arbeitsgemeinschaft der eine welt-landesnetzwerke in deutschland e.v.

DSGVO – ZENTRALE ANFORDERUNGEN

Berlin, 16. Mai 2018

*Liebe Kolleg*innen aus den Landesnetzwerken,*

ab dem 25. Mai 2018 greift die neue Datenschutz-Grundverordnung, die für alle Organisationen, Vereine und Unternehmen verbindlich ist.

*Wir haben uns in Broschüren eingelesen, Fortbildungen und Webinare besucht und uns mit Kolleg*innen aus den LNW und anderen Vereinen ausgetauscht. Das Ergebnis davon präsentieren wir euch mit folgendem Papier, indem wir einen Überblick über die Neuerungen und Regeln der neuen Datenschutz-Grundverordnung geben und die wichtigsten Punkte für eure Arbeit zusammenfassen.*

Am Ende des jeweiligen Kapitels findet ihr Hinweise, die ihr für die konkrete Umsetzung nutzen könnt. Auch Hinweise auf Musterformulare, die ihr bei der agl Geschäftsstelle anfragen könnt.

Viele Grüße

Carolina und Christa

Carolina Ritter
agl - Bürokoordination und Kommunikation
verwaltung@agl-einewelt.de

Christa Pashalides
agl - Referentin für Vorstand und Geschäftsführung
vorstand-assistenz@agl-einewelt.de

arbeitsgemeinschaft der eine welt-landesnetzwerke in deutschland e.v.

DATENSCHUTZRECHT ALLGEMEIN

„Ab dem 25. Mai 2018 gilt ein neues Datenschutzrecht (EU-Datenschutz-Grundverordnung und neues Bundesdatenschutzgesetz) mit verschärften **Transparenz- und Rechenschaftspflichten**. Es ist immer anwendbar, wenn personenbezogene Daten verarbeitet werden.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (nicht juristische Person) beziehen, z.B. **Name, Adresse, Kontodaten, E-Mail Adresse, IP-Adresse, Webtracking durch Cookies**."[1]

Im Folgenden sind sie zu einigen zentralen Punkten/Informationen zusammengestellt:

Inhaltsverzeichnis:

1 Datenschutzbeauftragter (DSB) 3
2 Verzeichnis von Verarbeitungstätigkeiten 4
3 Datenschutz-Verpflichtung von Beschäftigten 5
4 Informations- und Auskunftspflichten 5
5 Löschen von Daten 7
6 IT-Sicherheit 7
7 Auftragsverarbeitung 8
8 Datenschutzverletzungen 8
9 Datenschutz-Folgeabschätzung (DSFA) 9
10 Umgang mit Fotos im Internet 9
Links und Literatur 10

[1] BER (2017): Sie sind verhaftet. Regeln und Haftung bei Websites und Social Media von entwicklungspolitischen Nichtregierungsorganisationen, S. 12

1 DATENSCHUTZBEAUFTRAGTER (DSB)

In aller Regel ist nur dann ein DSB zu benennen, wenn *mindestens 10 Personen*[2] ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. „Ständig beschäftigt" ist, wer z. B. permanent Mitgliederverwaltung macht – „nicht ständig beschäftigt" ist dagegen bspw., wer als Übungsleiter nur mit den Namen seiner Mannschaft umgeht.

- DSK-Kurzpapier Nr. 12:
  www.lda.bayern.de/media/dsk_kpnr_12_datenschutzbeauftragter.pdf[3]

Zuständig für den zum Schutz personenbezogener Daten ist der Vorstand. Wenn der Verein mehr als neun Personen beschäftigt, muss er einen Datenschutzbeauftragten bestellen, der selbst nicht Vorstandsmitglied sein darf. Zu den Beschäftigten zählen nur bezahlte Mitarbeiter, keine Ehrenamtler.[4]

Es sollte kein Interessenskonflikt zwischen dem Datenschutzbeauftragten und datenverarbeitenden Mitarbeitern bestehen. Bei Personalunion aus einem Mitarbeiter der Personalabteilung oder EDV-Verantwortlichen und dem Datenschutzbeauftragten, liegt ein solcher Interessenkonflikt vor.

Es ist zwar nicht vorgeschrieben, aber wird dringend empfohlen die Benennung des DSB schriftlich festzuhalten, um gegenüber der Aufsichtsbehörde nachzuweisen, dass zu jedem Zeitpunkt tatsächlich der vom Gesetz geforderte Datenschutzbeauftragte benannt war.[5]

Die Kontaktdaten des DSB müssen der Aufsichtsbehörde mitgeteilt werden.

Aufgaben des DSB:

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten hinsichtlich ihrer Pflichten nach Datenschutzrecht
- Überwachung der Einhaltung der gesetzlichen Datenschutzvorschriften
- Beratung im Zusammenhang mit Datenschutz-Folgenabschätzungen
- Zusammenarbeit mit der Aufsichtsbehörde
- Anlaufstelle für die Aufsichtsbehörde in Fragen
- Beratung betroffener Personen
- Verzeichnis erstellen
- Datenschutzrichtlinien erstellen
- Besuch von Fortbildungen/Schulungen zum DSGVO

[2] Maßgeblich ist die Zahl der Köpfe, nicht die Zahl der Stellen der Personen.
[3] Bayerisches Landesamt für Datenschutzaufsicht: Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an kleine Unternehmen, Vereine, etc. Muster Verein: https://www.lda.bayern.de/media/muster_1_verein.pdf
[4] Vereinsknowhow.de/ bnve e.V.: Vereinsinfobrief Nr. 340 – Ausgabe 1/2018 – 10.01.2018, Seite 1
[5] Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine, C.H.Beck, S. 35

Rechtlich gesehen bleibt die Verantwortlichkeit beim Geschäftsführer oder dem Vereinsvorstand. Sie geht nicht auf den Datenschutzbeauftragen über.

HINWEIS:

➔ Die wenigsten werden in der Situation sein, eine*n Datenschutzbeauftragte*r beauftragen zu müssen, es empfiehlt sich dennoch eine*n Zuständige*n im Team für Datenschutz zu benennen und dies schriftlich festzuhalten. Die oben genannten Aufgaben fallen in diesem Fall auch an.

2 VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

Um über einen Überblick über die Daten zu bekommen, die man sammelt, empfiehlt es sich ein Verzeichnis von Verarbeitungstätigkeiten zu erstellen. Das Verarbeitungsverzeichnis wird von einer Behörde meist dann eingefordert werden, wenn ein Verstoß gegen die DSGVO vorliegt. **Ein meldepflichtiger Verstoß gegen die DSGVO liegt beispielsweise bereits vor, wenn der Versand von E-Mails an mehrere persönliche E-Mailadressen nicht unter „bcc" erfolgt, sondern für alle Empfänger sichtbar über „An" oder „cc" getätigt wird.**

Liegt ein Verstoß gegen die DSGVO vor und eine Organisation kann das durch die Behörde angeforderte Verzeichnis nicht vorlegen, wird das als Missachtung des DSGVO mit den entsprechenden Folgen bewertet werden.

Vereine, die regelmäßige Mitgliederverwaltung und Beitragsabrechnung machen, müssen ein vom Umfang her sehr überschaubares Verzeichnis ihrer Verarbeitungstätigkeiten führen.

- BayLDA Muster-Verzeichnis für kleine Vereine:
  www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf
- DSK-Kurzpapier Nr. 1:
  www.lda.bayern.de/media/dsk_kpnr_1_verzeichnis_verarbeitungstaetigkeiten.pdf
- DSK-Muster-Verzeichnis allgemein:
  www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf[6]

Das Verzeichnis von Verarbeitungstätigkeiten enthält mehrere Verfahrensbeschreibungen. In den Verfahrensbeschreibungen werden die Verarbeitungsschritte von personenbezogenen Daten dokumentiert. Aus den Dokumenten muss hervorgehen, welche personenbezogenen Daten das

[6] Bayerisches Landesamt für Datenschutzaufsicht: Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an kleine Unternehmen, Vereine, etc. Muster Verein: https://www.lda.bayern.de/media/muster_1_verein.pdf

Unternehmen mit Hilfe welcher Verfahren auf welche Weise verarbeitet und welche technisch-organisatorischen Maßnahmen zum Schutz dieser Daten dabei getroffen wurden.

HINWEIS:

- ➔ Muss nicht veröffentlicht werden, nur für interne Ablage. Bei Anfrage für Aufsichtsbehörden vorhalten
- ➔ Welche Daten werden erhoben, für welchen Zweck? (nicht zu kleinteilig)
- ➔ Werden diese Daten an Dritte weitergegeben? (z.B. an Post für Versand, Mailchimp Newsletterversand)
- ➔ Muster in der Broschüre „Erste Hilfe zur DSGVO“

3 DATENSCHUTZ-VERPFLICHTUNG VON BESCHÄFTIGTEN

Bei der Aufnahme der Tätigkeit sind Beschäftigte, die mit personenbezogenen Daten umgehen, zu informieren und dahingehend zu verpflichten, dass die Verarbeitung der personenbezogenen Daten auch durch sie nach den Grundsätzen der DS-GVO erfolgt.

- BayLDA Info-Blatt zur Verpflichtung: www.lda.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf

4 INFORMATIONS- UND AUSKUNFTSPFLICHTEN

Jeder Verantwortliche hat den betroffenen Personen schon bei der Datenerhebung bestimmte Informationen über die Verarbeitung ihrer Daten zu geben. Ein Verein muss bspw. Informationen auf der Homepage und der Satzung leicht zugänglich bereithalten. Die betroffenen Personen (z.B. Vereinsmitglieder) haben auch das Recht, Auskunft über die Verarbeitung ihrer Daten zu erhalten.

- DSK-Kurzpapier Nr. 6: www.lda.bayern.de/media/dsk_kpnr_6_auskunftsrecht.pdf
- DSK-Kurzpapier Nr. 10: www.lda.bayern.de/media/dsk_kpnr_10_informationspflichten.pdf

Es bestehen Informationspflichten bevor personenbezogene Daten verarbeitet werden. Die betroffenen Personen müssen über die Verarbeitung in einer transparenten und einfachen Weise in präziser Sprache informiert werden (insbesondere zum Zweck der Verarbeitung). Die Rechtsgrundlage (in der Regel Vertrag oder Einwilligung) als auch die Rechte der Betroffenen sind explizit zu nennen.[7]

[7] BER (2017): Sie sind verhaftet. Regeln und Haftung bei Websites und Social Media von entwicklungspolitischen Nichtregierungsorganisationen, S. 13

In vielen Fällen müssen die Betroffenen die Erlaubnis zum Erheben, Verarbeiten und Nutzen der Daten geben. Das ist nicht erforderlich, wenn Daten im Rahmen einer vertraglichen Beziehung erhoben werden müssen. Bei Vereinen ist diese vertragliche Beziehung die Mitgliedschaft. Die für die Mitgliederverwaltung erforderlichen Daten dürfen also in jeden Fall verwendet werden. Das gleiche gilt, wenn die Daten zur Erfüllung einer rechtlichen Verpflichtung erforderlich sind. Das gilt z.B. für Spender. Hier müssen die Spendenbescheinigungen mit ihren Daten 10 Jahre aufbewahrt werden.[8]

Die Einwilligung muss:

- Freiwillig sein
- Für einen bestimmten Zweck
- Klar und verständlich informiert
- Information darüber enthalten, dass die Einwilligung jederzeit widerrufen werden kann (ohne Angabe von Grund)
- Einwilligung erfolgt durch eindeutig bestätigte Handlung [sog. opt-in]. Achtung: sog. opt-out reicht nicht aus (bereits vorangehaktes Kästchen).

HINWEIS:

➔ Newsletter: Die meisten Firmen, die die Newsletter verschicken (z.B. Mailchimp) haben bereits auf die neue DGSVO aufgerüstet.

➔ Alte Verteiler: Auf Nachfrage bei einer Fortbildung, hat der Anwalt ausgesagt, dass alte Adressen zum „Altbestand“ gehören und man die Einwilligung nicht nachträglich einholen muss. Wer aber auf Nummer sicher gehen möchte, sollte bei einem der nächsten Versände des Newsletters/Einladungen o.ä. einen Hinweis auf die neue DSGVO geben mit der Möglichkeit sich auszutragen. Dies könnte ein möglicher Text sein:

Liebe Freundinnen und Freunde,
in regelmäßigen Abständen informieren wir Sie mit einem Newsletter über die Arbeit im Eine Welt Landesnetzwerk xy.
Ab 25. Mai 2018 gilt die EU-Datenschutz-Grundverordnung. Wir möchten Sie gerne auch in Zukunft über unsere Aktivitäten auf dem Laufenden halten. Ihre persönlichen Daten (Name und Email-Adresse) verwenden wir ausschließlich für den Versand unserer Newsletter, die wir mit unserem Email-Programm (Hinweis: ggbf. andere Programme) versenden.
Wenn Sie unsere Informationen wie bisher erhalten möchten, müssen Sie nichts weiter unternehmen. Sie erteilen uns damit die Genehmigung, Sie weiterhin über unsere Aktivitäten zu informieren. Wenn Sie dies nicht wünschen, senden Sie uns bitte eine Email an: xy mit dem Betreff „unsubscribe“.

[8] Vereinsknowhow.de/ bnve e.V.: Vereinsinfobrief Nr. 340 – Ausgabe 1/2018 – 10.01.2018, Seite 1

➔ Die Einwilligung der Daten ist zweckgebunden. Adressen, die man für einen Zweck erworben hat, sollten nicht ohne Einwilligung für einen anderen Zweck genutzt werden, z.B. Teilnehmerlisten für Newsletter.

5 LÖSCHEN VON DATEN

Sobald keine gesetzliche Grundlage (z. B. steuerliche Aufbewahrungspflicht) mehr für die Speicherung von personenbezogenen Daten besteht, sind diese zu löschen. In der Regel ist dies bspw. erst der Fall nach Ausscheiden eines Vereinsmitglieds.

- DSK-Kurzpapier Nr. 11: www.lda.bayern.de/media/dsk_kpnr_11_vergessenwerden.pdf[9]

6 IT-SICHERHEIT

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.

BayLDA-Kurzpapier Nr. 1: www.lda.bayern.de/media/baylda_ds-gvo_1_security.pdf[10]

Schutzziele gegen unbefugte Zugriffe: **Vertraulichkeit** (z.B. bei Nutzung des PCs im öffentlichen Raum, z.B. in der Bahn), **Integrität** (Zugriffskonzepte mit unterschiedlichen Berechtigungen, z.B. für Praktikant*innen), **Verfügbarkeit** (z.B. Online-Software regelmäßig updaten, proaktiv untersuchen).

HINWEIS:

➔ Bei Ausscheiden von Mitarbeiter*innen an Entzug der Zugriffsrechte denken (z.B. auf Datenbank, cloud)

➔ Erstellung von IT-Sicherheitsrichtlinien für alle Mitarbeiter*innen (z.B. Passwortrichtlinien für PCs). IT-Sicherheit ist Chefsache, muss von Geschäftsführung und Vorstand mitgetragen werden.

[9] Bayerisches Landesamt für Datenschutzaufsicht: Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an kleine Unternehmen, Vereine, etc. Muster Verein: https://www.lda.bayern.de/media/muster_1_verein.pdf
[10] Bayerisches Landesamt für Datenschutzaufsicht: Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an kleine Unternehmen, Vereine, etc. Muster Verein: https://www.lda.bayern.de/media/muster_1_verein.pdf

7 AUFTRAGSVERARBEITUNG

Sobald Verantwortliche Dienstleistungen (z. B. Buchhaltung) in Anspruch nehmen, um personenbezogene Daten in ihrem Auftrag durch andere Unternehmen verarbeiten zu lassen, ist ein schriftlicher Vertrag zur Auftragsverarbeitung erforderlich.

- DSK-Kurzpapier Nr. 13: www.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf
- BayLDA-Formulierungshilfe zum Vertrag: www.lda.bayern.de/media/muster_adv.pdf[11]

Externe Dienstleister mit denen Verein zusammenarbeitet, bezeichnet die DS-GVO "Auftragsverarbeiter". Hier sind folgende Punkte zu beachten:

- eine sorgfältige Auswahl des Dienstleiters ("Auftragverarbeiters")
- In eine entsprechende vertragliche Vereinbarung sollten Regelungen zum Datenschutz aufgenommen werden.
- Kontrolle: Der Auftragsverarbeiter sollte seine Datenschutzmaßnahmen (am besten vertraglich) darstellen. Eventuell sollte der Verein das kontrollieren.
- Beendigung des Vertrages: Müssen Unterlagen zurückgegeben werden? Sind Löschungen vorzunehmen?[12]

HINWEIS:

➔ Liegt vor, wenn Dritte Daten weisungsabhängig bearbeiten, der Auftragsgeber entscheidet über Zweck und Mittel der Verarbeitung, z.B. externe Lohnbüros aber NICHT: Steuerberater, IT-Support

8 DATENSCHUTZVERLETZUNGEN

Kommt es bei der Verarbeitung personenbezogener Daten zu Sicherheitsvorfällen (z. B. Diebstahl, Hacking, Fehlversendung, Verlust von Geräten mit unverschlüsselten Vereinsdaten), so bestehen gesetzliche Meldepflichten: Die Aufsichtsbehörde ist im Regelfall darüber in Kenntnis zu setzen, betroffene Personen dagegen nur bei hohem Risiko.

- BayLDA-Kurzpapier Nr. 8: www.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf

[11] Bayerisches Landesamt für Datenschutzaufsicht: Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an kleine Unternehmen, Vereine, etc. Muster Verein: https://www.lda.bayern.de/media/muster_1_verein.pdf
[12] Vereinsknowhow.de/ bnve e.V.: Vereinsinfobrief Nr. 340 – Ausgabe 1/2018 – 10.01.2018, Seite 4

- BayLDA-Online-Service zur Meldung: www.lda.bayern.de/de/datenpanne.html13

Drastische Änderungen enthält die DS-GVO bei der Höhe der Bußgelder. Im Extremfall können bis zu 40 Mio. Euro anfallen. Damit soll eine abschreckende Wirkung erzielt werden. Natürlich werden bei Vereinen im Fall von Verstößen keine so dramatischen Beträge fällig, vier- bis fünfstellige Bußgelder sind aber denkbar.

Nach Artikel 82 der DS-GVO haben Personen, die wegen eines Verstoßes gegen die Verordnung einen immateriellen Schaden erleiden, einen Schadensersatzanspruch. Ein solcher immaterieller Schaden kann beispielweise in einer Rufschädigung bestehen.[14]

HINWEIS:

- ➔ Die Gefahr von hohen Bußgeldern wird von Fachleuten als gering eingeschätzt. Wenn man die Checkliste befolgt, ist man relativ auf der sicheren Seite.
- ➔ Jedes BL hat eine Datenschutzaufsichtsbehörde, die verpflichtet ist Auskunft und Beratung zu leisten. Bei Unsicherheiten kann man sich an die Behörde wenden.

9 DATENSCHUTZ-FOLGEABSCHÄTZUNG (DSFA)

Hat eine Verarbeitung personenbezogener Daten ein hohes Risiko für die betroffenen Personen, so muss das spezielle Instrument der Datenschutz-Folgenabschätzung durchgeführt werden. Ein solch hohes Risiko ist jedoch der Ausnahmefall und nicht die Regel.

- DSK-Kurzpapier Nr. 5: www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf15

10 UMGANG MIT FOTOS IM INTERNET[16]

Fotos enthalten personenbezogene Daten, auch wenn kein Name mit veröffentlicht wird. Es gibt das „Recht am eigenen Bild“ (KUG). **Es muss immer vorher eine Einwilligung eingeholt werden!**

[13] Bayerisches Landesamt für Datenschutzaufsicht: Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an kleine Unternehmen, Vereine, etc. Muster Verein: https://www.lda.bayern.de/media/muster_1_verein.pdf

[14] Vereinsknowhow.de/ bnve e.V.: Vereinsinfobrief Nr. 340 – Ausgabe 1/2018 – 10.01.2018, Seite 4

[15] Bayerisches Landesamt für Datenschutzaufsicht: Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an kleine Unternehmen, Vereine, etc. Muster Verein: https://www.lda.bayern.de/media/muster_1_verein.pdf

[16] Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine, C.H.Beck, S. 50ff.

Davon ausgeschlossen sind:

- Bilder aus dem Bereich der Zeitgeschichte
- Bilder, in den Personen als Beiwerk erscheinen
- Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die Personen teilgenommen haben
- Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient

HINWEIS:

- ➔ Fotos der Mitarbeiter sollten mit Einwilligung veröffentlicht werden. Muster einer Einwilligungserklärung kann bei der agl angefragt werden!
- ➔ **Besser im Regelfall: Erst fragen, dann veröffentlichen!**

LINKS UND LITERATUR

https://www.datenschutz-wiki.de/Hauptseite

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

Bayerisches Landesamt für Datenschutzaufsicht (2017): Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine. Das Sofortmaßnahmen-Paket, C. H. Beck (http://www.beck-shop.de/erste-hilfe-datenschutz-grundverordnung-unternehmen-vereine/productview.aspx?product=21443886)

Webinar von Haus des Stiftens: https://www.hausdesstiftens.org/

www.datenschutz-portal.com/Dokumente/Anlage_Arbeitsvertrag_Geheimhaltungserklaerung.pdf

www.iww.de/vb/archiv/bundesdatenschutzgesetz-gilt-auch-fuer-vereine-datenschutz-im-verein-diese-massnahmen-muss-der-vorstand-ergreifen-f18138