Datenschutzrechtliche Hinweise für alle Rechteinhaber (unabhängig von der Rechtegruppe) in NaMi

Grundlage Datenverarbeitung

Der Bundesamt Sankt Georg e.V. (BSG e. V.) als Rechtsträger der Deutschen Pfadfinderschaft Sankt Georg (DPSG) und seine Untergliederungen erheben, verarbeiten und nutzen personenbezogene Daten seiner Mitglieder unter Einsatz von Datenverarbeitungsanlagen zur Durchführung und Verwaltung der Mitgliedschaft und Erfüllung der in seiner Satzung und der zugehörigen Ordnungen aufgeführten Zwecke und Aufgaben.

Die oben genannten verarbeiteten Daten beziehen sich auf alle im „Antrag zur Mitgliedschaft in der DPSG“ vom Mitglied angegebenen Daten. Darüber hinaus werden im Laufe der Mitgliedschaft Daten zu Veranstaltungsteilnahmen, Amtsausübungen, Bankverbindungen sowie erteilte SEPA-Lastschriftmandate und die Namensnennung auf der Beitragsrechnung an die Gruppierung gespeichert. Rechtsgrundlage ist § 6 Abs. 1 KDG.

Nutzungsbedingungen Mitgliederverwaltung / Datenschutzbelehrung

Alle Benutzerinnen und Benutzer der Mitgliederverwaltung müssen im Rahmen der Freischaltung die Nutzungsbedingungen akzeptieren. Die Anerkennung der Nutzungsbedingungen wird für jeden einzelnen Benutzer-Account elektronisch dokumentiert.

Verpflichtung auf die Vertraulichkeit für Benutzer der Mitgliederverwaltung der DPSG / BSG e. V.

Die Verpflichtung auf die Vertraulichkeit besteht auch nach der Beendigung meiner, mit dem entsprechenden Recht versehenden, Tätigkeit für den BSG e.V. fort. Ich nehme zur Kenntnis, dass die persönlichen Zugangsdaten nicht weitergegeben werden und nur von mir persönlich genutzt werden dürfen. Die Zugangsdaten sind vor dem unbefugten Zugriff durch Dritte zu schützen.

Mit der Beantragung der persönlichen Zugangsdaten zur Mitgliederverwaltung und der damit verbundenen Zugangsberechtigung erkläre ich in Bezug auf die Vertraulichkeit und Integrität personenbezogener Daten die Vorgaben der geltenden Datenschutzvorschriften einzuhalten.

Die einschlägigen gesetzlichen Vorschriften verlangen, dass personenbezogene Daten so verarbeitet werden, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit und Integrität ihrer Daten gewährleistet werden.

Nach diesen Vorschriften ist es untersagt, personenbezogene Daten unbefugt oder unrechtmäßig zu verarbeiten oder absichtlich oder unabsichtlich die Sicherheit der Verarbeitung in einer Weise zu verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugter Offenlegung oder unbefugtem Zugang führt. Verstöße gegen die Datenschutzvorschriften können ggf. mit Geldbuße, Geldstrafe oder Freiheitsstrafe geahndet werden. Entsteht der betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein Schadenersatzanspruch entstehen.

Die Mitgliederdaten werden mit Hilfe der Internet-Datenbank „NaMi“ erfasst und verwaltet. Das Erheben, Verarbeiten, Nutzen, Speichern, Veränderung, Übermitteln, Sperren und Löschen unterliegt den Bestimmungen des KDG bzw. der DSGVO gültig in der jeweils gültigen Fassung. Mit der Beantragung der persönlichen Zugangsdaten zur Mitgliederverwaltung und der damit verbundenen Zugangsberechtigung willige ich ein, dass alle mir zur Verfügung gestellten personenbezogenen Daten nur unter Berücksichtigung der Vorgabe des KDG verarbeitet und genutzt werden dürfen. Ohne dieses Einverständnis kann eine Benutzung der NaMi nicht gewährt werden.

Ich bestätige ferner, dass ich die mir zur Verfügung gestellten personenbezogenen Daten ausschließlich für Vereinszwecke verwende.

Ich nehme zur Kenntnis, dass die persönlichen Zugangsdaten nicht weitergegeben werden und nur von mir persönlich genutzt werden.

Weitergabe von Daten aus der Mitgliederverwaltung

Die Weitergabe von Daten innerhalb der DPSG (in elektronischer, gedruckter oder anderer Form) ist nur zulässig, soweit dies zur Erfüllung satzungsgemäßer Aufgaben erforderlich ist. Dabei ist das Prinzip der Datensparsamkeit zu wahren, d.h. es dürfen nur genau die Daten weitergegeben werden, die zur Ausübung der jeweiligen Tätigkeit benötigt werden (d.h. z.B. keine Kontodaten an Gruppenleiterinnen und Gruppenleiter, Gruppenleiterinnen und Gruppenleiter erhalten nur die Mitgliederliste ihrer Gruppe und nicht des gesamten Stammes). Darüber hinaus ist auf die Sicherheit der Daten zu achten, d.h. sie sind angemessen vor Zugriff oder Manipulation durch Unbefugte zu schützen.

Eine Weitergabe der Daten an Dritte ist nur im Rahmen rechtlicher Verpflichtungen, einer Auftragsdatenverarbeitung im Rahmen des Vereinszwecks oder nach ausdrücklicher, auf den jeweiligen Einzelfall bezogenen, Zustimmung der betroffenen Person zulässig.

In jedem Fall sind die Empfänger von Daten auf das Datengeheimnis zu verpflichten, die Verpflichtung ist zu dokumentieren.

Ausgetretene Mitglieder / Löschung von Daten

Datenätze von Mitgliedern, die der

- **Datenweiterverwendung zugestimmt** haben, verbleiben im System. Die Änderungshistorie dieser Datensätze wird nach 365 Tagen gelöscht.

- **Datenweiterverwendung nicht zugestimmt** haben werden im System sofort gelöscht. Eine Wiederherstellung des Datensatzes in Hinblick auf eine weitere Mitgliedschaft ist nicht mehr möglich. Die Änderungshistorie dieser Datensätze wird nach 90 Tagen gelöscht.

Das Speichern dieser Daten ist darin begründet, nachträglich eventuelle Beitragsrückstände oder sonstige Ansprüche und Forderungen einzuholen, oder nicht erfolgte Rechnungsstellung nachzuholen, die sich aus der Mitgliedschaft ergeben.

Auf Wunsch des Mitglieds können die Daten nach Einzelfallprüfung entsprechend dem Vorgehen in der NaMi unverzüglich gelöscht werden.
Daten ausgetretener Mitglieder dürfen nur für solche, sich unmittelbar aus der Mitgliedschaft ergebenden, satzungsgemäßen Zwecke verwendet werden. Eine Weitergabe dieser Daten ist grundsätzlich nicht gestattet.

Weitere gesetzliche Aufbewahrungspflichten bleiben bestehen. Soweit für bestimmte Daten längere Speicherfristen gelten (z.B. aufgrund von gesetzlichen Anforderungen oder zur Dokumentation von bestimmten Wahlämtern), so sind diese Daten nur für die Mitgliederverwalter/innen der Untergliederungen und der Bundesebene unter entsprechender Datenschutz-Verpflichtung zugänglich.

Anlage zur Verpflichtung auf die Vertraulichkeit

Die vorliegende Auswahl gesetzlicher Vorschriften soll euch einen Überblick über das datenschutzrechtliche Regelwerk geben. Der Überblick erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen erhaltet ihr auf Nachfragen beim betrieblichen Datenschutzbeauftragten unter datenschutz@dpsg.de oder in eurer Diözese.

Begrifflichkeiten

„**Personenbezogene Daten**" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. (Auszug: §4, 1 KDG)

„**Verarbeitung**" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung; (Auszug §4, 3KDG)

Grundsätze der Verarbeitung

Personenbezogene Daten müssen a) auf **rechtmäßige** und in einer für die betroffene Person **nachvollziehbaren** Weise **verarbeitet** werden; b) für **festgelegte**, **eindeutige** und **legitime Zwecke erhoben** werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; c) dem **Zweck angemessen** und erheblich sowie auf das für die Zwecke der Verarbeitung **notwendige Maß** beschränkt sein; insbesondere sind **personenbezogene Daten** zu **anonymisieren** oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und der Aufwand nicht außer Verhältnis zum angestrebten Schutzzweck steht; d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden; e) in einer Form **gespeichert** werden, die die **Identifizierung** der betroffenen Personen nur **so lange ermöglicht**, wie es für die Zwecke, für die sie verarbeitet

werden, **erforderlich** ist; f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich **Schutz** vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen. (Auszug § 7, 1 KDG)

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – **Vernichtung, Verlust, Veränderung**, unbefugte **Offenlegung** von oder unbefugten **Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden. (Auszug §26, 2KDG)

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten **ausschließlich auf Weisung** des Verantwortlichen verarbeiten, es sei denn, dass sie nach kirchlichem Recht, dem Recht der Europäischen Union oder dem Recht ihrer Mitgliedstaaten zur Verarbeitung verpflichtet sind. (Auszug §30 KDG).

Der Verantwortliche meldet der Datenschutzaufsicht unverzüglich die **Verletzung** des Schutzes personenbezogener Daten, wenn diese Verletzung eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt. Erfolgt die Meldung nicht binnen 72 Stunden, nachdem die Verletzung des Schutzes personenbezogener Daten bekannt wurde, so ist ihr eine Begründung für die Verzögerung beizufügen. (Auszug 33, 1 KDG).

Haftung, Schadensersatz und Geldbußen

(1) Jede Person, der wegen eines Verstoßes gegen dieses Gesetz ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf **Schadenersatz** gegen die kirchliche Stelle als Verantwortlicher oder Auftragsverarbeiter. (2) Ein **Auftragsverarbeiter haftet** für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus diesem Gesetz nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat. (3) Ein Verantwortlicher oder ein Auftragsverarbeiter ist von der Haftung gemäß Absatz 1 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. (4) Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen. (Auszug §50, 1-4 KDG)

(1) Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter vorsätzlich oder fahrlässig gegen Bestimmungen dieses Gesetzes, so kann die Datenschutzaufsicht eine **Geldbuße** verhängen. (5) Bei Verstößen werden im Einklang mit Absatz 3 Geldbußen von bis zu 500.000 EUR verhängt. (Auszug §51, 1 und 5 KDG)

Weitere Informationen unter
https://www.datenschutz-kirche.de/node/297
https://dpsg.de/de/fuer-mitglieder/datenschutz-heute.html

Stand: 03.08.2018