Entwurf Stand: 01.07.2020

Deutscher Psoriasis Bund e.V. (DPB)
Ordnung über den Datenschutz (DS O) [ENTWURF]

Abschnitt A ALLGEMEINE REGELN

1. Vorwort

Im Deutschen Psoriasis Bund e.V. (DPB) werden fortlaufend personenbezogene Daten verarbeitet. Der Schutz dieser Daten ist dem Verein ein wichtiges Anliegen. Dies erfordert ein umfassendes Datenschutz- und Informationssicherheits-Managementsystem.

In dieser Ordnung über den Datenschutz (DS O) wird beschrieben, welche Arten von personenbezogenen Daten erhoben werden, wie diese Daten genutzt werden, an wen sie übermittelt werden und welche Wahlmöglichkeiten und Rechte betroffene Personen im Zusammenhang mit der Verarbeitung von Daten haben. Außerdem wird beschrieben, mit welchen Maßnahmen die Sicherheit der Daten gewährleistet wird und wie Personen Kontakt mit dem Verein aufnehmen können, wenn sie Fragen zur Datenschutzpraxis haben.

Diese Ordnung regelt die datenschutzkonforme Informationsverarbeitung und bestehende Verantwortlichkeiten. Alle für den Verein tätigen Personen sind zur Einhaltung dieser Ordnung verpflichtet.

Mit der in dieser Ordnung gewählten vereinfachten Sprachform sind jeweils alle gesetzlich anerkannten Geschlechterformen gemeint.

Auszug aus der DPB-Satzung (§ 16):

Zur Erfüllung seiner Zwecke verarbeitet der Verein personenbezogene Daten seiner Mitglieder und gegebenenfalls weiterer Personen. Die Verarbeitung personenbezogener Daten erfolgt unter Einhaltung der gesetzlichen Regelungen und Bestimmungen mit datenschutzrechtlichem Charakter. Näheres zur Verarbeitung und zum Schutz personenbezogener Daten im Verein regelt eine Ordnung über den Datenschutz (DS O).

2. Verpflichtung und Schulung von Beschäftigten

Jeder Beschäftigte des Vereins, der Umgang mit personenbezogenen Daten hat, ist auf einen vertraulichen Umgang mit personenbezogenen Daten zu verpflichten. Die Verpflichtung erfolgt unter Verwendung der hierfür vorgesehenen Formulare und unter Aushändigung der entsprechenden Merkblätter (siehe Anlagen 5, 6, 7, 8 und 9). Eine Ausfertigung der jeweiligen Verpflichtungserklärung ist zur Personalakte zu nehmen.

Für die Verpflichtung der Beschäftigten und ihre Schulung im Bereich des Datenschutzes ist, sofern kein Datenschutzbeauftragter bestellt ist, der Geschäftsführer verantwortlich.

3. Verpflichtung und Schulung von ehrenamtlich Aktiven

Im Verein ehrenamtlich Aktive sind – bevor ihnen personenbezogene Daten zugänglich gemacht werden – auf einen vertraulichen Umgang mit personenbezogenen Daten zu verpflichten. Die Verpflichtung erfolgt unter Verwendung des hierfür vorgesehenen Formulars und unter Aushändigung des entsprechenden Merkblattes (siehe Anlagen 2 und 3). Eine Ausfertigung der Verpflichtungserklärung ist in der Geschäftsstelle aufzubewahren.

Für die Verpflichtung der ehrenamtlich Aktiven und ihre Schulung im Bereich des Datenschutzes ist, sofern kein Datenschutzbeauftragter bestellt ist, der Geschäftsführer verantwortlich.

4. Datenschutzbeauftragter (DSB)

Sobald für die automatisierte Erhebung und Verarbeitung personenbezogener Daten ständig mehr als neunzehn Personen (Beschäftigte, ehrenamtlich Aktive etc.) tätig werden, ist ein Datenschutzbeauftragter (DSB) zu bestellen.

Die dann weiteren, nicht in den folgenden Abschnitten aufgeführten, für den Datenschutzbeauftragten geltenden Bestimmungen sind aus der Anlage 1 ersichtlich.

Abschnitt B ERHEBUNG UND VERARBEITUNG VON PERSONENBEZOGENEN DATEN

1. Datenerhebung

Die Erhebung und Verarbeitung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen erfolgen. Sollten auch Daten zur Gesundheit erhoben und/oder gespeichert werden, sind die besonderen Voraussetzungen für die Erhebung und Verarbeitung sensibler Daten gemäß Art. 9 der EU-Datenschutz-Grundverordnung (DSGVO) zu beachten. Grundsätzlich dürfen nur solche Informationen verarbeitet und genutzt werden, die zur betrieblichen Aufgabenerfüllung bzw. zur Aufgabenerfüllung des Vereins erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen.

Es wird sichergestellt, dass Betroffene keinen Entscheidungen unterworfen werden, die ausschließlich auf einer automatisierten Datenverarbeitung beruhen und zugleich den Betroffenen gegenüber eine rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen (z.B. „Profiling“).

Vor Einführung neuer Arten der Datenerhebung ist die die Zulässigkeit bestimmende Zweckbestimmung der Daten durch den für die Anwendung Verantwortlichen schriftlich zu dokumentieren. Grundsätzlich ist eine Zweckänderung nur dann zulässig, wenn die Verarbeitung mit denjenigen Zwecken vereinbar ist, für die die Daten ursprünglich erhoben worden sind. Die im Rahmen der Zweckänderung genutzten Abwägungskriterien sind einzeln zu prüfen. Die Prüfung ist darüber hinaus auch zu einem ordnungsgemäßen Nachweis zu dokumentieren.

Eine Zweckänderung ist auch zulässig, wenn eine Einwilligung der betroffenen Person durch den Verantwortlichen eingeholt wird. Gleichzeitig hat der für die Verarbeitung Verantwortliche vor der Erhebung bzw. Speicherung von Daten schriftlich festzulegen, ob und in welcher Art und Weise der gesetzlichen Benachrichtigungspflicht des Betroffenen zu genügen ist.

2. Datenverarbeitung

Falls andere Stellen Informationen über Betroffene anfordern, dürfen diese ohne Einwilligung der Betroffenen nur herausgegeben werden, wenn hierfür eine gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes legitimes Interesse des Vereins besteht und die Identität des Anfragenden zweifelsfrei feststeht. Im Zweifel ist, sofern kein Datenschutzbeauftragter bestellt ist, der Geschäftsführer zu kontaktieren.

3. Sicherheit der Datenverarbeitung

Für jedes Verfahren der Datenverarbeitung ist eine dokumentierte Schutzbedarfsfeststellung sowie eine Analyse bzgl. der für den Betroffenen möglichen Risiken zu erstellen. Diese berücksichtigt Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Wahrscheinlichkeit des Eintritts einer solchen Gefahr.

Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität der Daten sowie der Belastbarkeit der datenverarbeitenden Systeme ist ein allgemeines Sicherheitskonzept zu erstellen. Das Konzept orientiert sich an der zuvor erstellten Schutzbedarfsfeststellung und der Risikoanalyse. Dieses Konzept ist maßgeblich für alle weiteren Verfahren der Datenverarbeitung.

Die Regelungen des Art. 32 DSGVO, insbesondere zur Realisierung der Datensicherungsgebote für zu treffende Maßnahmen, sind zu beachten.

4. Transparenz der Datenverarbeitung

Über Verfahren der Datenverarbeitung, die den Umgang mit personenbezogenen Daten betreffen, ist ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO zu führen. Sofern ein Datenschutzbeauftragter bestellt ist, führt er das Verzeichnis. Der für das Verfahren Verantwortliche meldet ihm dies zeitnah. Gleiches gilt für Veränderungen.

Sofern ein Datenschutzbeauftragter bestellt ist, ist er über die Planung der Einführung neuer Verarbeitungstätigkeiten bzw. der Veränderung bestehender Verfahren über Zweck und Inhalt der Anwendung und die Erfüllung der Benachrichtigungspflicht zu informieren. Bei standardisierten Erhebungen (Fragebögen, Eingabefelder auf der Internet-Homepage etc.) ist ihm der Erhebungsbogen etc. zur Abstimmung vorzulegen.

Bei der Erhebung und Nutzung von Gesundheitsdaten ist bei jeder Einführung bzw. Veränderung bestehender Verfahren der Datenverarbeitung eine Datenschutz-Folgenabschätzung erforderlich.

Macht ein Betroffener von seinem Auskunftsrecht nach Art. 15 DSGVO oder seinem Korrektur- oder Widerspruchsrecht nach Art. 16 und Art. 21 DSGVO Gebrauch, erfolgt die Bearbeitung, sofern kein Datenschutzbeauftragter bestellt ist, durch den Geschäftsführer. Auskunfts- und Einsichtsrechte von Beschäftigten werden durch den Geschäftsführer erfüllt.

Es ist sicherzustellen, dass dem Betroffenen seine Daten auf Wunsch in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden können. Welcher Standard diesen Anforderungen genügt, ist im Vorfeld einvernehmlich vom Geschäftsführer festzulegen.

5. Rechenschafts- und Dokumentationspflicht

Die Einhaltung der Vorgaben, die sich aus dieser Ordnung ergeben, muss jederzeit nachweisbar sein („Accountability“). Eine Nachweisbarkeit hat insbesondere durch eine schlüssige und nachvollziehbare schriftliche Dokumentation der getroffenen Maßnahmen und der dazugehörigen Abwägungen zu erfolgen.

Abschnitt C DATENHALTUNG, VERSAND UND LÖSCHUNG

1. Datenhaltung

Die Speicherung von Daten erfolgt grundsätzlich auf den hierfür zur Verfügung gestellten Netzlaufwerken. Eine Speicherung auf mobilen Datenträgern oder in Cloudspeichern (z.B. Flashspeicher, Streamer-Bänder) bedarf der Genehmigung durch den Geschäftsführer und der Registrierung der diese Datenträger einsetzenden Benutzer. Bei Netzwerken ist der Geschäftsführer für die Sicherung der Daten verantwortlich, die auf dem Server gespeichert sind.

2. Versand von personenbezogenen Daten

Soweit technisch bedingt ein anderer Speicherort erforderlich ist (z.B. Notebook, Desktop-PC) ist der jeweilige Benutzer für die Durchführung der Datensicherung selbst verantwortlich. Ist ein Netzzugang möglich (z.B. bei Notebook/Tablet mit WLAN), ist zumindest einmal wöchentlich der aktuelle Datenbestand auf das für den Benutzer reservierte Netzlaufwerk zu überspielen. Die gewählten Datensicherungsmaßnahmen sind in dem Verzeichnis von Verarbeitungstätigkeiten zu dokumentieren.

3. Löschung von personenbezogenen Daten

Gesetzliche Aufbewahrungsfristen und Löschungstermine sind von dem über die Verarbeitung der Daten Entscheidenden in seiner Verantwortung zu beachten. Der Geschäftsführer ist über die Einhaltung der Termine insbesondere im Hinblick auf die Löschung personenbezogener Daten in Sicherungskopien zu informieren.

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

Abschnitt D BESCHAFFUNG UND NUTZUNG VON HARD- UND SOFTWARE

1. Beschaffung von Hard- und Software

Die Beschaffung von Hard- und Software erfolgt grundsätzlich auf Anforderung des Geschäftsführers. Bereits bei der Auswahl von Hard- und Software wird das Prinzip der Gewährleistung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als ein tragendes Kriterium beachtet.

Falls mit der Beschaffung ein neues Verfahren der Verarbeitung personenbezogener Daten eingeführt werden soll, ist, sofern bestellt, der Datenschutzbeauftragte rechtzeitig vorab zu informieren. Bei der Verarbeitung von besonders sensiblen Daten gemäß Art. 9 DSGVO müssen alle Verfahren und Systeme, die personenbezogene Daten verarbeiten, einer Risikoanalyse unterzogen werden und verpflichtend ist eine Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 3 DSGVO. Die Beschaffung erfolgt erst nach Durchführung der Datenschutz-Folgenabschätzung und, sofern bestellt, Stellungnahme des Datenschutzbeauftragten. Im Zweifel entscheidet der Vorstand.

2. Nutzung von Hard- und Software

Private Hard- und Software darf nicht zur Verarbeitung personenbezogener Daten Verwendung finden. Die dienstliche Nutzung privater Hard- und Software im heimischen und außerbetrieblichen Bereich (z.B. private Notebooks) ist nicht gestattet.

Der Geschäftsführer führt ein Verzeichnis der eingesetzten Hardware und der verwendeten Anwendungsprogramme.

Bei Verdacht des Diebstahls von Hard- und Software, des unbefugten Zugriffs auf personenbezogene Daten, von Sabotage etc. sind der Geschäftsführer und, sofern bestellt, der Datenschutzbeauftragte unverzüglich zu informieren. Näheres regeln der hierfür vorgesehene Meldebogen und das entsprechende Merkblatt (siehe Anlagen 8 und 9).

Abschnitt E EXTERNE DIENSTLEISTER, WARTUNG UND AUFTRAGSVERARBEITUNG

Sollen externe Dienstleister erstmals mit der Verarbeitung personenbezogener Daten bzw. mit einzelnen Verarbeitungsschritten (z.B. Erhebung, Löschung = Entsorgung) bzw. mit Tätigkeiten (z.B. Wartung, Reparatur), bei denen sie die Möglichkeit der Kenntnis personenbezogener Daten bekommen, beauftragt werden, ist, sofern bestellt, der Datenschutzbeauftragte vor der Beauftragung unter Vorlage des den Anforderungen des Art. 28 DSGVO genügenden Vertragsentwurfes und unter Vorlage der Kriterien der erfolgten bzw. nachfolgend vorgesehenen Auftragskontrolle zu informieren.

Entsprechendes gilt, wenn der Verein für Wartungstätigkeiten die Dienste eines Dritten in Anspruch nehmen will oder der Verein Datenverarbeitung im Auftrag Dritter wahrnehmen will.

Abschnitt F GELTUNG

Im Übrigen sind die Satzung und die weiteren Ordnungen des Vereins jeweils sinngemäß anzuwenden.

Diese Ordnung über den Datenschutz (DS O) mit ihren Anlagen tritt mit ihrer Beschlussfassung durch die Mitgliederversammlung in Kraft.

Verabschiedet durch Beschluss der Mitgliederversammlung am XX.XX.20XX.

ANLAGEN

Anlage 1	Bestimmungen zum Datenschutzbeauftragten (DSB)
Anlage 2	Verpflichtung auf die Vertraulichkeit und das Fernmeldegeheimnis für ehrenamtlich Aktive
Anlage 3	Merkblatt für ehrenamtlich Aktive zur Verpflichtung auf die Vertraulichkeit und das Fernmeldegeheimnis
Anlage 4	Datenschutzerklärung gegenüber Beschäftigten
Anlage 5	Verpflichtung auf die Einhaltung der datenschutzrechtlichen Anforderungen für Beschäftigte
Anlage 6	Verpflichtung auf die Vertraulichkeit und das Fernmeldegeheimnis für Beschäftigte
Anlage 7	Merkblatt für Beschäftigte zur Verpflichtung auf die Vertraulichkeit und das Fernmeldegeheimnis
Anlage 8	Meldebogen für Datenschutz- und Sicherheitsereignisse
Anlage 9	Merkblatt für Beschäftigte zur Meldepflicht bei Datenpannen
Anlage 10	Priorisierungstabelle für Datenschutzereignisse