Richtlinie zur Datenschutz Organisation

Bund der Pfadfinderinnen und Pfadfinder e.V.

1. Grundsätze

Der Schutz personenbezogener Daten ist uns ein wichtiges Anliegen. Deshalb verarbeiten wir die personenbezogenen Daten unserer Mitarbeitenden und Mitglieder in Übereinstimmung mit den anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit.

In dieser Datenschutzrichtlinie wird beschrieben, mit welchen Maßnahmen wir die Sicherheit der Daten gewährleisten und wie betroffene Personen Kontakt mit uns aufnehmen können, wenn sie Fragen zu unserer Datenschutzpraxis haben.

Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die insoweit bestehende Verantwortlichkeit des Bundes der Pfadfinderinnen und Pfadfinder e.V.

Sie richtet sich an

- Die ehrenamtlichen Systemadministratoren/IT Mitarbeitende
- Die Bundesgeschäftsführung
- Hauptamtliche Mitarbeitende
- Ehrenamtliche Mitarbeitende
- Den*Die betriebliche Datenschutzbeauftragte*n

Dabei gelten folgende Grundsätze:

Die Hard- u. Software ist für vereinsinterne Aufgaben zu verwenden und gegen Verlust und Manipulation zu sichern. Eine Nutzung für private Zwecke bedarf der ausdrücklichen Genehmigung.

Die Mitarbeitenden sind in ihrem jeweiligen Verantwortungsbereich für die Umsetzung der Richtlinie verantwortlich. Die Einhaltung muss von ihnen regelmäßig kontrolliert werden.

2. Der*Die betriebliche Datenschutzbeauftragte

2.1 Der Bund der Pfadfinderinnen und Pfadfinder e.V. hat nach Maßgabe des Artikels 37 DS-GVO eine*n betriebliche*n Datenschutzbeauftragte*n bestellt. Die Kontaktdaten der*des Datenschutzbeauftragten sind zu finden unter: https://meinbdp.de/display/BUND/Datenschutz-Grundverordnung

Der*Die Datenschutzbeauftragte nimmt die Kraft Gesetzes und aus dieser Richtlinie zugewiesenen Aufgaben bei weisungsfreier Anwendung seines*ihres Fachwissens wahr.

2.2. Der*Die Datenschutzbeauftragte unterrichtet und berät die Bundesgeschäftsführung, den Bundesvorstand und die Beschäftigten hinsichtlich ihrer Datenschutzpflichten. Ihm*Ihr obliegt die Überwachung und Einhaltung der Datenschutzvorschriften einschließlich der Sensibilisierung und Schulung der Mitarbeitenden.

Im Falle risikoreicher Datenverarbeitungen steht der*die Datenschutzbeauftragte den Verantwortlichen beratend bei der Risikoabschätzung zur Seite.

2.3. Der*Die Datenschutzbeauftragte unterrichtet unmittelbar die Bundesgeschäftsführung.

2.4. Der*Die Datenschutzbeauftragte wird frühzeitig in alle Datenschutzfragen eingebunden und wird sowohl von der Bundesgeschäftsführung, dem Bundesvorstand und den Beschäftigten bei der Erfüllung seiner*ihrer Aufgaben unterstützt.

2.5. Der Bund der Pfadfinderinnen und Pfadfinder e.V. hat ein Verzeichnis über alle Verarbeitungsvorgänge zu führen. Alle Mitarbeitenden haben die dafür notwendigen Informationen zu den Verfahren zusammenzutragen. Diese Informationen werden gem. des Art. 30 DS-GVO dokumentiert.

Auf Anfrage stellt der Verein der Aufsichtsbehörde das Verzeichnis zur Verfügung.

2.6. Die Mitarbeitenden können sich unmittelbar mit Hinweisen, Anregungen oder Beschwerden an den*die Datenschutzbeauftragte wenden, wobei absolute Vertraulichkeit gewahrt wird.

3. Beschaffung von Hard- und Software

3.1. Die Beschaffung von Hard- und Software erfolgt grundsätzlich durch die Haupt-und ehrenamtlichen Systemadministrator*innen/IT Mitarbeitenden. Bereits bei der Auswahl von Hard- und Software wird das Prinzip der Gewährleistung von Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen als ein tragendes Kriterium betrachtet.

3.2. Falls mit der Beschaffung ein neues Verfahren der Verarbeitung eingeführt werden soll, ist der*die Datenschutzbeauftragte rechtzeitig vorab zu informieren. Die Beschaffung erfolgt erst nach Stellungnahme des*der Datenschutzbeauftragten. Diese*r prüft, ob eine Datenschutz-Folgenabschätzung erforderlich ist.

3.3. Private Hard- u. Software darf nicht zur Verarbeitung personenbezogener Daten verwendet werden. Die dienstliche Nutzung im heimischen und außerbetrieblichen Bereich bedarf der Genehmigung der Bundesgeschäftsführung.

3.4. Die Verantwortlichen der IT führen ein Verzeichnis der eingesetzten Hardware und der verwendeten Anwendungsprogramme. Der*Die Datenschutzbeauftragte kann auf das Verzeichnis jederzeit zugreifen.

4. Verpflichtung/Schulung der Mitarbeitenden

4.1. Alle Mitarbeitenden, die Umgang mit personenbezogenen Daten haben, sind zu einem vertraulichen Umgang mit personenbezogenen Daten zu verpflichten.

4.2. Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Formulars.

5. Transparenz der Datenverarbeitung

5.1. Über Verfahren, die den Umgang mit personenbezogenen Daten betreffen, führt der*die Datenschutzbeauftragte ein Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DS-GVO. Die Mitarbeitenden melden die Daten zeitnah gemäß den Vorgaben dem*der Datenschutzbeauftragten. Gleiches gilt für Veränderungen.

5.2. Unabhängig von dieser Meldung ist der*die Datenschutzbeauftragte bei der Planung der Einführung neuer Verarbeitungen bzw. Veränderung bestehender Verfahren über Zweck und Inhalt der Anwendung und der Erfüllung der Benachrichtigungspflicht zu informieren.

5.3. Soweit der*die Datenschutzbeauftragte feststellt, dass die beabsichtigte Verarbeitung einer Datenschutz-Folgeabschätzung unterliegt, teilt er*sie dies der Bundesgeschäftsführung umgehend mit.

5.4. Machen Betroffene von ihrem Auskunftsrecht nach Art. 15 DS-GVO oder dem Korrektur- oder Widerspruchsrecht nach Art. 16 und Art. 21 DS-GVO Gebrauch, so erfolgt die zentrale Bearbeitung durch den*die Datenschutzbeauftragte*n.

Auskunft und Einsichtsrechte von Mitarbeitenden werden durch die Bundesgeschäftsführung erfüllt.

6. Erhebung und Verarbeitung von personenbezogenen Daten

6.1. Die Erhebung und Verarbeitung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen erfolgen. Hierbei sind auch die besonderen Voraussetzungen für die Erhebung und Verarbeitung sensibler Daten gem. Art. 9 Abs. 1 DS-GVO zu beachten. Grundsätzlich dürfen nur solche Informationen verarbeitet und genutzt werden, die zur Aufgabenerfüllung erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen.

6.2. Vor Einführung neuer Arten von Datenerhebungen ist die Zulässigkeit durch den*die zuständigen Mitarbeitende*n schriftlich zu dokumentieren.

6.3. Falls andere Stellen Informationen über Betroffene anfordern, dürfen diese ohne Einwilligung des*der Betroffenen nur gegeben werden, wenn hierfür eine gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes, legitimes Interesse des Vereins besteht.

7. Datenhaltung/Versand/Löschung

7.1 Die Speicherung von Daten erfolgt grundsätzlich auf dem hierfür zur Verfügung gestellten Netzlaufwerk und in verschlüsselter Form sowohl auf einem Onsite- als auch einem Offsite-Backup.

Für die Sicherung auf dem Server sind die vom Vorstand beauftragten Administrator*innen verantwortlich, die Onsite-Backups erfolgen vollständig automatisiert, die Offsite-Backups halb-automatisch durch die Geschäftsführung.

Eine Speicherung auf mobilen Datenträgern bedarf der Genehmigung durch die Bundesgeschäftsführung.

7.2. Soweit technisch bedingt ein anderer Speicherort erforderlich ist (z.B. Notebook), ist der*die jeweilige Benutzer*in für die Durchführung der Datensicherung verantwortlich.

7.3. Bei Weiter- oder Rückgabe nicht mehr benötigter IT-Komponenten ist der*die Benutzer*in verpflichtet, dafür zu sorgen, dass zuvor sämtliche Daten wirksam gelöscht wurden.

8. Externe Dienstleister/Auftragsverarbeiter/Wartung

Sollen externe Dienstleister erstmals mit der Verarbeitung von Daten beauftragt werden, bei denen sie die Möglichkeit der Kenntnis personenbezogener Daten bekommen, so ist der*die Datenschutzbeauftragte hinzuzuziehen.

Der Vertragsentwurf wird von ihm*ihr hinsichtlich den Anforderungen des Art. 28 DS-GVO geprüft.

9. Sicherheit der Verarbeitung

9.1. Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität der Daten, ist ein allgemeines Sicherheitskonzept zu erstellen.

9.2. Neben dieser Richtlinie bestehen ergänzende Regelungen. Hierzu gehören u.a.:

- Richtlinien zur Nutzung von Notebooks,
- Arbeitsanweisung zur Nutzung von Passwörtern (im Rahmen der Mitarbeitenden-Unterweisung),
- Arbeitsanweisung zur PC-und Laptopnutzung (im Rahmen der Mitarbeitenden-Unterweisung),
- Dienstvereinbarung über die private Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz,
- Nutzungsbedingungen Mitgliederverwaltung