DATENSCHUTZORDNUNG

des

DLRG Landesverbandes

Rheinland-Pfalz e.V.

In Kraft: 24.01.2026

DATENSCHUTZORDNUNG des

DLRG Landesverbands Rheinland-Pfalz e.V.

§ 1 Regelungsbereich

(1) Die Datenschutzordnung regelt auf Grundlage des Bundesdatenschutzgesetzes (BDSG), sowie der EU-Datenschutzgrundverordnung (EU-DSGVO) verbindlich den Umgang mit personenbezogenen Daten, insbesondere das Erheben, Verarbeiten (speichern, verändern, übermitteln, sperren und löschen) und Nutzen solcher Daten im DLRG Landesverband Rheinland-Pfalz e.V. und dem zugehörigen Landesjugendbüro Rheinland-Pfalz, im Folgenden als „Verein“ bezeichnet.

(2) Zur besseren Lesbarkeit werden die in diesem Verzeichnis genannten personenbezogenen Bezeichnungen, die sich zugleich auf Angehörige aller Geschlechter beziehen, generell nur in der männlichen Form angeführt. Dies soll keine Geschlechterdiskriminierung oder eine Verletzung des Gleichheitsgrundsatzes zum Ausdruck bringen.

(3) Zu den geschützten Daten gehören neben den personenbezogenen Daten der Vereinsmitglieder auch Daten zu Personen, die zum Verein. in einem vertraglichen oder sonstigen Verhältnis stehen (z.B. Kursteilnehmer, externe Referenten, Beitragszahler für Mitglieder, Erziehungsberechtigte, Lieferanten, Ministerien, Geschäfts- u. Kooperationspartner, befreundete/artverwandte Organisationen u.a.).

(4) Die Datenschutzordnung gilt sinngemäß für die Bezirke/Kreisverbände und deren Untergliederungen im Landesverband Rheinland-Pfalz, soweit diese keine eigenen entsprechenden Regelungen für sich und ihre Untergliederungen getroffen haben.

§ 2 Datenschutzziele des Vereins

(1) Der Verein als Verantwortlicher ist sich der hohen Bedeutung des Schutzes von personenbezogenen Daten, insbesondere von besonderen personenbezogenen Daten und Daten von Kindern, gegenüber Mitgliedern, Mitarbeitenden, Bewerbern und Partnern in seinem täglichen Handeln bewusst.

(2) Die Überwachung der Einhaltung der Datenschutzziele ist kein einmaliger Prozess, sondern eine immer wiederkehrende Aufgabe. Der Verein möchte sich somit kontinuierlich im Datenschutz verbessern und weiterentwickeln.

(3) Auf Grund der großen Bedeutung des Datenschutzes sind alle Funktionsträger sowie hauptberufliches Personal des Vereins sowie alle anderen Personen (z.B. reguläre Mitglieder und weitere Ehrenamtliche), die personenbezogene Daten, für die der Verein verantwortlich ist, verarbeiten oder nutzen, dazu verpflichtet, die entsprechenden Datenschutzbestimmungen für die Verarbeitungstätigkeit zu beachten und einzuhalten.

§ 3 Verantwortlichkeiten

(1) Der VEREIN ist – wie bereits oben erwähnt – für die Einhaltung der Regelungen zum Datenschutz nach der DSGVO und des BDSG verantwortlich. Diese Verantwortung für die Einhaltung des Datenschutzes wird über alle Funktionsebenen bis zum einzelnen Mitglied oder Mitarbeitenden für seinen Tätigkeits- und Verantwortungsbereich delegiert.

(2) Die Ziele des Datenschutzes des VEREINs werden durch folgende Feststellungen und Maßnahmen für den Alltag im Vereinsleben für Ehrenamt und Hauptamt konkretisiert.

§ 4 Nutzung der Daten

(1) Personenbezogene Daten dürfen nur für die satzungsgemäßen Zwecke des Vereins erhoben, verarbeitet und genutzt werden (laut Art. 6 Abs. 1 lit. b DSGVO für die Erfüllung des Mitgliedschafts- bzw. Teilnahmevertrags und Art. 6 Abs. 1 lit. f DSGVO zur Wahrung berechtigter Interessen des VEREINs).

(2) Die Verarbeitung von freiwillig zur Verfügung gestellten Daten, die nicht für die Zwecke der Satzungserfüllung nötig sind, z. B. Veröffentlichung von Fotos und Videos, ist eine Einwilligung nach Art. 6, Abs. 1 lit. a DSGVO einzuholen.

(3) Darüber hinaus dürfen Daten von Nichtmitgliedern (z.B. Handwerker und Lieferanten) gespeichert und verarbeitet und genutzt werden, wenn dies zur Wahrung der berechtigten Interessen der DLRG erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein überwiegendes schutzwürdiges Interesse am Ausschluss der Verarbeitung oder Nutzung hat (vgl. Art. 6, Abs. 1, lit f) DSGVO).

(4) Der Verein nutzt die Daten seiner Vereinsmitglieder nur für Aktivitäten im Rahmen der Vereinssatzung bzw. dieser Datenschutzordnung. Außerdem sind die Verarbeitungstätigkeiten personenbezogener Daten im Verzeichnis der Verarbeitungstätigkeiten festgehalten.

(5) Die Daten dürfen nur von Mitgliedern oder Mitarbeitern des Vereins genutzt werden, deren Tätigkeit einen Zugriff auf diese Daten notwendig macht. Der Zugriff auf die gespeicherten Daten ist nur in dem Umfang zulässig, den die jeweilige Tätigkeit erfordert.

§ 5 Erheben von Daten

(1) Mitgliederdaten

a) Für Zwecke der Mitgliederverwaltung werden bei Eintritt eines Mitglieds oder im Rahmen einer nachträglichen erforderlichen Ergänzung in der Regel folgende Daten erhoben:

- Nachname
- Vorname
- Geschlecht
- Geburtsdatum
- Familienstatus
- Adresse
- Telefonnummer, bei Minderjährigen eine Notfallrufnummer eines Sorgeberechtigten
- Emailadresse
- Eintritts- und Zugangsdatum
- Letzte DLRG-Gliederung
- Bankverbindung
- mindestens ein Erziehungsberechtigter (nur bei Minderjährigen)

Bei Eintritt wird das Mitglied auch Mitglied im DLRG Bundesverband, gemäß Satzung des Bundesverbandes und des Landesverbandes. In Sonderfällen kommt es zu einer Verantwortlichkeitsteilung bzgl. der personenbezogenen Daten, z.B. wenn ein Mitglied Funktionen ausübt oder beim Bundesverband aktiv wird durch Schulungen oder Rettungseinsätze.

Der Verein hat keinen unmittelbaren Zugriff auf die personenbezogenen Mitgliederdaten anderer Gliederungen bzw. setzt bei gegenseitigen Zugriffen immer eine Vertraulichkeitsverpflichtungserklärung der Zugreifenden voraus.

Alle weiteren Daten, die vom Verein im Rahmen der Aufnahme als Mitglied, der Anmeldung zu Veranstaltungen oder sonstigen Datenerhebungen erfolgen, sind in der Regel freiwillig. Hierauf wird bei Erhebung der Daten hingewiesen. Anmeldungen zu Veranstaltungen erfordern zwingend die Angabe und Zustimmung zur Verarbeitung dieser Daten im Rahmen der Veranstaltungsteilnahme, sonst ist die Teilnahme nicht möglich.

b) Es werden weitere Daten (z.B. Ausbildungsnachweise, Sportausweise, Ehrungen, Gremienzugehörigkeit) erhoben, wenn dies zur Mitgliederverwaltung und zur Tätigkeit des Mitglieds

im Verein erforderlich ist. Dieses können außerdem Daten zur Tauglichkeit und Gesundheit (sofern notwendig), sowie Einverständniserklärungen von Erziehungsberechtigten sein.

Weitere Daten im Verein umfassen auch die Unterstützung bei der Beantragung von Sonderurlaub beim Arbeitgeber für Vereinsmitglieder (nach § 42 HKJGB). Hier werden Daten zum Arbeitgeber und zum dortigen Ansprechpartner verarbeitet. Ebenso werden Daten zur Erstellung der Jugendleiter-Card (insbesondere Name, Ausbildung, Stundenleistung Erste Hilfe, Name der Gliederung und Foto) erfasst.

Im Fall von Einsatztätigkeiten des Mitglieds werden weitere Daten erhoben, soweit dieses für einen ordnungsgemäßen Einsatz des Mitglieds, sowie der Fürsorgepflicht der DLRG gegenüber dem Mitglied (Zweck der Gesundheitsvorsorge und Arbeitsmedizin) notwendig ist.

Insbesondere können diese sein:

- Ausbildung/Prüfungen
- Daten über den Gesundheitszustand (einschl. Vorerkrankungen, Allergien, Medikamente, Impfstatus)
- Tauglichkeit (ärztliche Bescheinigung) für eine bestimmte Tätigkeit
- Bekleidungsgrößen
- Name und Adresse, Telefon- bzw. Faxnummer des Arbeitgebers
- Name, Anschrift und Telefonnummern von nahen Angehörigen
- Führerschein

c) Gesundheits- und Tauglichkeitsdaten, wie ärztliche Bescheinigungen für Bootsführerscheine, Impf- und Tauglichkeitsnachweise. Diese werden aufgrund der Satzung des Vereins erhoben und unterliegen den Voraussetzungen des Art. 9 Abs. 2 DSGVO.

d) Videodaten und Bildmaterial, z. B. aus Schulungen oder Öffentlichkeitsarbeit, die auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO oder einer Einwilligung verarbeitet werden.

e) Social-Media-Daten, einschließlich Nutzernamen und Interaktionen, soweit für Verbandszwecke erforderlich.

(2) Daten bei Notfällen und Wasserrettung

a) Für Zwecke der Erstellung von Einsatzprotokollen, Transportbelegen und Abrechnungen sowie zur Dokumentation werden von den Betroffenen insbesondere folgende Daten erhoben:

- Nachname
- Vorname
- Geschlecht
- Geburtsdatum
- Adresse
- Krankenkasse bzw. Kostenträger
- Kassennummer
- Versichertennummer
- Name des Arbeitgebers
- Adresse des Arbeitgebers
- Einsatzdatum und Einsatzort
- Erstbefund/Messwerte/Verletzungen/Maßnahmen
- Name und Anschrift des Hausarztes
- Name und Telefonnummer von Angehörigen

b) Die Daten werden von den jeweiligen Einsatzkräften und ggf. vom zuständigen Verbandsarzt erhoben.

c) Vom Verein wird ein Nachweis geführt, in das der Vor- und Nachname sowie das Geburtsdatum des Betroffenen eingetragen werden.

(3) Datenerhebung bei Lehrgängen mit Tauglichkeitsbescheinigung

a) Für die Teilnahme an bestimmten Lehrgängen ist eine ärztliche Tauglichkeitsbescheinigung erforderlich. Die Bereitstellung der Tauglichkeitsbescheinigung ist erforderlich für die Teilnahme an dem betroffenen Lehrgang. Ohne Upload (oder eine gleichwertige, vom Verein zugelassene Nachweisform) ist eine Teilnahme nicht möglich.

b) Die Tauglichkeitsbescheinigung enthält in der Regel Name, Geburtsdatum, Eignungsfeststellung (geeignet/nicht geeignet), Ausstellungsdatum/Gültigkeit und Angaben zur ausstellenden Stelle (z. B. Praxis/Stempel/Unterschrift). Diagnosen oder detaillierte Befunde sind nicht erforderlich und sollen nicht hochgeladen werden.

c) Zweck der Verarbeitung ist die Prüfung der Teilnahmevoraussetzung, zur Organisation und Durchführung des Lehrgangs (Teilnehmerlisten, Zugangsberechtigungen, Dokumentation) sowie zur Sicherheit der Teilnehmenden.

d) Für die allgemeinen Verarbeitungen zur Lehrgangsorganisation ist die rechtliche Grundlage zur Datenverarbeitung Art. 6 Abs. 1 lit. b DSGVO (Vertrag/Teilnahme) und ergänzend Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an sicherer Durchführung). Für die Gesundheitsdaten in der Bescheinigung ist die rechtliche Grundlage die ausdrückliche Einwilligung der Teilnehmenden gemäß Art. 9 Abs. 2 lit. a DSGVO.

e) Die Einwilligung wird in manchen Fällen, in denen es ein zu unterzeichnendes Anmeldeformular gibt, gesondert eingeholt, protokolliert und ist jederzeit widerruflich (Widerruf wirkt für die Zukunft und kann die Teilnahmevoraussetzungen berühren). In den Fällen, in denen es kein solches Anmeldeformular gibt, geht der VEREIN bei Upload der Tauglichkeitsbescheinigung von einem konkludenten Verhalten zur Einwilligung zur Datenverarbeitung der Teilnehmenden bzgl. ihrer Gesundheitsdaten aus.

f) Die Daten werden ausschließlich innerhalb des Vereins verarbeitet. Die Verarbeitung erfolgt innerhalb der EU/des EWR. Sofern ausnahmsweise Drittländerzugriffe möglich sind, setzt der Verein EU-Standardvertragsklauseln und zusätzliche Schutzmaßnahmen ein.

g) Übermittlung und Speicherung erfolgen verschlüsselt; Zugriffe sind rollenbasiert und durch starke Authentifizierung geschützt. Es gilt das Prinzip der Datenminimierung (nur erforderliche Angaben).

(4) Erhebung von Daten Dritter

a) Der Verein erhebt Daten von anderen Personen als von Vereinsmitgliedern (insbesondere Referenten, Lieferanten, Gästen, Zuschauern, Besuchern, Teilnehmern an Veranstaltungen) soweit dies für berechtigte Interessen des Vereins notwendig ist und keine besonderen Schutzbedürfnisse der Betroffenen bestehen.

b) Bei Gästen, Zuschauern und Besuchern beschränkt sich dies im Regelfall auf die Legitimation der Anwesenheit, also Identifizierung als Angehöriger eines Vereinsmitglieds oder sonstiger Interessent. Bei Teilnehmern an Veranstaltungen, welche letztlich dem Versicherungsschutz des Vereins unterliegen, erhebt der Verein notwendige und freiwillige Daten analog dem in §2 Ziffer 1 beschriebenen Umfang und Verfahren.

c) Die Erhebung von Personaldaten der hauptberuflich Beschäftigten des Vereins gehört zu den Pflichten des Vereins.

d) Erhebung von Daten von Besuchern des Internetauftrittes des Vereins erfolgt über das s.g. Internet Service Center (ISC) des DLRG Bundesverbandes. Vom Verein werden in diesem

Zusammenhang personenbezogenen Daten erhoben, gespeichert und verarbeitet (insbesondere bei Anmeldung zu Lehrgängen). Beim Besuch des Internetauftritts kann außerdem das Surf-Verhalten statistisch ausgewertet werden. Die Analyse des Surf-Verhaltens erfolgt in der Regel anonym; das Surf-Verhalten kann nicht zurückverfolgt werden. Weitere Hinweise zur Erhebung von Daten über den Internetauftritt werden in der Datenschutzerklärung der Website des Vereins gegeben.

e) Der Verein nutzt außerdem diverse Plattformen aus dem Bereich Social Media, insb. Facebook. Hier gelten die Datenschutzbestimmungen des jeweiligen Betreibers. Außerdem existieren im Verein eigene Datenschutzerklärungen für die jeweiligen von ihm genutzten bzw. betriebenen Seiten dieser Plattformen, die auf den Seiten jeweils verlinkt sind.

f) Der Verein erhebt Daten von Spendern und Sponsoren (meist juristische Personen).

g) Der Verein erhebt und speichert Daten Dritter im Rahmen der Zusendung des Magazins „Lebensretter“ und der Publikationen des Landesverbandes. In diesem Zusammenhang ist keine separate Einwilligung erforderlich. Die Zusendung erfolgt auf Basis der Rechtsgrundlage des berechtigten Interesses des Vereins (Art. 6, Abs. 1, lit f) DSGVO).

h) Der Verein erhebt und speichert Daten Dritter im Rahmen der Zusendung des „Newsletters“. Die Verarbeitung der in das Newsletter-Anmeldeformular eingegebenen Daten erfolgt ausschließlich auf Grundlage der Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) des Newsletters-Abonnenten.

(5) Speicherung und Verarbeitung der Daten

(1) Die Daten werden analog und elektronisch gespeichert und verarbeitet. Zuständig für die Erhebung und Verarbeitung der Daten ist die Geschäftsstelle des Vereins, das Landesjugendbüro der DLRG-Jugend Rheinland-Pfalz, bzw. jeder andere, mit der Datenverarbeitung beauftragte Funktionsträger bzw. hauptberufliche Mitarbeiter des Landesverbands.

(2) Der Verein nimmt im Rahmen der Satzungserfüllung oder im Rahmen seines berechtigten Interesses Datenverarbeitung mit Software-Produkten vor. Für weitere Informationen verweist der Verein auf die jeweiligen Datenschutzerklärungen für solche Software-Produkte (z.B. für die Nutzung von Microsoft 365).

(3) Die Daten dürfen nur von Mitgliedern oder Mitarbeitern des Vereins genutzt werden, deren Tätigkeit einen Zugriff auf diese Daten notwendig macht. Der Zugriff auf die gespeicherten Daten ist nur in dem Umfang zulässig, den die jeweilige Tätigkeit erfordert.

§ 6 Verpflichtung auf das Datengeheimnis

(1) Die mit der Erfassung, Verarbeitung und Nutzung von personenbezogenen Daten beauftragen Funktionsträger (Vorstand, ehrenamtliche Mitarbeiter) sowie hauptamtliche Mitarbeiter werden schriftlich auf die Wahrung des Datengeheimnisses verpflichtet.

(2) Diese Verpflichtung wird dokumentiert und revisionssicher aufbewahrt.

§ 7 Auftragsverarbeitungen

(1) Eine Auftragsverarbeitung liegt in der Regel dann vor, wenn der Verein und seine Gliederungen mit Firmen zusammenarbeitet und zwischen den Beteiligten ein Datenaustausch stattfindet (Beispiel: Druckerei mit Weitergabe von Adressdaten).

(2) Zur Durchführung der Vereinbarten Arbeiten werden Daten von Gliederungen des VEREINs an den Auftragnehmer übermittelt. Die Grundlage für diesen Datenaustausch bilden ein Leistungsvertrag und ein Vertrag zur Auftragsverarbeitung (AV). Ein AV-Vertrag (AVV) ist immer dann abzuschließen, wenn personenbezogene Daten an Drittfirmen weitergegeben

werden, diese für diesen Arbeitsauftrag notwendig sind, der Verein weisungsbefugt bleibt und die Daten vom Dienstleister (Firma) nicht zu eigenen Geschäftszwecken weiterverwendet werden.

(3) Diese Firma ist im datenschutzrechtlichen Sinne nicht Dritter, sondern Teil der verantwortlichen Stelle. Neue Firmen, mit denen noch kein AVV geschlossen wurde, dürfen personenbezogene Daten im Auftrag des Vereins erst verarbeiten, wenn ein AV-Vertrag besteht. Diesen kann man in der Regel beim Dienstleister erfragen bzw. ein Muster beim Datenschutzbeauftragten des Vereins erhalten.

(4) Es gibt einige Ausnahmen, bei denen ein Datenaustausch nicht eines AVV bedarf:

- Postdienste für den Brieftransport, dazu gehören auch Kurierdienste
- Inkassobüros, die das Mahnwesen betreiben
- Rechtsanwälte, Steuerberater, Betriebsärzte
- Bankinstitute für den Geldtransfer
- Hotels

§ 8 Weitergabe von Daten

(1) An andere DLRG-Funktionsträger, hauptberufliche Mitarbeiter und Teilnehmer von Veranstaltungen dürfen personenbezogene Daten im Einzelfall weitergegeben werden, wenn das auskunftsersuchende Mitglied ein berechtigtes Interesse glaubhaft macht und kein Grund zu der Annahme besteht, dass der Betroffene ein überwiegendes schutzwürdiges Interesse am Ausschluss der Verarbeitung oder Nutzung seiner Daten hat (vgl. Art. 6 Abs. 1, lit f) DSGVO).

(2) Eine Veröffentlichung oder Weitergabe von personenbezogenen Daten in Einzelfällen oder durch die Weiterleitung von Daten an Dritte, insbesondere an Wirtschaftsunternehmen oder Medienvertreter ist nur zulässig, wenn eine Einwilligung des oder der betroffenen Vereinsmitglieder vorliegt (Art. 4 Nr. 9 Satz 1 DSGVO)

(3) Personenbezogene Daten können darüber hinaus für weitere satzungsmäßige Zwecke an Bezirke/ Kreisverbände, andere Landesverbände, die DLRG-Bundesgeschäftsstelle oder an andere DLRG-Gliederungen oder Krankenkassen und Versicherungen übermittelt werden.

(4) Pressemitteilungen und Auskünfte gehören zur normalen Öffentlichkeitsarbeit eines Vereins. Personenbezogene Daten werden in diesem Rahmen nur dann veröffentlicht, wenn es sich um einen Bericht über eine sowieso öffentliche Veranstaltung handelt und schutzwürdige Interesse der Mitglieder dem nicht entgegenstehen.

(5) Verlangen Behörden und Zuwendungsgeber im Rahmen der Nachweisführung der ordnungsgemäßen Verwendung von Zuwendungen die Vorlage von Listen mit personenbezogenen Daten der Betroffenen, ist der Verein zur Übermittlung entsprechender notwendiger Daten berechtigt.

(6) Gegenüber Arbeitgebern verweist der Verein auf den Grundsatz der Datendirekterhebung bei seinem Mitarbeiter. Anfragen einer Versicherung werden ausschließlich im Rahmen der Schadensabwicklung in notwendigem Umfang beantwortet. Hierbei beruft sich der Verein auf die Weitergabe der Daten nach berechtigtem Interesse (vgl. Art. 6, Abs. 1 lit. f) DSGVO).

§ 9 Sperrung und Löschung von Daten

(1) Um eine weitere Verarbeitung oder Nutzung einzuschränken oder unmöglich zu machen, sind die erhobenen Daten nach bestimmten Voraussetzungen zu sperren oder zu löschen. Die Löschung von Daten findet durch – je nach Software-Funktionalitäten – geeignete Kennzeichnung bzw. Löschung statt.

(2) Personenbezogene Daten dürfen nur so lange gespeichert werden, wie dies der Vereinszweck laut Satzung erfordert. Nach Wegfall der Zweckbestimmung (z.B. Austritt, Ausschluss oder Tod eines Mitglieds) sind die Daten zu sperren und nach Wegfall der Voraussetzungen nach §35 (3) BDSG zu löschen. Konkret sind die folgenden Daten nach den Fristen im Anhang dieser Datenschutzordnung zu löschen. Ausgenommen sind Daten, die im Rahmen der Vereinshistorie aufbewahrt werden.

(3) Sofern vom Verein erhobene und gespeicherte personenbezogene Daten nachweislich unrichtig sind, hat der Betroffene einen Anspruch auf Berichtigung. Darüber hinaus sind personenbezogene Daten zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit, noch die Unrichtigkeit feststellen lässt.

(4) Der Verein stellt sicher, dass die zu löschenden Daten – z.B. durch mehrfaches Überschreiben, den Einsatz entsprechender Computerprogramme, oder durch Zerstörung der Datenträger – unumkehrbar unlesbar gemacht werden. Schriftliche Unterlagen sind durch geeignete Geräte zu vernichten.

(5) Ist eine Löschung der personenbezogenen Daten wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich, reicht eine dauerhafte Sperrung der Daten aus. Das Gleiche gilt, wenn Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(6) Der Vorstand wird ermächtigt, Änderungen und Ergänzungen zu Löschfristen per Vorstandsbeschluss zu beschließen.

§ 10 Technische und Organisatorische Maßnahmen (TOM) & Sicherheitsvorkehrungen

(1) Durch geeignete Maßnahmen wird sichergestellt, dass nur berechtigte Mitglieder, die mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten beauftragt sind, Zugang zu den Rechnern des Vereins haben, die der Verein zur Speicherung und Verarbeitung personenbezogener Daten nutzt. Die Geschäftsräume sind bei Abwesenheit der Berechtigten abzuschließen. Unberechtigten Personen ist der Zugang zu diesen Rechnern zu verweigern.

Der Verein hat die notwendigen Sicherheitsvorkehrungen durch vertragliche Verpflichtung seiner Dienstleister (z.B. IT, Druckerei etc.) und durch weitere technische und organisatorische Maßnahmen sicherzustellen und diese sorgfältig auszuwählen (nach Art. 28, Abs. 1 DSGVO). Diese Maßnahmen können auf Anfrage beim Verein eingesehen werden.

(2) Soweit personenbezogene Daten zentral gespeichert und verarbeitet werden, sind die Sicherheitsvorkehrungen durch vertragliche Verpflichtung des Auftragnehmers vorzunehmen. Die Datenverarbeitung soll dabei in einem den IT-Sicherheitsstandards entsprechenden, nach Möglichkeit ISO 27001 zertifizierten, Rechenzentrum erfolgen.

(3) Der Verein hat für seine ehrenamtlichen Funktionsträger und hauptamtlichen Mitarbeiter jeweils konkrete Regelungen mit technischen und organisatorischen Maßnahmen für den Vereinsalltag erlassen. Diese Regelungen enthalten unter anderem Sicherheitsvorkehrungen im Umgang mit E-Mails und Messengern. Diese sind ebenso zu beachten wie die Verpflichtungen auf das Datengeheimnis. Diese Regelungen gelten im Speziellen, sofern Mitglieder personenbezogene Daten auf ihren privaten Endgeräten (einschließlich Laptops, Notebooks, Handys und Tablets) speichern und nutzen. Dies ist grundsätzlich nur für satzungsmäßige Zwecke und nur zur Ausübung der konkreten Funktion unter Beachtung der vorliegenden Datenschutzordnung zulässig.

(4) Die Nutzung von Cloud-Diensten (z. B. Microsoft 365/SharePoint) ist zulässig, wenn die Datensicherheit und der Datenschutz vertraglich und technisch sichergestellt sind. Hierzu schließt der Verein mit dem Anbieter einen Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO ab. Sofern personenbezogene Daten in Drittländer übermittelt werden oder ein Zugriff aus Drittländern möglich ist, sind geeignete Garantien zu Vereinbaren, in der Regel die

EU-Standardvertragsklauseln einschließlich einer dokumentierten Transferfolgenabschätzung. Rechenzentrumsstandorte innerhalb der EU/des EWR sind vorrangig zu wählen.

(5) Für alle Cloud-Dienste gilt das Prinzip „need-to-know". Der Verein setzt ein Rollen- und Berechtigungskonzept um, nach dem nur diejenigen Personen Zugriff erhalten, die diesen für ihre konkrete Aufgabe benötigen. Freigaben werden sparsam erteilt, regelmäßig überprüft und – soweit möglich – befristet. Daten werden während der Übertragung und im Ruhezustand verschlüsselt gespeichert. Öffentliche oder anonyme Freigabelinks sind zu vermeiden; externe Teilungen erfolgen nur, wenn sie für Vereinszwecke erforderlich und freigegeben sind.

(6) Endgeräte, mit denen auf Vereinsdaten in der Cloud zugegriffen wird, sind durch aktuelle Sicherheitsupdates, ein sicheres Sperrkonzept und eine starke Authentifizierung zu schützen. Der Zugriff auf Cloud-Konten erfolgt grundsätzlich mit Mehrfaktor-Authentifizierung und starken Passwörtern/Passphrasen. Wo verfügbar, ist die vollständige Festplattenverschlüsselung zu aktivieren. Der Einsatz privater Endgeräte ist nur unter Beachtung dieser Anforderungen und der vorliegenden Datenschutzordnung zulässig.

§ 11 Social Media

(1) Mitglieder, die ihre Vereinszugehörigkeit nennen, bewegen sich zwischen Privat- und Vereinsrolle. Wer nicht beauftragt ist, handelt privat und entscheidet selbst über diese Angabe. In jedem Fall sind die Privatsphäre-Einstellungen passend zu wählen.

(2) Jede Veröffentlichung liegt in der Verantwortung der/des Beitragenden. Das Internet vergisst nicht; Inhalte lassen sich meist nicht vollständig entfernen. Vor dem Posten sollten die Beiträge noch einmal geprüft werden und bei Unsicherheiten lieber eine zweite Person gegenlesen lassen.

(3) Soziale Netzwerke sind (faktisch) öffentlich. Auch geschützte Inhalte können weitergeleitet werden; eine Kontrolle über die weitere Nutzung ist kaum möglich.

(4) Vereinsinterne oder vertrauliche Angaben – insbesondere Daten von Kindern, Erziehungsberechtigten, Spenderinnen/Spendern – dürfen nicht veröffentlicht werden.

(5) Bild- und Tonaufnahmen von Kindern und Jugendlichen werden nur mit vorheriger Einwilligung der Erziehungsberechtigten veröffentlicht. Widerrufe sind zu beachten; betroffene Inhalte sind dann zu entfernen.

(6) Die Kommunikation sollte freundlich, sachlich und authentisch sein. Beleidigungen, Diskriminierungen und abwertende Kommentare, z. B. wegen Geschlecht, Religion oder Herkunft, sind tabu.

(7) Partei-politische Meinungsäußerungen sind nicht mit dem Engagement im Verein zu verknüpfen.

(8) Urheber-, Marken- und Persönlichkeitsrechte sind zu achten: nur eigenes oder korrekt lizenziertes Material verwenden; Zitate kennzeichnen und Einwilligungen einholen, wo es erforderlich ist.

(9) Nur beauftragte Personen veröffentlichen im Namen des VEREINs. Kommentare und Beiträge müssen Persönlichkeitsrechte achten; Verstöße werden entfernt und entsprechend dokumentiert.

§ 12 Foto- und Videoaufnahmen

(1) Wenn es sich um Aufnahmen größerer Menschenansammlungen handelt, sind Foto- und Videoaufnahmen unproblematisch. Laut Kunsturhebergesetz gilt dies für Versammlungen, Aufzüge und ähnliche Vorgänge. Also auch für Demonstrationen, Veranstaltungen, Streikversammlungen.

(2) Wenn die Fotos oder Videos weniger als ca. 10 Menschen darstellen und sie nicht nur "Beiwerk" zu anderen Hauptmotiven sind, bedarf es der Einwilligung der aufgenommenen Personen nach Art. 6, Abs. 1, lit. a) DSGVO. Hier sind folgende Punkte zu beachten:

a) Eine Vorlage zur Einwilligungserklärung ist beim Verein zu erfragen.
b) Die Unterzeichnung einer entsprechenden Einwilligungserklärung ist stets freiwillig.
c) Die Einwilligung kann jederzeit ohne Angabe von Gründen und für die Zukunft widerrufen werden.
d) Die Einwilligungserklärungen werden beim Verein verschlusssicher aufbewahrt.

§ 13 Betroffenenrechte

(1) Jeder Betroffene (Mitglieder oder Dritte) hat das Recht, Auskunft über die zu seiner Person gespeicherten Daten, deren Herkunft, den Empfänger oder die Kategorien von Empfängern, an die die Daten weitergegeben werden und Zweck der Speicherung zu verlangen (Art. 15 DSGVO).

(2) Das Ersuchen ist schriftlich oder in Textform an den Vorstand des Vereins oder der Untergliederung mit eigener Rechtspersönlichkeit zu richten, wobei die Art der personenbezogenen Daten über die Auskunft begehrt wird, näher bezeichnet werden soll.

(3) Jeder Betroffene hat das Recht, seine erteilte Einwilligung zur Verarbeitung seiner personenbezogenen Daten jederzeit gegenüber dem Verein oder seiner Gliederungen zu widerrufen. Für Mitglieder hat dies zur Folge, dass sie ihre Mitgliedschaft in der DLRG kündigen.

(4) Jeder Betroffene hat das Recht, gemäß Art. 16 DSGVO die unverzügliche Berichtigung unrichtiger oder Vervollständigung seiner gespeicherten Daten zu verlangen.

(5) Jeder Betroffene hat das Recht, gemäß Art. 17 DSGVO die Löschung seiner gespeicherten Daten zu verlangen, soweit nicht die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information, zur Erfüllung einer rechtlichen Verpflichtung, aus Gründen des öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

(6) Jeder Betroffene hat das Recht, gemäß Art 18 DSGVO die Einschränkung der Verarbeitung seiner personenbezogenen Daten zu verlangen, soweit die Richtigkeit der Daten von ihm bestritten wird, die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt; der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, der Betroffene sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder die betroffene Person Widerspruch gegen die Verarbeitung gemäß Artikel 21 Absatz 1 DSGVO eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

(7) Jeder Betroffene hat das Recht, gemäß Art. 20 DSGVO seine personenbezogenen Daten, die er dem Verein bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesebaren Format zu erhalten oder die Übermittlung an einen anderen Verantwortlichen zu verlangen.

(8) Jeder Betroffenen hat gemäß Art. 21 DSGVO das Recht Widerspruch gegen die Verarbeitung seiner personenbezogenen Daten einzulegen, wenn die Verarbeitung auf Grundlage von berechtigtem Interesse gemäß Art. 6 Abs 1 lit. f) erfolgt, soweit für den Widerspruch Gründe vorliegen, die sich aus der besonderen persönlichen Situation der betroffenen Person ergeben. Der Widerspruch ist gegenüber dem Verein geltend zu machen, eine E-Mail an datenschutz@rlp.dlrg.de ist dazu ausreichend.

(9) Jeder Betroffenen hat gemäß Art. 77 DSGVO das Recht, sich bei einer Aufsichtsbehörde zu beschweren.

§ 14 Datenschutzbeauftragter

(1) Zur Gewährleistung des Datenschutzes wird im Verein nach § 38 BDSG ein Datenschutzbeauftragter bestellt. Dieser ist dem Landesverbandspräsidenten unmittelbar unterstellt und in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei.

(2) Er hat uneingeschränkten Zugang zu den erhobenen Daten und ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

(3) Jedes Mitglied hat das Recht sich jederzeit mit Fragen und Anträgen an die Geschäftsstelle des Vereins zu wenden. Hier werden die Anfragen entsprechend koordiniert und ggf. dem Datenschutzbeauftragten zugeleitet. Die Koordinationsstelle zu Datenschutzfragen wird Auskunft über die wesentlichen Bestimmungen der DSGVO und des BDSG erteilen.

(4) Der Datenschutzbeauftragte des Vereins ist zu erreichen unter: DLRG Landesverband Rheinland-Pfalz e.V., Bergstraße 18, 56332 Lehmen, E-Mail: datenschutz@rlp.dlrg.de

§ 15 Datenpannen

(1) Wenn personenbezogene Daten offengelegt werden, Dritte unerlaubten Zugriff auf diese haben oder gespeicherte Daten dauerhaft verloren gehen, liegt eine Datenpanne vor.

(2) Mitglieder sind angehalten, schnellstmöglich Information an den Datenschutzbeauftragten zu geben, der sich dann an die an das zuständige Datenschutzkoordinationsteam des Vereins wendet und eine evtl. Weitermeldung der Datenpanne an die zuständige Aufsichtsbehörde diskutiert.

(3) Da Fristen (in der Regel 72 Stunden bis zu einer evtl. Weitermeldung an die Aufsichtsbehörde) eingehalten werden müssen, ist eine umgehende Meldung essenziell.

§ 16 Weitere Regelungen

(1) Der Vorstand wird ermächtigt, weitere Regelungen und Verfahrensanweisungen zur Ergänzung diese Datenschutzordnung durch Vorstandsbeschluss in Kraft zu setzen.

(2) Diese Einzelregelungen und Verfahrensanweisungen sind den Gliederungen bekannt zu geben.

Anhang: Liste Löschfristen für DLRG-Unterlagen

Name der Unterlagen	Aufbewahrungsfrist	Bemerkungen
EH Teilnehmerliste ohne Rechnungsbezug	5 Jahre	Gemäß DGUV G 304-001 Ziffer 2.4.6
EH Teilnehmerliste mit Rechnungsbezug	10 Jahre	
SAN Teilnehmerliste	10 Jahre	
Tauglichkeits- und Gesundheitsdaten	spätestens sechs Monate nach Beendigung des Lehrgangs oder der Tätigkeit	
Liste bzw. Prüfungskarten TN Schwimmausbildung	10 Jahre	Gemäß PO S/RS
Liste bzw. Prüfungskarten Rettungsschwimmausbildung	10 Jahre	Gemäß PO S/RS
Bootstagebuch / Funktagebuch	10 Jahre	lt. Referatsleitung Bootswesen
Fahrtenbuch	10 Jahre	lt. Referatsleitung Bootswesen
Teilnehmerlisten Kurse Bootswesen	10 Jahre	lt. Referatsleitung Bootswesen
Liste bzw. Prüfungskarten Bootsführerausbildung	10 Jahre	lt. Referatsleitung Bootswesen
Einsatztagebuch/ Einsatzdokumentation für die Krankenkasse	10 Jahre	
Wachtagebuch / Wachberichte	5 Jahre	
Mitgliederverwaltung (nach Austritt oder bei Todesfall)	2 Jahre	**Sperren** bei Austritt, löschen nach spätestens 2 Jahren, **Löschen** im Todesfall
Abrechnung KatS-Einsätze	10 Jahre	
Einsatzprotokolle für Standard-WRD-Einsätze	5 Jahre	
Einsatzdaten aus Wasserrettungs- und Notfalleinsätzen	10 Jahre	
Teilnehmerlisten mit Rechnungsbezug	10 Jahre	
Sonstiger Schriftverkehr ohne Rechnungsbezug	5 Jahre	
Schriftverkehr mit Dauerverpflichtung:	unbegrenzt, solange gültig	
Funktagebuch	1 Jahr	
Verpflichtungserklärungen	unbegrenzt	z.B. Verschwiegenheitspflicht gilt auch nach Austritt
ATN	wie Mitgliederverwaltung	