aussagen in diesem Skript wurden nach bestem Wissen und Gewissen gemacht. Bitte haben Sie Verständnis dafür, dass ich für meine Aussagen keine Haftung übernehmen kann. Sie stellen keine Rechtsberatung dar und ersetzen ggf. nicht die Beratung durch einen Rechtsanwalt. Sie können sich in Zweifelsfragen auch an die zuständige Aufsichtsbehörde wenden.

Vorwort

Am 25. Mai 2018 tritt die EU-Datenschutz-Grundverordnung (DS-GVO)[1] in Kraft. Sie ersetzt das bisher geltende Bundesdatenschutzgesetz (BDSG), welches zum gleichen Zeitpunkt in einer geänderten Fassung in Kraft tritt[2]. Beide Vorschriften sind ab diesem Zeitpunkt parallel anzuwenden, wobei die DS-GVO ausschließt, dass nationale Regelungen den Regelungen der Verordnung entgegenstehen können. Nationale Regelungen dürfen die Verordnung nur in bestimmten Teilen ergänzen/konkretisieren/verschärfen/an nationale Eigenheiten anpassen.

Die DS-GVO stärkt die Rechte betroffener Personen durch:

- verstärkte Transparenzpflichten bei der Erhebung personenbezogener Daten
- verschärfte Anforderungen an die Dokumentation des Verantwortlichen und
- ein erweiterte Rechte der betroffenen Person.

Die DS-GVO verschärft die Anforderungen an die verantwortliche Stelle durch:

- erhöhte Aufklärungs-, Dokumentations- und Nachweispflichten
- teilweise drastisch höhere Bußgelder, die durch die Aufsichtsbehörden verhängt werden können.

Um die Umsetzung zu erleichtern, wurden Formulare und Checklisten erarbeitet. Diese geben den Kenntnisstand zum Zeitpunkt der jeweiligen Überarbeitung dieses Dokumentes wieder. Sofern Bestimmungen der DS-GVO auszulegen sind/waren, gibt diese Übersicht die Meinung des Verfassers wieder. Sie muss nicht „richtig“ sein; insbesondere die Auffassung der Aufsichtsbehörden kann eine andere sein. Es wird daher empfohlen, die im Internet bereitgestellten Hinweise der Aufsichtsbehörde (s. Linkliste) regelmäßig auf die darin getroffenen Auffassung hin zu lesen. Der Autor lehnt ausdrücklich eine Haftung ab!

Etwas persönliches zum Thema

Als langjähriger Datenschutzbeauftragter ist mir das Thema Datenschutz mit all seinen Feinheiten „an's Herz gewachsen“. Ich nehme den Datenschutz sehr ernst, lebe ihn für mich persönlich (Selbstdatenschutz) und respektiere den Anspruch meiner Mitmenschen auf Datenschutz!

Auch wenn Ihnen viele meiner Ausführungen als „überzogen“ erscheinen sollten, entsprechen sie einer „Guten Praxis“ (Best Pratice) in Bezug auf den Datenschutz, denn „Daten, die nicht vorhanden sind müssen nicht geschützt werden!“. Das Thema der fehlenden Regelungen („Arbeitsanweisungen“) hat mich während meiner beruflichen Tätigkeit oft beschäftigt. Es schadet nicht, auch etwas selbstverständliches aufzuschreiben. Bei Nachfragen der Aufsichtsbehörden hat es sich immer als nützlich erwiesen, wenn vorher eindeutige Regelungen aufgestellt waren. Mehr Ausführungen dazu finden Sie in Ziff. 5.11. Interessierte mögen sich im Internet unter dem Stichwort „Organisationsverschulden“ weiter informieren.

---

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Amtsblatt der Europäischen Union L 119/1

2 Bundesdatenschutzgesetz vom 30. Juni 2017 in der Fassung des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU), BGBl I, S. 2097

1. Ziel und Anwendungsbereich der DS-GVO

Die DS-GVO schützt die personenbezogenen Daten betroffener Personen vor unerlaubter Erhebung, Verarbeitung und Weitergabe durch öffentliche und nicht-öffentliche Stellen. Die Verarbeitung personenbezogener Daten unterliegt einem Verbot mit Erlaubnisvorbehalt.

Sie nimmt dabei Bezug auf die Charta der Grundrechte der Europäischen Union:

> *„Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta") sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten." (Erwägungsgrund Nr. 1)*

Das BDSG a.F. nahm Bezug auf das „Recht auf informationelle Selbstbestimmung", welches durch das „Volkszählungsurteil"[3] des Bundesverfassungsgerichts geschaffen wurde.

Von der Anwendung ausgenommen ist lediglich eine Erfassung und Verarbeitung personenbezogener Daten **durch eine natürliche Person** „zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit" (Erwägungsgrund Nr. 18 mit einer beispielhaften Aufzählung, sowie Art. 2 Abs. 2 lit. c)). Somit wird eine Verarbeitung durch einen Verein **immer** von der DS-GVO erfasst.

2. Schutzzweck

> *„Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten." (Art. 1 Abs. 1)*

Der Schutzzweck „bei der Verarbeitung personenbezogener Daten" und der „freie Verkehr solcher Daten" scheinen auf den ersten Blick widersprüchlich. Berücksichtigt man allerdings die Tatsache, dass die DS-GVO in allen Mitgliedsländern unmittelbar gilt (im Gegensatz zu einer Richtlinie muss sie nicht mehr durch nationale Gesetze umgesetzt werden) wird erkennbar, dass der Verordnungsgeber den Gedanken des Binnenmarktes konsequent umgesetzt hat. Unterschiede im nationalen Datenschutzrecht sind mit der Verordnung beseitigt und können einem grenzüberschreitenden Datenverkehr nicht mehr entgegenstehen. Die DS-GVO regelt die Weitergabe personenbezogener Daten über die Grenzen der Mitgliedsländer.

3. Begriffe

3.1 personenbezogene Daten

> *„"personenbezogene Daten" (sind) alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person")" (Art. 4 Ziff. 1)*

Das BDSG a.F. formulierte ähnlich als:

> *„"Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)." (§ 3 Abs. 1 BDSG a.F.)*

Personenbezogene Daten sind also alle denkbaren Informationen über eine natürliche Person wie Alter, Wohnort, Beruf usw.. Voraussetzung ist aber, dass es sich um eine natürliche Person han-

3 Az. 1 BvR 209, 269, 362, 420, 440, 484/83

delt – juristische Personen (Vereine, GmbH, AG) genießen „Datenschutz“ aufgrund anderer Rechtsvorschriften (z.B. nach dem Handelsgesetzbuch).

3.1.1 besondere personenbezogene Daten

Durch die DS-GVO werden bestimmte Kategorien von Daten als „besondere geschützte Daten“ einem Verarbeitungsverbot unterworfen. Dies sind Daten, die

- die rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen,
- die Gewerkschaftszugehörigkeit betreffen,

sowie

- genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,

außerdem

- Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. (Art. 9 Abs. 1)

Eine Verarbeitung dieser Daten ist grundsätzlich „untersagt“ und kann nur mit einer „ausdrücklichen Einwilligung“ der betroffenen Person (Art. 9 Abs. 2 lit. a DS-GVO) oder aufgrund andere Erlaubnistatbestände (Art. 9 Abs. 2 lit b-j) erfolgen. Diese Regelung entspricht der des § 3 Abs. 9 BDSG a.F.

3.2 „Identifiziert“ oder „identifizierbar“

Die betroffene Person muss schon konkret „bekannt“ oder mit vorhandenem oder beschaffbarem Zusatzwissen identifizierbar sein:

- „Die Frau mit den roten Turnschuhen“ ist in einem voll besetzten Fußballstadion wohl nicht identifizierbar, in einem Kreis von 10 oder 20 Personen wohl eher.
- Sofern über einen ausreichend langen Zeitraum Informationen zu Personen gesammelt werden, sind diese irgendwann „identifizierbar“. Insoweit sind anonymisierte Daten mit Vorsicht zu genießen.

3.2 Verarbeitung

> *„“Verarbeitung“ (ist) jede mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten“ (Art. 4 Ziff. 2)*

Der Begriff der Verarbeitung umfasst alle denkbaren Tätigkeiten, die mit personenbezogenen Daten ausgeführt werden. Art. 4 Ziff. 2 führt weitere „Tätigkeiten“ aus (s. dort).

3.3 Verantwortlicher

> *„“Verantwortlicher“ (ist) die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;“ (Art. 4 Ziff. 7)*

Der „Verantwortliche“ ist Adressat der Regelungen der DS-GVO. Er trägt gegenüber der betroffenen Person und der Aufsichtsbehörde die Verantwortung für einen den Regelungen der Vorordnung entsprechenden Umgang mit personenbezogenen Daten. Er kann sich dieser Verantwortung nicht entledigen.

- Im Fall eines Vereins ist der Vorstand Verantwortlicher, sofern durch die Satzung keine weitergehenden Regelungen getroffen werden[4].

3.4 Auftragsverarbeiter

„"Auftragsverarbeiter" (ist) eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;" (Art. 4 Ziff. 8)

Bedient sich der Verantwortliche eines (oder mehrerer) Dritten bei der Verarbeitung personenbezogener Daten, werden diese als Auftragsverarbeiter für ihn tätig. Gebräuchlich ist heute z.B. die Nutzung von externen Plattformen („Cloud"), in denen Daten verarbeitet und/oder gespeichert werden; das ist eine Auftragsdatenverarbeitung.

3.5 Empfänger und Dritter

„"Empfänger" (ist) eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht." (Art. 4 Ziff. 9)

„"Dritter" (ist) eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;" (Art 4 Ziff. 10)

Die etwas „sperrigen" Formulierungen zum Empfänger stellt klar, dass Empfänger jeder ist, dem personenbezogene Daten „offengelegt" werden. Das BDSG a.F. formulierte hier etwas verständlicher, dass Empfänger „ jede Person oder Stelle(ist), **die Daten erhält**." (§ 3 Abs. 8 BDSG a.F.). Dritter ist jede andere Person.

3.6 Einwilligung

„"Einwilligung" der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;" (Art. 4 Ziff. 11)

Der Einwilligung der betroffenen Person zur Verarbeitung ihrer Daten kommt in der DS-GVO eine zentrale Bedeutung zu. Sie ist nach dem Grundsatz von Treu und Glauben Voraussetzung für die rechtmäßige Verarbeitung durch den Verantwortlichen. Mit der Einwilligung sind besondere Informations- und Dokumentationspflichten für den Verantwortlichen verbunden!

4. Grundsätze (Art. 5)

Bei der Verarbeitung personenbezogener Daten sind zu beachten:

4.1 Zweckbindung (Art. 5 Abs. 1 lit b)

Personenbezogene Daten dürfen nur für die Zwecke verarbeitet oder an Dritte weitergegeben werden, für die sie erhoben wurden. Eine Änderung der Zweckbindung ist nur unter bestimmten Voraussetzungen zulässig. Die Vorschriften des § 28 BDSG a.F. waren ähnlich ausgestaltet.

---

4 „§ 26 BGB Vorstand und Vertretung
(1) Der Verein muss einen Vorstand haben. Der Vorstand vertritt den Verein gerichtlich und außergerichtlich; er hat die Stellung eines gesetzlichen Vertreters. Der Umfang der Vertretugsmacht kann durch die Satzung mit Wirkung gegen Dritte beschränkt werden.
(2) Besteht der Vorstand aus mehreren Personen, so wird der Verein durch die Mehrheit der Vorstandsmitglieder vertreten. Ist eine Willenserklärung gegenüber einem Verein abzugeben, so genügt die Abgabe gegenüber einem Mitglied des Vorstands."

4.2 Datenminimierung (Art. 5 lit c)

Das bedeutet, dass nur die Daten erhoben werden, die z.B. zur Betreuung eines Vertrages tatsächlich erforderlich sind. Das die Kenntnis weiterer Daten „nützlich“ ist oder „die Arbeit erleichtert“ ist dabei unbedeutend. Eine gleich lautende Pflicht besteht schon in § 3a BDSG a.F..

4.3 Richtigkeit (Art. 5 lit d)

Personenbezogene Daten müssen „richtig“ und „aktuell“ sein, wenn sie verarbeitet werden. Eine Aktualisierung ist folglich dann nicht mehr erforderlich, wenn die Daten nicht mehr weiter verarbeitet werden sollen, aber noch aufbewahrt werden („archiviert“) müssen. Ansonsten sind die Voraussetzungen zu schaffen, dass diese Daten berichtigt oder gelöscht werden können.

4.4 Anonymisierung (Art. 5 lit e)

Im Gegensatz zum BDSG a.F. welchen eine Verpflichtung zur Löschung nicht mehr benötigter Daten vorsah (s. § 35 Abs. 2 Nr. 3 und 4), geht die DS-GVO davon aus, dass Daten (mindestens) so zu anonymisieren sind, dass ein Bezug zu einer Person nicht mehr hergestellt werden kann.

4.5 „Integrität und Vertraulichkeit“ (Art. 5 lit f)

Durch technische und organisatorische Maßnahmen ist sicher zu stellen, dass personenbezogene Daten vor unbefugter Verarbeitung, unbeabsichtigtem Verlust und Zerstörung geschützt sind. Diese Verpflichtung fand sich schon teilweise in den nach § 9 BDSG a.F. vorgeschriebenen technischen und organisatorischen Maßnahmen, die zum Schutz personenbezogener Daten zu treffen waren. Wegen der besonderen Bedeutung ist diesem Grundsatz ein eigenes Kapitel gewidmet.

4.6 Rechtmäßigkeit der Verarbeitung (Art. 6)

Jede Verarbeitung personenbezogener Daten muss eine Rechtsgrundlage haben. Für die Datenverarbeitung eines Vereins wird dies in der Regel die Einwilligung der betroffenen Person sein, die sich auf das zugrunde liegende „Vertragsverhältnis“, nämlich die Mitgliedschaft bezieht.

4.7 Anwendung bei einer „Verarbeitung“ in Papierform

Die DS-GVO ist unabhängig davon anzuwenden, ob personenbezogene Daten in Papierform oder als Datei (in einem Computersystem) vorliegen:

> *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. (Art. 2 Abs. 1 DS-GVO)*

5. Praktische Anwendung - To-Do-Liste

5.1 Erhebung und Einwilligung

Mit der Begründung des Mitgliedsverhältnisses werden die für die Betreuung der Mitgliedschaft erforderlichen personenbezogenen Daten erhoben. Dies geschieht in der Regel durch einen schriftlichen Aufnahmeantrag, der durch das zukünftige Mitglied ausgefüllt und unterzeichnet wird.

Dabei soll der Antrag

- nur die Daten abfragen, die zur Betreuung des Mitgliedsverhältnisses tatsächlich benötigt werden (s. Ziff. 4.2 Datenminimierung) und

muss

- die klare und unmissverständliche Einwilligung zur Erhebung, Speicherung und Verarbeitung dieser Daten enthalten und
- die vorgeschriebenen Informationen nach Art. 13 enthalten.

5.1.1 Form der Einwilligung

Da der Verantwortliche das Vorliegen der Einwilligung jederzeit nachweisen können muss (s. Art. 7 Abs. 1) kann nur empfohlen werden, die Einwilligung in schriftlicher Form einzuholen. Die denkbare Einwilligung in elektronischer Form erscheint angesichts dieser Nachweispflicht nicht praktikabel.

Da die Einwilligung im textlichen Zusammenhang mit den zu erhebenden Daten steht, sollte sie von diesen optisch abgesetzt und z.B. durch eine Hervorhebung (Fettdruck der Überschrift) besonders kenntlich gemacht werden.

Durch die vorgeschriebene „klare und einfache Sprache“ verbieten sich missverständliche und verschachtelte Formulierungen. Es gilt: „So einfach und verständlich wie möglich formulieren!“

5.1.2 Inhalt der Einwilligung

Der unter Ziff. 3.6 wiedergegebene Text der DS-GVO macht deutlich, dass eine Formulierung wie „Ich stimme der Erhebung zu“ nicht ausreichend sein dürfte. Entsprechend dem Wortlaut der Verordnung sollte als Überschrift z.B. die Formulierung „Einwilligung zur Erhebung, Speicherung und Verarbeitung meiner Daten“ gewählt werden.

5.2 Erhebung und Einwilligung zur Weitergabe

Für den Fall, dass die personenbezogenen Daten an andere Stellen weitergegeben werden sollen bedarf dies einer Rechtsgrundlage oder der Zustimmung der betroffenen Person. Diese Regelung entspricht denen des § 28 Abs. 3 BDSG a.F., nach der eine „Übermittlung“ zu anderen Zwecken unter bestimmten Voraussetzungen zulässig war.

Eine Weitergabe liegt z.B. bei Vereinen dann vor, wenn Mitgliederdaten an übergeordnete „Abteilungen“ innerhalb des Vereins (z.B. von der Tennisabteilung an die Badminton-Abteilung) oder andere Gliederungen (Landesverband, Bundesverband) übermittelt werden[5]. In diesen Fällen muss die Einwilligung zur Weitergabe ebenfalls – nach entsprechender Aufklärung über Anlass und Zweck der Weitergabe – eingeholt werden.

Ein Weg, die Einwilligung zur Weitergabe zu „umgehen“ wäre eine Bestimmung in der Satzung der jeweiligen Untergliederung, nach der mit einer Mitgliedschaft in der Untergliederung eine Mitglied-

5 siehe „Datenschutz im Verein nach der Datenschutzgrundverordnung (DS-GVO)“ des Landesbeauftragten für Datenschutz und die Informationsfreiheit Baden-Württemberg unter Ziffer 5.4

schaft im Landes- bzw. Bundesverband „erworben“ würde. Im Ergebnis bleiben sich beide Wege gleich, statt einer freiwilligen Einwilligung nach Art. 6 Abs. 1 lit a) käme Art. 6 Abs. 1 lit b) zur Anwendung, da der Beitritt in einen Verein einem Vertragsabschluss gleichzusetzen ist[6]

Nach der mir vorliegenden Kommentierung sind die „Wege“ der Einwilligung gleichwertig:

> *„Damit die Verarbeitung personenbezogener Daten (…) überhaupt rechtmäßig ist, muss mindestens eine der Voraussetzungen des Art. 6 Abs. erfüllt sein. (…) Die einzelnen Tatbestände sind voneinander unabhängig und haben alle die gleiche auf die Zulässigkeit abzielende Funktionalität.“*[7]

5.3 Informationspflichten

Zusammen mit der Erhebung sind Informationspflichten nach Art. 13 Abs. 1 gegenüber der betroffenen Person zu erfüllen. Sie ist aufzuklären über

- den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
  - dies sind die Namen des/der Vorsitzenden (vertretungsberechtigte Vorstandsmitglieder)
- gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten
  - sofern ein solcher bestellt werden muss, oder auf freiwilliger Basis bestellt wurde
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen
  - dies ist eine Aufzählung der vorgesehenen Fälle einer Verarbeitung
- sowie die Rechtsgrundlage für die Verarbeitung
  - dies kann im Falle eines Vereins nur die Einwilligung der betroffenen Person sein
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
  - wenn eine solche beabsichtigt oder erforderlich ist (s. Ziff. 5.2).

Außerdem ist die betroffene Person aufzuklären über

- die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
  - dies wird in der Regel die Dauer der Mitgliedschaft betreffen. Sofern z.B. aus statistischen Gründen (z.B. Festlegung der Mitgliederzahl zum Ende eines Jahres) eine Löschung nicht in Betracht kommt, können die Daten anonymisiert oder in einen abgetrennten Datenbestand überführt werden. Sind Daten aufgrund gesetzlicher Vorschriften für einen bestimmten Zeitraum aufzubewahren (z.B. aus steuerlichen Gründen für 10 Jahre) ist eine Überführung in einen gesonderten Datenbestand erforderlich.
  - **Achtung: Über ausgestellte Spendenbescheinigungen sind die Nachweise (= Durchschrift der Bescheinigung) für die Dauer von 10 Jahren aufzubewahren!** Es empfiehlt sich, über diese Bescheinigungen eine separate Datei anzulegen und vom übrigen Datenbestand getrennt aufzubewahren.
- 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.

---

6 siehe „Datenschutz im Verein nach der Datenschutzgrundverordnung (DS-GVO)“ des Landesbeauftragten für Datenschutz und die Informationsfreiheit Baden-Württemberg unter Ziffer 1.3.1

7 s. Paal-Pauly „Datenschutz-Grundverordnung“ (Beck'sche Kompakt-Kommentare) zu Art. 6 DS-GVO, S. 89,90

5.4 Verarbeitung

Verarbeitung ist jede „Tätigkeit“, die mit personenbezogenen Daten ausgeführt wird. Dies kann also das Erstellen von Anschreiben sein, die Erstellung einer Liste mit Mitgliedern, die zur Zahlung der Mitgliedsbeiträge aufgefordert werden etc..

5.5 Eigenes Angebot im Internet

5.5.1 Inhalte prüfen

Sofern eine eigene Seite im Internet zum Abruf bereitgehalten wird, können dort personenbezogene Daten erhoben werden. Dies kann wissentlich oder auch unwissentlich geschehen. Unwisssentlich dann, wenn die verwendete Software ohne weiteres Zutun Daten von Besuchern an Dritte übermittelt.

Beispiele:

- Beim Betrieb einer Webseite mit der Software „WordPress“ können angemeldete Benutzter ein Bild von sich automatisch anzeigen lassen (sog. „Gravatar“). Dabei werden Daten an einen externen Dienst übermittelt, welcher die Tatsache einer Anmeldung speichert.
- Die Nutzung des Dienstes „Google Analytics“ durch ein Web-Angebot übermittelt fortlaufend Informationen über Besucher an Google.

In beiden Fällen ist der Betreiber des Angebotes für die Erhebung und Speicherung verantwortlich! Er hat die Besucher aufzuklären und haftet für Verstöße gegen das Datenschutzrecht!

Einen Link zu einer Seite, auf der WordPress bzw. eine Vielzahl von Plugins auf ihre Konformität mit der DS-GVO überprüft werden findet man im Linkverzeichnis.

Empfehlung:

- Es wird dringend empfohlen, auf die Nutzung von Angeboten zu verzichten, die Daten an Dritte übermitteln.

5.5.2 Serverstandort prüfen

Es sollte geprüft werden, wo die Server des Hosters (also des Dienstleisters, der die Anbindung an das Internet und die Bereitstellung der Seiten erledigt) ihren Standort haben. Die Server sollten in Europa stehen, damit der Hoster der DS-GVO unterliegt.

5.5.3 Auftragsdatenverarbeitung prüfen

Sofern auf der Webseite personenbezogene Daten erfasst werden / eingegeben werden können, wird der Hoster als Auftragsdatenverarbeiter tätig. Es ist zwingend ein „Vertrag über eine Auftragsdatenverarbeitung“ abzuschließen. Außerdem muss sich der Anbieter der Seiten (also der jeweilige Kreisverband) davon überzeugen, dass der Auftragsdatenverarbeiter geeignete technische und organisatorische Maßnahmen zum Schutz dieser Daten getroffen hat. Ein seriöser Hoster stellt diese Informationen zur Verfügung.

5.5.4 Datenschutzerklärung

Sofern auf der Seite personenbezogene Daten erhoben werden, ist eine entsprechende Datenschutzerklärung erforderlich. Hierzu bitte Google bemühen! Stichworte „Datenschutzerklärung DSGVO“.

Empfehlung:

- Bitte die Entwicklung in diesem Bereich im Auge behalten! Jetzt werden sehr umfangreiche Erklärungen angeboten; ob das so notwendig (oder ausreichend) ist lässt sich noch nicht beurteilen

Das Muster des Kreisverbandes Bochum ist beigefügt. Bitte beachten, dass ohne Interaktion des Nutzers hier keine personenbezogenen Daten durch den Kreisverband bzw. das Angebot erhoben und gespeichert werden. Die Seiten werden mit dem System WordPress verwaltet; es sind keine PlugIns installiert, die selbständig Daten an Dritte übermitteln.

5.6 Nutzung der E-Mail

Der Versand einer E-Mail gleicht dem Versand einer Postkarte! Personenbezogene Daten dürfen nicht per E-Mail übertragen werden!

Auch wenn es nicht der geübten Realität entspricht, sollen E-Mails keine personenbezogenen Daten enthalten. E-Mails können während der Übertragung im Internet von Dritten zur Kenntnis genommen und ggf. verfälscht werden. Eine E-Mail wird nicht auf direktem Weg übertragen, sondern durch eine unbestimmte Anzahl von Systemen gespeichert und befördert. Jede Person, die (berechtigt oder unberechtigt) Zugriff auf ein solches System hat, kann die enthaltenen Daten zur Kenntnis nehmen!

Empfehlungen:

- Personenbezogene Daten verschlüsseln
  - entweder als Anhang (zip-Datei mit Passwort) oder
  - durch die Installation von entsprechenden Tools (z.B. GNU PGP, Enigmail etc.)
- Nutzung von E-Mail-Servern, die in Deutschland gehostet werden und deren Betreiber die E-Mail „made in Germany“ unterstützen wie web.de, gmx, T-online, strato, freenet.de, 1&1.

Wichtig:

➔ Es ist immer wieder zu beobachten, dass in einer E-Mail an einen großen Verteiler die Funktion „CC“ (Carbon Copy = Durchschrift) genutzt wird! Damit sehen alle Empfänger der E-Mail die anderen angeschriebenen Empfänger! Neben dieser zweifelhaften Verfahrensweise (welche m.E. gegen den Datenschutz verstößt!) erzeugt ein Klick auf „Antworten“ i.d.R. eine Mail an alle ursprünglichen Empfänger.

➔ Daher für Kreise von Empfängern spezielle Verteiler (Gruppen) anlegen!

5.7 Nutzung von Speicherdiensten (Dropbox etc.)

Bei der Nutzung von Speicherdiensten können personenbezogene Daten außerhalb der EU abgelegt werden und dem Zugriff von ausländischen Diensten unterliegen. Dies kann problematisch sein, da eine „Übermittlung“ von personenbezogenen Daten in Länder außerhalb der EU einer Regelung bedarf. Zumindest der sog. „Privacy Shiled“ für eine Übermittlung in die USA ist rechtlich zweifelhaft. Am 06.10.2015 erklärte der Europäische Gerichtshof gar den Vorgänger „Safe Harbour“ für ungültig. Von daher wird ein Dienst empfohlen, welcher seinen Standort (mindestens) in Europa hat.

Problematisch bei einer Nutzung von Speicherdiensten kann die fehlende Zugriffsberechtigung an Dateien sein. Es kann unzulässig sein, eine (große) Datei einer Vielzahl von Personen zur Verfügung zu stellen, die für sich einzeln nur einen Teil der Informationen benötigen (s. Ziff. 4.2 und 5.2).

Empfehlungen:

- Wenn überhaupt, einen Speicherdienst nutzen, welcher in Europa speichert. Daten und Zugriffsberechtigungen so aufbereiten, dass jede Person nur die Daten erhält, die sie zur Aufgabenerfüllung benötigt. Daten möglichst verschlüsseln; Passwörter auf separatem Weg übermitteln.

5.8 Facebook, WhatsApp & Co

Bei der Nutzung „Sozialer Medien“ zu beachten:

- Die Freigabe des Adressbuches bzw. aller Kontakte in WhatsApp erfüllt den Tatbestand einer Ordnungswidrigkeit, da hierzu die Einwilligung der betroffenen Personen zur Übermittlung ihrer Daten an den Anbieter erforderlich ist (s. 3. Tätigkeitsbericht zum Datenschutz: Nicht-öffentlicher Bereich des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit).

Meine persönliche Meinung:

- Facebook ist KEIN soziales Medium, weil es vorrangig dazu dient, Informationen über die Nutzer zu gewinnen und diese zu vermarkten.
- Das Facebook die Daten von 1,5 Milliarden (!) Nutzern in die USA verlagert hat, spricht für sich (Link dazu: https://www.heise.de/newsticker/meldung/Wegen-der-DSGVO-Facebook-verschiebt-Daten-von-1-5-Milliarden-Nutzern-aus-Irland-4027584.html)

Empfehlung:

- Statt einer Mitteilung über Facebook oder einer Nachricht über WhatsApp tut es auch eine simple E-Mail oder ein Anruf.

5.9 Rechte der betroffenen Person

5.9.1 Auskunftsrecht

Die betroffene Person kann vom Verantwortlichen Auskunft über die zu ihrer Person gespeicherten Daten verlangen. Hierzu ist ihr eine Auflistung aller Daten zur Verfügung zustellen. Nähere Informationen enthält Art. 15 DS-GVO. Die Zeitschrift c't (Verlag Heise Medien GmbH & Co. KG) hat hierfür ein schönes Muster zur Verfügung gestellt (Link in der Linkliste).

5.9.2 Übertragbarkeit

Nach Art. 20 hat die betroffene Person ein Recht darauf, dass ihre Daten zu einem anderen Anbieter „übertragen“ werden. Für den Bereich der Europa-Union fällt mir im Moment kein konkretes Szenario ein, da z.B. die Übertragung der Mitgliedsdaten zwischen den Unterorganisationen im zentralen Mitgliedssystem gelöst ist (Zuordnung zu einem anderen Kreisverband).

Beim Betrieb einer eigenen Webseite kann ggf. die Übertragung von Kommentaren und eigenen Inhalten gefordert werden. WordPress bietet hierzu entsprechende Werkzeuge an.

5.9.3 Recht auf Berichtigung, Löschung und Widerruf einer erteilten Einwilligung

Das Recht auf Berichtigung ist selbst erklärend. Das Recht auf Löschung (aller) personenbezogener Daten bzw. der Widerruf einer erteilten Einwilligung bedeutet bei einem Mitglied den Austritt aus der Europa-Union. Beim Widerruf einer erteilten Einwilligung wird die Rechtmäßigkeit der bisherigen Speicherung ausdrücklich nicht beeinflusst (Art. 13 Abs. 2 lit. c)).

5.10 Bestellung eines Datenschutzbeauftragten

Die Bestellung eines Datenschutzbeauftragten ist in der Regel nicht erforderlich. Dabei gilt, dass die Regel des § 38 Abs. 1 BDSG n.F.: „soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen“ nur dann zutrifft, wenn die Kerntätigkeit des Verantwortlichen in der Durchführung von Verarbeitungsvorgängen besteht. Es müssen also mehr als 10 Personen in einem Unternehmen (Verein) mit der Verarbeitung von personenbezogenen Daten beschäftigt sein, dessen **Kerntätigkeit die Verarbeitung solcher Daten ist**. Vereine wie die Europa-Union verfolgen aber als „Kerntätigkeit“ nicht die Verarbeitung

personenbezogener Daten. Bitte hierzu auch die Ausführungen zur Datenschutzfolgeabschätzung beachten (s. Ziff. 5.14).

Ausnahme:

- Die Kerntätigkeit des Verantwortlichen besteht in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 (s. Art. 37 Abs. 1 lit. c)).

5.11 Verzeichnis der Verarbeitungstätigkeiten

Jeder Verantwortliche hat ein Verzeichnis der Verarbeitungstätigkeiten zu erstellen, in dem bestimmte Angaben zu machen sind (s. Art. 30). Die Aufsichtsbehörden empfehlen die Ergänzung um die Punkte „Einwilligung“ bzw. Rechtsgrundlage der Verarbeitung und „Speicher- / Löschungsfristen“ (s. Kurzpapier Nr. 1 der DSK).

Das Verzeichnis ist nicht öffentlich[8], muss also der betroffenen Person nicht zugänglich gemacht werden[9]. Es ist auf Verlangen der Aufsichtsbehörde vorzulegen. Das Verzeichnis kann schriftlich oder elektronisch geführt werden. Es soll vorgenommene Änderungen zeigen (Historie) und in der vorher gültigen Form für ein Jahr aufbewahrt werden.

Empfehlung:

- Zuerst eine Bestandsaufnahme machen („Was haben wir wo zu welchem Zweck gespeichert?“), dann das Verzeichnis erstellen.
- Das Muster des Kreisverbandes Bochum nutzen und an die eigenen Gegebenheiten anpassen.

Weitere Informationen enthält das Kurzpapier Nr. 1 der DSK.

5.12 Technische und organisatorische Maßnahmen

Zur Sicherung personenbezogener Daten sind technische und organisatorische Maßnahmen zu treffen. Bisher waren diese in der Anlage zu § 9 BDSG a.F. detailliert aufgeführt, jetzt ist Art. 32 DS-GVO zu beachten. Dort sind keine konkreten Forderungen aufgestellt, lediglich müssen durch den Verantwortlichen „geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“ getroffen werden.

Technische und organisatorische Maßnahmen sollen sicherstellen, dass

- die Vertraulichkeit (nur Befugte können Daten zur Kenntnis nehmen),
- die Verfügbarkeit (Daten können im Schadensfall in einer angemessen Zeit wiederhergestellt werden) und
- die Authentizität (eine „Verfälschung“ der Daten kann erkannt werden)

durch den Verantwortlichen gewährleistet ist.

Zuerst ist eine Einschätzung erforderlich, was für die Daten ein „angemessenes Schutzniveau“ ist. Dazu bietet sich eine Einteilung in eine der Schutzbedarfskategorien nach dem Grundschutzhandbuch des BSI an. Im Muster des Verzeichnisses der Verarbeitungstätigkeiten (s. Ziff. 10) ist eine solche Schutzbedarfsfeststellung als Anlage enthalten, sie kann übernommen werden, wenn lediglich „normale“ personenbezogene Daten (Namen, Anschrift, Geburtsdatum, Bankverbindung etc.) gespeichert werden. **Ausdrücklich nicht gilt dies**, wenn besonders geschützte Daten nach Art. 9

8 so das Bayerische Landesamt für Datenschutzaufsicht in „Erste Hilfe zur Datenschutz-Grundverordnung“ - Das Sofortmaßnahmen-Paket, C.H. Beck, Kapitel 3, Ziffer 3

9 Zitat: „Gleichfalls entfällt die bisherige Regelung im BDSG, welche ein allgemeines öffentliches Verfahrensverzeichnis mit einem Einsichtsrecht für jedermann sowie eine detaillierte interne Verarbeitungsübersicht beim Datenschutzbeauftragten vorsah.“ Ziffer 2 des Kurzpapiers Nr. 1 der DSK

DS-GVO gespeichert werden! Dann sind ggf. weitere Maßnahmen erforderlich (ggf. Datenschutzfolgeabschätzung nach Art. 35 DS-GVO).

Die technischen und organisatorischen Maßnahmen bestehen aus

- Regelungen bzgl. der eingesetzten Technik und
- Arbeitsanweisungen an die Personen, die Zugang zu den Daten haben.

Regelungen bzgl. der eingesetzten Technik sollen sicherstellen, dass

- die eingesetzten Systeme „aktuell" sind
- vor Schadsoftware gesichert sind und
- Daten regelmäßig gesichert werden.

Die Checkliste und die Arbeitsanweisung (Ziff. 7) enthalten Hinweise, was beachtet werden sollte.

Auch wenn die Arbeitsanweisung zunächst etwas „überzogen" erscheint, ist er dennoch wichtig, da fehlende Regelungen ein Organisationsverschulden bzw. eine Haftung des Vereins begründen können (s. § 31 BGB[10]).

Im Fall eines Datenschutzverstoßes (s. nachfolgende Ausführungen) dienen die Regelungen dazu, gegenüber der Aufsichtsbehörde nachzuweisen, dass die erforderlichen Vorkehrungen getroffen wurden, um die personenbezogenen Daten zu schützen.

Für einen Verein gibt das Bayerische Landesamt für Datenschutz an: „Um die personenbezogenen Daten bei der Verarbeitung zu schützen, sind Standardmaßnahmen im Regelfall ausreichend. Dazu gehören u.a. aktuelle Betriebssysteme und Anwendungen, Passwortschutz, regelmäßige Backups, Virenscanner und Benutzerrechte. Soweit private PCs genutzt werden, ist sicherzustellen, dass nur berechtigte Personen auf die Daten zugreifen können.".[11]

5.13 Meldung von Datenschutzverstößen

Neu ist die Verpflichtung, im Fall eines Datenschutzverstoßes nach Art. 33 DS-GVO diesen der zuständigen Aufsichtsbehörde zu melden. Es sollte geregelt werden, wer innerhalb welcher Frist wen verständigt und wer für die Meldung an die Aufsichtsbehörde zuständig ist. Es empfiehlt sich eine schriftliche Regelung (ist im Muster der Arbeitsanweisung enthalten). Die Meldefrist an die Aufsichtsbehörde beträgt 72 Stunden, nachdem der Verstoß bekannt geworden ist!

5.14 Datenschutzfolgeabschätzung

Werden als „Kerntätigkeit" (des Verantwortlichen) besondere Kategorien von personenbezogenen Daten „umfangreich" verarbeitet (s. Art. 9 DS-GVO), eine systematische Überwachung durchgeführt, oder „neue" Techniken eingesetzt, ist vor dem Einsatz eine Datenschutzfolgeabschätzung nach Art. 35 DS-GVO durchzuführen. Die Datenschutzbeauftragten der Länder und der Datenschutzbeauftragte des Bundes geben sog. „Positiv- Negativlisten" für den nicht-öffentlichen Bereich heraus, in denen Verarbeitungstätigkeiten aufgeführt werden, die einer Datenschutzfolgeabschätzung unterliegen. Für NRW ist die erste Version einer Positivliste verfügbar (s. Linkliste). Diese Listen der Datenschutzbeauftragten der Länder und des Bundes werden dem Europäischen Datenschutzausschuss übermittelt (Art. 35 Abs. 4 und 5).

Empfehlung:

- (Nicht nur) wegen der besonderen Sensibilität der besonderen Daten (s. Art. 9) sollte auf eine Erhebung und Speicherung wo immer möglich verzichtet werden!

---

10 § 31 BGB: „Haftung des Vereins für Organe"
Der Verein ist für den Schaden verantwortlich, den der Vorstand, ein Mitglied des Vorstands oder ein anderer verfassungsmäßig berufener Vertreter durch eine in Ausführung der ihm zustehenden Verrichtungen begangene, zum Schadensersatz verpflichtende Handlung einem Dritten zufügt.

11 siehe: https://www.lda.bayern.de/media/baylda_ds-gvo_1_security.pdf

Achtung:

- Sofern eine Tätigkeit einer Datenschutzfolgeabschätzung unterliegt, löst dies – unabhängig von der Zahl der Beschäftigten – die Pflicht zur Bestellung eines Datenschutzbeauftragten aus! (§ 38 Abs. 1 Satz 2 BDSG n.F.)

5.15 Recht am eigenen Bild

In vielen Zusammenhängen wird nach der Änderung bzgl. der Veröffentlichung von Fotos gefragt. Hierzu folgende Feststellungen:

- Auch bisher war eine Veröffentlichung von Fotos, die Personen zeigen, nur unter bestimmten Voraussetzungen zulässig (s. § 22 und 23 „Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie“ (KurhG))
- Ohne explizite Einwilligung der betroffenen Person ist eine Veröffentlichung ggf. rechtswidrig und kann zu Schadenersatzansprüchen führen.

Nach derzeitiger Kenntnis ist das KurhG weiterhin anzuwenden[12] und es ergeben sich keine Änderungen der (relativ konkreten) Rechtslage.

5.16 Newsletter

Mit einem Newsletter werden interessierte Personen regelmäßig mit Informationen per E-Mail „versorgt“. Es sind verschiedene Voraussetzungen zu erfüllen, um einen Newsletter rechtssicher zu nutzen.

5.16.1 Nutzung eines Dienstleisters

Wird für die Bestellung (=abonnieren) und den Versand ein Dienstleister genutzte (z.B. MailChimp, Newsletter2Go, CleverReach etc.), gelten die Vorschriften über die Auftragsdatenverarbeitung (Art. 28) und es ist zu prüfen

- Wo hat der Dienstleister seinen Sitz?
  - ein Dienstleister mit Sitz in den USA kann problematisch werden (s. Ausführungen zum Privacy Shield unter Ziff. 5.7)
- Kann mit dem Dienstleister ein Vertrag geschlossen werden, welcher der DS-GVO entspricht?

Hinweis:

- Die Erhebung der Daten für den Newsletterversand hat im Rahmen der DS-GVO zu erfolgen! Also unter Beachtung der Grundsätze einer freiwilligen Einwilligung, Beachtung der Informationspflichten, Nachweispflichten (Art. 7 Abs. 1) etc.. Als Muster kann die Information aus der Beitrittserklärung genutzt werden.

5.16.2 Nutzung „in eigener Regie“

Wird kein Dienstleister genutzt gelten auch die Hinweise zu Ziff. 5.16.1!

5.16.3 „Double-Opt-In“

Die herrschende Rechtsmeinung fordert für Newsletter ein Double-Opt-In-Verfahren. Eine Anmeldung zum Newsletter erzeugt eine Antwort an die angegebene E-Mail-Adresse, die einen Link zu einer Bestätigung enthält. Erst danach ist die Einwilligung zum Bezug wirksam.

5.16.4 „richtig“ versenden

Ein Newsletter wird an einen Verteiler gesandt, nicht an eine Unmenge von „CC“-Empfängern! Siehe hierzu Ziff. 5.6.

12 https://www.heise.de/newsticker/meldung/DSGVO-Ende-der-Fotografie-oder-halb-so-schlimm-4052969.html

5.16.5 „Messung der Reichweite“

Dienstleister bieten eine Messung der Reichweite an. Dazu wird im Newsletter ein Link zu einer Grafik eingebettet. Diese Grafik (z.B. ein 1x1 Pixel großes weißes „Bild“) wird beim öffnen der E-Mail von einem Server geladen. Durch eine (für den Empfänger) unsichtbare Verlinkung kann festgestellt werden, welche Empfänger den Newsletter geöffnet haben.

➔ Hierüber ist die betroffene Person aufzuklären, da dies ein Erheben von personenbezogenen Daten bedeutet! Ich rate von der Nutzung solcher Techniken ab, da mir solche Arbeitsweisen „suspekt“ sind, da letztlich nicht sichergestellt werden kann, was mit diesen Daten geschieht.

Tipp zum Selbstdatenschutz:

- Viele E-Mail-Programme bieten die Einstellung, solche Links in E-Mails nur auf Nachfrage zu öffnen. Das sollte als Grundeinstellung gesetzt sein.

5.16.6 Information bestehender Empfänger

Sollte bereits ein Newsletter (mit dokumentierter Einwilligung der Empfänger) betrieben werden, empfehle ich, die Empfänger „bei Gelegenheit“ daran zu „erinnern“ und den Informationspflichten nach Ziff. 5.3 nachzukommen. Nach bisheriger Rechtslage erteilte Einwilligungen gelten fort!

5.17 Folgen von Rechtsverstößen

5.17.1 Recht auf Schadenersatz

Durch eine nicht den Vorschriften der DS-GVO (und ggf. den Vorschriften des BDSG) entsprechende Verarbeitung personenbezogener Daten steht der betroffenen Person ggf. Schadenersatz zu (Art. 82).

5.17.2 Sanktionen durch die Aufsichtsbehörden (Verhängung von Bußgeldern)

Die DS-GVO sieht bei Verstößen die Verhängung von Bußgeldern vor (Art. 83). Dies betrifft u.a. Verstöße gegen:

- die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;
  - Erhebung nach Rechtsmäßigkeit, Treu und Glauben, Beachtung der Zweckbindung, Datenminimierung etc.
  - Rechtmäßigkeit der Verarbeitung (fehlende Einwilligung oder Rechtsgrundlage)
  - Fehlerhafte Einwilligung
  - Verarbeitung besonders geschützter Daten ohne Einwilligung bzw. Rechtsgrundlage
- die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;
  - Recht auf Löschung, Übertragbarkeit, Auskunft etc.
- die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;
  - fehlender Beschluss der Kommission zur Zulässigkeit einer Übermittlung

Rechtsverstöße können mit einem Bußgeld von bis zu 20.000.000 EUR geahndet werden, alternativ mit einem Bußgeld in Höhe von 4% des Jahresumsatzes eines Konzerns – je nachdem, welcher Betrag höher ist.

Die Verordnung bestimmt dazu, dass die Sanktion: „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.“ (Art. 83 Abs. 1). Es ist also nicht zu erwarten, dass ein Verstoß gegenüber einem Kreisverband mit einem Bußgeld sanktioniert wird, welches die finanziellen Verhältnisse überschreitet. Im übrigen wird im Rahmen eines Bußgeldverfahrens der Rechtsweg eröffnet.

5.17.3 Darf man wegen des Verstoßes gegen die DS-GVO abmahnt werden?

Eine Abmahnung ist eine Aufforderung, eine bestimmte Handlung zu unterlassen und eine entsprechende (strafbewehrte) Unterlassungserklärung abzugeben. Zur Abmahnung berechtigt sind Wettbewerber, Verbände zur Förderung von gewerblichen Interessen (etwa: Verbraucherschutz oder die Zentrale zur Bekämpfung unlauteren Wettbewerbs) und die Kammern. Verbraucher dürfen generell nicht abmahnen – sie können dies allerdings über Abmahnvereine tun. Bei Verstößen gegen das Urheber- und Markenrecht darf nur der Inhaber der Rechte, die vermeintlich verletzt werden, aktiv werden.

Eine Abmahnung kommt also vorrangig bei der Verletzung gewerblicher Interessen und dann **durch Mitbewerber** in Frage. Besucher einer informativen Webseite sind keine Verbraucher, da auf dieser Seite keine Waren/Dienstleistungen angeboten werden! Eine Abmahnung durch „Mitbewerber“ (welche sich u.a. auf das Gesetz gegen den unlauteren Wettbewerb stützen würde) ist also unwahrscheinlich.

Selbst bei einem Verstoß gegen datenschutzrechtliche Vorschriften ist eine Abmahnung aufgrund wettbewerbsrechtlicher Vorschriften unwahrscheinlich. Siehe hierzu z.B. : http://www.abmahnungs-abwehr.de/abmahnungen/erste-abmahnungen-wegen-dsgvo/

6. Offene Fragen

6.1 Mitgliedersystem des Bundesverbandes

Der Bundesverband der Europa-Union hat mit der Firma bbg bitbase group GmbH einen Vertrag über die Bereitstellung eines Mitgliederverwaltungssystems abgeschlossen. Dieses System ist Cloud-basiert und enthält die Mitgliederdaten aller Landes- bzw. Kreisverbände. Dabei handelt es sich um eine Auftragsdatenverarbeitung durch einen Auftragsdatenverarbeiter i.S. des Art. 28. Der Bundesverband ist dafür zuständig, dass die mit der bbg bitbase Group geschlossenen Verträge der DS-GVO entsprechen und die sonstigen Pflichten eines Auftragsdatenverarbeiters durch die bbg bitbase Group eingehalten werden (z.B. Meldepflicht bei Datenschutzverstößen). Der Bundesverband muss diese Verarbeitung in seinem Verzeichnis der Verarbeitungstätigkeiten nachweisen (s. Art. 30 DS-GVO). Trotzdem habe ich in mein Muster der Verarbeitungstätigkeiten das Mitgliedersystem ebenfalls aufgenommen, da es auch durch mich bzw. den Kreisverband Bochum mit Daten „gefüllt“ wird.

Erwartung:

Der Bundesverband sollte allen Untergliederungen (schriftlich) mitteilen,

- dass eine Aufnahme in das Verzeichnis **seiner** Verarbeitungstätigkeiten erfolgt ist
- die Verträge mit der bbg bitbase Group den Vorschriften der DS-GVO entsprechen.

6.2 Mitgliedschaft in der Europa-Union als Datum i.S. des Art. 6

Nach Art. 6 DS-GVO zählt die „politische Meinung“ zu den besonders geschützten Daten. Es kann der Eindruck entstehen, dass die Mitgliedschaft in der Europa-Union als politische Meinung gewertet werden kann.

Ich bin der Meinung, dass dies nicht der Fall ist, da die Europa-Union eine überparteiliche Organisation ist und mit einer Mitgliedschaft keine politische Meinung im Sinn einer Überzeugung für eine Partei zum Ausdruck gebracht wird. Hier kann nur abgewartet werden, wie sich die Meinung der Aufsichtsbehörden entwickelt.

7. Checkliste

Checkliste zur Umsetzung der DS-GVO

I. Wo stehen wir?

- Liegen von Mitgliedern Erklärungen nach alten Recht vor (Textvorschlag des Bundesverbandes mit Verweis auf BDSG a.F.)?
  - falls nein: ggf. bei nächster Gelegenheit nachholen, dabei neues Muster nutzen
- Wo sind Daten von Mitgliedern gespeichert?
  - Übersicht erstellen und entscheiden, ob dies zukünftig so bleiben soll/muss
  - Die Übersicht ist Grundlage für das Verzeichnis der Verarbeitungstätigkeiten
- Wer hat Zugriff auf die Mitgliederdaten?
  - Soll/muss das in Zukunft so bleiben?
- Gibt es angemessen Sicherheitsmaßnahmen?
  - Wer hat Zugriff auf den PC?
  - Datensicherung auf einem externen Medium?
    - Wird das Sicherungsmedium an einem sicheren Ort verwahrt (außerhalb des Aufstellungsortes für den PC!)?
  - Virenschutz, Installation von Updates?
- Gibt es einen Newsletter?
  - Zustimmung zum Versand des Newsletters überprüfen (Double-Opt-In), ggf. nachholen
- Wird eine Webseite betrieben?
  - Wo steht der Server, wer ist Auftragnehmer?
  - Welche personenbezogenen Daten werden vom Hoster gespeichert?
    - IP-Adressen aus technischen oder Sicherheitsgründen etc.
  - ggf. nachfragen und Vertrag über Auftragsdatenverarbeitung schließen
  - Impressum anpassen
- Wird das Medium E-Mail genutzt?
  - Welcher Hoster/Provider wird genutzt?
  - Regelungen zum (Nicht)Versand von personenbezogenen Daten mit Verschlüsselung?

II. Einwilligungserklärung/neue Beitrittserklärung

- Muster benutzen und anpassen (insbesondere falls SEPA-Mandat eingeholt wird)

III. Verzeichnis der Verarbeitungstätigkeiten

- Übersicht auswerten und nach Muster Verzeichnis erstellen
- sicher stellen, dass Änderungen am Verzeichnis nachvollzogen werden können und die vorherige Version für (mindestens) 1 Jahr aufbewahrt wird

- das Verzeichnis ist nicht öffentlich!

IV. Sicherstellen, dass Betroffene Personen ihre Rechte ausüben können

- Hinweise zu den Rechten sind in der Einwilligungserklärung enthalten
  - Auskunftsrecht (= Auszug aus dem Verzeichnis der Verarbeitungstätigkeiten)
    - ggf. Muster erstellen, in dem alles erklärt wird
    - (s. Muster des Heise-Verlages) „Datenschutzrechtliche Selbstauskunft nach DSGVO“
  - Recht auf Löschung
    - bedeutet den Austritt aus der Europa-Union!
  - Recht auf Übertragbarkeit
    - ggf. denkbar bei Fotos oder eigenen Beiträgen auf der Webseite.

V. Auf Anfragen der Aufsichtsbehörde vorbereitet sein!

- Aufsichtsbehörde ist die jeweilige Landes-Datenschutzbehörde. Für NRW die Landebeauftragte für den Datenschutz und Informationsfreiheit NRW, ggf. kann sich auch die Bundesbeauftragte mit Fragen an Verantwortliche wenden

VI. Auf den „Ernstfall“ vorbereitet sein

- Werden personenbezogene Daten gespeichert, die ein besonderes Risiko für die betroffen Person beinhalten können?
  - Muss das sein?
  - Im Fall einer Datenschutzverletzung muss ggf. die betroffene Person benachrichtigt werden!
- Sicher stellen, das bei Datenschutzverstößen die Meldepflicht an die Aufsichtsbehörde eingehalten werden kann (72 Stunden!)
  - Wer ist für die Meldung zuständig, wer muss noch informiert werden (Vorstand)?

VII. (Schriftliche) Verfahrensregelungen erarbeiten / Dokumentation

- Inhalt
  - Umgang mit Mitgliederdaten, Einsatz von Technik, Meldung von Verstößen
  - Löschfristen, Aufbewahrungsfristen, Datensicherung etc.
- Neuen Vorstandsmitgliedern zur Kenntnis geben, Kenntnisnahme bestätigen lassen!
- ggf. in das Verzeichnis der Verarbeitungstätigkeiten entsprechende Verweise / Anlagen aufnehmen.

VII. Rückkoppelung

- Regelmäßige Kontrolle der Regelungen, ggf. anpassen!

8. Muster einer Arbeitsanweisung für den Umgang mit personenbezogenen Daten

Europa-Union Deutschland
Kreisverband Irgendwo

XX.05.2018

Arbeitsanweisung „Umgang mit personenbezogenen Daten und dabei eingesetzten technischen Hilfsmittel“

Die nachfolgende Arbeitsanweisung regelt für den Kreisverband Irgendwo den Umgang mit personenbezogen Daten und die Nutzung der dabei eingesetzten technischen Hilfsmittel. Er gilt für alle durch den Kreisverband Irgendwo erhobenen, von anderen Stellen erhaltenen und durch ihn gespeicherten Daten.

1. Begriffsbestimmungen

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

Erheben ist das Beschaffen personenbezogener Daten bei der betroffenen Person oder Dritten.

Verarbeitung ist jede Nutzung personenbezogener Daten.

Weitergabe ist die Übermittlung personenbezogener Daten an andere (natürliche) Personen und juristische Personen des öffentlichen oder Privatrechts.

Technische Hilfsmittel sind alle zur Bearbeitung eingesetzten Werkzeuge wie Computer (auch Tablets und Smartphones), Drucker, Faxgeräte, Software und das Internet.

2. Grundsatz

Mit personenbezogenen Daten ist so umzugehen, dass das Recht auf Schutz personenbezogener Daten betroffener Personen nicht beeinträchtigt wird. Alle Funktionsträger gehen daher sensibel mit den ihnen zugänglichen Daten um.

3. Zugang zu personenbezogenen Daten

Zugang zu den durch den Kreisverband Irgendwo und in der zentralen Mitgliederverwaltung des Bundesverbandes gespeicherten Daten erhalten nur Funktionsträger, die diesen zu festgelegten Zwecken benötigen. Eine Übersicht ist als Anlage 1 beigefügt.

4. Pflicht zur Verschwiegenheit

Alle Funktionsträgern, die Zugang zu personenbezogenen Daten haben, wahren gegenüber anderen Personen Verschwiegenheit über diese personenbezogenen Daten.

5. Weitergabe personenbezogener Daten

Eine Weitergabe personenbezogener Daten ist nur im Rahmen der von den betroffenen Personen erteilten Einwilligung, gesetzlich oder der durch die Satzung des Kreisverbandes Irgendwo vorgesehenen Fälle zulässig.

Jede Weitergabe zu anderen Zwecken und an andere Stellen stellt einen Verstoß gegen die Vorschriften des Datenschutzes[13] dar und ist der Aufsichtsbehörde zu melden. Sofern aufgrund dieses Verstoßes ein Bußgeld gegen den Kreisverband Irgendwo festgesetzt wird, behält sich der Kreisverband die Geltendmachung von Ersatzansprüchen gegen die betreffende Person vor.

6. Einsatz technischer Hilfsmittel

Zur Speicherung und Verarbeitung personenbezogener Daten können vom Kreisverband Irgendwo bereitgestellte oder von berechtigten Funktionsträgern zur Verfügung gestellte Hilfsmittel (Computer, Drucker, Faxgeräte, Software, Internet) benutzt werden. Dabei sind die folgenden Regelungen zu beachten:

a) Der Computer bzw. das darauf eingesetzte Betriebssystem und die zur Verarbeitung eingesetzte Software sind durch die vom Hersteller bereitgestellten Updates auf dem aktuellen Stand zu halten. Betriebssysteme und Software, für die keine Updates mehr zur Verfügung gestellt werden, dürfen nicht genutzt werden.
b) Der Computer ist durch einen Passwortschutz gegen unbefugten Zugriff zu schützen.
c) Sofern „besondere geschützte Daten“[14] i.S. des Art. 9 Abs. 2 DS-GVO gespeichert werden, sind diese zu verschlüsseln.
d) Sofern ein Computer auch von anderen Personen genutzt wird, ist eine Trennung der Benutzer (z.B. unterschiedliche Benutzerkonten) erforderlich.
e) Vom Kreisverband Irgendwo zur Verfügung gestellten technische Hilfsmittel dürfen nicht zu privaten Zwecken genutzt werden. Insbesondere die Speicherung privater Daten auf den technischen Hilfsmitteln ist nicht zulässig.
f) Der Computer muss über eine Software zum Schutz gegen Schadprogramme („Anti-Viren-Software“) verfügen, welche fortlaufend aktualisiert wird.
g) Es ist ein regelmäßiges Backup auf einem externen Datenträger (Festplatte, DVD etc.) anzufertigen, welches an einem sicheren Ort unterzubringen ist und die Wiederherstellung der Daten ermöglicht.
h) Nicht benötigte oder fehlerhafte Ausdruck, die personenbezogene Daten enthalten sind so zu vernichten, dass Dritte eine Kenntnisnahme nicht mehr möglich ist (z.B. Schreddern).
i) Der Computer (insbesondere Tablets und Notebooks) ist gegen Diebstahl zu sichern; dies gilt insbesondere auf Reisen.
j) Personenbezogen Daten dürfen nicht ohne Sicherung gegen unbefugte Kenntnisnahme (z.B. Verschlüsselung) per E-Mail übertragen werden.
k) Sofern Faxgeräte zur Übertragung personenbezogener Daten genutzt werden, ist dafür zu sorgen, dass Dritte empfangene Faxsendungen nicht unbefugt zur Kenntnis nehmen können.
l) Personenbezogene Daten dürfen nicht auf gegen unbefugten Zugriff (z.B. durch Verschlüsselung) geschützte Datenträger (z.B. USB-Sticks) kopiert und transportiert werden.
m) Personenbezogene Daten dürfen nicht ohne Schutz (Verschlüsselung) gegen unbefugten Zugriff auf Speicherdiensten („Cloud“) gespeichert werden. Speicherdienste, deren Server nicht im Gebiet der Europäischen Union ihren Standort haben, dürfen nicht genutzt werden.
n) Unbrauchbare, fehlerhafte und nicht mehr lesbare Datenträger sind so zu vernichten, dass Dritten eine Kenntnisnahme der darauf gespeicherten Daten nicht mehr möglich ist.

---

13 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Amtsblatt der Europäischen Union L 119/1 vom 4.5.2016, Bundesdatenschutzgesetz vom 30. Juni 2017, BGBl I, Nr. 44, S. 2097

14 Das sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

o) Daten des Kreisverbandes sind auf Datenträgern von Funktionsträger zur Verfügung gestellten technischen Hilfsmitteln so zu kennzeichnen (z.B. Ablage in eindeutigen Ordnern), dass sie im Falle einer Beschlagnahme durch die Strafverfolgungsbehörden als zum Kreisverband gehörend erkennbar sind.

Für vom Kreisverband Irgendwo zur Verfügung gestellte technische Hilfsmittel trägt der Kreisverband die Verantwortung für die Einhaltung dieser Regelungen; für von Funktionsträgern zur Verfügung gestellte/eingesetzten technische Hilfsmittel der jeweilige Funktionsträger.

Stellt ein Funktionsträger private technische Hilfsmittel zur Verfügung, hat es ggf. Kontrollen durch die Aufsichtsbehörde zu dulden. Das Grundrecht auf Unverletzlichkeit der Wohnung wird insoweit dadurch eingeschränkt.

7. Meldepflicht nach Art. 33 DS-GVO

Verstöße gegen Datenschutzvorschriften sind der Aufsichtsbehörde zu melden. Sofern sich diese im Einflussbereich eines Funktionsträgers ereignen, hat dieses innerhalb von 24 Stunden den / die Vorsitzenden zu informieren, welche/welcher innerhalb der vorgesehenen Frist die Aufsichtsbehörde informiert/informieren.

8. Kenntnisnahme

Jeder Funktionsträger des Kreisverbandes Irgendwo, welches Zugang zu personenbezogenen Daten erhält, bestätigt die Kenntnisnahme dieser Arbeitsanweisung und den Erhalt einer Ausfertigung durch Unterschrift.

Durch den Vorstand des Kreisverbandes Irgendwo in der Sitzung am XX.XX.2018 beschlossen

Für die Richtigkeit

Schriftführer

Anlage 1:

Verzeichnis der Funktionsträger, die Zugang zu personenbezogenen Daten haben

Name	Zugriff auf	eingerichtet	gelöscht
Fritz Mustermann	Mitgliedersystem des Bundes	1.1.2017	31.12.2018

9. Muster einer Beitrittserklärung

Hinweis:

Das Muster ist an die Gegebenheiten des Verbandes anzupassen. Dies betrifft insbesondere

- die vertretungsberechtigte(n) Person(en) (Verantwortliche)
- die zuständige Beschwerdestelle (Landesdatenschutzbeauftragte(r)) bitte hierzu in der Liste im Anhang nachsehen
- die Einholung eines SEPA-Mandates zum Einzug der Mitgliedsbeiträge
- und die Höhe der Mitgliedsbeiträge, falls diese von denen des Bundesverbandes abweichen

Beitrittserklärung

Ja, ich möchte Mitglied der Europa-Union Deutschland, Kreisverband XXXXXX werden.
Meine persönlichen Daten:

Name, Vorname
wohnhaft in Postleitzahl, Ort:
Straße, Hausnummer:
geboren am:
E-Mail-Adresse:

Ich verpflichte mich, den satzungsgemäßen Beitrag zu zahlen, und zwar

☐ 24,-- EUR im Jahr (ermäßigt für SchülerInnen und Studierende)
☐ 48,-- EUR im Jahr (MIndestbeitrag)
☐ ___ EUR im Jahr (Selbsteinschätzung).

Fällige Beiträge werden durch den Kreisverband jährlich angefordert, indem ein vorbereiteter Überweisungsbeleg übersandt wird. Sofern Sie Ihre Beiträge mittels Dauerauftrag überweisen wollen, nutzen Sie dazu die unten angegebene Bankverbindung.

Der Kreisverband XXXXX ist wegen Förderung internationaler Gesinnung, der Toleranz auf allen Gebieten der Kultur und des Völkerverständigungsgedankens nach § 5 Abs. 1 Nr. 9 des Körperschaftssteuergesetzes von der Körperschaftssteuer und nach § 3 Nr. 6 des Gewerbesteuergesetzes von der Gewerbesteuer befreit. Für Mitgliedsbeiträge und Zuwendungen werden Ihnen Bescheinigungen ausgestellt.

Datum, Unterschrift

Einwilligung zur Erhebung, Speicherung, Verarbeitung und Übermittlung meiner personenbezogenen Daten

Ich willige ein, dass meine personenbezogenen Daten in dem auf der Rückseite genannten Umfang durch die Europa-Union Deutschland Kreisverband XXXXXX. erhoben, gespeichert, verarbeitet und übermittelt werden.

Datum, Unterschrift

Bankverbindung:
Sparkasse XXXXX• IBAN: DE68 0000000000000 • BIC:XXXXXXXXXX

Informationen zum Datenschutz und Ihren Rechten

► Erhebung personenbezogener Daten (Art. 6 und 7 der Datenschutz-Grundverordnung[15] - DS-GVO)
Mit dieser Beitrittserklärung werden Ihre personenbezogenen Daten im erforderlichen Umfang mit Ihrer Einwilligung erhoben.

► Information nach Art. 13 DS-GVO

Name und Kontaktdaten des Verantwortlichen (Art 13 Abs. 1 Buchst. a):
Europa-Union Deutschland, Kreisverband XXXXXXXX, Vorsitzender: Fritz Mustermann

Ansprechpartner:
Name
Straße
PLZ Ort
Tel.:
E-Mail:

Verarbeitung und Rechtsgrundlage der Datenverarbeitung (Art 13 Abs. 1 Buchst. c):
Ihre personenbezogenen Daten werden zum Zweck der Begründung und Betreuung des Mitgliedsverhältnisses verarbeitet (Anschreiben/Informationen – auch per E-Mail, Aufforderung zur Zahlung der Mitgliedsbeiträge etc.) Rechtsgrundlage für die Verarbeitung Ihrer personenbezogenen Daten ist Ihre umseitige Einwilligung.

Empfänger und Kategorien von Daten (Art 13 Abs. 1 Buchst. e):
Ihre personenbezogenen Daten - mit Ausnahme Ihrer Bankverbindung - werden der Europa-Union Nordrhein-Westfalen e.V. (Landesverband) und der Europa-Union Deutschland e.V. (Bundesverband) zur schriftlichen Kontaktaufnahme und ggf. Betreuung auf elektronischem Weg zur Verfügung gestellt. Eine Übermittlung an andere Stellen findet **nicht** statt!

Zeitdauer der Speicherung und Löschung Ihrer personenbezogenen Daten (Art. 13 Abs. 2 Buchst. a):
Ihre personenbezogenen Daten werden für die Dauer Ihrer Mitgliedschaft gespeichert und verarbeitet. Sofern Sie noch eine Bescheinigung für steuerliche Zwecke über gezahlte Mitgliedsbeiträge erhalten, werden die Daten nach Erstellung dieser Bescheinigung gelöscht. Aus steuerlichen Gründen sind Nachweise über ausgestellte Spendenbescheinigungen für die Dauer von 10 Jahren durch die Europa-Union aufzubewahren. Dies geschieht durch eine gesonderte Archivierung; eine weitere Verarbeitung oder Nutzung dieser Daten findet nicht statt.

Auskunfts-, Berichtigungs-, Löschungs-, Widerrufs und Beschwerderecht:
Sie haben jederzeit das Recht gegenüber den o.g. Verantwortlichen Auskunft nach Art. 15 DS-GVO über die zu Ihrer Person gespeicherten Daten und die Berichtigung nach Art. 16 DS-GVO oder Löschung der gespeicherten Daten nach Art. 17 DS-GVO zu verlangen. Sofern Sie von Ihrem Recht auf Löschung oder teilweisen bzw. ganzen Widerruf Gebrauch machen, endet damit Ihre Mitgliedschaft in der Europa-Union.

Beschwerdestelle
Sie können sich jederzeit an die zuständige Beschwerdestelle wenden:
Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
Kavalleriestr. 2-4
40213 Düsseldorf
Telefon: 0211/38424-0
Fax: 0211/38424-10
E-Mail: poststelle@ldi.nrw.de

15 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Amtsblatt der Europäischen Union L 119/1 vom 4.5.2016

10. Muster einer Datenschutzerklärung auf einer Webseite

„Datenerhebung und Datenschutz

Datenerhebung durch den Anbieter dieses Webangebotes

Dieses Webangebot erhebt keine personenbezogenen Daten. Eine Ausnahme stellen Daten dar, die von Ihnen hier (freiwillig) eingegeben und an uns in elektronischer Form versandt werden. Dies betrifft Daten, die Sie in einem ggf. vorhanden Kontaktformular eingeben und mittels des Schaltknopfes „Senden“ an uns übermittelt werden.

Datenerhebung durch den technischen Dienstleister

Dieses Webangebot wird durch die domainfactory GmbH auf einem Server bereitgestellt, welcher seinen Standort in Deutschland hat.

Der verwendete Webserver erfasst beim Aufruf dieses Webangebotes folgende Informationen:

- abgerufene Domain (hier „europa-union-bochum.de“ bzw. „.eu“)
- die dabei verwendete IP-Adresse Ihres Computers
- abgerufene Informationen
- Useragent (der von Ihnen bzw. Ihrem Computer verwendete Browser)
- Zeitpunkt der Anfrage
- Status Code (standardisierte numerische Angaben, die z.B. darstellt, ob die Anfrage erfolgreich beantwortet werden konnte)

um die Funktionsfähigkeit seiner informationstechnologischen Systeme und der Technik im Fall eines Fehlers sich zu stellen und um Strafverfolgungsbehörden im Falle eines Cyberangriffes die zur Strafverfolgung notwendigen Informationen bereitzustellen.

Diese Daten werden durch domainfactory für die Dauer von drei Tagen gespeichert und danach überschrieben (rotierende Speicherung). Ein Zugriff auf diese Daten seitens des Betreibers dieses Webangebotes findet nicht statt.

Cookies

Dieses Webangebot nutzt keine Cookies. Sofern Sie aber einen Beitrag kommentieren werden durch das verwendete System Cookies gesetzt, welche

- den verwendeten Namen der kommentierenden Person
- die angegebene E-Mail-Adresse und
- die ggf. angegebene Web-Adresse (URL) auf Ihrem Computer speichern.

Sofern Sie in Ihrem Kommentar personenbezogene Daten angeben (z.B. Ihren realen Namen), werden diese ebenfalls in elektronischer Form gespeichert und an uns übermittelt.

Speicher- / Löschfristen

Sofern Sie uns über ein Kontaktformular oder die Kommentarfunktion personenbezogene Daten übermitteln, werden diese durch uns gespeichert und nach Bearbeitung / Beantwortung Ihrer Frage von uns gelöscht.

Schutz Ihrer personenbezogener Daten bei einer Kommunikation mit uns

Bitte beachten Sie, dass Nachrichten, die in elektronischer Form (z.B. über ein Kontaktformular oder per E-Mail) über das Internet übermittelt werden, von Dritten unbefugt zur Kenntnis genommen und u.U. verfälscht werden können. Wir empfehlen im Zweifelsfall eine schriftliche oder telefonische Kontaktaufnahme.“

11. Muster „Verzeichnis der Verarbeitungstätigkeiten“

Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO[16]

für die Europa-Union Deutschland Kreisverband XXXX

Version	erstellt am	durch	gültig ab
0.1 (initiale Version)	8.2.2018		Entwurf
0.2	15.3.2018		Entwurf
1.0	17.5.2018		25.5.2018

16 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Amtsblatt der Europäischen Union L 119/1 vom 4.5.2016

Vorschlag für die Gliederung:

a) Zweck der Verarbeitung:

b) Kategorien betroffener Personen und personenbezogener Daten – Art. 30 Abs. 1 S. 2 lit. c

c) Kategorien von Empfängern – Art. 30 Abs. 1 S. 2 lit. d

d) Speicherdauer – Art. 30 Abs. 1 S. 2 lit. f

e) Technische und organisatorische Maßnahmen – Art. 30 Abs. 1 S. 2 lit. g

f) Rechtsgrundlage der Verarbeitung, Informationspflicht

Vorbemerkung

Die Europa-Union Deutschland Kreisverband XXXXXX. ist ein rechtsfähiger eingetragener Verein, welcher Daten seiner Mitglieder und an der Arbeit der Europa-Union interessierter Personen erhebt, in elektronischer Form speichert, verarbeitet und übermittelt. Dazu bedient sie sich

- einer privaten Datenverarbeitungsanlage (PC des Geschäftsführers)
- einem Mitglieder-Verwaltungssystem (Kameon), welches bereitgestellt wird durch die

  bbg bitbase group GmbH
  Am Heilbrunnen 47
  72766 Reutlingen.

Aufgrund der hierarchischen Struktur der Europa-Union Deutschland (Bundesverband und Gliederung in Landes-, Kreis bzw. Ortsverbände) ist die Übermittlung von Mitgliedsdaten an den Landesverband Nordrhein-Westfalen und den Bundesverband zwingend erforderlich um z.B. die diesen zustehenden Beitragsanteile zu berechnen. (**Anmerkung:** Hier ist auch aufzuführen, wenn der Landesverband den Einzug der Mitgliedsbeiträge übernimmt!)

Dieses Verzeichnis der Verarbeitungstätigkeiten wird in elektronischer Form geführt. Es kann jederzeit an die zuständige Aufsichtsbehörde in elektronischer oder körperlicher Form (Ausdruck) übermittelt werden. Die Historie dieses Dokumentes ergibt sich aus der in der Titelseite dargestellten Tabelle, in der Änderungen dokumentiert werden. Nach einer Änderung wird zur Dokumentation des vorherigen Zustandes die vorherige Version dieses Dokumentes für den Zeitraum eines Jahres aufbewahrt (Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO).

Name und Kontaktdaten des Verantwortlichen (Art. 13 Abs. 1 lit. a DSGVO):

Der Vorstand der Europa-Union Deutschland, Kreisverband XXXXX., vertreten durch den / die Vorsitzenden XXXXX, diese vertreten durch:

Name – Geschäftsführer der Europa-Union Deutschland Kreisverband XXXX
Straße
Postleitzahl Ort
Tel.:
Fax:
E-Mail:

als für die Verwaltung der Mitgliederdaten zuständige Person.

Datenschutzbeauftragter:

Die Bestellung eines Datenschutzbeauftragten ist nicht erforderlich.

Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO:

Die Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO ist nicht erforderlich, da u.a. keine Daten nach Art. 35 Abs. 3 lit. a-c, insbesondere nach Art. 9 Abs. 1 erhoben / gespeichert / verarbeitet werden[17] und die zur Verarbeitung der personenbezogenen Daten verwendeten Techniken keine „neuen“ sind.

Hinweis:

> *Diese Einschätzung erfolgt vorbehaltlich einer Einstufung durch eine Aufsichtsbehörde und Aufnahme in eine Liste nach Art. 35 Abs. 4!*

17 Es ist noch zu klären, ob die Mitgliedschaft / das Interesse an der Europa-Union eine „politische Meinung i.S. des Art. 9 Abs. 1 darstellt. Ich meine nicht, da die Europa-Union eine politische aber überparteiliche Organisation ist.

Verzeichnis

I. Mitgliederdaten – Verarbeitung durch den Kreisverband

a) Zweck der Verarbeitung

Zweck der Verarbeitung der personenbezogenen Daten ist die Betreuung des/der Mitgliedsverhältnisse(s) der Mitglieder des Kreisverbandes. Dies umfasst:

- den Ausdruck personalisierter Anschreiben z.B. zur Information über Veranstaltungen
- Einzug der Mitgliedsbeiträge / Aufforderung zur Zahlung von Mitgliedsbeiträgen
- die Nachweisung gezahlter Mitgliedsbeiträge zur Ausstellung entsprechender Bescheinigungen[18]
- den Versand von Gratulationsschreiben (Geburtstag) ab Vollendung des 60. Lebensjahres
- ggf. den Kontakt per E-Mail

b) Kategorien betroffener Personen und personenbezogener Daten - Art. 30 Abs. 1 S. 2 lit. c

betroffene Personen:

aktive Mitglieder des Kreisverbandes Bochum

personenbezogene Daten:

1. Name, Vorname
2. Anschrift (Straße, Hausnummer und Ort)
3. Geburtsdatum
4. E-Mail-Adresse
5. Höhe des Beitrages
6. Höhe des in den vergangenen Jahren gezahlten Beitrages
7. ggf. Bankverbindung (IBAN)

c) Kategorien von Empfängern – Art. 30 Abs. 1 S. 2 lit. d

1. Europa-Union Deutschland Landesverband Nordrhein-Westfalen e.V.,
2. Europa-Union Deutschland e.V. - Bundesverband

d) Speicherdauer – Art. 30 Abs. 1 S. 2 lit. f

Die Daten werden für die Dauer des Mitgliedsverhältnisses gespeichert. Eine Löschung erfolgt mit Beendigung der Mitgliedschaft, sofern nicht zu steuerlichen Zwecken eine Bescheinigung über gezahlte Mitgliedsbeiträge zu erstellen ist. Da diese Daten aus steuerlichen Gründen (Nachweis über ausgestellte Spendenbescheinigungen gegenüber den zuständigen Finanzbehörden) für die Dauer von 10 Jahren aufzubewahren sind, werden die Daten in eine gesonderte Datei (Textdatei im pdf-Format) überführt und getrennt vom übrigen Datenbestand archiviert. Nach Ablauf der Aufbewahrungsfrist werden die Daten gelöscht.

e) Technische und organisatorische Maßnahmen – Art. 30 Abs. 1 S. 2 lit. g

Optional:

18 Der Kreisverband Bochum e.V. ist als gemeinnützig anerkannt. Mitgliedsbeiträge können steuerlich geltend gemacht werden. Die Vorlage einer solchen Bescheinigung entfällt ab dem Steuerjahr 2019.

- Für den Umgang mit personenbezogenen Daten und die Nutzung technischer Hilfsmittel wurde durch Beschluss des Vorstandes vom XXXX eine Regelung erstellt.

Technische Maßnahmen:

Zum Schutz der personenbezogenen Daten vor unbefugten Zugriff, einer nicht dem Zweck entsprechenden Verarbeitung, Verlust usw. werden der Sensibilität[19] der Daten entsprechende technische Maßnahmen getroffen. Dies sind:

- eine ständige Aktualisierung des eingesetzten Betriebssystems und der zur Verarbeitung genutzten Software auf dem Datenverarbeitungsgerät
  - eingesetztes Betriebssystem: Linux Mint (derzeit Version 18.3)
  - eingesetzte Software: LibreOffice (derzeit Version 6.0)
- eine regelmäßige Sicherung der Daten auf einer externen Festplatte, die sich an einem sicheren Ort befindet
- (**Anmerkungen:** Bei einem Computer mit Windows ist hier der Virenschutz zu erwähnen. Wird der Computer auch von anderen Personen genutzt, sind entweder technische Maßnahmen (z.B. Verschlüsselung) zu treffen, die ein unbefugtes Verändern/Löschen/zur Kenntnis nehmen verhindern. In diesem Fall sind mindestens organisatorische Maßnahmen erforderlich – schriftliche Anweisung, die zu dokumentieren ist)

Organisatorische Maßnahmen:

Zugang zum Datenverarbeitungsgerät hat nur der Verantwortliche; weitere organisatorische Maßnahmen erübrigen sich somit. (**Anmerkung:** Wird der Computer von mehreren Personen benutzt sind ggf. Regelungen erforderlich, wie sicher gestellt wird, dass diese Personen nicht unbefugt auf diese Daten zugreifen und sie verändern/löschen/zur Kenntnis nehmen können).

Bei einer elektronischen Kommunikation werden über Empfänger- und Absenderangaben hinaus keine personenbezogenen Daten übermittelt.

f) Rechtsgrundlage der Verarbeitung, Informationspflicht

Rechtsgrundlage der Verarbeitung ist die Einwilligung der betroffenen Person. Die Einwilligung wurde zusammen mit der Beitrittserklärung erteilt. Darin werden auch die in Art. 13 DS-GVO vorgeschriebenen Informationen gegeben. Beitrittserklärungen werden archiviert.

19 s. Anlage „Schutzbedarfsfeststellung“

II. Mitgliederdaten – Auftragsdatenverarbeitung

Aufgrund eines zwischen der Europa-Union Deutschland e.V. (Bundesverband) und der bbg GmbH geschlossenen Vertrages stellt die bbg GmbH das Mitgliederverwaltungssystem Kameon dem Bundesverband und allen Landes- und Kreisverbänden zur Verfügung.

Hierbei handelt es sich um eine Auftragsdatenverarbeitung i.S. des Art 30 Abs. 2., welche im Verzeichnis der Verarbeitungstätigkeiten der bbg GmbH und dem Verzeichnis der Auftragsdatenverarbeitung des Bundesverbandes zu dokumentieren ist. Das Auftragsverhältnis ist zwischen dem Bundesverband und der bbg GmbH begründet worden. Es wird davon ausgegangen, dass dieses entweder der geltenden Rechtslage entspricht oder zeitnah angepasst wird. Verantwortlich hierfür ist der Bundesverband.

III. Kontaktdaten

a) Zweck der Verarbeitung:

Zweck der Verarbeitung der personenbezogenen Daten ist die Betreuung von an der Arbeit der Europa-Union interessierten Personen. Dies umfasst:

- den Ausdruck personalisierter Anschreiben z.B. zur Information über Veranstaltungen
- ggf. den Kontakt per E-Mail

b) Kategorien betroffener Personen und personenbezogener Daten - Art. 30 Abs. 1 S. 2 lit. c

betroffene Personen:

Personen, die sich für die Arbeit der Europa-Union interessieren und dies entsprechend bekundet haben (z.B. Eintragung in eine bei einer Veranstaltung ausgelegten Liste)

personenbezogene Daten:

1. Name, Vorname
2. Anschrift (Straße, Hausnummer und Ort)
3. ggf. E-Mail-Adresse

c) Kategorien von Empfängern – Art. 30 Abs. 1 S. 2 lit. d

Es findet keine Übermittlung statt

d) Speicherdauer – Art. 30 Abs. 1 S. 2 lit. f

Die Daten werden für die Dauer eines bekundeten Interesses gespeichert. Eine Löschung erfolgt sofern Briefpost oder E-Mails nicht mehr zustellbar sind, oder die betroffene Person dies wünscht..

e) Technische und organisatorische Maßnahmen – Art. 30 Abs. 1 S. 2 lit. g

Optional:

- Für den Umgang mit personenbezogenen Daten und die Nutzung technischer Hilfsmittel wurde durch Beschluss des Vorstandes vom XXXX eine Regelung erstellt.

Technische Maßnahmen:

Zum Schutz der personenbezogenen Daten vor unbefugten Zugriff, einer nicht dem Zweck entsprechenden Verarbeitung, Verlust usw. werden dem Schutzbedarf[20] der Daten entsprechende technische Maßnahmen getroffen. Dies sind:

- eine ständige Aktualisierung des eingesetzten Betriebssystems und der zur Verarbeitung genutzten Software auf dem Datenverarbeitungsgerät
  - eingesetztes Betriebssystem: Linux Mint (derzeit Version 18.3)
  - eingesetzte Software: LibreOffice (derzeit Version 6.0)
- eine regelmäßige Sicherung der Daten auf einer externen Festplatte, die sich an einem sicheren Ort befindet
- (**Anmerkungen:** Bei einem Computer mit Windows ist hier der Virenschutz zu erwähnen. Wird der Computer auch von anderen Personen genutzt, sind entweder technische Maß-

20 s. Anlage „Schutzbedarfsfeststellung“

nahmen (z.B. Verschlüsselung) zu treffen, die ein unbefugtes Verändern/Löschen/zur Kenntnis nehmen verhindern. In diesem Fall sind mindestens organisatorische Maßnahmen erforderlich – schriftliche Anweisung, die zu dokumentieren ist)

Organisatorische Maßnahmen:

Zugang zum Datenverarbeitungsgerät hat nur der Verantwortliche; weitere organisatorische Maßnahmen erübrigen sich somit. (**Anmerkung:** Wird der Computer von mehreren Personen benutzt sind ggf. Regelungen erforderlich, wie sicher gestellt wird, dass diese Personen nicht unbefugt auf diese Daten zugreifen und sie verändern/löschen/zur Kenntnis nehmen können).

Bei einer elektronischen Kommunikation werden über Empfänger- und Absenderangaben hinaus keine personenbezogenen Daten übermittelt.

f) Rechtsgrundlage der Verarbeitung, Informationspflicht

Rechtsgrundlage der Verarbeitung ist die Einwilligung der betroffenen Person. Die Einwilligung wurde zusammen mit dem Wunsch nach Übersendung von Information explizit erteilt Darin werden auch die in Art. 13 DS-GVO vorgeschriebenen Informationen gegeben. Die Unterlagen werden archiviert.

III. Betrieb einer Internet-Präsenz

(www.europa-union-XXXX.de bzw. .eu)

a) Zweck der Verarbeitung:

Zweck der Internet-Präsenz ist die Darstellung der Arbeit der Europa-Union in Wort und Bild. Personenbezogenen Daten werden bei der Nutzung des Angebots durch die Europa-Union XXXXX nicht erhoben.

b) Kategorien betroffener Personen und personenbezogener Daten - Art. 30 Abs. 1 S. 2 lit. c

betroffene Personen:

(theoretisch) Nutzer auf der ganzen Welt

personenbezogene Daten:

entfällt

c) Kategorien von Empfängern – Art. 30 Abs. 1 S. 2 lit. d

Es findet keine Übermittlung statt

d) Speicherdauer – Art. 30 Abs. 1 S. 2 lit. f

Durch die Europa-Union werden keine Daten gespeichert.

e) Technische und organisatorische Maßnahmen – Art. 30 Abs. 1 S. 2 lit. g

Technische Maßnahmen:

Der Standort des Servers, auf dem das Angebot bereitgehalten wird, ist in Deutschland.

Organisatorische Maßnahmen:

Auf einer eigenen Seite des Angebotes werden Nutzer auf den Datenschutz und die technischen Gegebenheiten des Internet hingewiesen.

Anlage:

Schutzbedarfsfeststellung[21] - Art. 32 Abs. 2 DSGVO „angemessenes Schutzniveau“

Um den Schutzbedarf von Daten und IT-Systemen einschätzen zu können, wird im allgemeinen das IT-Grundschutzhandbuch des Bundesamt für Sicherheit in der Informationstechnik (BSI) verwendet. Dieses sieht vor, dass bei der Erstellung eines Sicherheitskonzeptes eine Schutzbedarfsanalyse durchgeführt. Die Feststellung des Schutzbedarfes soll es ermöglichen, die notwendigen und angemessen Vorkehrungen (technische und organisatorische Maßnahmen) zum Schutz personenbezogener Daten und der bei der Verarbeitung eingesetzten Systeme zu treffen.

Da der Schutzbedarf sich meistens nicht ohne weiteres quantifizieren lässt, wird auf eine Einteilung in Kategorien zurückgegriffen:

Schutzbedarfskategorien/-stufen	
"normal" – Stufe I	Die Schadensauswirkungen sind begrenzt und überschaubar.
"hoch" – Stufe II	Die Schadensauswirkungen können beträchtlich sein.
"sehr hoch" - Stufe III	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Diese Einteilung kann auf den Schutzbedarf der personenbezogenen Daten und zur Verarbeitung eingesetzten Systeme angewendet werden. Um die Schutzbedarfskategorien "normal", "hoch" und "sehr hoch" voneinander abgrenzen zu können, bietet es sich an, die Grenzen für die einzelnen Schadensszenarien zu bestimmen. Zur Orientierung, welchen Schutzbedarf ein potentieller Schaden und seine Folgen erzeugen, dienen die folgende Übersicht, die entsprechend angepasst wurde:

- **Schutzbedarfskategorie normal (niedrig bis mittel), Stufe I:**
  - Ein möglicher Schaden hätte nur begrenzte und überschaubare Auswirkungen auf den Kreisverband:
    - Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen allenfalls geringfügige juristische Konsequenzen oder Konventionalstrafen.
    - Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten nur geringfügige Auswirkungen auf die davon Betroffenen und würden von diesen toleriert.
    - Die persönliche Unversehrtheit wird nicht beeinträchtigt.
    - Die internen Abläufe des Kreisverbandes werden allenfalls unerheblich beeinträchtigt. Ausfallzeiten von mehr als 24 Stunden können hingenohttps://www.datenschutzzentrum.de/dsgvo/mmen werden.
    - Das Ansehen des Kreisverbandes bei den Mitgliedern und in der Öffentlichkeit wird nicht beeinträchtigt.

- **Schutzbedarfskategorie hoch, Stufe II:**
  - Ein möglicher Schaden hätte beträchtliche Auswirkungen auf den Kreisverband:
    - Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen schwerwiegende juristische Konsequenzen oder hohe Konventionalstrafen.
    - Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten beträchtliche Auswirkungen auf die davon Betroffenen und würden von diesen nicht toleriert.
    - Die persönliche Unversehrtheit wird nicht beeinträchtigt.
    - Die Abläufe des Kreisverbandes werden erheblich beeinträchtigt. Ausfallzeiten dürfen maximal 24 Stunden betragen.

21 s. Bundesamt für Sicherheit in der Informationstechnik (BSI) - BSI-Standard 100-2

        - Das Ansehen des Kreisverbandes bei den Mitgliedern und in der Öffentlichkeit wird erheblich beeinträchtigt.

- **Schutzbedarfskategorie sehr hoch, Stufe III:**

    - Ein möglicher Schaden hätte katastrophale Auswirkungen auf den Kreisverband:
        - Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen juristische Konsequenzen oder Konventionalstrafen, welche die Existenz des Kreisverbandes gefährden.
        - Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten ruinöse Auswirkungen auf die gesellschaftliche oder wirtschaftliche Stellung der davon Betroffenen.
        - Die persönliche Unversehrtheit wird ggf. beeinträchtigt.
        - Die Abläufe im Kreisverband werden so stark beeinträchtigt, dass Ausfallzeiten, die über 2 Stunden hinausgehen, nicht toleriert werden können.
        - Das Ansehen des Kreisverbandes bei den Mitgliedern und in der Öffentlichkeit wird grundlegend und nachhaltig beschädigt.

Anmerkung:

Die Darstellung der Schutzbedarfskategorien berücksichtigt bei der Aussage zu einem Verstoß gegen Gesetze und Vorschriften, nicht die von einer Aufsichtsbehörde möglicherweise zu verhängenden Bußgelder wegen eines Verstoßes gegen die Datenschutz-Grundverordnung. Sie dient lediglich dazu, den angemessenen Schutzbedarf der Daten/Systeme einzuordnen!

Schutzbedarfsfestlegung:

Aufgrund der Art der erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten und den zur Verarbeitung eingesetzten Systeme erscheint die Festlegung des Schutzbedarfes „normal“ bzw. „niedrig bis mittel“ gerechtfertigt.

Somit sind als technische und organisatorische Maßnahmen solche ausreichend und angemessen, die diesem Schutzbedarf gerecht werden. Hierzu können die Maßnahmen des IT-Grundschutzhandbuches genutzt werden, sofern eine Anwendung sinnvoll ist.

11. Abkürzungsverzeichnis

BDSG – Bundesdatenschutzgesetz
BDSG a.F. - Bundesdatenschutzgesetz alte Fassung (bis zum 25. Mai 2018)
BDSG n.F. - Bundesdatenschutzgesetz neue Fassung (ab dem 25. Mai 2018)
BGB – Bürgerliches Gesetzbuch
DS-GVO (auch: DSGVO) – Datenschutz-Grundverordnung
DSK - Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

12. Liste der zuständigen Aufsichtsbehörden der Länder

Zuständige Aufsichtsbehörden für die Datenverarbeitung durch nicht-öffentliche Stellen sind nach § 40 BDSG n.F. die „nach Landesrecht zuständigen Behörden“. Dies sind in der Regel die Landesbeauftragten für den Datenschutz. Der Bundesdatenschutzbeauftragte führt ein Verzeichnis, welches unter diesem Link abrufbar ist:

https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html

Bitte beachten, dass die jeweiligen Landesdatenschutzbeauftragten und Aufsichtsbehörden nicht unbedingt identisch sind (z.B. in Bayern)! Im Verzeichnis des Bundesdatenschutzbeauftragten daher in der Rubrik „Aufsichtsbehörden für den nicht-öffentlichen Bereich“ nachsehen.

13. Linkliste

Hinweis: Da sich verlinkte Dokumente ändern können, sollte die Aktualität durch einen Besuch auf den entsprechenden Seiten geprüft werden. Bitte dort nachsehen, ob es ggf. eine neuere Version des Dokuments gibt.

Text der EU-Datenschutz-Grundverordnung:

http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02016R0679-20160504

Text des Bundesdatenschutzgesetzes (neue Fassung):

http://www.bgbl.de/xaver/bgbl/start.xav?tartbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s2097.pdf

Text des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (s. §§ 22, 23 zum Thema „Recht am eigenen Bild):

https://www.gesetze-im-internet.de/kunsturhg/KunstUrhG.pdf

Kurzpapiere der DSK u.a. abrufbar unter:

https://www.lfd.niedersachsen.de/startseite/dsgvo/anwendung_dsgvo_kurzpapiere/ds-gvo---kurzpapiere-155196.html

Nützliche Informationen des Bayerischen Landesamtes für Datenschutzaufsicht:

https://www.lda.bayern.de/de/datenschutz_eu.html

Informationen des BSI zum Thema Sicherheit:

https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/Massnahmen_gegen_Internetangriffe.html

Broschüre „Datenschutz im Verein nach der Datenschutzgrundverordnung (DS-GVO)“ des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg

https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/OH-Datenschutz-im-Verein-Stand-1.-Mai-2017.pdf

Muster der Zeitschrift c't zur Selbstauskunft (zu Ziff. 5.9.1)

ftp://ftp.heise.de/pub/ct/listings/1805-112.zip

Muster der Zeitschrift c't zur Auskunft über gespeicherte Daten (zu Ziff. 5.9.1)

https://www.heise.de/downloads/18/2/3/7/4/9/0/2/ct5F_Test_DSGVO.pdf

Die wichtigsten Antworten zur DSGVO des Bundesinnenministeriums (zuständig für Datenschutz):

https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2018/04/faqs-datenschutz-grundverordnung.html

Das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein (ULD) hat eine Reihe von Praxis-Guides zur Umsetzung der DS-GVO-Vorgaben herausgebracht, einer davon beispielsweise speziell auf die Bedürfnisse von Vereinen zugeschnitten:

https://www.datenschutzzentrum.de/dsgvo/

Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (**Achtung:** bitte regelmäßig auf Aktualität prüfen!):

https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/Liste-Art-35-4-NRW-NOeB_v1_.pdf

WordPress Plugins und ihre Konformität zur DS-GVO:

https://www.blogmojo.de/wordpress-plugins-dsgvo/

Copyright