~ Mitgliederinformation ~

DEUTSCHER TIERSCHUTZBUND E.V.

Aktuelle Änderungen im Datenschutzrecht

Am 24.05.2016 ist die neue EU-Datenschutzgrundverordnung (EU-DSGVO) in Kraft getreten. Sie entfaltet ihre Wirkung ab dem 25.05.2018. Da die EU-DSGVO Konkretisierungen im nationalen Recht vorsieht, hat der Gesetzgeber am 05.07.2017 das neue Bundesdatenschutzgesetz (BDSG) veröffentlicht, welches zum 25.05.2018 in Kraft tritt.

(A) Allgemeines

Zunächst wollen wir allgemeine Grundsätze vorstellen. Das Datenschutzrecht hat auch in ihrer Vereinstätigkeit weitreichende Auswirkungen. Zweck des Datenschutzrechts ist, dass der Einzelne davor geschützt werden soll, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Folgende Grundbegriffe sollten bekannt sein:

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Das sind beispielsweise Name, Alter, Familienstand, Geburtsdatum, Anschrift, Telefonnummer, E-Mail Adresse, Konto-, Kreditkartennummer, IP-Adresse, Sozialversicherungsnummer, usw. Im Verein sind das vor allem Namen, Adress- und Kontodaten von Spendern und Vertragspartnern, z.B. Personen, die Tiere vom Verein übernehmen, sowie die Daten der Mitgliederliste.

Verarbeitung sind alle Vorgänge, bei denen mit diesen geschützten Daten umgegangen wird.
Dazu gehört das Erheben, Erfassen, die Organisation, das Ordnen, die Speicherung, Anpassung oder Veränderung, das Auslesen, Abfragen, die Verwendung, Weiterleitung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Datensätzen.
Es ist dabei gleichgültig ob die Datenverarbeitung von Hand erfolgt oder am PC, mit Datenbanken oder einfachen Tabellen.

Verantwortlicher ist zunächst der Tierschutzverein, aber auch jede natürliche Person, die über die Verarbeitung von personenbezogenen Daten entscheidet. Dies ist im Verein vor allem der Vorstand. Der Vorstand kann einzelne Aufgaben auch beispielsweise auf einen Geschäftsführer oder die

Tierheimleitung übertragen, muss dann aber die Ausführung durch die beauftragten Personen kontrollieren.

Datenschutzpflichten: Das Datenschutzrecht trifft den Verein also hinsichtlich einer Reihe von Vorgängen, z.B. der Speicherung der personenbezogenen Mitgliederdaten, der Daten seiner Arbeitnehmer, aber auch bezüglich der Daten, die von jedem Finder eines Tieres oder jedem Übernehmer eines Tieres, usw. aufgenommen werden.

Grundsätze des Datenschutzes

Die bisher schon geltenden Grundsätze nach dem Bundesdatenschutzgesetz gelten auch mit der neuen EU-DSGVO weiterhin:

- **Datensicherheit** - Personenbezogene Daten sind durch technische Vorkehrungen (z.B. Passwortschutz) vor Missbrauch zu schützen.
- **Datenvermeidung** und **Datensparsamkeit** - Datenverarbeitungssysteme sind so einzurichten, dass möglichst wenige Daten gespeichert und weitergegeben werden.
- **Rechtmäßigkeit** - Das Verarbeiten ist zulässig, wenn der Betroffene zustimmt oder eine Rechtsvorschrift es gestattet.
- **Richtigkeit** - Überflüssige, unzulässige und bestrittene Daten sind zu sperren oder zu löschen. Unrichtige Daten müssen berichtigt werden.
- **Transparenz** - Bei der Datenverarbeitung muss für die Betroffenen klar sein was zu welchen Zwecken gespeichert wird.
- **Verantwortlichkeit** Die verantwortliche Stelle muss dem Betroffenen bekannt und für ihn erreichbar sein.
- **Verhältnismäßigkeit** Die verantwortliche Stelle muss die Verarbeitung personenbezogener Daten auf das Maß begrenzen, das für die Erreichung der (unternehmerischen) Ziele erforderlich ist.
- **Zweckbindung** - Jede Datenverarbeitung muss auf einen bestimmten legitimen Zweck begrenzt werden, z. B. Vertragsabwicklung, Werbung, Auswertung des Nutzerverhaltens.

Es gilt damit weiterhin, dass der Verein für eine sichere Datenverarbeitung verantwortlich ist und Personen Auskunft über die gespeicherten Daten geben muss und diese ggf. berichtigen und löschen muss, sofern er kein berechtigtes Interesse an der weiteren Speicherung hat. Ein berechtigtes Interesse besteht z.B. immer bei Mitgliederdaten, weil ein Verein nur so funktionieren kann. Kein Mitglied hat somit einen Anspruch sich aus der Mitgliederliste löschen zu lassen. Es hat aber z.B. einen Anspruch auf Berichtigung, wenn er umgezogen ist und seine Einladungen zur Mitgliederversammlung immer bei seiner Ex-Frau landen.

Desgleichen gilt weiterhin, dass jeder Mitarbeiter des Vereins (auch Ehrenamtliche) die mit der Verarbeitung personenbezogener Daten zu tun haben, eine Datenschutzverpflichtungserklärung unterschreiben muss, die dann zu seiner Akte genommen wird und die ihn auf die Gefahren des Missbrauchs hinweist, z.B. Schadenersatzpflichten.

(B) Neuerungen

Das neue Datenschutzrecht enthält über die oben genannten Grundsätze hinaus auch einige **Neuerungen**, welche sich durch die EU-DSGVO und das neue BDSG ergeben. Diese werden in der Folge vorgestellt.

1. Grundsätze des Datenschutzes; Rechenschaftspflicht

Wie oben für das BDSG enthält auch die EU-DSGVO zentrale Grundsätze des Datenschutzes. Diese sind in Art. 5 I geregelt. Diese sind von zentraler Bedeutung, da der Verein diese nicht nur jederzeit einhalten muss, sondern darüber hinaus verpflichtet ist die Einhaltung aller Datenschutzprinzipien nachzuweisen (**Rechenschaftspflicht** nach Art. 5 II EU-DSGVO).

Dies betrifft insbesondere folgende Pflichten:

(a) Rechtmäßigkeit und Transparenz der Verarbeitung:
Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;

(b) Grundsatz der Zweckbindung:
Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;

(c) Datenminimierung:
Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Ggf. ist dies durch weitgehende Pseudonymisierung zu erreichen.

(d) Datenrichtigkeit:
Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;

(e) Begrenzung der Speicherdauer:
Die Identifizierung der betroffenen Personen darf nur so lange möglich sein, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; zu beachten sind dabei die jeweiligen gesetzlichen Aufbewahrungspflichten.

(f) Integrität und Vertraulichkeit
Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung (entspricht der Datensicherheit gem. § 9 BDSG).

2. Betroffenenrechte und Informationspflichten

Dem Betroffenen stehen folgende Rechte zu:

- Recht auf Auskunft innerhalb eines Monats nach Anfrage (Art. 15 I EU-DSVGO)
- Recht auf Erhalt einer Kopie der gespeicherten Daten (Art. 15 III EU-DSGVO)
- Recht auf Berichtigung und Vervollständigung (Art. 16 EU-DSGVO)
- **Neu**: **Recht auf unverzügliche Löschung**, außer wenn die Löschung unverhältnismäßig wäre oder Aufbewahrungspflichten bestehen (Art. 17 EU-DSGVO)
- Recht auf Sperrung (Art. 18 EU-DSGVO)
- **Neu**: **Recht auf Datenübertragbarkeit** (Art. 20 EU-DSGVO), notwendig ist hierfür eine Software mit Exportfunktion; hierzu wird die EU Leitlinien veröffentlichen.
- Recht auf Widerspruch im Fall von berechtigtem Interesse oder Direktwerbung (Art. 21 EU-DSGVO)
- Recht auf Benachrichtigung bei Datenpannen (Art. 33 EU-DSGVO)

3. Transparente Information auf Anfrage:

Bei der erstmaligen Erhebung personenbezogener Daten muss der Verantwortliche den Betroffenen auch ohne Anfrage über Folgendes informieren (Art. 13-14 EU-DSVGO):

- Name und Kontaktdaten des Verantwortlichen
- Name und Kontaktdaten des Datenschutzbeauftragten, falls vorhanden
- Zweck sowie die Rechtsgrundlage für die Verarbeitung personenbezogener Daten
- Ggf. Empfänger von personenbezogenen Daten oder Kategorien von Empfängern
- Dauer der Datenspeicherung oder Kriterien für die Festlegung der Dauer
- Auskunftsrecht, Recht auf Berichtigung, Löschung, Widerspruch, Recht auf Datenübertragbarkeit (neu), Widerrufsrecht bzgl. der Einwilligung
- Beschwerderecht bei Aufsichtsbehörde
- Ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben ist.

Ansonsten muss der Verein auf berechtigte Anfragen zu gespeicherten Daten reagieren. Der Verein muss dazu nach Art. 12 EU-DSVGO geeignete Maßnahmen treffen, um Betroffenen alle notwendigen Informationen (vgl. Art. 13-14) und alle verpflichtenden Mitteilungen (vgl. Art. 15-22 und 34) in **präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache** zu übermitteln. Der Verein muss zudem Betroffenen erleichtern, ihre Rechte ausüben zu können und jederzeit Informationen bereithalten, wie sie dies tun können. Am besten sollten solche Informationen auf der Webseite verfügbar sein und auch bei Mitarbeitern hinterlegt sein, die entsprechende Anfragen bearbeiten.

Der Verein stellt Betroffenen Informationen über die ergriffenen Maßnahmen innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Wird er nicht tätig, muss er den Betroffenen innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür unterrichten und informiert über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

4. Neue Haftungsrisiken

Bei Verstößen gegen das Bundesdatenschutzgesetz waren bisher Bußgelder bis zu einer Höhe von 50.000 € möglich. Nach der neuen EU-DSGVO können je nach Verstoß theoretisch deutlich höhere **Geldbußen** von bis zu 10.000.000 € oder bei schwereren Verstößen sogar von bis zu **20.000.000 €** erhoben werden. Die Geldbußen müssen nach der EU-DSGVO wirksam, verhältnismäßig und abschreckend sein. Daher sind die Landesämter Gehalten entsprechend hohe Strafen auszusprechen, damit sich ein Datenmissbrauch künftig nicht mehr lohnt.

Es gibt darüber hinaus künftig ein **Beschwerderecht** bei der Aufsichtsbehörde sowie ein Recht auf wirksamen gerichtlichen Rechtsbehelf gegen den Verantwortlichen.

Zudem wurde das Recht auf Schadensersatz erheblich erweitert: so haftet der Verantwortliche nach der EU-DSGVO persönlich auf Schadensersatz und zwar für materiellen oder **immateriellen** Schaden (umgangssprachlich auch als Schmerzensgeld bezeichnet). Das ist besonders brisant, da sich Schmerzensgeldforderungen in der Regel nicht versichern lassen.

5. Compliance

Der Verantwortliche muss darüber hinaus geeignete technische und organisatorische Maßnahmen einrichten, um den rechtlichen Vorgaben entsprechen zu können.
Diese Maßnahmen sind unter Berücksichtigung der Art, des Umfangs und der Zwecke der Verarbeitung und der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken vorzunehmen, vgl. Art. 24 I EU-DSGVO.

Die Mitarbeiter, welche personenbezogene Daten verarbeiten, sind mit einem schriftlichen Formular auf das Datengeheimnis nach § 5 BDSG zu verpflichten und hinsichtlich der Risiken zu sensibilisieren. Eine Sensibilisierung kann durch Schulung der Mitarbeiter über den richtigen Umgang mit personenbezogenen Daten erreicht werden.

➔ **Ein Musterformular kann bei der Rechtsabteilung abgefragt werden.**

6. Aufbau einer Datenschutzorganisation

Größere Organisationen benötigen einen **Datenschutzbeauftragten**. Dazu werden in der Regel externe Fachleute (kostenpflichtig) angeworben. Er kann aber auch intern bestellt werden, wenn eine Person dazu befähigt ist („Fachkunde“, siehe § 4f Abs. 1 BDSG) oder bereit, entsprechende Fortbildungen zu absolvieren.

Das Gesetz ist hier leider ungenau: Nach der EU-DSGVO ist die Bestellung eines Datenschutzbeauftragten generell erforderlich, „*wenn die Kerntätigkeit des Verarbeitungsvorgangs nach der Art, des Umfangs oder des Zweckes eine regelmäßige und systematische Beobachtung erfordert und wenn umfangreich besondere Arten personenbezogener Daten verarbeitet werden“.*

Nach Art. 37 IV EU-DSGVO läuft die Bestellpflicht des Datenschutzbeauftragen parallel zu bestehenden nationalen Regelungen. Daher bleibt die Bestellpflicht für den Datenschutzbeauftragten nach § 4 f BDSG bestehen, wonach die Pflicht zur Bestellung eines Datenschutzbeauftragten besteht, wenn dauerhaft **zehn oder mehr Mitarbeiter** im Betrieb beschäftigt werden.

Die **Aufgaben** des Datenschutzbeauftragten ergeben sich direkt aus Art. 39 EU-DSGVO:

a) Unterrichtung und Beratung des Verantwortlichen hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;

b) Überwachung der Einhaltung der Datenschutzgesetze einschließlich der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter

c) Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35;

d) Zusammenarbeit mit der Aufsichtsbehörde;

e) Einbeziehung bei einem Sicherheitsvorfall nach Art. 33 EU-DSVGO.

Achtung: Wenn sich der geschäftsführende Vorstand nicht selbst um den Datenschutz kümmern will oder kann, sollte (unabhängig von der Pflicht zur Bestellung eines Datenschutzbeauftragten) eine Verantwortliche Person im Verein benannt werden („**Datenschutzverantwortlicher**"). Generell sind die Abläufe so zu regeln, dass die Mitarbeiter wissen, was zu tun ist und an wen sie sich im Zweifgel wenden können.

7. Datenschutzverzeichnis

Nach Art. 30 EU-DSGVO ist ein **Verzeichnis über die Datenverarbeitungstätigkeiten** zu erstellen.

Dieses Verzeichnis muss folgende Angaben enthalten:

- Name und Kontaktdaten des Verantwortlichen (= Verein) und seiner gesetzlichen Vertreter (Vorstand);
- Name und Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden);
- Zwecke der Verarbeitung von Daten im Verein;
- Beschreibung der Kategorien betroffener Personen und personenbezogener Daten;
- Bei Weitergabe von Daten: Kategorien von Empfängern;
- Fristen für die Löschung der Daten, nach Kategorie;
- Beschreibung der technischen und organisatorischen Maßnahmen zur Einhaltung der Grundsätze des Datenschutzes.

Dieses Verzeichnis ist den Aufsichtsbehörden auf Anfrage vorzulegen.

➔ **Ein entsprechendes Musterformular kann bei der Rechtsabteilung des Deutschen Tierschutzbundes angefordert werden.**

8. Auftragsdatenverarbeitung

Auftragsdatenverarbeitung ist die Verarbeitung personenbezogener Daten durch einen Dienstleister im Auftrag des Verantwortlichen. Darunter fallen beispielsweise: Ablage von personenbezogenen Daten auf externen Servern; Wartungsdienstleistungen von IT-Systemen, bei denen nicht ausgeschlossen werden kann, dass während der Wartung personenbezogene Daten zur Kenntnis gelangen; Entsorgung von Akten oder Datenträgern durch externe Unternehmen.

Es dürfen nur Auftragsverarbeiter mit **hinreichend Garantien** für geeignete technische und organisatorische Maßnahmen nach Art. 28 EU-DSGVO eingesetzt werden. Praktisch sind dazu folgende Schritte nötig:

- **Auftrag** - Vorherige gesonderte oder allgemeine schriftliche Genehmigung zum Tätigwerden durch den Verantwortlichen (= Verein);
- **Datenschutzvereinbarung** - schriftlicher Vertrag mit dem Auftragsdatenverarbeiter, mit folgendem Inhalt:
  - Gegenstand und Dauer der Verarbeitung,
  - Art und Zweck der Verarbeitung,
  - Art der personenbezogenen Daten, die Kategorien betroffener Personen,
  - Pflichten und Rechte nach Art. 28 III EU-DSGVO.

→Ein entsprechendes Vertragsmuster kann bei der Rechtsabteilung des Deutschen Tierschutzbundes angefordert werden.

9. Meldeverfahren bei Datenpannen

Sollten einmal Pannen bei der Datenverarbeitung entstehen („Lecks“) muss der verein umgehend tätig zu werden. Datenpannen liegen immer dann vor, wenn Dritte unrechtmäßig von gespeicherten personenbezogenen Daten Kenntnis nehmen können. Darüber hinaus auch weitere technische Verfügbarkeits- oder Integritätsverletzungen und auch die interne Weitergabe an unbefugte Mitarbeiter.

Nach der EU-DSVGO muss der Verantwortliche die Verletzungen in einem internen Verzeichnis dokumentieren. Weiterhin müssen solche Pannen den Betroffenen binnen 72 Stunden mitgeteilt werden. Darauf kann nur dann verzichtet werden, wenn kein Risiko für die Rechte der Betroffenen zu befürchten ist. Eine Verspätung muss immer bei der Aufsichtsbehörde gemeldet und begründet werden.

Die Meldung gegenüber dem Betroffenen muss in klarer und einfacher Sprache gehalten sein. Dabei müssen folgende Angaben enthalten sein:

- die Art der Verletzung,
- Name und Kontaktdaten des Datenschutzbeauftragen oder einer sonstigen Anlaufstelle,
- Beschreibung der wahrscheinlichen Folgen,
- Beschreibung der getroffenen Maßnahmen zur Behebung der Verletzung,
- Unterschrift des Vertretungsberechtigten (Vorstand).

Praxistipp: Bei größeren Vereinen sollte ein Managementsystem zur standardisierten Bearbeitung solcher Datenpannen eingerichtet werden.

10. Datenschutzfolgenabschätzung

Eine Datenschutzfolgenabschätzung ist nur durchzuführen, wenn nach Art, Umfang, Umstände und des Zwecks der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zu erwarten ist. Dies ist im Verein in der Regel dann der Fall, wenn sie bei ihrer Personalverwaltung auch mit Lohnpfändungen zu tun haben.

➔ **Sollten Sie davon betroffen sein, wenden Sie sich für weitergehende Informationen an die Rechtsabteilung des Deutschen Tierschutzbundes. Dort können auch entsprechende Muster angefordert werden.**

Zusammenfassung: Was ist zu tun?

Aus den oben geschilderten Änderungen ergeben sich verschiedene konkrete Handlungsverpflichtungen.

Zunächst sollten Sie einen **Datenschutzverantwortlicher** in Ihrem Verein benennen. Generell müssen alle Mitarbeiter, die Daten verarbeiten, wissen was im Einzelfall zu tun ist.

Im Einzelnen empfehlen wir folgende Handlungen.

➔ **Zur Gewährleistung der Rechenschaftsverpflichtung**

1. Risikobewertung – welche Daten werden erhoben und verarbeitet und welche Risiken bestehen hierbei.
2. Erstellung eines Datenschutzverzeichnisses über alle Verarbeitungstätigkeiten
3. Benennung eines Datenschutzbeauftragten (sofern erforderlich) und eines **Datenschutzverantwortlichen** im Verein
4. Einführung geeigneter technischer und organisatorischer Maßnahmen zur Sicherstellung des Datenschutzes im Verein und der einfachen Erfüllung von Auskunftspflichten. Idealerweise empfiehlt sich hier die Anschaffung passwortgeschützter Datenbanken nach aktuellem Stand der Technik (Sicherheit der Verarbeitung; Möglichkeit der Pseudonymisierung und Verschlüsselung).
5. Sicherstellung der Nachweiserbringung in Bezug auf die gesetzlichen Pflichten
6. Erstellen von Datenschutzrichtlinien
7. Schulung von Mitarbeitern
8. Verpflichtung aller Mitarbeiter auf das Datengeheimnis

Bei Auftragsdatenverarbeitung durch Dritte:

9. Überarbeitung der Genehmigungsprozesse und verwendeten Verträge (sofern vorhanden)

➔ **Zur Einhaltung der Informationspflichten**

1. Durchsicht von bestehenden Datenschutzerklärungen (auch online) und ggf. Anpassung, damit bekannt ist, welche Daten durch den Verein gespeichert werden und welche gesetzlichen Rechte die Betroffenen haben.
2. Ergänzung der verwendeten Verträge mit Datenschutzhinweisen

➔ **Zur Einhaltung der Betroffenenrechte**

1. Interne Prozesse schaffen, um mit Anfragen betroffener Personen umzugehen; Überprüfen ob IT-Systeme die jeweiligen Anforderungen erfüllen; Implementierung von Beschwerdemanagement, insbesondere Prozesse zur Einhaltung von Fristen
2. Einrichtung Datenpannenmanagementsystem inkl. System für Benachrichtigung Betroffener
3. Entwicklung geeigneter Formate zur Übertragung der Daten (Datenübertragbarkeit)

→Ein Muster für die Verpflichtung auf das Datengeheimnis der Mitarbeiter kann bei der Rechtsabteilung des Deutschen Tierschutzbundes angefordert werden.

→Bei Fragen oder Anregungen wenden Sie sich an die Rechtsabteilung des Deutschen Tierschutzbundes unter 089/60029166 oder rechtsabteilung@tierschutzakademie.de.