

**Verzeichnis der Verfahren zur Datenverarbeitung
der Deutschen Rheuma-Liga Berlin e.V.
Therapie-, Beratungs- und Selbsthilfezentrum**

Stand 28.03.2024

Gemäß Datenschutz Grundschutzverordnung hat jede datenverarbeitende Stelle, die personenbezogene Daten in einer automatisierten Datei speichert und verarbeitet, ein Verzeichnis von Verarbeitungstätigkeiten zu führen und verständlich darzustellen, wie die Datenverarbeitung i.S. des Gesetzes erfolgt.

1. Name und Anschrift der datenverarbeitenden Stelle und des/der Verantwortlichen

Deutsche Rheuma-Liga Berlin e.V.
Therapie-, Beratungs- und Selbsthilfezentrum
Mariendorfer Damm 161a
12107 Berlin

Geschäftsführer
Herr Gerd Rosinsky

Datenschutz Beauftragter
Herr Markus Pleyer

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

Deutsche Rheuma-Liga Berlin e.V. erhebt und verarbeitet im Rahmen ihres Organisationszweckes personenbezogene Daten für folgende Zwecke:

Lfd. Nummer	Zweck	Rechtsgrundlage der Datenverarbeitung
1.	Mitgliederverwaltung Abbuchung des Mitgliedsbeitrags, Zusendung von Informationen, Einladungen zu Mitgliederversammlungen und Veranstaltungen	<ul style="list-style-type: none"> • persönliche Einwilligungen der Mitglieder auf dem Mitgliedsantrag (Anlage) • Vertragsgrundlage Mitgliedschaft gemäß Mitgliedsantrag • Wahrung der berechtigten Interessen der Rheuma-Liga Berlin gemäß Satzung
2.	Webseite rheuma-liga-berlin.de	<ul style="list-style-type: none"> • persönliche Einwilligungen auf der Webseite • Wahrung der berechtigten Interessen der Rheuma-Liga Berlin gemäß Satzung
3.	Mitgliederzeitschrift Agil	<ul style="list-style-type: none"> • persönliche Einwilligungen • Vertragsgrundlage Mitgliedschaft gemäß Mitgliedsantrag • Wahrung der berechtigten Interessen der Rheuma-Liga Berlin gemäß Satzung • Vertrag zur Datenverarbeitung mit dem Westkreuz-Verlag GmbH

Lfd. Nummer	Zweck	Rechtsgrundlage der Datenverarbeitung
4.	Mitgliederzeitschrift „Mobil“ des Bundesverbandes	<ul style="list-style-type: none"> • persönliche Einwilligungen (Anlage) • Vertragsgrundlage Mitgliedschaft gemäß Mitgliedsantrag • Wahrung der berechtigten Interessen der Rheuma-Liga Berlin gemäß Satzung • Vertrag zur Datenverarbeitung mit der Firma muehlhausmoers (Anlage)
5.	Mailings für Spendenaufrufe oder Werbung für den Verein	<ul style="list-style-type: none"> • Wahrung der berechtigten Interessen der Rheuma-Liga Berlin gemäß Satzung bei Nicht Mitgliedern • Vertragsgrundlage Mitgliedschaft gemäß Mitgliedsantrag
6.	Abrechnung Ärztlicher Verordnungen durch die DVZ (Datenverarbeitungszentrum Gera um die Abrechnung mit den Krankenkassen/Kostenträgern vorzunehmen)	<ul style="list-style-type: none"> • persönliche Einwilligungen (Anlage) • Ermächtigung durch §§ 300, 301a, 302 SGB V • Vertrag zur Datenverarbeitung mit dem DVZ Gera (Anlage)
7.	(Externe) Soziale Beratung	<ul style="list-style-type: none"> • persönliche Einwilligungen (Anlage)
8.	<p>Mitarbeitende</p> <p>Zwecke des Beschäftigungsverhältnisses und Personalwirtschaft</p> <p>Erstellung von QM-Dokumentationen</p> <p>Erfüllung von zuwendungsrechtlichen, versicherungstechnischen und arbeitsrechtlichen Anforderungen</p> <p>Erstellung von Rechnungen</p> <p>Erstellung von Betriebskostenabrechnungen</p> <p>Durchführung von Lastschrifteinzugs-ermächtigungen</p> <p>Sicherstellung der Informations- und Kommunikationstechnologie</p>	<ul style="list-style-type: none"> • Anstellungsverhältnis • Zuwendungsbescheide • LHA/AnBest • Allgemeines Gleichbehandlungsgesetz • Altersteilzeitgesetz • Arbeitsgerichtsgesetz • Arbeitszeitgesetz • Aufwendungsausgleichsgesetz • Gesetz über Teilzeitarbeit und befristete Arbeitsverträge • Bürgerliches Gesetzbuch • Berufsbildungsgesetz • Beschäftigtenschutzgesetz • Betriebsrentengesetz • Betriebsverfassungsgesetz • Bundeselterngeld- und -Elternzeitgesetz • Bundesurlaubsgesetz • Einkommenssteuergesetz • Entgeltfortzahlungsgesetz • Familienpflegezeitgesetz • Kündigungsschutzgesetz • Mutterschutzgesetz • Nachweisgesetz • Pflegezeitgesetz • Zivilprozessordnung • persönliche Einwilligungen der Mitarbeiter/innen und Betroffenen • Wahrung der berechtigten Interessen des Unternehmens

3. Art der gespeicherten Daten

Lfd. Nr.	Programme/ Datenbanken	Art der Daten
1	<ul style="list-style-type: none"> • intern betriebener Fileserver (Microsoft) • intern betriebener Mailserver (Microsoft Exchange) • intern betriebene Datenbank Mikurs • intern betriebene Datenbank Cobra zentrales, intern betriebenes Backupsystem für sämtliche Daten 	<ul style="list-style-type: none"> • Vorname, Name, Titel • Geburtsdatum • Wohnanschrift • Telefonnummer, E-Mail-Adresse • Bankverbindung • Diagnosen, behandelnde Ärztin/Arzt • Krankenkasse, Rentenversicherung • Arbeit- oder Ausbildungsinstitution • Erwerbssituation/Einkommensart • Familienstand, häusliche Situation • Muttersprache, Migrationshintergrund • Grad der Behinderung, Pflegegrad, genutzte Hilfsmittel
2	rheuma-liga-berlin.de	<ul style="list-style-type: none"> • Name der abgerufenen Webseite • Datei, Datum und Uhrzeit des Abrufs • übertragene Datenmenge, Meldung über erfolgreichen Abruf • Browsertyp/Version Betriebssystem • Referrer URL (die zuvor besuchte Seite) • IP-Adresse und der anfragende Provider • sowie bei Nutzung eines mobilen Endgeräts zusätzlich: • Ländercode, Sprache, Geräte name, Name des Betriebssystems und –version
3	Postversand durch Westkreuz-Verlag GmbH Töpchiner Weg 198/200 12309 Berlin	<ul style="list-style-type: none"> • Vorname, Name, Titel • Wohnanschrift • Merkmal Mitgliedschaft
4	Postversand durch Firma muehlhaus & moers kommunikation GmbH Invalidenstr. 112 10115 Berlin	<ul style="list-style-type: none"> • Vorname, Name, Titel • Wohnanschrift • Merkmal Mitgliedschaft
5	Intern betriebener Mailserver (Microsoft Exchange)	<ul style="list-style-type: none"> • Vorname, Name, Titel • Emailadresse • Merkmal Mitgliedschaft/Nicht-Mitglied
6	DVZ Datenverarbeitungszentrum Gera GmbH dvz-gera.de Doktor-Friedrich-Wolf Str. 10, 07545 Gera	<ul style="list-style-type: none"> • Abrechnungsdaten • Vorname, Name, Titel • Geburtsdatum • Wohnanschrift • Bankverbindung • Diagnosen, behandelnde Ärztin/Arzt • Krankenkasse, Rentenversicherung • Verordnungsdaten

Lfd. Nr.	Programme/ Datenbanken	Art der Daten
7	<ul style="list-style-type: none"> • intern betriebener Fileserver (Microsoft) • intern betriebener Mailserver (Microsoft Exchange) • Datenbank mit Mandanten Rheuma-Liga sowie Sozialteam (eigener Server) 	<ul style="list-style-type: none"> • Vorname, Name, Titel • Geburtsdatum • Wohnanschrift • Telefonnummer, E-Mail-Adresse • Bankverbindung • Diagnosen, behandelnde Ärztin/Arzt • Krankenkasse, Rentenversicherung • Arbeit- oder Ausbildungsinstitution • Erwerbssituation/Einkommensart • Familienstand, häusliche Situation • Muttersprache, Migrationshintergrund • Grad der Behinderung, Pflegegrad, genutzte Hilfsmittel
8	<ul style="list-style-type: none"> • Personalwirtschaft Rechnungswesen Kassenprogramm • Verwaltungssoftware • System-Logdateien • Datenbank mit Mandanten Rheuma-Liga sowie Sozialteam (eigener Server) • intern betriebenes Backupsystem für sämtliche Daten • Telefonanlage: Mitel MiVoice Office 470 	<p>Abrechnungsdaten, Kontoverbindung, Elektronische Lohnsteuerabzugsmerkmale, Sozialversicherungsnummer, Qualifikationsmerkmale, Grad der Schwerbehinderung, personenbezogene Daten, Adressen/Kontaktdaten, Schulabschlüsse, Anwesenheitsdaten, Angaben zu Krankheit (im Betrieblichen Gesundheitsmanagement) Angaben zu Kooperationsunternehmen, Leistungs- und Verhaltensbeurteilungen</p> <p>Verbindungsdaten, Loginzeitpunkt, IP Adresse (Internet, Mail, Netzwerk), Verbindungsdaten (Telefonie)</p> <p>clientseitigen Windows Ereignisprotokolle für lokale Ereignisse</p> <p>Emailadressen Telefonkontakte</p>

4. Kreis der Betroffenen deren Daten erfasst werden

Lfd. Nr.	Betroffene
1	Mitglieder und Personen mit Interesse an einer Mitgliedschaft
2	Webseitennutzende
3	Mitglieder
4	Mitglieder
5	Öffentlichkeit/Mitglieder
6	Öffentlichkeit/Mitglieder
7	Öffentlichkeit/Mitglieder
8	Angestellte Mitarbeitenden, Honorarkräfte, Praktikanten Auszubildende, Bewerberinnen und Bewerber Ehrenamtliche / Bundesfreiwilligendienst

5. Übermittlung und Empfang von Daten

Lfd. Nr.	Betroffene
1	Empfang der Daten direkt von den Mitgliedern/an der Mitgliedschaft interessierten Übermittlung siehe 3 und 4 Versand Mitgliederzeitschriften
2	Empfang der Daten direkt von den Betroffenen nach Einwilligung durch klicken auf einen Bestätigungsbutton, Übermittlung von Browser-Typ/-Version; verwendetes Betriebssystem; Referrer-URL (die zuvor besuchte Seite); Hostname des zugreifenden Rechners (anonymisierte und gekürzte IP-Adresse); Uhrzeit der Serveranfrage bei Nutzung der Webseite an Google Inc. (https://www.google.de/intl/de/about/) (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
3	Auszug aus Mitgliederdatenbank Übermittlung für Postversand an Westkreuz-Verlag
4	Auszug aus Mitgliederdatenbank Übermittlung für Postversand durch Firma muehlhaus &
5	Veröffentlichung durch Emailversand
6	Empfang der Daten direkt von Betroffenen - Übermittlung zu DVZ Datenverarbeitungs- zentrum Gera GmbH
7	Empfang der Daten direkt von Betroffenen - Übermittlung zur Datenbank Rheuma-Liga und „Soz-Team“ (extern im Rechenzentrum gehostet)
8	Empfang der Daten direkt von Mitarbeitenden – Übermittlung an Zuwendungsgeber, Berufsgenossenschaft, Betriebsrat, Betriebsarzt, Finanzbehörden, Träger der gesetzlichen Sozialversicherung Mitarbeiter Debitorenbuchhaltung

6. Zugriffsberechtigte Personen oder Personengruppen

Lfd. Nr.	Zugriffsberechtigte Personen/-gruppen
1	<ul style="list-style-type: none"> • Mitarbeitenden, • IT Servicedienstleister Computer Manufaktur GmbH Franklinstraße 11 10587 Berlin
2	<ul style="list-style-type: none"> • Öffentlichkeitsarbeit • IT Servicedienstleister Computer Manufaktur GmbH Franklinstraße 11 10587 Berlin • Google Inc. (https://www.google.de/intl/de/about/) (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
3	<ul style="list-style-type: none"> • Mitarbeitenden • Westkreuz-Verlag GmbH
4	<ul style="list-style-type: none"> • Mitarbeitenden • muehlhaus & moers kommunikation GmbH

Lfd. Nr.	Zugriffsberechtigte Personen/-gruppen
5	<ul style="list-style-type: none"> • Mitarbeitenden • IT Servicedienstleister Computer Manufaktur GmbH
6	<ul style="list-style-type: none"> • Mitarbeitenden • DVZ Datenverarbeitungs-zentrum Gera GmbH • IT Servicedienstleister Computer Manufaktur GmbH
7	<ul style="list-style-type: none"> • Angehörige des Sozialberatungsteams
8	<ul style="list-style-type: none"> • Geschäftsführung

7. Technische und organisatorische Maßnahmen

Vertraulichkeit

Alle Mitarbeitenden der Deutsche Rheuma-Liga Berlin e.V. unterzeichnen beim Eintritt in die Organisation eine Verschwiegenheitsvereinbarung, welche den Umgang mit datenschutzrechtlich relevanten Daten regelt. Die Zuständigkeiten, Verantwortlichkeiten und Berechtigungen der Mitarbeitenden Deutsche Rheuma-Liga Berlin e.V. sind im Detail festgelegt. Personenbezogene Daten werden nur durch Befugte gemäß eines „Need to know-Prinzips“ verarbeitet. Die Zugriffsberechtigungen fürs Netzwerk bzw. einzelne Freigaben werden über persönliche Zugänge und eine zentrale Userverwaltung geregelt. Zusätzlich besitzen spezielle Softwarelösungen zur Verwaltung personenbezogener Daten eine eigene Userverwaltung.

Integrität

Zur Vermeidung unbefugter oder zufälliger Dateneingaben und -veränderungen sind die Rechner/der Netzwerkzugriff passwortgeschützt. Das Netzwerk ist durch eine Firewall gegen unbefugte Zugriffe aus dem Internet geschützt. Es erfolgt eine Datensicherung nach einem Datensicherungskonzept.

Verfügbarkeit

Die Datensicherung erlaubt die Wiederherstellung der Daten. Das gesicherte Netzwerk und relationale Datenbanken gewährleisten die Verfügbarkeit. Eine hohe Verfügbarkeit der Server ist durch den Einsatz von Raid-Systemen und USVs gewährleistet.

Authentizität

Durch die Aufgabenverteilung ist sichergestellt, dass personenbezogene Daten ihrem Ursprung nach zugeordnet werden können.

Revisionsfähigkeit

Die Zuständigkeit der Mitarbeitenden der Deutsche Rheuma-Liga Berlin e.V. sind geregelt. Ein Rollenkonzept bei den Zugriffsberechtigungen und individuelle Passwörter erlauben die Revision.

Transparenz

	Verzeichnis von Verarbeitungstätigkeiten gem. BDSG_DSGVO	Seite 7 von 8
--	---	---------------

Beschriebene und dokumentierte Datenprozesse und Datenbanken, protokollierte Netzwerkzugriffe und Berechtigungen, klare Befugnisse und Zuständigkeiten ermöglichen die transparente Datenverarbeitung.

8. Technik des Verfahrens einschließlich der eingesetzten Hard- und Software

Am Hauptstandort gibt es zentrale Server, die in einem gesicherten Serverraum stehen, zu dem nur der IT-Service Zutritt hat. Die Server sind durch Raid-Systeme gegen Datenverlust wegen Festplatten-Ausfalls geschützt. Die zentralen Server sind durch eine USV gegen Stromschwankungen geschützt.

Der Zugriff auf die PCs bzw. das Netzwerk und die Server ist nur mit einem Zugang (Benutzername/Passwort) möglich. Alle Mitarbeitenden, die die IT-Systeme nutzen sollen, bekommen einen persönlichen Zugang für die Anmeldung am PC/am Netzwerk und ein E-Mail-Konto. Die Mitarbeitenden sind darüber belehrt, dass Passwörter grundsätzlich nicht weitergegeben werden dürfen. Zugänge für Klienten haben grundsätzlich keinen Zugriff auf personenbezogene Daten.

Unternehmensinterne E-Mail (d.h. E-Mail innerhalb der Domain) gehen nicht unverschlüsselt über das Internet. Die Mitarbeitenden sind darüber belehrt, dass E-Mails mit personenbezogenen Daten nur End-to-End verschlüsselt gesendet werden dürfen.

Die Datenbestände von datenbankbasierten Anwendungen werden regelmäßig gesichert (Datensicherung der Anwendungssoftware). Alle zu sichernden Daten (inkl. der Datenbanksicherungen) werden nach einem Datensicherungskonzept (Mehrgenerationenprinzip) gesichert.

Alle PCs sind durch die Sicherheits-Software Sophos Endpoint Protection geschützt. Das Management der Antivirensoftware erfolgt auf einem zentralen Server. Betriebssystem und Anwendungssoftware auf den PCs sowie die Serversoftware werden regelmäßig aktualisiert.

Das Netzwerk ist durch eine Sophos Firewall gegen unerlaubte externe Zugriffe geschützt. Der interne Zugriff auf den Mailserver erfolgt über verschlüsselte Verbindungen (VPN). Der webbasierte Zugriff Mail über das Internet ist durch eine Verschlüsselung (https) geschützt, zusätzlich ist ein Zugang (Benutzername/Passwort) nötig.

Die Beratungsanliegen der Klienten werden durch die Sozialarbeitenden in einem geschützten Bereich der eigenen Vereinssoftware erfasst und sind nur für diese einsehbar. Der Klient wird auf diese Speicherung im Beratungsgespräch hingewiesen, widerspricht er, werden die Beratungsinhalte nicht erfasst und nicht gespeichert.

An Mitarbeitenden, die diese benötigen, werden Mobiltelefone/Smartphones für die dienstliche Nutzung ausgegeben. Bei der Ausgabe wird durch den Mitarbeiter eine Vereinbarung über die Überlassung und Nutzung eines Smartphone/Diensthandy unterzeichnet.

9. Fristen für die Sperrung und Löschung

Sämtliche Daten werden nach Wegfall der Notwendigkeiten der Speicherung der Daten gelöscht. Die Deutsche Rheuma-Liga Berlin e.V. ist auch zuwendungsfinanziert, daher gelten die jeweiligen Nachweispflichten aus der Landeshaushaltsordnung oder europäischer Vorgaben der Allgemeine Nebenbestimmungen für Zuwendungen zur Projektförderung die eine Speicherung von personenbezogene Daten zu Verwendungsnachweiszwecken erforderlich macht. Die Verarbeitung von Daten im Rahmen der Gesundheitsversorgung können den Aufbewahrungsregelungen der gesetzlichen Krankenversicherung SGB V unterliegen.

Im Folgenden sind die Fristen zur Löschung aufgeführt. Daten, die nicht im kund/innenbezogenen Prozess verwendet werden, werden zu Nachweiszwecken aufbewahrt und sind für andere Verwendungen gesperrt bis sie nach Wegfall der Nachweisverpflichtung gelöscht werden.

Lfd. Nr.	Löschfristen
1	5 Jahre nach Wegfall des Verwendungszweckes
2	24h nach Verlassen der Webseite gelöscht
3	nach Ausdruck gelöscht
4	nach Ausdruck gelöscht
5	2 Jahre nach Wegfall des Verwendungszwecks
6	Richtet sich nach den gesetzlichen Gegebenheiten des Sozialgesetzbuches und ist in der Datenschutzerklärung des Dienstleisters aufgeführt (s. www.dvz-gera.de/datenschutz.html)
7	Richtet sich nach den Vorgaben des Zuwendungsgebers (für Gesundheit zuständige Senatsverwaltung in Berlin) bzw. 10 Jahre.
8	nach Beendigung des Beschäftigungsverhältnis archiviert

Für alle Daten gelten die jeweils längeren Löschfristen, soweit diese durch Förderrichtlinien und/oder gesetzlichen Fristen und Nachweisfristen zwingend sind.

10. Datenübermittlung an Drittstaaten

Eine Datenübermittlung an ausländische Stellen findet nicht statt.

Bei der Nutzung von Google Analytics ist das Datenübermittlung an Google Inc.
(<https://www.google.de/intl/de/about/>) (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

11. Ergebnisse der Vorabkontrollen

Grundlage der Vorabkontrollen sind die vom Verantwortlichen für die IT vorgelegten Planungsunterlagen und eine Risikoabschätzung. Der Datenschutzbeauftragte führen die Vorabkontrollen durch. Das Ergebnis der Vorabkontrollen wird dokumentiert. Die Entscheidung über den Einsatz bzw. wesentliche Änderungen im automatisierten Verfahren erfolgt durch die Unterzeichnung des Freigabeprotokolls durch die Geschäftsführung.