Stand: 05-2019

Datenschutzrichtlinie
Deutscher Verband für Gebrauchshundsportvereine e.V. (DVG)

§1 Bedeutung, Ziel, Zugänglichkeit

[1] Diese Richtlinie ist die verbindliche Basis für einen rechtskonformen und nachhaltigen Schutz personenbezogener Daten im DVG.

[2] Mit dieser Richtlinie sollen die Persönlichkeitsrechte von Betroffenen gewahrt und geschützt werden.

[3] Diese Richtlinie muss für alle Beschäftigten sowie Mitglieder des DVG jederzeit leicht zugänglich und verständlich sein.

§2 Geltungsbereich

[1] Diese Richtlinie findet Geltung für den DVG einschließlich der Geschäftsstelle.

[2] Sie gilt auch persönlich für alle Beschäftigten des DVG.

[3] Die Gebote und Verbote dieser Richtlinie gelten für jeglichen Umgang mit personenbezogenen Daten, unabhängig ob dieses elektronisch oder in Papierform vonstattengeht. Letzteres nur, wenn die in Papierform verarbeiteten Daten in einem elektronischen System gespeichert werden sollen (Artikel 2 (1) DSGVO). Ebenso beziehen sie alle Arten von Betroffenen (Mitglieder, Kunden, Gäste, Lieferanten, Beschäftigte etc.) in ihren Geltungsbereich ein.

§3 Begriffsbestimmungen

[1] Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffene(r)). Personenbezogene Mitglieder- und Kundendaten gehören dabei ebenso zu den personenbezogenen Daten wie Personaldaten von Beschäftigten. Beispielsweise lässt der Name eines Ansprechpartners ebenso einen Rückschluss auf eine natürliche Person zu, wie dessen E-Mail-Adresse. Es genügt, wenn die jeweilige Information mit dem Namen des Betroffenen verbunden ist oder unabhängig hiervon aus dem Zusammenhang hergestellt werden kann. Ebenso kann eine Person bestimmbar sein, wenn die Information mit einem Zusatzwissen erst verknüpft werden muss, so z. B. beim Autokennzeichen. Das Zustandekommen der Information ist für einen Personenbezug unerheblich. Auch Fotos, Video- oder Tonaufnahmen können personenbezogene Daten darstellen.

[2] Besonders sensible Arten personenbezogener Daten sind z. B. Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder Grad der Schwerbehinderung.

[3] Erheben ist das Beschaffen von Daten über den Betroffenen[1].

[1] Zur besseren Lesbarkeit dieser Datenschutzrichtlinie, wurde für einige Begriffe (z. B. „der Betroffene“) die männliche Form gewählt, selbstverständlich beinhaltet dies jeweils auch die weibliche Form.

[4] Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten.
Im Einzelnen ist
- [a] Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung,
- [b] Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten.
- [c] Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
  - die Daten an den Dritten weitergegeben werden oder
  - der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
- [d] Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken (z. B, durch einen Vermerk oder die Entnahme aus einer Zugriffsberechtigung),
- [e] Löschen die Unkenntlichmachung gespeicherter personenbezogener Daten.

[5] Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt (z. B. die Auswertung bzw. Selektion personenbezogener Daten zur werblichen Ansprache).

[6] Anonymisieren ist das Verändern personenbezogener Daten derart. dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

[7] Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

[8] Verantwortliche Stelle ist die juristische Person innerhalb des DVG, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Wer im Einzelfall als verantwortliche Stelle anzusehen ist, richtet sich danach, wer über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

[9] Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle, so auch andere dem DVG angehörige juristische Personen.

[10] Auftragsdatenverarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch einen Auftragnehmer für einen Auftraggeber. Der Auftragnehmer darf die personenbezogenen Daten nur nach Weisung des Auftraggebers erheben, verarbeiten oder nutzen. Die Verantwortung für den Datenumgang verbleibt beim Auftraggeber als verantwortlicher Stelle,

§ 4 Datenschutzorganisation

Der DVG muss entsprechend der Maßgabe der DSGVO und des Bundesdatenschutzgesetzes (BDSG) einen Datenschutzbeauftragten (DSB) erst dann bestellen, wenn ständig mindestens 10 Mitarbeiter personenbezogene Daten erheben und automatisiert verarbeiten. Dabei ist es unerheblich, ob die 10 Personen in einem bezahlten Arbeitsverhältnis stehen, auch Ehrenamtliche werden mitgezählt.

§ 5 Umgang mit personenbezogenen Daten

[1] Die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten ist grundsätzlich verboten, es sei denn eine gesetzliche Norm erlaubt explizit den Datenumgang (Erlaubnisvorbehalt). Personenbezogene Daten dürfen nach dem BDSG grundsätzlich erhoben, verarbeitet oder genutzt werden, wenn eine gesetzliche Grundlage vorliegt.

- Bei einem bestehendes Vertragsverhältnis mit dem Betroffenen. Beispiel: Die Speicherung und Verwendung erforderlicher personenbezogener Daten im Rahmen eines Arbeitsverhältnisses oder Mitgliedsverhältnisses.
- Im Zuge der Vertragsanbahnung oder -abwicklung mit dem Betroffenen. Beispiel: Ein Mitglied fordert Informationen zu einer Veranstaltung an und meldet sich zu dieser an oder ein Gast/Mitglied bucht ein Zimmer in Hemer. Die erforderlichen Daten zur Zusendung des Informationsmaterials sowie zur Abwicklung der Veranstaltung z.B. Bestätigung der Teilnahme sowie Zahlung der Gebühr dürfen erhoben, verarbeitet und genutzt werden.
- Wenn und soweit der Betroffene eingewilligt hat. Beispiel: Ein Mitglied meldet sich zu einem DVG Hundesport-Turnier an.
- Wenn eine spezielle Rechtsvorschrift außerhalb der DSGVO und des BDSG die Verarbeitung erfordert. Beispiele: Erfüllung der satzungsmäßig festgelegten Ziele des DVG, gesetzliche Aufbewahrungsfristen (HGB) und Abgabenordnung (AO).

[2] Personenbezogene Daten sind für einen zuvor festgelegten Zweck zu verarbeiten und dementsprechend nur insofern zu verwenden oder weiter zu übermitteln, als dies mit dem ursprünglich festgelegten Zweck vereinbar ist, eine Datenhaltung ohne Zweck, so beispielsweise die Vorratsdatenspeicherung. ist unzulässig.

[3] Die Änderung einer Ziel- und Zweckbestimmung, die einem Datenumgang ursprünglich zugrunde gelegt wurde, ist ebenfalls nur mit einer gesetzlichen Erlaubnisnorm oder der Einwilligung des Betroffenen zulässig.

[4] Personenbezogene Daten sollen grundsätzlich direkt beim Betroffenen erhoben werden. Eine Erhebung aus anderen Quellen (Internet, Social Media, Auskunfteien) ist ohne ein zwingendes gesetzliches Erfordernis unzulässig. Besteht ein gesetzliches Erfordernis, ist der Betroffene unverzüglich über die Datenerhebung zu informieren soweit eine gesetzliche Regelung dem nicht entgegensteht.

[5] Der Betroffene ist bei der Erhebung seiner personenbezogenen Daten über die Zweckbestimmung, die Identität der verantwortlichen Stelle sowie die Empfänger seiner personenbezogenen Daten zu informieren.

[6] Personenbezogene Daten müssen grundsätzlich sachlich richtig sein. Der Umfang der Datenverarbeitung sollte hinsichtlich der festgelegten Zweckbestimmung erforderlich und relevant sein. Der jeweilige Geschäftsbereich, die jeweilige Abteilung bzw. Betriebstätte hat für die Umsetzung durch die Etablierung entsprechender Prozesse Sorge zu tragen. Ebenso sind Datenbestände regelmäßig auf ihre Richtigkeit, Erforderlichkeit und Aktualität hin zu überprüfen.

[7] Falls möglich, sollte auf einen personenbezogenen Datenumgang verzichtet werden. Pseudonyme oder anonyme Datenverarbeitungen sind vorzuziehen. Beispielsweise kann es im Rahmen einer statistischen Auswertung von Daten nicht notwendig sein, den Vollnamen eines Betroffenen zu kennen und zu verwenden. Vielmehr kann diese Information durch einen Zufallswert ersetzt werden, der eine Unterscheidbarkeit der zugrunde liegenden Information ebenfalls gewährleisten kann.

§ 6 Besondere personenbezogene Daten

Besondere personenbezogene Daten dürfen grundsätzlich nur mit Einwilligung des Betroffenen oder ausnahmsweise aufgrund einer expliziten gesetzlichen Erlaubnis erhoben, verarbeitet oder genutzt werden. Ferner sind zusätzliche technische und organisatorische Maßnahmen (z. B. Verschlüsselung beim Transport, minimale Rechtevergabe) zum Schutz besonderer personenbezogener Daten zu ergreifen.

§ 7 Datenübermittlung/Datenweitergabe

[1] Die Übermittlung von personenbezogenen Daten an Dritte ist nur aufgrund gesetzlicher Erlaubnis oder der Einwilligung des Betroffenen zulässig.

[2] Befindet sich der Empfänger personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums bedarf es besonderer Maßnahmen zur Wahrung von Rechten und Interessen Betroffener. Eine Datenübermittlung ist zu unterlassen, wenn bei der empfangenden Stelle kein angemessenes Datenschutzniveau vorhanden ist oder beispielsweise über besondere Vertragsklauseln nicht hergestellt werden kann.

§ 8 Externe Dienstleister

[1] Sofern externe Dienstleister Zugriff auf personenbezogene Daten erhalten sollen, ist der Datenschutzbeauftragte (falls berufen) oder die verantwortliche Stelle vorab zu informieren.

[2] Dienstleister mit einem möglichen Zugriff auf personenbezogene Daten sind vor der Auftragserteilung sorgfältig auszuwählen, Die Auswahl ist zu dokumentieren und sollte insbesondere die folgenden Aspekte berücksichtigen:
- Fachliche Eignung des Auftragnehmers für den konkreten Datenumgang,

- Technisch-organisatorische Sicherheitsmaßnahmen,
- Erfahrung des Anbieters im Markt-
- Sonstige Aspekte, die auf eine Zuverlässigkeit des Anbieters schließen lassen (Datenschutz-Dokumentationen, Kooperationsbereitschaft. Reaktionszeiten etc.).

[3] Soll ein Dienstleister personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen, bedarf es des Abschlusses eines Vertrags zur Auftragsdatenverarbeitung. Hierin sind Datenschutz- und IT-Sicherheitsaspekte zu regeln.

[4] Der Dienstleister ist im Hinblick auf die mit ihm vertraglich vereinbarten technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen. Das Ergebnis ist zu dokumentieren.

§ 9 Datenvermeidung, Datensparsamkeit, Privacy by Design

[1] Der Umgang mit personenbezogenen Daten ist an dem Ziel auszurichten. so wenige Daten wie möglich von einem Betroffenen zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist.

[2] Entsprechendes gilt für die Auswahl und Gestaltung von Datenverarbeitungssystemen, der Datenschutz ist von Anfang an in die Spezifikationen und die Architektur von Datenverarbeitungssystemen zu integrieren, um die Einhaltung der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes zu erleichtern („Privacy by Design").

§ 10 Rechte von Betroffenen

[1] Betroffene haben das Recht auf Auskunft über die im Verein über ihre Person gespeicherten personenbezogenen Daten.

[2] Bei der Bearbeitung von Anfragen ist die Identität des Betroffenen zweifelsfrei festzustellen.

[3] Die Auskunftserteilung erfolgt wegen der Dokumentationspflicht in der Regel auf schriftlichem Weg und beinhaltet, neben den zur Person vorhandenen Daten, auch die Empfänger von Daten sowie den Zweck der Speicherung.

[4] Betroffene haben einen Anspruch auf Berichtigung ihrer personenbezogenen Daten, wenn sich diese als unrichtig erweisen.

[5] Personenbezogene Daten sind unter den folgenden Voraussetzungen zu loschen: Ihre Speicherung ist unzulässig oder es handelt sich um besondere personenbezogene Daten, deren Richtigkeit nicht bewiesen werden kann, oder die Kenntnis der Daten ist für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich.

[6] An die Stelle einer Löschung kann eine Sperrung von Daten treten, wenn eine Kenntnis der Daten für die Erfüllung des Zwecks der Speicherung zwar nicht mehr erforderlich ist, jedoch gesetzliche, satzungsmäßige oder vertragliche Aufbewah-

rungsfristen entgegenstehen, oder schutzwürdige Interessen der Betroffenen beeinträchtigt würden. Oder eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

[7] Widerspricht der Betroffene der Verarbeitung oder Nutzung seiner Daten für Zwecke der Werbung [vgl. § 13], ist eine weitere Verarbeitung oder Nutzung für diese Zwecke unzulässig.

§ 11 Auskunftsersuchen Dritter über Betroffene

Sollte eine Stelle Informationen über Betroffene fordern, so beispielsweise Mitglieder oder Beschäftigte des DVG ist eine Weitergabe von Informationen nur zulässig, wenn die Auskunft gebende Stelle ein berechtigtes Interesse hierfür darlegen kann, und eine gesetzliche Norm zur Auskunft verpflichtet, sowie die Identität des Anfragenden oder der anfragenden Stelle zweifelsfrei feststeht.

§ 12 Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)

Wegen der regelmäßig bzw. immer wieder kehrend erfolgenden Mitgliederverwaltung (z. B. Aktualisierung des Mitgliederverzeichnisses aufgrund von Vereinsbeitritten) führt der DVG eine Übersicht über die Verfahren zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten (Verzeichnis von Verarbeitungstätigkeiten). Auf Verlangen der zuständigen Aufsichtsbehörde stellt der DVG dieses Verzeichnis wie gesetzlich vorgeschrieben ~~unverzüglich~~ zur Verfügung.

§ 13 Werbung

[1] Die werbliche Ansprache von Betroffenen per Brief, Telefon, Fax, oder E-Mail ist grundsätzlich nur zulässig, wenn der Betroffene zuvor in die Verwendung seiner Daten zu Werbezwecken eingewilligt hat.

[2] Ausnahmen sind nur beim Vorliegen einer Erlaubnisnorm zulässig, z.B. wenn der Betroffene schon in der Vergangenheit Werbung erhalten hat, und dem nicht widersprochen hat (konkludente Einverständniserklärung).

§ 14 Schulung

Beschäftigte, die ständig oder regelmäßig Zugang zu personenbezogenen Daten haben, solche Daten erheben oder Systeme zur Verarbeitung solcher Daten entwickeln, sind in geeigneter Weise über die datenschutzrechtlichen Vorgaben zu schulen. Die regelmäßige, angemessene Schulung ist zu dokumentieren.

§ 15 Datengeheimnis

Beschäftigten ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Sie werden vor Aufnahme ihrer Tätigkeit auf das Datengeheimnis gemäß DSGVO verpflichtet. Die Verpflichtung erfolgt in der Regel durch den Präsidenten des DVG und soll dokumentiert werden.

§ 16 Beschwerden

[1] Jeder Betroffene hat das Recht, sich über eine Verarbeitung seiner Daten zu beschweren, sollte er sich hierdurch in seinen Rechten verletzt fühlen. Ebenso können Beschäftigte Verstöße gegen diese Verbandsrichtlinie jederzeit anzeigen.

[2] Die zuständige Stelle für die oben genannten Beschwerden ist der Landesbeauftragte für Datenschutz und Informationsfreiheit, Nordrhein-Westfalen, Postfach 20 04 44, 40102 Düsseldorf, Tel.: 0211/38424-0, Fax: 0211/38424-10, E-Mail: poststelle@ldi.nrw.de.

§ 17 Verfügbarkeit, Vertraulichkeit und Integrität von Daten

[1] In Abhängigkeit der Art der Daten und deren Schutzbedürftigkeit hat für jedes Verfahren eine dokumentierte Schutzbedarfsfeststellung und Risikoanalyse zu erfolgen. Dies gilt insbesondere für besondere personenbezogene Daten gem. § 3 Abs. 2 dieser Richtlinie.

[2] Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität von Daten wird ein allgemeines Sicherheitskonzept erstellt, das für alle Verfahren angewendet wird („TOMs“ = technisch organisatorische Maßnahmen). Zum Beispiel sind Türen unbesetzter Räume zu verschließen. Wirksame Maßnahmen zur Zugangskontrolle an Geräten (z.B. Passwort) müssen vorhanden und aktiviert sein. Systemzugänge sind in Abwesenheit stets zu sperren.

[3] Passwörter ermöglichen einen Zugang zu Systemen und den darin gespeicherten personenbezogenen Daten. Sie stellen eine persönliche Kennung des Nutzers dar und dürfen nicht übertragen werden. Es ist sicherzustellen, dass Passwörter stets unter Verschluss gehalten werden.

[5] Zugriffe auf personenbezogene Daten sollen nur diejenigen Personen erhalten, die im Zuge ihrer Aufgabenwahrnehmung Kenntnis von den jeweiligen Daten erhalten müssen („Need-to-Know-Prinzip"). Zugriffsberechtigungen müssen genau und vollständig festgelegt und dokumentiert sein.

[6] Wartungsarbeiten an Systemen oder Telekommunikationseinrichtungen durch externe Dienstleister sind zu beaufsichtigen. Ferner ist zu gewährleisten, dass Dienstleister nicht unbefugt auf personenbezogene Daten zugreifen können, Fernwartungszugänge sind nur im Einzelfall zu gewähren und müssen dem Prinzip der minimalen Rechtevergabe folgen, Fernwartungsaktivitäten sind nach Möglichkeit aufzuzeichnen oder zu protokollieren.

§ 18 Unrechtmäßige Kenntniserlangung von Daten („Datenpanne“, Art. 33 u. 34 DSGVO)

[1] Sollten Verbandsdaten unrechtmäßig Dritten offenbart worden sein, z. B. durch einen Hacker-Angriff, ist darüber innerhalb von 72 Stunden (ohne schuldhafte Verzögerung), die zuständige Aufsichtsbehörde zu informieren.

[2] Die Meldung hat alle relevanten Informationen zur Aufklärung des Sachverhalts zu umfassen. insbesondere die empfangende Stelle, die betroffenen Personen sowie Art und Umfang der übermittelten Daten.

[3] Die Erfüllung einer etwaigen Informationspflicht gegenüber Betroffenen oder der Aufsichtsbehörde erfolgt durch den DVG Vorstand, es sei denn, es wurde ein Datenschutzbeauftragter bestellt.

§ 19 Folgen von Verstößen

Ein fahrlässiger oder gar mutwilliger Verstoß gegen diese Richtlinie kann arbeitsrechtliche, strafrechtliche und zivilrechtliche Maßnahmen nach sich ziehen.

§ 20 *Aktualisierung der Richtlinie*

Im Rahmen der Fortentwicklung des Datenschutzrechts sowie technologischer oder organisatorischer Veränderungen wird diese Richtlinie regelmäßig auf einen Anpassungs- oder Ergänzungsbedarf hin überprüft. Änderungen an dieser Richtlinie sind formlos wirksam. Die Beschäftigten sind umgehend und in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis zu setzen.

Diese Ordnung wurde vom DVG Vorstand am 13.04.2019 beschlossen und tritt in der jetzigen Form zum 01.05.2019 in Kraft.