Datenschutzkonzept

DLRG Kreisverband Ingolstadt e.V.

Stand: 06/2025

Vorwort

Hinweis zur Datenschutzgrundverordnung des DLRG Kreisverband Ingolstadt e.V.

Information zur Datenverarbeitung gemäß EU-Datenschutzgrundverordnung (DS-GVO)

Sehr geehrte Mitglieder und Freunde unseres DLRG Kreisverbandes Ingolstadt e.V.

Mit der Überarbeitung und Anpassung der vorherigen Version unserer EU-Datenschutzgrundverordnung (DS-GVO) aus dem Jahr 2018 möchten wir Sie über die aktuelle Verwendung Ihrer personenbezogenen Daten im DLRG Kreisverband Ingolstadt e.V. informieren:

Mit Ihrer Unterschrift auf dem Mitgliedsantrag haben Sie zugestimmt, dass der DLRG Kreisverband Ingolstadt e.V. personenbezogene Daten erfasst und verarbeitet. Dies beinhaltet insbesondere die Erhebung, Speicherung, Veränderung, Nutzung, Übermittlung, Einschränkung, Löschung und Vernichtung dieser Daten.

Die Grundlage für den Umgang mit personenbezogenen Daten bildet unsere Datenschutzordnung, die sich an den Vorgaben der DS-GVO sowie des Bundesdatenschutzgesetzes (BDSG) orientiert. Sie regelt den Schutz und die Verarbeitung von Informationen, die sich auf identifizierte oder identifizierbare natürliche Personen beziehen – insbesondere Vereinsmitglieder.

Zu den geschützten Daten zählen nicht nur die Daten unserer Mitglieder, sondern auch personenbezogene Informationen von Personen, die in einem vertraglichen oder sonstigen rechtlichen Verhältnis zum Verein stehen.

Die Verarbeitung der Daten erfolgt ausschließlich für vereinsinterne Zwecke.

Bitte informieren Sie den Vorstand des DLRG Kreisverbandes Ingolstadt e.V. unverzüglich über Änderungen Ihrer personenbezogenen Daten, damit wir Ihre Daten stets auf dem aktuellen Stand halten können.

Der DLRG Kreisverband Ingolstadt ist Teil der DLRG Landesverband Bayern e.V. Die für unseren Kreisverband verbindliche Datenschutzerklärung basiert auf der Datenschutzordnung des Landesverbandes und kann jederzeit auf unserer Website eingesehen werden:

👉 https://ingolstadt.dlrg.de

In der Datenschutzordnung finden Sie detaillierte Informationen darüber, welche Daten zu welchen Zwecken verarbeitet werden.

Inhaltsverzeichnis

Vorwort 2

I Grundlagen und Aufbau 4

1. Regelungsbereich 4
2. Zielrichtung 4
3. Zuständig- und Verantwortlichkeiten 5

II. Sicherheitskonzept für die allgemeine Datenverarbeitung 6

1. Schulung und Verpflichtung der Mitarbeitenden 6
2. Aktenführung und Aktenaufbewahrung 6
3. Archivierung und Aufbewahrungsfristen 6
4. Auskünfte und Datenübermittlung 7

III. Sicherheitskonzept für die automatisierte Datenverarbeitung 7

1. EDV-Zugriff 7
2. EDV-Nutzung durch Mitarbeitende 7
3. Passwortrichtlinien 7
4. Externe Dienstleister 7
5. Hardware- und Softwareverwaltung 8
6. Dienstlich bereitgestellte Geräte 8
7. Mobile Endgeräte 8
8. Datenverwaltung 8
9. Datensicherung 8
10. Verfahren (Verzeichnis der Verarbeitungstätigkeiten) 9

IV. Datenschutzrichtlinien 10

1. Verarbeitung personenbezogener Daten 10
2. Verpflichtung auf das Datengeheimnis 10
3. Weitergabe von Daten 10
4. Einschränkung und Löschung von Daten 11
5. Sicherheitsvorkehrungen 11
6. Auskunftsrecht 11
7. Recht auf Datenübertragbarkeit 12
8. Datenschutzbeauftragter und Beschwerderecht 12

V. Anhang 13

Anhang A: Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 EU-DSGVO 13
Anhang B: Aufbewahrungsfristen und Löschkonzept gemäß Art. 17 DSGVO 18
Anhang C: Verpflichtungserklärung Vorstand 19
Anhang D: Verpflichtungserklärung Übungsleiter und Referatsleiter 20
Merkblatt zur Verpflichtungserklärung 21
Anhang E: Dokumentation der eingesetzten IT-Systeme 23
Anhang F: Vertrag über Auftragsverarbeitung mit Anlage TOMs 24

I. Grundlagen und Aufbau

1. Regelungsbereich

Die Datenschutzordnung regelt auf Grundlage der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) den Umgang mit Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person – insbesondere Mitglieder der dem DLRG Landesverband Bayern e.V. angehörenden DLRG Orts-,Kreis- und Bezirksverbände e.V.– beziehen (personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO).

Erfasst werden u.a. die Erhebung, Speicherung, Veränderung, Verwendung, Übermittlung, Einschränkung, Löschung und Vernichtung von personenbezogenen Daten. Zu den geschützten Daten gehören neben den personenbezogenen Daten der Mitglieder der DLRG e.V. auch Daten von Personen, die zum DLRG Landesverband Bayern e.V. in einem vertraglichen oder sonstigen rechtlichen Verhältnis stehen (z.B. Kursteilnehmer, Lieferanten, Sponsoren, etc.).

2. Zielrichtung

Der DLRG Kreisverband Ingolstadt e.V. orientiert sich bei der Verarbeitung personenbezogener Daten an einem umfassenden Datenschutzkonzept. Ziel ist es, ein hohes Maß an Datensicherheit zu gewährleisten. Dabei stehen insbesondere folgende Schutzziele im Vordergrund:

- **Integrität**: Schutz vor unbeabsichtigter oder vorsätzlicher Veränderung von Programmen oder Daten,
- **Vertraulichkeit**: Schutz vor unbefugtem Zugriff oder Kenntnisnahme durch Dritte,
- **Verfügbarkeit**: Sicherstellung, dass Daten und Systeme vor Verlust, Diebstahl oder Zerstörung geschützt sind.

Das Datenschutzkonzept unterteilt die erforderlichen Sicherheitsmaßnahmen in folgende Bereiche:

- Allgemeine Datenverarbeitung
- Automatisierte Datenverarbeitung
- Nutzung von Internetdiensten
- Nutzung von Telekommunikationsdiensten
- Zusätzliche Maßnahmen zum Schutz sensibler personenbezogener Daten

Diese Struktur gewährleistet ein systematisches und hohes Sicherheitsniveau in allen relevanten Bereichen der Datenverarbeitung.

Grundlage für die Festlegung und Weiterentwicklung dieser Sicherheitsmaßnahmen bildet eine regelmäßig durchzuführende Bestandsaufnahme zur aktuellen Datensicherheitssituation. Diese umfasst unter anderem Arbeitsplatzanalysen, Risikoanalysen und die Bewertung der technischen und organisatorischen Maßnahmen (TOMs) in ihrer jeweils aktuellen Fassung. Ergänzend fließen die Dokumentationen zur Zusammensetzung der eingesetzten IT-Systeme in die Bewertung ein (siehe Anhang E).

3. Zuständig- und Verantwortlichkeiten

Die Verantwortung für die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung liegt beim Vorstand des DLRG Kreisverbands Ingolstadt e.V. als Vertreter der verantwortlichen Stelle. Diese ist insbesondere zuständig für den Erlass verbindlicher Dienstanweisungen sowie interner Regelungen zum Datenschutz und zur Datensicherheit – sowohl im konventionellen als auch im technischen Bereich.

Die operative Verantwortung für die Einhaltung der geltenden Datenschutz- und Datensicherheitsvorschriften tragen die Geschäftsführung sowie die Leitungen der datenverarbeitenden Fachbereiche, insbesondere:

- Schatzmeisterei / Mitgliederverwaltung
- Ausbildung Schwimmen und Rettungsschwimmen
- Wettkämpfe
- Ausbildung Erste Hilfe

Um Unklarheiten, Zuständigkeitslücken oder widersprüchliche Regelungen zu vermeiden, sind alle Datenschutzregelungen regelmäßig zu überprüfen und bei Bedarf zu aktualisieren. Jede Fassung sollte ein eindeutiges Erstellungsdatum enthalten.

1. **Überwachung:**

   Die Überprüfung und Überwachung der im Datenschutzkonzept definierten Sicherheitsmaßnahmen obliegt der verantwortlichen Stelle. Die zuständigen Vorstandsmitglieder mit Datenschutzverantwortung sind hierbei einzubeziehen. Alle Überprüfungsergebnisse sind gemäß den gesetzlichen Dokumentationspflichten schriftlich festzuhalten.

2. **Fortschreibung:**

   Das Datenschutzkonzept wird regelmäßig im Rahmen der technisch-organisatorischen Maßnahmen gemäß Art. 24 ff. EU-DSGVO fortgeschrieben. Dabei ist zu bewerten, ob die bestehenden Maßnahmen weiterhin geeignet, wirksam und zweckmäßig sind.

3. **Inkrafttreten:**

Dieses Datenschutzkonzept tritt am 01.07.2025 in Kraft und ersetzt alle bisherigen Versionen.

Ingolstadt, den 28.06.2025

Unterschriften:

Dr. Christian Fuchs, 1. Vorsitzender

Katharina von Kap-herr, stv. Vorsitzende

II. Sicherheitskonzept für die allgemeine Datenverarbeitung

1. Schulung und Verpflichtung der Mitarbeitenden

Alle Mitarbeitenden des DLRG Kreisverbands Ingolstadt e.V. sind über die geltenden datenschutzrechtlichen Bestimmungen zu informieren und regelmäßig zu schulen. Die Teilnahme an diesen Schulungen ist durch eine unterschriebene Verpflichtungserklärung zu dokumentieren. Diese wird physisch im Ordner *„Datenschutz“* und digital im Ordner „Datenschutz“ in der DLRG-Cloud des Kreisverbands Ingolstadt e.V. abgelegt und dient als Nachweis der Unterrichtung.

Die Schulungen sind spätestens alle zwei Jahre zu wiederholen. Neue Mitarbeitende sind zeitnah nach Aufnahme ihrer Tätigkeit zu schulen. Für bereits geschulte Mitarbeitende sind regelmäßige Auffrischungen vorzusehen, um das Bewusstsein für Datenschutz und Datensicherheit dauerhaft zu gewährleisten.

2. Aktenführung und Aktenaufbewahrung

Daten, die mithilfe von Standard- oder Fachsoftware verarbeitet werden, dürfen nur dann ausgedruckt und in Papierakten übernommen werden, wenn dies gesetzlich vorgeschrieben ist oder zur ordnungsgemäßen Aufgabenerfüllung erforderlich erscheint.

Papierakten mit personenbezogenen Daten sind so aufzubewahren, dass kein unbefugter Zugriff erfolgen kann. Sie sind grundsätzlich in abschließbaren Schränken oder anderen geeigneten Aufbewahrungseinrichtungen zu verwahren – auch während laufender Bearbeitung (Clear-Desk-Regelung).

Papierabfälle, die personenbezogene Informationen enthalten, sind datenschutzkonform durch einen Aktenvernichter zu entsorgen.

3. Archivierung und Aufbewahrungsfristen

Die Archivierung erfolgt bereichsbezogen. Besonders schutzwürdige Daten – wie z. B. Personal- und Gesundheitsdaten – sind besonders gesichert aufzubewahren und vor unbefugtem Zugriff zu schützen.

Sind solche Unterlagen zur Erfüllung der Aufgaben nicht mehr erforderlich und stehen keine Aufbewahrungsfristen entgegen, sind sie unverzüglich und datenschutzkonform zu vernichten – unabhängig davon, ob sie elektronisch oder in Papierform vorliegen. Die Vernichtung muss so erfolgen, dass ein Zugriff Dritter ausgeschlossen ist (z. B. durch Schreddern).

Soweit keine gesetzlichen Vorgaben bestehen, orientiert sich die Aufbewahrungsdauer an den jeweils aktuellen Empfehlungen des Fachverbands (z. B. KGSt).

Die Einhaltung und Überwachung der Aufbewahrungsfristen obliegt den zuständigen Ressortleitungen und wird vom Vorstand überwacht.

4. Auskünfte und Datenübermittlung

Vor jeder Auskunftserteilung oder Datenweitergabe ist die Identität der anfragenden Person zweifelsfrei zu prüfen.

Die Fachbereichsleitungen sind für die Entscheidung über die Notwendigkeit der Datenweitergabe verantwortlich und legen verbindliche Verfahrensregelungen für die Auskunftserteilung fest. Dabei sind stets die datenschutzrechtlichen Anforderungen zu berücksichtigen.

III. Sicherheitskonzept für die automatisierte Datenverarbeitung (Technisch Organisatorische Maßnahmen - TOMs)

1. EDV-Zugriff

Der Zugriff auf verschlüsselte Datenbestände darf ausschließlich durch autorisierte Mitarbeitende des zuständigen Fachbereichs erfolgen. Gleiches gilt für die Verwaltung und Einsicht in Benutzerprofile.

2. EDV-Nutzung durch Mitarbeitende

Alle Nutzerinnen und Nutzer von EDV-Systemen (PCs, Laptops, Tablets, Smartphones) sind vor Aufnahme ihrer Tätigkeit in den datenschutzkonformen Umgang mit der Technik einzuweisen. Dies umfasst auch die ordnungsgemäße Nutzung dienstlich bereitgestellter sowie privat genutzter Hardware und Software.

Zudem ist über die vorhandene Speicherinfrastruktur zu informieren.

3. Passwortrichtlinien

Jede Benutzerin und jeder Benutzer hat eine persönliche Zugangskennung mit einem mindestens achtstelligen Passwort zu verwenden. Die Systemanforderungen regeln die genauen Passwortvorgaben.

Beim Verlassen des Arbeitsplatzes ist die Bildschirm-Sperre zu aktivieren, beispielsweise durch **Windows-Taste + L**. Nach spätestens 10 Minuten Inaktivität aktiviert sich die Sperre automatisch.

4. Externe Dienstleister

Der Einsatz externer Dienstleister muss auf Basis eines schriftlichen Vertrags geregelt werden. Dabei sind die Vorgaben der EU-DSGVO zur Auftragsverarbeitung zu beachten. Der Leistungsumfang sowie die Aufgaben sind detailliert zu beschreiben.

5. Hardware und Softwareverwaltung

Dienstlich genutzte Geräte können durch die DLRG Kreisverband Ingolstadt e.V. beschafft und inventarisiert werden. Auch private Geräte, die für dienstliche Zwecke verwendet werden, sind dem Kreisverband zu melden und in das Geräteverzeichnis aufzunehmen (siehe auch Anhang E: Geräteverzeichnis).

Das Geräteverzeichnis enthält u. a.:

- Aufstellungsort
- Gerätetyp und -art
- Seriennummer
- ggf. ergänzende Informationen

Alle Veränderungen (z. B. Austausch, Reparatur, Verschrottung) sind im Verzeichnis zu dokumentieren. Die Konfigurationsdaten (z. B. IP-Adressen) sind vor unbefugtem Zugriff zu schützen. Es ist grundsätzlich lizenzierte Standardsoftware mit aktuellen Sicherheitsupdates zu verwenden.

6. Dienstlich bereitgestellte Geräte

Das Ressort IT/EDV ist verantwortlich für die Installation, Konfiguration und den Netzwerkzugang der Geräte. Nur für dienstliche Zwecke notwendige Anwendungen werden installiert. Die Entscheidung darüber trifft der zuständige EDV-Beauftragte.

7. Mobile Endgeräte (z. B. Notebooks, Tablets, Smartphones)

Die Nutzung zur Verarbeitung personenbezogener Daten ist ausschließlich zu dienstlichen Zwecken zulässig. Der Zugriff ist passwortgeschützt (siehe Punkt 3).

8. Datenverwaltung

- Datenbestände sind entsprechend der geltenden Dienstanweisungen zu sichern.
- Zugriffsrechte sind funktional abgestuft zu vergeben.
- Muster und Textbausteine dürfen nur anonymisiert dauerhaft gespeichert werden.
- Private Daten dürfen nicht auf dienstlichen Geräten gespeichert werden.

9. Datensicherung

Zur Sicherstellung der Verfügbarkeit und Wiederherstellbarkeit von Daten sind regelmäßige inkrementelle Backups erforderlich. Zusätzlich erfolgen wöchentliche und monatliche Sicherungen.

Die Backup-Funktionalität sowie die Wiederherstellung der Daten sind regelmäßig zu testen und zu dokumentieren.

Werden Daten auf externen Datenträgern gespeichert oder weitergegeben, müssen diese:

- verschlüsselt,
- geprüft,
- und eindeutig gekennzeichnet sein.

Die Nutzung ist zu überwachen, um Missbrauch bei Verlust oder Diebstahl zu verhindern.

10. Verfahren (Verzeichnis der Verarbeitungstätigkeiten)

Alle eingesetzten Verfahren sind in einem Verzeichnis gemäß **Art. 30 EU-DSGVO** zu dokumentieren (siehe Anhang A). Dieses enthält mindestens folgende Angaben:

1. Name und Kontaktdaten der verantwortlichen Stelle und ggf. des Datenschutzbeauftragten
2. Zweck(e) der Verarbeitung
3. Beschreibung der betroffenen Personengruppen und der verarbeiteten Datenarten
4. Kategorien von Empfängern
5. Fristen für die Datenlöschung (soweit möglich)
6. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (TOMs) nach Art. 32 Abs. 1 DSGVO; Siehe dazu auch III. Sicherheitskonzept für die automatisierte Datenverarbeitung.

IV. Datenschutzrichtlinien

1. Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten dürfen ausschließlich zur Erfüllung der satzungsgemäßen Aufgaben des DLRG Kreisverbandes Ingolstadt e.V. (§ 2 der Satzung) erhoben, gespeichert, genutzt oder anderweitig verarbeitet werden.

(2) Die Verarbeitung personenbezogener Daten von Mitgliedern und Dritten (z. B. Dienstleister oder Lieferanten) ist ebenfalls zulässig, wenn sie zur Vertragserfüllung notwendig ist. Eine weitergehende Verarbeitung ist erlaubt, sofern sie im berechtigten Interesse des Vereins liegt und keine überwiegenden schutzwürdigen Interessen der betroffenen Person entgegenstehen (Art. 6 Abs. 1 DSGVO). Unter diesen Voraussetzungen dürfen die Daten auch von Mitarbeitenden in den Bereichen Verbandskommunikation und Social Media genutzt werden, sofern § 9 beachtet wird.

2. Verpflichtung auf das Datengeheimnis

(1) Personen, die mit der Verarbeitung personenbezogener Daten betraut sind, dürfen diese nicht unbefugt nutzen. Gemäß Art. 24 Abs. 1 DSGVO sind alle entsprechenden Mitglieder und Funktionsträger des DLRG Kreisverbandes Ingolstadt e.V. schriftlich auf die Einhaltung der datenschutzrechtlichen Vorgaben (Art. 5 Abs. 1 lit. f und Art. 32 Abs. 4 DSGVO) zu verpflichten.

(2) Diese Verpflichtung ist zu dokumentieren und sicher aufzubewahren (siehe Anhang C und D).

3. Weitergabe von Daten

(1) Eine Weitergabe personenbezogener Daten an andere Vereinsmitglieder ist nur zulässig, wenn ein berechtigtes Interesse glaubhaft gemacht wird und keine überwiegenden Interessen der betroffenen Person entgegenstehen (Art. 6 Abs. 1 Lit. f DSGVO).

(2) Die Weitergabe von Mitgliederdaten an Dritte, z. B. Unternehmen oder Medien, ist nur mit vorheriger Einwilligung der betroffenen Person erlaubt.

(3) Vereinsmitglieder können eine Mitgliederliste zur Wahrnehmung satzungsgemäßer Rechte erhalten, sofern sie schriftlich versichern, die Daten ausschließlich zu diesem Zweck zu verwenden und diese anschließend zurückzugeben oder zu vernichten.

(4) Für satzungsgemäße Zwecke wie Kostenerstattungen oder Ehrungen dürfen personenbezogene Daten an übergeordnete DLRG-Gliederungen oder Einrichtungen übermittelt werden. Dies entfällt, wenn berechtigte Einwände vorliegen und dadurch keine rechtlichen Verpflichtungen verletzt werden.

4. Einschränkung und Löschung von Daten

(1) Personenbezogene Daten sind einzuschränken oder zu löschen, sobald sie für den Vereinszweck nicht mehr erforderlich sind.

(2) Die Speicherung erfolgt nur solange, wie sie durch den Vereinszweck (§ 2 der Satzung) gerechtfertigt ist. Bei Austritt, Ausschluss oder Tod eines Mitglieds sind die Daten zu löschen, es sei denn, offene Verpflichtungen bestehen weiterhin. In diesem Fall sind sie zu sperren und nach Erfüllung zu löschen.

(3) Kassenrelevante Daten dürfen bis zu zehn Jahre nach dem Ende der Mitgliedschaft oder dem Todesfall aufbewahrt und sind danach zu löschen.

(4) Für das Funktagebuch gelten gesonderte Datenschutzregelungen und Löschfristen. Für alle übrigen Daten gelten die Löschfristen laut Anhang 1.

(5) Die Löschung erfolgt dauerhaft und irreversibel, etwa durch mehrfaches Überschreiben oder Zerstörung der Datenträger.

(6) Wenn eine Löschung technisch nicht möglich oder mit unverhältnismäßigem Aufwand verbunden ist, genügt eine dauerhafte Einschränkung. Gleiches gilt bei entgegenstehenden Interessen der betroffenen Person.

(7) Vereinsmitglieder haben das Recht auf Berichtigung, Vervollständigung, Einschränkung oder Löschung ihrer gespeicherten personenbezogenen Daten gemäß DSGVO und BDSG.

5. Sicherheitsvorkehrungen

(1) Der Zugang zu vereinseigenen Rechnern ist auf berechtigte Personen zu beschränken. Geschäftsräume sind bei Abwesenheit zu verschließen.

(2) Werden personenbezogene Daten durch externe Dienstleister verarbeitet, sind diese vertraglich zur Einhaltung der Sicherheitsstandards – idealerweise nach ISO 27001 – zu verpflichten.

(3) Der Zugang zu Daten ist passwortgeschützt und beschränkt sich auf den zur Aufgabenerfüllung erforderlichen Umfang.

(4) Die Nutzung privater Geräte zur Verarbeitung personenbezogener Daten ist nur mit Zustimmung des Vorstands zulässig und ausschließlich zweckgebunden. Nach dem Ausscheiden aus dem Amt sind alle Daten unverzüglich zu löschen.

(5) Der Verlust eines Geräts mit personenbezogenen Daten ist unverzüglich den zuständigen Vorständen zu melden, einschließlich Angaben zum Geräteschutz.

6. Auskunftsrecht

(1) Jedes Vereinsmitglied kann gemäß Art. 15 DSGVO und § 34 BDSG Auskunft über die zu seiner Person gespeicherten Daten, etwaige Empfänger sowie den Zweck der Speicherung verlangen.

(2) Das Auskunftsersuchen ist schriftlich an den Vorstand zu richten und sollte konkret angeben, auf welche Daten sich das Ersuchen bezieht.

7. Recht auf Datenübertragbarkeit

(1) Nach Maßgabe von Art. 20 DSGVO können Vereinsmitglieder die sie betreffenden, vom Verein automatisiert verarbeiteten Daten in einem strukturierten, maschinenlesbaren Format anfordern.

(2) Auf Wunsch übermittelt der DLRG Kreisverband die Daten direkt an eine benannte externe Stelle.

8. Datenschutzbeauftragter und Beschwerderecht

(1) Ein Datenschutzbeauftragter ist gemäß § 38 BDSG zu benennen, wenn in der Gliederung ständig mehr als 10 Personen mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind. Er ist dann dem Vorstand direkt unterstellt, weisungsfrei in seiner fachlichen Tätigkeit und zur Verschwiegenheit verpflichtet.

(2) Die Vergangenheit hat gezeigt, dass im DLRG Kreisverband Ingolstadt diese Grenze zu keiner Zeit überschritten wird und die Benennung eines Datenschutzbeauftragten aus diesem Grund nicht notwendig ist. Somit wird mit Inkrafttreten der neuen Datenschutzverordnung auf eine weitergehende Benennung eines Datenschutzbeauftragten verzichtet.

(3) Betroffene können sich jederzeit mit Anliegen oder Beschwerden an die Vorsitzenden des DLRG Kreisverbandes Ingolstadt e.V. wenden.

(4) Darüber hinaus besteht ein Beschwerderecht bei der zuständigen Aufsichtsbehörde: Bayerisches Landesamt für Datenschutzaufsicht (BayLDA).

V. Anhang

Anhang A: Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 EU-DSGVO

1. Verwendete Verfahren / Software

1.1 DLRG-Manager

- **Speicherort:**
  Server des DLRG-Präsidiums
- **Zugriffsberechtigte:**
  Vorstandsmitglieder
- **Rechtsgrundlage:**
  Auftragsverarbeitungsvertrag mit dem Präsidium
- **Einwilligung:**
  erfolgt im Rahmen der Anmeldung zur Mitgliedschaft

1.2 Internet Service Center (ISC) der DLRG

- **Speicherort:**
  Server des DLRG-Präsidiums
- **Zugriffsberechtigte:**
  Vorstandsmitglieder, Übungsleiter, (jeweils nur für ihre eigene Gruppe), IT-Beauftragte, Kursanwärter
- **Rechtsgrundlage:**
  Auftragsverarbeitungsvertrag mit dem Präsidium
- **Einwilligung:**
  erfolgt im Rahmen der Anmeldung zum Kurs
- **Hinweis:**
  Zustimmung zur Verwendung von Fotos für dienstliche Zwecke ist integriert

1.3 Helferstammdatei, (MS Excel)

- **Speicherort:**
  DLRG-Cloud-Speicher des DLRG KV Ingolstadt
- **Zugriffsberechtigte:**
  Vorstandsmitglieder
- **Einwilligung:**
  Schriftliche Erklärung auf einem Formblatt je Helferin/Helfer
- **Hinweis:**
  Zustimmung zur Verwendung von Fotos ist inbegriffen

1.3 Stammdatei für Wettkämpfe, (MS Excel)

- **Speicherort:**
  DLRG-Cloud-Speicher des DLRG KV Ingolstadt
- **Zugriffsberechtigte:**
  Vorstandsmitglieder, Referenten
- **Einwilligung:**
  Schriftliche Erklärung auf dem Anmeldeformular je Wettkampfteilnehmer als Sportler oder Helfer
- **Hinweis:**
  Zustimmung zur Verwendung von Fotos ist inbegriffen

2. Geschäftsführung – Mitgliederverwaltung

Zwecke der Datenverarbeitung:

- **Verwaltung der Mitgliedsdaten über den DLRG-Manager**
  Verarbeitete Daten: Name, Vorname, Geburtsdatum, Anschrift, Telefon, E-Mail, Bankverbindung, Eintrittsdatum, Mitgliedsnummer, Ehrungen
- **Abrechnung von Kurs- und Lehrgangsgebühren über das ISC**
  Verarbeitete Daten: Name, Vorname, Geburtsdatum, Anschrift, Telefon, E-Mail, Bankverbindung
- **Übermittlung von Daten an übergeordnete DLRG-Stellen**
  Verarbeitete Daten: Qualifikationen nach Prüfungsordnungen

3. Ausbildung

Zwecke der Datenverarbeitung:

- **Lehrgangsverwaltung über ISC**
  Verarbeitete Daten: Name, Vorname, Geburtsdatum, Anschrift, Telefon, E-Mail, Teilnahmevoraussetzungen
- **Teilnehmernachweise und Urkundenerstellung (ggf. über Helferstammdatei)**
- **Personalentwicklung**
  Verarbeitete Daten: Name, Vorname, Geburtsdatum, Anschrift, Telefon, E-Mail, Qualifikationen nach Prüfungsordnungen und gesetzlich vorgeschriebene Ausbildungen
- **Teilnehmerdokumentation während des Kurses**
  Verarbeitete Daten: Anwesenheit, abgelegte Prüfungen

4. Jugendbildungsmaßnahmen und -veranstaltungen

Zwecke der Datenverarbeitung:

- **Organisation und Durchführung von Maßnahmen der DLRG-Jugend** (z. B. Gruppenstunden, Jugendfahrten, Spieleabende)
  Verarbeitete Daten: Name, Vorname, Geschlecht, Geburtsdatum/-ort, Anschrift, Telefon, E-Mail; Bei Minderjährigen zusätzlich: Kontaktdaten der Eltern
- **Zugriffsberechtigte:** Jugendvorstand, Referenten, Betreuer, Ausbilder

5. Ehrungen

Zwecke der Datenverarbeitung:

- **Durchführung von Ehrungen gem. Ehrungsordnungen der DLRG**
  Verarbeitete Daten: Name, Geburtsdatum, Adresse, Gliederungszugehörigkeit, Eintrittsdatum, erhaltene Ehrungen, Stellungnahmen, DRSA-Besitz
- **Datenweitergabe:** An Vorstände, Kommunen, übergeordnete Stellen

6. Reisekosten- und Auslagenabrechnung

Zwecke der Datenverarbeitung:

- **Abrechnung von Reisekosten und Auslagen**
  Verarbeitete Daten: Name, Adresse, Bankverbindung, Reisedaten, Rechnungsinformationen
  Bei Auslagen: Art, Menge, Preis, Lieferanten, Dienstleistungen
- **Empfänger:** Vorstand, Schatzmeisterin (Freigabe), Banken

7. Lizenzverwaltung

Zwecke der Datenverarbeitung:

- **Verwaltung von Lizenzen nach den DLRG-Prüfungsordnungen**
  Verarbeitete Daten: Name, Geburtsdatum, Geschlecht, Adresse, E-Mail, Lizenznummer, Gültigkeit, Nachweise
- **Empfänger:** Referenten, zuständige Untergliederungen

8. Beschaffung nach BayRDG

Zwecke der Datenverarbeitung:

- **Abwicklung von Beschaffungen und Führung des Inventarverzeichnisses**
  Von Mitgliedern: Name, Funktion, E-Mail, Telefonnummer
  Von Lieferanten: Rechnungs- und Lieferdaten

9. Spender- und Sponsorendaten

Zwecke der Datenverarbeitung:

- **Spendenverwaltung und -kommunikation**
  Verarbeitete Daten: Name, Titel, Geburtstag, Adresse, Telefonnummer, E-Mail, Spendenhöhe, Datum, unter Umständen Projektbezug

10. Online-Frankierung

Zwecke der Datenverarbeitung:

- **Erstellung von Versandmarken**
  Verarbeitete Daten: Name, Adresse, Funktion
- **Empfänger:** Deutsche Post AG / DHL

11. Sportförderung

Zwecke der Datenverarbeitung:

- **Antragstellung und Abrechnung von Sportfördermitteln beim BLSV**
  Antragsteller: Name, E-Mail, Telefonnummer
  Übungsleiter: Name, Lizenznummer, Gültigkeit
- **Speicherort:** Server der DLRG Landesverband Bayern e.V.

12. Sicherung des Posteingangs

Zwecke der Datenverarbeitung:

- **Posteingangssicherung (z. B. Scans)**
  Verarbeitete Daten: Name, Adresse, Telefonnummer, E-Mail, Fax, DLRG-Zugehörigkeit, Funktion, Signaturdaten, Vertragsdaten
- **Empfänger:**
  Vorstände, Referenten, Fachübungsleiter, ggf. Banken, Steuerberater, Bezirks-, Landes- und Bundesverband der DLRG

13. Abrechnung von Erste-Hilfe-Kursen

Zwecke der Datenverarbeitung:

- **Abrechnung mit Ministerium (BayStMI)**
  Verarbeitete Daten: Name, Geburtsname, Schul- und Kursdaten
- **Empfänger:**
  Schatzmeisterei, DLRG Bundesverband, Ministerium

14. Personalverwaltung

Zwecke der Datenverarbeitung:

- **Verwaltung von Vertragsverhältnissen (Arbeits-, Honorar-, Werkverträge)**
  Verarbeitete Daten: Personenstammdaten, Steuer- und Sozialdaten, Bankverbindung, Vertragsdaten, Arbeitszeiten, Krankmeldungen, Qualifikationen, Verpflichtungserklärungen
- **Empfänger:**
  Schatzmeisterei, zuständige Vorstandsmitglieder

15. Übermittlung an Versicherungen

Zwecke der Datenverarbeitung:

- **Vertragsabwicklung mit Versicherungsunternehmen**
  Übermittlung personenbezogener Daten erfolgt nur zweckgebunden und auf vertraglicher Grundlage

16. Zuständigkeiten im Datenschutz

Datenschutzbeauftragter

- **Aufgaben:**
  Überwachung der Einhaltung datenschutzrechtlicher Vorgaben
  Beratung des Vorstands
  ggf. Kommunikation mit der Aufsichtsbehörde
- **Hinweis:**
  Aufgrund der festgelegten Anzahl Zugriffsberechtigter (<10 Personen) ist **kein Datenschutzbeauftragter** zu benennen (§ 38 BDSG).

Zugriffsberechtigte Personen (Stand 06/2025):

- Vorsitzende: Dr. Christian Fuchs, Katharina von Kap-herr
- Geschäftsführung/Schatzmeisterin: Aysun Henke
- Ausbildungsleitung: Dr. Antje Grundheber, Christian Bretschneider
- IT/Administration: Thomas Mente, Emily Labus
- Jugendvorstand: Emily Labus
- Jugendreferentin Wettkampf: Maja Boldt
- Übungsleitungen/Prüfungsabnehmen:
  Je eine verantwortliche Person pro Ausbildungsgruppe

Die Personen aus 4., 5. und 7. sind zum Teil bereits unter 1. bis 4. benannt.

Die Übungsleitung hat darauf zu achten, dass insgesamt weniger als 10 Personen gleichzeitig mit der Datenverarbeitung betraut sind.

Aufgrund dieser Festlegung der Anzahl von Zugriffsberechtigten ist ein Datenschutzbeauftragter NICHT zu benennen.

Anhang B:

Aufbewahrungsfristen und Löschkonzept gemäß Art. 17 DSGVO

1. Aufbewahrungsfristen

Unterlagen / Datenkategorie	Aufbewahrungsfrist	Rechtsgrundlage / Bemerkung
Mitgliedsunterlagen	Unverzüglich nach Austritt zu löschen, sofern keine gesetzlichen Fristen entgegenstehen	Ausnahmen: z. B. Geschäftsvorgänge mit Mitgliedern (siehe unten)
Mitgliederverwaltung	10 Jahre	§ 147 AO (Abgabenordnung)
Geschäftsvorgänge (z. B. Rechnungen)	10 Jahre	§ 147 AO
Ausbildungsunterlagen	10 Jahre	z. B. Teilnahmebescheinigungen, Prüfungsnachweise
Helferstammdatei	Unverzüglich nach Beendigung der Mitarbeit	Ausnahme: 10 Jahre bei enthaltenen Ausbildungs-nachweisen
Unterlagen zu Jugendveranstaltungen	10 Jahre	z. B. Teilnehmerlisten, Aufsichtspflichten
Verpflichtungserklärungen	Unbegrenzt	z. B. zur Verschwiegenheit oder IT-Sicherheit

2. Zuständigkeiten für Löschung und Datenpflege

Datenkategorie	Zuständig für Löschung und Datenpflege
Mitgliedsunterlagen	Vorstand / Geschäftsführung
Geschäftsvorgänge	Vorstand / Geschäftsführung
Ausbildungsunterlagen	Technische- bzw. Ausbildungsleitung
Helferstammdatei	Technische Leitung

Anhang C: Verpflichtungserklärung Vorstand

Deutsche Lebens-Rettungs-Gesellschaft

Kreisverband Ingolstadt e.V.
Dr. Christian Fuchs
Vorsitzender des Vorstands
Harderstrasse 24
85049 Ingolstadt
E-Mail: vorstand@ingolstadt.dlrg.de
Internet: ingolstadt.dlrg.de

DLRG e.V. | Kreisverband Ingolstadt | Harderstrasse 24 | 85049 Ingolstadt

An die
DLRG Kreisverband Ingolstadt e.V.
Harderstrasse 24
85049 Ingolstadt

Verpflichtungserklärung zum Datenschutz für Vorstandsmitglieder

Als Vorstandsmitglied der Deutschen Lebens-Rettungs-Gesellschaft e.V. (DLRG) habe ich Zugriff auf vertrauliche Daten. Ich verpflichte mich daher, den erhöhten Sicherheitsinteressen der DLRG Rechnung zu tragen.

Ich erkläre, dass ich nicht unbefugt personenbezogene Daten erheben, verarbeiten oder nutzen werde und dass ich die durch meine Aufgaben zur Kenntnis gelangten Daten streng vertraulich behandeln und Dritten nicht zugänglich machen werde.

Ich bestätige, dass ich nach § 5 BDSG auf das Datengeheimnis verpflichtet und in diesem Zusammenhang über die gesetzlichen Vertraulichkeitspflichten belehrt bin.

Ich habe zur Kenntnis genommen, dass die Vertraulichkeitsregeln auch nach Beendigung der Aufgabe/meiner Tätigkeit zu beachten sind.

§ 5 BDSG Datengeheimnis
Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort. Das Merkblatt zur Verpflichtungserklärung habe ich erhalten und den Inhalt zur Kenntnis genommen.

Name	Vorname	Geburtsdatum

Ort, Datum	Unterschrift

Anhang D: Verpflichtungserklärung Übungsleiter und Referatsleiter

Deutsche Lebens-Rettungs-Gesellschaft

DLRG e.V. | Kreisverband Ingolstadt | Harderstrasse 24 | 85049 Ingolstadt

An die
DLRG Kreisverband Ingolstadt e.V.
Harderstrasse 24
85049 Ingolstadt

Kreisverband Ingolstadt e.V.
Dr. Christian Fuchs
Vorsitzender des Vorstands
Harderstrasse 24
85049 Ingolstadt
E-Mail: vorstand@ingolstadt.dlrg.de
Internet: ingolstadt.dlrg.de

Verpflichtungserklärung zum Datenschutz
für Übungsleiter, Referatsleiter und alle mit der Datenverarbeitung vertrauten Personen

Als Mitglied der Deutschen Lebens-Rettungs-Gesellschaft e.V. (DLRG) habe ich Zugriff auf vertrauliche Daten.
In meiner Funktion als _____ verpflichte ich mich
Beschreibung der Funktion des Mitglieds
daher, den erhöhten Sicherheitsinteressen der DLRG Rechnung zu tragen.

Ich erkläre, dass ich nicht unbefugt personenbezogene Daten erheben, verarbeiten oder nutzen werde und dass ich die durch meine Aufgaben zur Kenntnis gelangten Daten streng vertraulich behandeln und Dritten nicht zugänglich machen werde.

Ich bestätige, dass ich nach § 5 BDSG auf das Datengeheimnis verpflichtet und in diesem Zusammenhang über die gesetzlichen Vertraulichkeitspflichten belehrt bin.

Ich habe zur Kenntnis genommen, dass die Vertraulichkeitsregeln auch nach Beendigung der Aufgabe/meiner Tätigkeit zu beachten sind.

§ 5 BDSG Datengeheimnis
Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort. Das Merkblatt zur Verpflichtungserklärung habe ich erhalten und den Inhalt zur Kenntnis genommen.

_____

Name Vorname Geburtsdatum

_____

Ort, Datum Unterschrift

Merkblatt zur Verpflichtungserklärung

für Vorstände, Übungsleiter, Referatsleiter und alle mit der Datenverarbeitung vertrauten Personen

§ 42 BDSG

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,
1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,
1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.
(3) 1 Die Tat wird nur auf Antrag verfolgt. 2 Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde. (…)

§ 43 BDSG

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig
1. entgegen § 30 Abs. 1 ein Auskunftsverlangen nicht richtig behandelt oder
2. (…)

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.
(3)…

§ 202a Abs. 1 StGB

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Daten im Sinne des Abs. 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 303a Abs. 1 StGB

Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft

§ 4 GeschGehG

(1) Ein Geschäftsgeheimnis darf nicht erlangt werden durch
1. unbefugten Zugang zu, unbefugte Aneignung oder unbefugtes Kopieren von Dokumenten, Gegenständen, Materialien, Stoffen oder elektronischen Dateien, die der rechtmäßigen Kontrolle des Inhabers des Geschäftsgeheimnisses unterliegen und die das Geschäftsgeheimnis enthalten oder aus denen sich das Geschäftsgeheimnis ableiten lässt, oder
2. jedes sonstige Verhalten, das unter den jeweiligen Umständen nicht dem Grundsatz von Treu und Glauben unter Berücksichtigung der anständigen Marktgepflogenheiten entspricht.

(2) Ein Geschäftsgeheimnis darf nicht nutzen oderoffenlegen, wer
1. das Geschäftsgeheimnis durch eine eigene Handlung nach Abs. 1
   a) Nummer 1 oder
   b) Nummer 2
   erlangt hat.
2. gegen eine Verpflichtung zur Beschränkung der Nutzung des Geschäftsgeheimnisses verstößt oder
3. gegen eine Verpflichtung verstößt, das Geschäftsgeheimnis nicht offenzulegen. …

§ 23 GeschGehG

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen,

1. entgegen § 4 Abs. 1 Nr. 1 ein Geschäftsgeheimnis erlangt,
2. entgegen § 4 Abs. 2 Nr. 1 Buchst. a ein Geschäftsgeheimnis nutzt oder offenlegt oder
3. ...

(2) Ebenso wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen, ein Geschäftsgeheimnis nutzt oder offenlegt, das er durch eine fremde Handlung nach Abs. 1 Nr. 2 oderNr. 3 erlangt hat.

(3) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs oder aus Eigennutz entgegen § 4 Abs. 2 Nr. 2 oder Nr. 3 ein Geschäftsgeheimnis, das eine ihm im geschäftlichen Verkehr anvertraute geheime Vorlage oder Vorschrift technischer Art ist, nutzt oder offenlegt

(4) Mit Freiheitsstrafe bis zu fünf Jahren wird bestraft, wer

1. In den Fällen des Abs. 1 oder des Abs. 2 gewerbsmäßig handelt,
2. In den Fällen des Abs. 1 Nr. 2 oder Nr. 3 oder des Abs. 2 bei der Offenlegung weiß, dass das Geschäftsgeheimnis im Ausland genutzt werden soll, oder
3. in den Fällen des Abs. 1 Nr. 2 oder des Abs. 2 das Geschäftsgeheimnis im Ausland nutzt.

(5) Der Versuch ist strafbar.

(6)...

(7) § 5 Nr. 7 des Strafgesetzbuchs gilt entsprechend. Die §§ 30 und 31 des Strafgesetzbuchs gelten entsprechend, wenn der Täter zur Förderung des eignen oder fremden Wettbewerbs oder aus Eigennutz handelt. (...)

Art. 83 DS-GVO

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Art. 58 Abs. 2 Buchst. a bis h und i verhängt. (...)

(3) Verstößt ein Verantwortlicher oder ein Auftragsdatenverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.

(4) Bei Verstößen gegen folgende Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher Betrag höher ist:

a) die Pflichten der Verantwortlichen und der Auftragsdatenverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43; (...)

(5) Bei Verstößen gegen folgende Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher Betrag höher ist:

a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Art. 5, 6, 7 und 9;

b) die Rechte der betroffenen Person gemäß den Art. 12 bis 22;

c) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Art. 12 bis 22;

d) die Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden.

e) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Art. 58 Abs. 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Art. 58 Abs. 1.

(6) Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Art. 58 Abs. 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist. (...)

Anhang E: Geräteverzeichnis

Dokumentation der eingesetzten IT-Systeme zum Stand 06/2025

Gerätetyp und -art	Aufstellungs-ort	Seriennummer	Eigentümer	Datum (Zugang/Abgang)

Hinweise:

Dienstlich genutzte Geräte können durch den Kreisverband Ingolstadt e.V. beschafft und inventarisiert werden. Auch private Geräte, die für dienstliche Zwecke verwendet werden, sind dem Kreisverband zu melden und in das Geräteverzeichnis aufzunehmen.

Alle Veränderungen (z. B. Austausch, Reparatur, Verschrottung) sind im Verzeichnis zu dokumentieren. Die Konfigurationsdaten (z. B. IP-Adressen) sind vor unbefugtem Zugriff zu schützen. Es ist grundsätzlich lizenzierte Standardsoftware mit aktuellen Sicherheitsupdates zu verwenden.

Vertrag über Auftragsverarbeitung

zwischen der

DLRG Gliederung (gemäß elektronischer Bestätigung)

- Auftraggeber –

und der

Deutschen Lebens-Rettungs-Gesellschaft e.V., Im Niedernfeld 1-3, 31542 Bad Nenndorf

-Auftragnehmer-

wird folgender Vertrag über Auftragsverarbeitung i. S. d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO) geschlossen.

Präambel

Die Deutsche Lebens-Rettungs-Gesellschaft e.V. (im Folgenden: DLRG e.V.) bildet mit ihren Landesverbänden, Bezirken, Kreisverbänden, Ortsgruppen und Ortsverbänden einen Gesamtverband. Zur Unterstützung der Erfüllung der satzungsgemäßen Aufgaben ermöglicht der Bundesverband seinen Gliederungen die unentgeltliche Nutzung eines E-Mail-Systems, eines Content-Management-Systems und weiterer (webbasierter) Software (z.B. Lehrgangsverwaltung), im Folgenden: „Dienste“ genannt.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

(1) Gegenstand der Vereinbarung ist die Auftragsverarbeitung durch den DLRG e.V. für seine Landesverbände, Bezirke, Kreisverbände, Ortsgruppen und Ortsverbände im Rahmen der Nutzung der angebotenen Dienste.

(2) Die Vereinbarung wird auf unbestimmte Zeit geschlossen. Sie endet, wenn der Auftraggeber die Nutzung der Dienste einstellt.

(3) Der Funktionsumfang der Dienste wird auf den Webseiten des Auftragnehmers (siehe z.B. https://wiki.dlrg.de) detailliert beschrieben.
Durch die angebotenen Dienste können, je nach Nutzungsumfang durch die jeweilige Gliederung,
- Daten von Mitgliedern (z.B. Personenstammdaten und Qualifikation),
- Daten der Nutzerinnen und Nutzer der Dienste (Log-Files),
- Teilnehmerinnen und Teilnehmern an Veranstaltungen (insbesondere Personenstammdaten) und
- Besucherinnen und Besuchern der Webseiten (Log-Files)

verarbeitet werden.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DS-GVO).

(2) Der Auftraggeber erteilt seine Weisungen im Sinne des Datenschutzrechts in der Regel durch die Nutzung der durch die Dienste angebotenen Funktionen. Sofern es einen zwingenden Bedarf für eine darüber hinausgehende datenschutzrechtliche Weisung gibt, wird diese dem Auftragnehmer über die E-Mail-Adresse des Auftragnehmers (webmaster@dlrg.de) erteilt.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten; außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der DS-GVO (s. Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im

Zusammenhang mit der Verarbeitung auf Dauer sicherstellen und dem Schutzbedarf der Daten Rechnung tragen. Die vom Auftragnehmer ergriffenen technischen und organisatorischen Maßnahmen sind in der Anlage beschrieben.

(3) Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vereinbarte Schutzniveau nicht unterschritten wird.

(4) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

(5) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort. Der Auftragnehmer darf zu Erbringung der Dienste weitere Auftragsverarbeiter in Anspruch nehmen. Er informiert den Auftraggeber über die Inanspruchnahme weiterer Auftragsverarbeiter über seine Webseiten (https://wiki.dlrg.de) oder per E-Mail an die Webmaster-Funktionsadresse des Auftraggebers.

(6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden, über seine Webseiten oder per E-Mail an die Webmaster- Funktionsadresse des Auftraggebers. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen.

(7) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

(8) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, und dafür ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(9) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist.

(10) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

(11) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 11 entsprechend.

(3) Der Auftraggeber gewährleistet, dass seine Webmaster-Funktionsadresse regelmäßig abgerufen wird.

§ 5 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten und der Reichweite seiner Verantwortung bei dem Nachweis einer den Rechtsvorschriften entsprechenden Verarbeitung, sofern eine Datenschutzaufsichtsbehörde einen entsprechenden Nachweis vom Auftraggeber verlangt und ermöglicht erforderlichenfalls Inspektionen gem. Art. 28 Abs. 3 lit. h DS-GVO.

§ 7 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der

Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der DS-GVO liegen.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(4) Es gilt das Deutsche Recht.

§ 8 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

für den Auftragnehmer:

Ute Vogt
Präsidentin
Deutsche Lebens-Rettungs-Gesellschaft e.V.

für den Auftraggeber:

gem. elektronischer Bestätigung
(zeichnungsberechtigter Vertreter)

Anlage zum Vertrag über Auftragsverarbeitung

Beschreibung der technischen und organisatorischen Maßnahmen gem. § 3 Abs. 2 des Vertrages (Stand November 2024)

1. Allgemeine organisatorische Maßnahmen

Organisationsregeln

Die im Vertrag genannten Dienste werden vom Auftragnehmer durch den Arbeitskreis Internet (AKI) bereitgestellt. Der AKI arbeitet nach Organisationsregeln, die insbesondere folgendes vorsehen:

- Anforderungen an die Qualifikation der Mitglieder des AKI,
- Verpflichtung auf das Datengeheimnis,
- eine Einarbeitungszeit vor der Mitgliedschaft,
- ein Rechtemanagement (Grundsatz: nur die Zugriffsrechte, die für die Mitarbeit benötigt werden),
- Verantwortlichkeiten und
- Regelungen zur Gewährleistung des Datenschutzes.

Softwareentwicklung

Neuer Code wird erst nach Sichtung und Freigabe durch einen anderen Entwickler produktiv eingesetzt. Der Code wird auf Einhaltung von Standards und auf mögliche Sicherheitslücken untersucht.

2. In Art. 32 DS-GVO erwähnte Maßnahmen

Verschlüsselung

Der clientseitige Zugriff auf die Systeme der DLRG (z.B. Webdienste, E-Mail-Service) ist mit einer Transportverschlüsselung gesichert.

Gewährleistung der Vertraulichkeit

Zutrittskontrolle

- Die Systeme werden selbstverwaltet auf Ressourcen eines zertifizierten Diensteanbieters in einem von dessen Rechenzentren betrieben.

Zugangskontrolle

- Dokumentierte Zuordnung von Benutzerrechten,
- Authentifizierung mit Username/Password, Multifaktorauthentifizierung,
- Authentifizierung per SSH Key,
- Einsatz von VPN-Technologie,
- Zuordnung von Benutzerprofilen zu IT-Systemen,
- Einsatz von spezifischen Sicherheits-Gateways
- Verschlüsselung von Datenträgern und Back-Up-Datenträgern

Zugriffskontrolle

- Vorhandenes Berechtigungskonzept,
- streng limitierte Auswahl der administrativen Zugänge,
- Protokollierung von Zugriffen auf IT-Systeme,
- Rechteverwaltung gemäß Richtlinien durch zentrale Instanz, beschränkte Anzahl der Administratoren

Trennungskontrolle

- Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden getrennt verarbeitet.
- Systeme werden gekapselt (Sandboxing)

Gewährleistung der Integrität

- Weitergabekontrolle
- Optionale Ende-zu-Ende-E-Mail-Verschlüsselung (PGP)
- VPN-Tunnel mit zentralem VPN-Gateway

Eingabekontrolle

- Protokollierung von Zugriffen auf IT-Systeme (Eingabe/Löschung) mit individuellen Benutzerprofilen
- Rechtevergabe auf Basis eines Berechtigungskonzeptes des AK IT
- Die Auftragnehmer berechtigen Personen für die genutzten Dienste nach ihrem eigenen Berechtigungskonzept selbst.

Gewährleistung der Verfügbarkeit

- Verfügbarkeitskontrolle
- Backup der relevanten Systeme in einer anderen Verfügbarkeitszone
- Absicherung der Systeme mittels Firewall
- Sicherheits Incident Prozesse sind definiert.
- Wiederherstellungsprozesse werden einer regelmäßigen Prüfung unterzogen.

Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

- Notfallmanagement
- Wiederherstellungsprozess
- Regelmäßiges Testen der Wiederherstellung

Gewährleistung der Belastbarkeit der Systeme

- Relevante Systeme sind als Hochverfügbarkeitssysteme aufgebaut.
- Monitoring System mit Alarmierung per Email bei Überschreitung der Grenzwerte wird eingesetzt.

3. Weitere Maßnahmen

- „Privacy by Design“ (Art. 25 Abs. 1 DSGVO): In den unterschiedlichen Apps werden nur die zwingend erforderlichen Daten erhoben.
- Ein Prozess für das Erkennen und Melden von Datenschutzverletzungen ist eingerichtet.

4. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Der Arbeitskreis IT überprüft regelmäßig die implementierten technischen und organisatorischen Maßnahmen und ergreift erforderlichenfalls neue Maßnahmen, wenn das Risiko für die Verletzung der Rechte und Freiheiten natürlicher Personen steigt.

5. Weitere Auftragsverarbeiter nach Art. 28 DSGVO

Die Auswahl weiterer Auftragsverarbeiter erfolgt insbesondere unter Berücksichtigung von vorhandenen Zertifizierungen innerhalb der ISO-27000-Reihe oder vergleichbarer Standards. Die technischen und organisatorischen Maßnahmen der weiteren Auftragsverarbeiter sind in Dokumenten dieser beschrieben.