Version 2.0
August 2022

DVMB
Das Netzwerk zur Selbsthilfe
Deutsche Vereinigung
Morbus Bechterew
Landesverband
Nordrhein-Westfalen e.V.

Datenschutzkonzept

gemäß Datenschutz-Grundverordnung (DS-GVO)

Deutsche Vereinigung Morbus Bechterew
Landesverband Nordrhein-Westfalen e.V.
Huckarder Str. 2 – 8
44147 Dortmund

Der DVMB Landesverband Nordrhein-Westfalen e.V. ist eine ehrenamtlich geführte Selbsthilfeorganisation, eingetragen im Vereinsregister Amtsgericht Köln unter VR 8874 / 84,
Gemeinnützigkeit anerkannt (Steuer-Nummer 314/5704/5217).

Inhaltlich Verantwortlicher gemäß § 55 Abs. 2 RStV: Peter de Beyer (Vorsitzender)

Inhalt

1. Präambel

Im Rahmen der Mitgliederbetreuung und Sportangebote, verarbeitet der Landesverband und seine Selbsthilfegruppen, in vielfacher Weise, personenbezogene Daten. Die Aufgaben und Ziele sind in der Satzung verbindlich festgelegt. Siehe (https://www.dvmb-nrw.de/wir/landesverband/satzung/).

Um die Vorgaben der EU-Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes zu erfüllen, Datenschutzverstöße zu vermeiden und einen einheitlichen Umgang mit personenbezogenen Daten innerhalb der Selbsthilfeorganisation zu gewährleisten, gilt für alle Verantwortliche in der DVMB Landesverband Nordrhein-Westfalen e.V., die erstellte „Datenschutz-Ordnung".
Wir verarbeiten „Auf rechtmäßiger Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbarer Weise", Daten.

Der Schutz Ihrer personenbezogenen Daten, ist uns ein großes Anliegen.

Alle Verantwortliche haben eine „Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes" abgegeben und werden regelmäßig zum Datenschutz unterwiesen.

2. Abgrenzung Datenschutzkonzept zum Datenschutzmanagementsystem

Das Datenschutzkonzept ist ein Dokument, welches die grundlegenden Prinzipien wiedergibt. Es soll dabei eine zentrale Rolle im Datenschutzmanagement spielen und kann als Zusammenfassung aller Maßnahmen zum Datenschutz gesehen werden. Es dient hauptsächlich dem Nachweis aller Rechenschafts- und Dokumentationspflichten gem. DS-GVO und ist damit ein praktisches Instrument für den Verantwortlichen.

Im Gegensatz dazu, ist das Datenschutzmanagementsystem (DSM) die Niederschrift der Umsetzung der DS-GVO und BDSG-neu. Als ein operatives Instrument (Datenschutz-Dokumentation), regelt es den laufenden Datenschutz mit Hilfe von Datenschutzprozessen nach festgelegten Vorgaben.

3. Einleitung

Dieses Datenschutzkonzept, beruht auf den in Art. 5 Absatz 1 DS-GVO formulierten Grundsätzen wie Zweckbindung, Datenminimierung, Speicherbegrenzung sowie Integrität, Recht auf Vergessenwerden, Vertraulichkeit und der Rechtmäßigkeit der Verarbeitung (Art. 6 DS-GVO).
Die von der DS-GVO geforderte Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 Absatz 2), die Verantwortung des Verantwortlichen (Art. 24 Absatz 1), der Einhaltung der Betroffenenrechte (Art. 13-20), der Meldepflicht bei Datenschutzverletzung (Art. 33-34) und der Nachweis-und Rechenschaftspflicht (Art 5. Absatz 2 und Art. 24 Absatz 1), ist gewährleistet.
Ein Kontroll-und Verbesserungsprozess wird mindestens 1x jährlich durchgeführt (Art. 32 Absatz 1), u.a. basierend auf der Checkliste, enthalten im letzten Kapitel dieses Datenschutzkonzeptes.

4. Tätig- und Verantwortlichkeiten

Als Selbsthilfeorganisation verarbeiten wir eine Vielzahl von (auch personenbezogenen) Daten, ganz oder teilweise automatisiert, um unsere Aufgaben und Pflichten gegenüber unseren Mitgliedern, Krankenkassen, Vertragspartnern, Dienstleistern, Behörden und sonstigen Dritten zu erfüllen. Die Geschäftsstelle, der Vorstand und die Selbsthilfegruppen befinden sich in der EU.

Verantwortliche Stelle im Sinne des Datenschutzgesetzes ist:

Deutsche Vereinigung Morbus Bechterew
Landesverband Nordrhein-Westfalen e.V.
Vorsitzender: Peter de Beyer
Huckarder Str. 2-8
44147 Dortmund

5. Datenschutzbeauftragter (DSB)

Die Verarbeitung besonders schutzwürdige Kategorien personenbezogene Daten nach Art. 9 Absatz 1 DS-GVO (Gesundheitsdaten), stellt eine Kerntätigkeit der Selbsthilfegruppen dar.
Zu dem hinwirken auf Einhaltung der Datenschutz-Grundverordnung (DS-GVO) und anderer Vorschriften wurde ein Vereinsdatenschutzbeauftragter von dem Vorstand bestellt:

Winfried Certa
Geschwister-Scholl-Str. 10
59379 Lüdinghausen

6. Weiterbildung des Datenschutzbeauftragten und Stand der Technik

- Für die regelmäßige Fort- und Weiterbildung nutzt der DSB in hohem Maße für seine Arbeit, Fachbücher und das Internet.
- Die Teilnahme an internen (vom Bundesverband) und externen Seminaren wird von DSB wahrgenommen.
- Der Austausch mit den Datenschutzbeauftragten der anderen Landesverbände in der DVMB, erfolgt bei Bedarf über Telefon, Internet und auf Veranstaltungen des Bundesverbandes.
- Die weitere interne Erarbeitung und auch Erprobung von Dokumenten zu den Themen im Datenschutz, wird im eingerichteten Arbeitskreis Datenschutz, besprochen.

7. Sensibilisierung der Mitglieder / Mitarbeiter und Dienstleister

Besonders wichtig. ist die Sensibilisierung aller relevanten Mitglieder / Mitarbeiter und Dienstleister. Nur mit informierten und achtsamen Mitarbeitenden können Sicherheitsmaßnahmen wirksam umgesetzt und eventuelle Sicherheitsvorfälle rechtzeitig erkannt werden. Sobald die Ursache eines Sicherheitsvorfalls identifiziert wurde, müssen Maßnahmen zu dessen Behebung ergriffen, und dokumentiert werden.

Die jährlich stattfindenden Datenschutzschulungen bei den Arbeitstreffen, ist ein fester Bestandteil des Datenschutzmanagements. Hierbei werden durch den Datenschutzbeauftragten aktuelle Themen und wichtige Updates aus dem Datenschutz an die Mitglieder / Mitarbeiter geschult. Zur Lernkontrolle, diskutiert der DSB die Themen in der Schulung und beantwortet Rückfragen der Teilnehmer. In dem Schulungsnachweis bestätigen die Teilnehmer mit ihrer Unterschrift, dass sie teilgenommen und den Inhalt verstanden haben.

8. Datenverarbeitungen / Datenverarbeitungszwecke

Die DVMB LV NRW e.V. ist als Selbsthilfeorganisation nach Art. 30 der Datenschutz-Grundverordnung (DS-GVO) verpflichtet, ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Dieses ist, auf Anfrage der Landesbeauftragte für Datenschutz und Informationsfreiheit NRW (LDI), zur Verfügung zu stellen.

Die Beschreibung der Geschäftsprozesse (Verarbeitungstätigkeiten), ist in drei Gruppen unterteilt:

1. Für den Vorstand / Vorstandschaft und Geschäftsstelle wurden die Tätigkeiten: Mitgliederverwaltung, Büroorganisation, Öffentlichkeitsarbeit, E-Mailverarbeitung, Finanzbuchhaltung, Weiterbildung Kassierer, Lohn- u. Gehaltszahlungen, Weiterbildung Gruppensprecher, Internetbetreuung, Einkauf, Redakteur, Datenschutzorganisation, ermittelt.
2. Für die Selbsthilfegruppen wurden die Tätigkeiten: Mitgliederverwaltung, Büroorganisation, E-Mailverarbeitung, Kassierer, Abrechnung mit Krankenkassen, ermittelt.
3. Für die Nutzer der Internetseiten des Landesverbandes (https://www.dvmb-nrw.de) und der Selbsthilfegruppen ist eine umfangreiche Datenschutzerklärung aufgeführt.

9. Datenschutz-Folgenabschätzung / Risikobeurteilung

Der Datenschutz – Folgenabschätzung ist die sogenannte Schwellwertanalyse vorangestellt, mittels der ermittelt wird, ob eine Datenverarbeitung grundsätzlich einem hohen Risiko unterliegt.

Als Grundlage für die Risikoanalyse dient das Verarbeitungsverzeichnis der Verarbeitungstätigkeiten Verantwortlicher nach Art. 30 DS-GVO. In der Risikobeurteilung wurden bei jeder Verarbeitungstätigkeit, der Grad der Schwere / des Schadens und der Grad Eintrittswahrscheinlichkeit, folgenden Punkte ermittelt:

1. Wie hoch ist der Schutzbedarf? Wie sensibel sind die Daten für den Betroffenen?
2. Wie hoch ist die Eintrittswahrscheinlichkeit? Wie interessant sind die Daten überhaupt für einen Dritten (z.B. Hacker)?

Wer personenbezogene Daten verarbeitet, ist nach der DS-GVO verpflichtet, im Verhältnis zum Risiko nach dem Stand der Technik angemessene (nicht, neueste und teuerste) Maßnahmen zum Schutz der Daten zu ergreifen, diese regelmäßig zu überprüfen und erforderlichenfalls upzudaten.

Einem hohen Risiko unterliegen, lt. Datenschutzgruppe Artikel 29, vertrauliche oder höchst persönliche Daten (besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DS-GVO).

Bei den Abrechnungen mit den Krankenkassen werden besondere Kategorien personenbezogener Daten (Gesundheitsdaten) verarbeitet. Der Personenkreis, der die Daten verarbeitet, wird regelmäßig unterwiesen. Auf der Unterschriftenliste bei dem Reha-Sport, werden aus Datenschutzgründen (Kenntnisnahme von Dritte), die personenbezogenen Daten erst bei der Abrechnung komplett eingetragen. Die ärztlichen Verordnungen (Rezepte) sind grundsätzlich bei der Gruppenleitung deponiert.

Die Online-Datenübermittlung zu den Abrechnungsstellen der Krankenkassen erfolgt mittels TAN. Die Handhabung entspricht der Vorgehensweise wie bei Electronic Banking. Einzureichende Papierunterlagen an die Abrechnungsstellen oder Krankenkassen, werden per Einwurfeinschreiben verschickt.

ERGEBNIS: Das Risiko = Schwere x Eintritt, ist als noch vertretbar einzustufen.
Es ist keine Datenschutz – Folgenabschätzung erforderlich.

10. Beschreibung der technisch-organisatorischen Maßnahmen (TOM´s)

Die EU-Datenschutzgrundverordnung (DS-GVO) stellt hohe Anforderungen an den Schutz personenbezogener Daten. Um die Sicherheit dieser Daten zu gewährleisten, verlangt die DS-GVO von Unternehmen und auch Vereine, dass sie **technische und organisatorische Maßnahmen (TOM)** ergreifen. Hierzu gehören unter anderem folgende Maßnahmen:

1. Gewährleistung der Vertraulichkeit
2. Gewährleistung der Integrität (Korrektheit der Daten und korrekte Funktionsweise der Systeme)
3. Gewährleistung der Verfügbarkeit
4. Gewährleistung der Belastbarkeit der Systeme
5. Wiederherstellung der Verfügbarkeit der Daten
6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM

In dieser Checkliste finden Sie konkrete Maßnahmen, die getroffen wurden, um die Anforderungen der DS-GVO zu erfüllen. Die Maßnahmen in der rechten Tabellenspalte sind die Vorgaben der DVMB LV NRW e.V. Abweichende Maßnahmen aus der Musterliste, sind durch den Zusatzpunkt ☒ …, ergänzt.

1. Gewährleistung der Vertraulichkeit

Es soll durch geeignete Maßnahmen sichergestellt werden, dass personenbezogene Daten nur einem **bestimmten Empfängerkreis zugänglich** sind.

Zutrittskontrolle: *Maßnahmen, mit denen Sie verhindern, dass Unbefugte Zutritt zu Datenverarbeitungsanlagen haben, mit denen personenbezogene Daten verarbeitet oder genutzt werden.*	☒ manuelles Schließsystem ☒ Schließsystem mit Sicherheitsschlössern ☒ Schlüsselregelung für Beschäftigte ☒ Personenkontrolle am Empfang ☒ Verschließen der Türen bei Abwesenheit ☒ … Büroräume der Geschäftsstelle dürfen nur mit Begleitung betreten werden. Anwesenheit nach Geschäftsschluss durch berechtigte DVMB-Mitglieder wird protokolliert. Mitglieder des Vorstandes und der Ortsgruppen haben ihr Büro in häuslicher Wohnung. Es wird durch sie sichergestellt, dass Türen und Fenster geschlossen sind, wenn sie nicht zu Hause sind.
Zugangskontrolle: *Maßnahmen, mit denen Sie verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.*	☒ Einsatz von Benutzerprofilen mit unterschiedlichen Berechtigungen ☒ Pflicht zur Passwortnutzung ☒ Authentifikation durch Benutzername und Passwort ☒ … Aufgrund minimaler Infrastruktur und überwiegend dezentraler Datenhaltung, besteht eine geringe Anforderung an IT-Systemen im Landesverband und Ortsgruppen. Es gibt nur einen Server für den E-Mail Account. IT-Systeme beinhalten überwiegend Einzelplatzrechner mit ihren Peripheriegeräten.
Zugriffskontrolle: *Maßnahmen, mit denen Sie gewährleisten, dass nur berechtigte Personen auf die entsprechenden Daten zugreifen können, und dass diese nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.*	☒ Nutzer-Berechtigungskonzept ☒ Passwortrichtlinie ☒ ordnungsgemäße Vernichtung von Datenträgern ☒ Einsatz von Aktenvernichtern ☒ Inanspruchnahme von Dienstleistern zur Datenvernichtung (inkl. Protokollierung der Vernichtung) ☒ Aufbewahrung von Datenträgern in abschließbaren Schränken ☒ Aufbewahrung von Aktenordnern in abschließbaren Schränken ☒ … Falls eine zweite Person den Rechner benutzt muss eine eigene Berechtigung (Account) zu ihren verarbeitenden Daten eingerichtet werden. Sie muss sich mit eigenem Passwort anmelden. Es dürfen keine sensitiven Unterlagen, wie z.B. Mitgliederlisten, offen liegen. Für die Nutzung von Passwörter ist eine separate Regelung „Regeln zur Nutzung von Passwörter bei der DVMB LV NRW e.V.“ erstellt.

Trennungsgebot: *Maßnahmen, durch die Sie gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.*	☒ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern ☒ Festlegung von Datenbankrechten durch Vorgaben im Berechtigungskonzept ☒ Trennung von Produktiv- und Testsystem ☒ … Die Trennung der Mitgliederdaten von Kontodaten ist durch die Auswechselbarkeit der Datenträger (CD, DVD, USB-Stick und ext. Festplatte zu gewährleisten.
Auftragskontrolle: *Maßnahmen, durch die Sie gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.*	☒ sorgfältige Auswahl des Auftragnehmers (Überprüfung des Dienstleisters) ☒ vorherige Prüfung und Dokumentation der beim Auftragnehmer existierenden TOMs ☒ schriftliche Vereinbarung mit dem Auftragnehmer ☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit ☒ Datenschutzbeauftragter beim Auftragnehmer ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags ☒ vertraglich festgelegte Kontrollrechte gegenüber dem Auftragnehmer ☒ regelmäßige Überprüfung des Auftragnehmers und seiner Tätigkeiten ☒ vertraglich festgelegte Vertragsstrafen bei Verstößen ☒ … Die Weitergabe von besondere Kategorien personenbezogenen Daten, erfolgt ausschließlich zur Leistungsabrechnung mit den Krankenkassen. Soweit möglich werden die Daten online über sichere Internetseiten, per E-Mail verschlüsselt, oder unverschlüsselt per Post (Einwurfeinschreiben) an den Empfänger übertragen.
Pseudonymisierung:	☒ Nutzung von pseudonymisierten Daten bei Datenübermittlung an externe Dienstleister ☒ getrennte Aufbewahrung von pseudonymisierten Daten und Zusatzinformationen ☒ … Die Mitgliederdaten vom Bundesverband sind mit Nummern versehen. Die Ortsgruppen haben die Möglichkeit, mit diesen Personennummern, anstelle der Namen zu arbeiten.

Verschlüsselung:	☒ Nutzung von Windows 10 Bitlocker ☒ Verschlüsselung von E-Mail-Inhalten (S/MIME, PGP o. ä.) ☒ Verschlüsselung der Website (SSL/TLS) ☒ … Wer nicht die Möglichkeit einer Verschlüsselung hat, ist angewiesen die Daten per Post zu versenden.

2. Gewährleistung der Integrität

Es soll durch geeignete Maßnahmen sichergestellt werden, dass die **Korrektheit** von personenbezogenen Daten und die korrekte Funktionsweise von Systemen gewährleistet wird.

Eingabekontrolle: *Maßnahmen, mit denen Sie gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt wurden.*	☒ individuelle Benutzernamen für Nutzer ☒ sichere Aufbewahrung von Papierunterlagen ☒ Nachvollziehbarkeit durch Berechtigungskonzept ☒ … Mitarbeiter sind verpflichtet, stets mit ihre eigenen Accounts/Passwort zu arbeiten. Diese Berechtigung darf nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.
Weitergabekontrolle: *Maßnahmen, mit denen Sie gewährleisten, dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können – sei es bei der elektronischen Übertragung, während ihres Transports oder ihrer Speicherung auf Datenträger.*	☒ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form (wenn möglich) ☒ verschlüsselte E-Mail-Übertragung (SSL/TLS) ☒ Verschlüsselung der E-Mail-Inhalte ☒ Verschlüsselung der E-Mail-Übertragung (durch Provider) ☒ vertraglich vereinbarte Rechte und Pflichten in Bezug auf die Datenweitergabe ☒ festgelegte Löschfristen ☒ sichere Transportverpackungen ☒ Nutzung von mobilen Datenträgern mit Verschlüsselungsfunktion ☒ Regelungen zum sicheren Transport von Datenträgern ☒ … Personenbezogene Daten (Mitgliederlisten) dürfen nur verschlüsselt übersendet werden. Alle Mitglieder /Mitarbeiter sind zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

3. Gewährleistung der Verfügbarkeit

Es soll durch geeignete Maßnahmen sichergestellt werden, dass **EDV-Systeme** die an sie gestellten Anforderungen **zuverlässig** erfüllen.

Verfügbarkeitskontrolle: *Maßnahmen, durch die Sie gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.*	☒ Schutzsteckdosenleisten für EDV-Geräte ☒ Datensicherungskonzept ☒ regelmäßiges Testen der Funktionsweise der Datensicherung ☒ regelmäßiges Testen der Rückspielbarkeit der Daten aus der Datensicherung ☒ Notfallkonzept ☒ Aufbewahrung von Datensicherung an sicherem, ausgelagertem Ort ☒ … Die Mitgliederdaten werden vierteljährlich verschlüsselt vom Bundesverband geschickt.

4. Gewährleistung der Belastbarkeit der Systeme

Durch geeignete Maßnahmen soll die Belastbarkeit der EDV-Systeme sichergestellt werden, so dass diese etwaige Software-Mängel, eine erhöhte Anzahl von Anfragen sowie Angriffe durch Viren, sonstige Malware oder Hacker etc. abwehren können.

Belastbarkeit der IT-Systeme:	☒ Antiviren-Software ☒ Software-Firewall ☐ …

5. Wiederherstellung der Verfügbarkeit

Es soll durch geeignete Maßnahmen sichergestellt werden, dass nach einem Systemfehler oder einem Ausfall des Systems die **Funktionsfähigkeit so schnell wie möglich wiederhergestellt** werden kann.

Wiederherstellbarkeit von IT-Systemen:	☒ Datensicherungen / Backups ☒ sorgfältig ausgewählter IT-Dienstleister ☒ … Datensicherung von Dateien ist monatlich auf externem Datenträger durchzuführen. Die Aufbewahrung der Sicherungskopien hat in einem abgeschlossenen Schrank, in einem separate Raum zu erfolgen.

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM

Es soll durch geeignete Maßnahmen sichergestellt werden, dass der Stand der **Informations-sicherheit regelmäßig geprüft und aktualisier**t wird, und dass dies auch dokumentiert wird.

Informations-Sicherheits-Management-System (ISMS):	☒ regelmäßige Prüfung der TOMs (mind. 1x jährlich) durch Vorsitzenden und dem Arbeitskreis Datenschutz zusammen mit Datenschutzbeauftragten ☒ Einsatz Datenschutzchecklisten (Information Security Management System) ☒ … Es ist ein Datenschutz- und Informationssicherheits- Team (Arbeitskreis Datenschutz) eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt.

11. Impressum und Datenschutzerklärungen

Auf den (DS-GVO – konform) betriebenen Webseiten des Landesverbandes NRW und den Selbsthilfegruppen, sind das Impressum und die Datenschutzerklärung, unter folgen Links zu erreichen:

- https://www.dvmb-nrw.de/datenschutz/
- https://www.dvmb-nrw.de/impressum/
- https://www.dvmb-nrw.de/gruppen/*Gruppenname*/metanavigation/datenschutz/
- https://www.dvmb-nrw.de/gruppen/*Gruppenname*/metanavigation/impressum/

12. Betroffenenrechte wahren

Grundsätzlich stellen wir jedem neuen Mitglied in der Selbsthilfegruppe und auch den Teilnehmern von Rehasport, in dem Infoblatt Datenschutz und der Einwilligungserklärung zum Reha-Sport, ihre Rechte in Papierform zur Verfügung. Für alle Nutzer bzw. Betroffenen, steht die jeweils aktuelle Version ihrer Rechte auf der Website im Kapitel 6, „Ihre Rechte“ auf unserer Homepage im Sinne von Transparenz und Vertrauen zum Download bereit. Siehe (https://www.dvmb-nrw.de/datenschutz/).

- Auskunftsrecht nach Artikel 15 DSGVO
- Recht auf Berichtigung nach Artikel 16 DSGVO
- Recht auf Löschung nach Artikel 17 DSGVO
- Recht auf Einschränkung nach Artikel 18 DSGVO
- Recht auf Datenübertragbarkeit nach Artikel 20 DSGVO
- Recht auf Widerspruch nach Artikel 21 DSGVO
- Recht auf Widerrufsrecht nach Artikel 7 Absatz 3 DSGVO
- Recht auf Beschwerde nach Artikel 77 DSGVO

12.1. Betroffenenrechte: Prozessketten

Betroffene Personen haben das Recht Auskunft über ihren verarbeiteten personenbezogenen Daten zu verlangen (Art. 15 DSGVO). Daneben haben die betroffenen Personen ein Recht auf Löschung, Sperrung und Berichtigung (Art. 16 und 17 DSGVO).

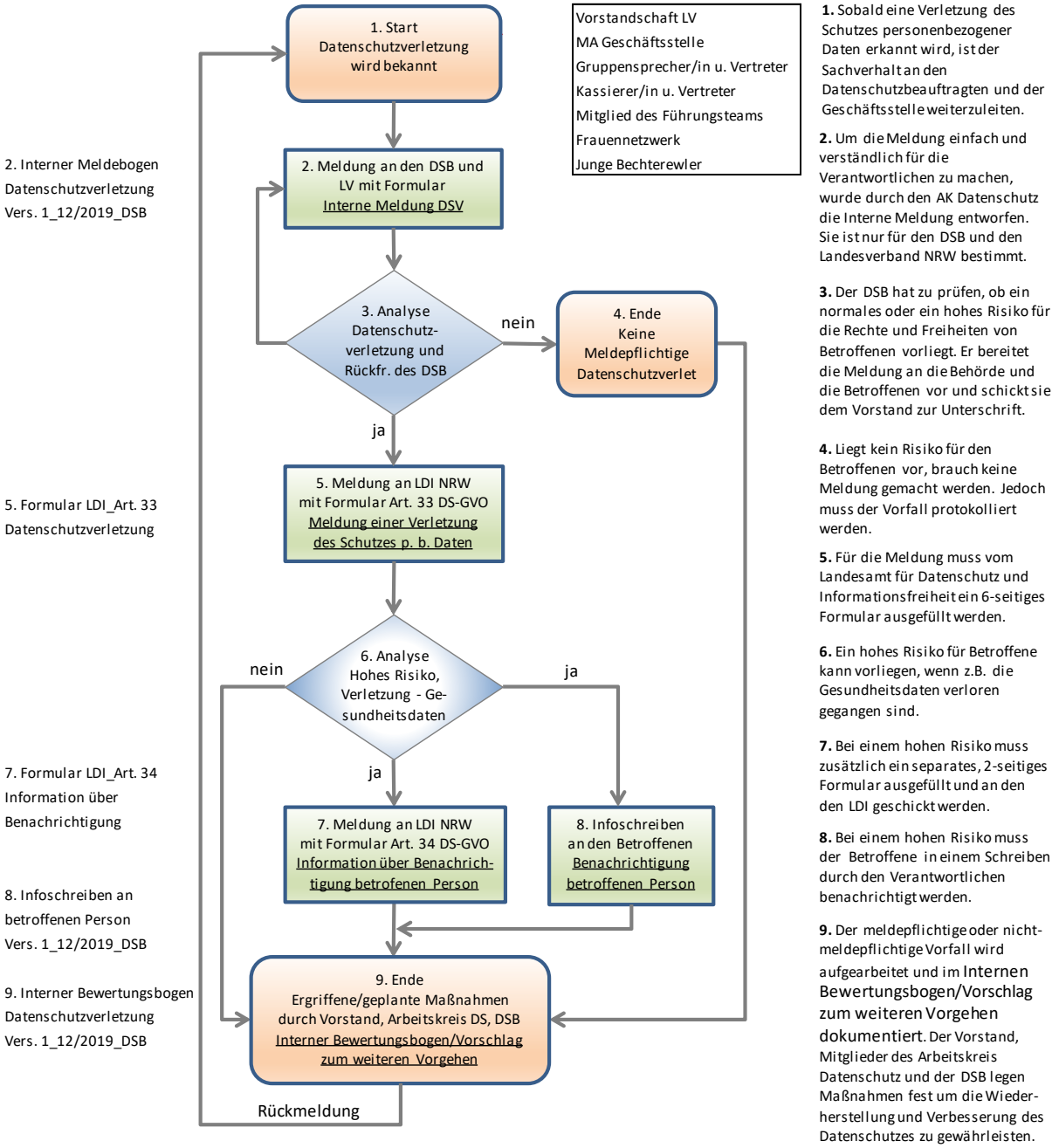
Die Anfragen (Auskunftsverlangen) von Mitglieder / Betroffene, werden an die Geschäftsstelle weitergeleitet und von dort aus, schriftlich, zusammen mit der zuständigen Selbsthilfegruppe, in einem vorbereiteten Schreiben beantwortet.

12.2. Meldung von Datenschutzverletzungen: Prozessketten

Um den Melde- bzw. Informationspflichten nachkommen zu können, ist in der Deutschen Vereinigung Morbus Bechterew Landesverband Nordrhein-Westfalen e.V. ein Prozess implementiert. Sobald die Verletzung des Schutzes personenbezogenen Daten erkannt wird, ist der Sachverhalt an den Datenschutzbeauftragten und den Landesverband weiterzuleiten. Der Datenschutzbeauftragte bewertet den Sachverhalt und prüft, ob ein normales oder ein hohes Risiko für die Rechte und Freiheiten von Betroffenen vorliegt (bzw. ob überhaupt ein Risiko vorliegt).

Vorgehen bei einer Verletzung des Schutzes personenbezogener Daten (Art. 33 DS-GVO)

Dokument	Flussdiagramm	Verantwortliche	Bemerkung



2. Interner Meldebogen Datenschutzverletzung Vers. 1_12/2019_DSB

5. Formular LDI_Art. 33 Datenschutzverletzung

7. Formular LDI_Art. 34 Information über Benachrichtigung

8. Infoschreiben an betroffenen Person Vers. 1_12/2019_DSB

9. Interner Bewertungsbogen Datenschutzverletzung Vers. 1_12/2019_DSB

Vorstandschaft LV
MA Geschäftsstelle
Gruppensprecher/in u. Vertreter
Kassierer/in u. Vertreter
Mitglied des Führungsteams
Frauennetzwerk
Junge Bechterewler

1. Sobald eine Verletzung des Schutzes personenbezogener Daten erkannt wird, ist der Sachverhalt an den Datenschutzbeauftragten und der Geschäftsstelle weiterzuleiten.

2. Um die Meldung einfach und verständlich für die Verantwortlichen zu machen, wurde durch den AK Datenschutz die Interne Meldung entworfen. Sie ist nur für den DSB und den Landesverband NRW bestimmt.

3. Der DSB hat zu prüfen, ob ein normales oder ein hohes Risiko für die Rechte und Freiheiten von Betroffenen vorliegt. Er bereitet die Meldung an die Behörde und die Betroffenen vor und schickt sie dem Vorstand zur Unterschrift.

4. Liegt kein Risiko für den Betroffenen vor, brauch keine Meldung gemacht werden. Jedoch muss der Vorfall protokolliert werden.

5. Für die Meldung muss vom Landesamt für Datenschutz und Informationsfreiheit ein 6-seitiges Formular ausgefüllt werden.

6. Ein hohes Risiko für Betroffene kann vorliegen, wenn z.B. die Gesundheitsdaten verloren gegangen sind.

7. Bei einem hohen Risiko muss zusätzlich ein separates, 2-seitiges Formular ausgefüllt und an den den LDI geschickt werden.

8. Bei einem hohen Risiko muss der Betroffene in einem Schreiben durch den Verantwortlichen benachrichtigt werden.

9. Der meldepflichtige oder nicht-meldepflichtige Vorfall wird aufgearbeitet und im Internen Bewertungsbogen/Vorschlag zum weiteren Vorgehen dokumentiert. Der Vorstand, Mitglieder des Arbeitskreis Datenschutz und der DSB legen Maßnahmen fest um die Wiederherstellung und Verbesserung des Datenschutzes zu gewährleisten.

Die Dokumente lassen sich über die Kachel öffnen

13. Checkliste für den jährlichen Kontroll-und Verbesserungsprozess

Die folgende Checkliste bezieht sich auf die aktuellen **T**echnischen und **O**rganisatorischen **M**aßnahmen zum Schutz personenbezogener Daten. Sie dient als Umsetzungshilfe für die Prüfung und Dokumentation des Umsetzungszustandes der Sicherheitsmaßnahmen der TOM. Ebenso ist sie der Nachweis der Bemühungen zur Umsetzung der IT-Sicherheit für die DVMB Landesverband NRW e.V.

Nr.	Frage	Bemerkung	OK
	1. Gewährleistung der Vertraulichkeit		
1.	Sind Türen und Fenster im „Büro“ der häuslichen Wohnung verschlossen, wenn verantwortlichen Gruppenmitglieder nicht zu Hause sind?		☐
2.	Werden die Büros mit Publikumsverkehr nur in Begleitung, oder durch berechtigte DVMB-Mitglieder betreten?		☐
3.	Befinden sich in Büros mit Publikumsverkehr, Aktenordner und Datenträger mit personenbezogenen Daten in abschließbaren Schränken?		☐
4.	Werden bei der Benutzung des PC, zur Authentifikation (Nachweis der Identität) Benutzername und Passwort genutzt?		☐
5.	Werden bei der Benutzung des PC von mehreren Personen, unterschiedliche Berechtigungen (Benutzername und Passwort) genutzt?		☐
6.	Besteht eine schriftliche Vereinbarung mit dem Auftragnehmer, z.B. bei Abrechnung Rehasport mit den Abrechnungsstellen der KK?		☐
7.	Sind die genehmigten Anträge auf Kostenübernahme der Krankenkassen, nur bei berechtigte Personen (Gruppenleitung) aufbewahrt?		☐
8.	Werden für die Abrechnung mit den Krankenkassen, die Unterschriftenlisten nur mit Name versehen, zum Rehasport mitgenommen?		☐
9.	Werden die besondere personenbezogene Daten, den KK zur Abrechnung verschlüsselt, oder per Post (Einwurfeinschreiben) übertragen?		☐
10.	Werden E-Mails und Inhalte mit personenbezogenen Daten verschlüsselte, oder wenn nicht möglich, die Dokumente per Post versendet?		☐
11.	Ist bei allen Mobiltelefonen/Smartphones die Eingabe der Geräte-PIN aktiviert?		☐
	2. Gewährleitung der Integrität		
12.	Sind mobile Datenträger mit personenbezogenen Daten z.B. USB-Stick verschlüsselt, oder wenn nicht möglich, verschlossen aufbewahrt?		☐
13.	Haben alle Mitglieder, die mit personenbezogenen arbeiten, eine Verpflichtungserklärung zum Datenschutz abgegeben?		☐
14.	Werden die Löschfristen für personenbezogene Daten (max. 10 Jahre), für die verschiedenen Datenkategorien jährlich geprüft u. eingehalten?		☐
	3. Gewährleistung der Verfügbarkeit		
15.	Wird zum Verlust oder Schutz von personenbezogenen Daten, die Funktionsweise der Datensicherung regelmäßig getestet?		☐
	4. Gewährleistung der Belastbarkeit der Systeme		
16.	Sind auf dem PC automatische Updates, eine Bildschirmsperre eingerichtet und ist eine Firewall, ein Virenschutzprogramm installiert?		☐
	5. Wiederherstellung der Verfügbarkeit		
17.	Werden monatlich Datensicherungen/Backups auf einem externen Datenträger durchgeführt und an einem separaten Ort aufbewahrt?		☐

Hinweis:
Falls eine Maßnahme nicht zutrifft, ist bei Bemerkung: „Nicht zutreffend“ einzutragen oder zu streichen.
Der mögliche Verbesserungsbedarf ist auf einem zusätzlichen Blatt zu beschreiben.

Datum, Ort Unterschrift Gruppe

14. Zusammenfassung

Wir sehen das hier dokumentierte Datenschutzniveau mit den gesetzten TOM´s für uns als Selbsthilfeorganisation auch aufgrund unserer finanziellen, technischen und organisatorischen Beschränkungen als angemessen und ausreichend an.
Wir können also mit guten Gewissen sagen:

Liebe Mitglieder, Beschäftigte, Interessenten!

Vertrauen ist die Grundlage und Voraussetzung für unsere Beratungs- und Selbsthilfeleistungen. Daher sind auch alle Ihre persönlichen, beruflichen und Gesundheitsdaten bei uns in guten Händen.

Wir sichern Ihnen zu, dass wir sorgsam und streng vertraulich damit umgehen und unsere Datenschutzmaßnahmen immer auf den aktuellen Gesetzesstand entsprechend und unsere Soft- und Hardware stets auf dem aktuellen Stand sind.

Darauf können Sie vertrauen.

26.08.2022, Dortmund _____

Datum, Ort Unterschrift

Hinweis: Ein Original dieses Datensicherheitskonzepts mit Unterschrift ist in unserem Archiv abgelegt

Änderungshistorie

- 28.08.2021, Erstellung Dokument
  Vers. 1_2021_08_28

- 26.08.2022, Anpassung der „Checkliste für den jährlichen Kontroll- und Verbesserungsprozess“, auf die aktuellen Technischen Organisatorischen Maßnahmen
  Vers. 2_2022_08_26

Anhang

- Verpflichtung zur Wahrung der Vertraulichkeit
  und zur Beachtung des Datenschutzes

- Meldung einer Verletzung des Schutzes
  personenbezogener Daten (Art. 33 DS-GVO)

Verpflichtung zur Wahrung der Vertraulichkeit
und zur Beachtung des Datenschutzes

Gültigkeit mit Anwendbarkeit der DSGVO ab 25. Mai 2018

DVMB
Das Netzwerk zur Selbsthilfe
Deutsche Vereinigung
Morbus Bechterew
Landesverband
Nordrhein-Westfalen e.V.

☐ Vorstandschaft	☐ MA Geschäftsstelle
☐ Gruppensprecher/innen	☐ stv. Gruppensprecher/in
☐ Ansprechpartner/innen	☐ stv. Ansprechpartner/in
☐ Mitglied des Führungsteams	☐ Kassierer/in
☐ Frauennetzwerk	☐ Junge Bechterewler

(Bitte deutlich in Druckschrift schreiben)

Örtliche Gruppe: .....

Vor- und Nachname: .....

Straße und Hausnummer: .....

PLZ und Wohnort: .....

Telefonnummer zur Veröffentlichung: ..... /. .....

E-Mail: ..... Geburtsdatum .....
Freiwillige Angabe

Sehr geehrtes DVMB Mitglied,

da Sie im Rahmen Ihrer Tätigkeit möglicherweise mit personenbezogenen Daten in Kontakt kommen, verpflichte ich Sie hiermit zur Beachtung des Datenschutzes, insbesondere zur Wahrung der Vertraulichkeit.

Ihre Verpflichtung besteht umfassend. Sie dürfen personenbezogene Daten selbst nicht ohne Befugnis verarbeiten und Sie dürfen anderen Personen diese Daten nicht unbefugt mitteilen oder zugänglich machen.

Unter einer Verarbeitung versteht die EU-Datenschutz-Grundverordnung (DSGVO) jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

„Personenbezogene Daten“ im Sinne der DSGVO sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Ihre Verpflichtung besteht ohne zeitliche Begrenzung und auch nach Beendigung Ihrer Tätigkeit fort.

Unter Geltung der DSGVO können Verstöße gegen Datenschutzbestimmungen nach § 42 DSAnpUG-EU (BDSG-neu) sowie nach anderen Strafvorschriften mit Freiheits- oder Geldstrafe geahndet werden. Datenschutzverstöße können zugleich eine Verletzung ehren- oder hauptamtliche Pflichten bedeuten und entsprechende Konsequenzen haben.

Datenschutzverstöße sind ebenfalls mit möglicherweise sehr hohen Bußgeldern für die Selbsthilfegruppe bedroht, die gegebenenfalls zu Ersatzansprüchen Ihnen gegenüber führen können.

Ein unterschriebenes Exemplar dieses Schreibens reichen Sie bitte an die Geschäftsstelle des Landesverbandes zurück.

Dortmund, im Mai 2018

Für den Vorstand des Landesverbandes Nordrhein-Westfalen e.V.

gez.

Peter de Beyer
Vorsitzender

Über die Verpflichtung auf das Datengeheimnis und die sich daraus ergebenden Verhaltensweisen wurde ich unterrichtet. Das Merkblatt zur Verpflichtungserklärung mit dem Abdruck der hier genannten Vorschriften habe ich erhalten.

Ort, Datum Unterschrift des Verpflichteten

Merkblatt zum Datengeheimnis

Art. 4 DSGVO Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;
2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

Strafvorschriften des § 42 DSAnpUG-EU (BDSG-neu)

(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,

3. ohne hierzu berechtigt zu sein, verarbeitet oder
4. 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) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.

Meldung einer Verletzung des Schutzes personenbezogener Daten (Art. 33 DS-GVO)

DVMB
Das Netzwerk zur Selbsthilfe
Deutsche Vereinigung
Morbus Bechterew
Landesverband
Nordrhein-Westfalen e.V.

2. Meldende Person, Funktion, Name Anschrift

(DVMB Gruppe xxx, DVMB Vorstandsmitglied, DVMB Mitarbeiter/in)

_____

_____

Um die Meldefrist von 72 Stunden nicht zu überschreiten (Art. 33 Abs.1), soll möglichst nach bekanntwerden der Verletzung die Meldung per E-Mail und/oder Telefon an den Datenschutzbeauftragten des DVMB Landesverbandes Nordrhein-Westfalen erfolgen:

Winfried Certa
Geschwister-Scholl-Str. 10
59348 Lüdinghausen
Tel.: 02591 792910
E-Mail: winfried.certa@dvmb-nrw.de

(bitte immer auch unverzüglich eine Kopie an den Vorstand des Landesverbandes Nordrhein-Westfalen senden: Geschäftsstelle des Landesverbandes NRW, Huckarder Str. 2 - 8, 44147 Dortmund)

Ein Datenschutzverstoß kann an vielen Stellen, von jedem Mitglied in der DVMB und zu jeder Zeit passieren. Dementsprechend müssen alle wissen, was in einem solchen Fall zu tun ist. Der/die Gruppensprecher/in, Mitglied des Führungsteams usw., melden den Vorfall an den Datenschutzbeauftragten. Der DSB hat nun die Aufgabe, alle notwendigen Informationen zusammenzutragen und den Fall dem Verantwortlichen (Vorstand) zu melden. Parallel werden sofort Maßnahmen ergriffen um den Datenverstoß zu stoppen, sofern er noch im Verlauf ist.

Diese Meldung ist nur für den Datenschutzbeauftragten und der DVMB Landesverband NRW e.V. bestimmt. Der DSB überträgt hieraus die Daten auf das Formular der Datenschutzbehörde, wenn die Verletzung zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

4. Weitere an der Verletzung des Schutzes personenbezogener Daten Beteiligte

Sind an der Verletzung des Schutzes personenbezogener Daten, Dritte beteiligt?

☐ **ja** ☐ **nein**

Rolle des Dritten im Rahmen der Verarbeitung _____

Kontaktdaten des Dritten: _____

_____

Dritte sind Personen außerhalb der DVMB Landesverband NRW e.V. Das könnten z.B. Auftragsverarbeiter (Abrechnungsstellen mit den Krankenkassen) oder gemeinsamer Verantwortlicher, z.B. Bundesverband (Verwaltung der Mitgliederliste) sein.
Auftragsverarbeiter unterliegen keine Meldepflicht. Sie sind aber verpflichtet, denjenigen zu unterstützen, der sie beauftragt hat und deshalb meldepflichtig ist.

5. Informationen zur Verletzung des Schutzes personenbezogener Daten

A1) Zeitpunkt/ -raum der Verletzung des Schutzes personenbezogener Daten *(Beginn des Verstoßes)* **Datum**_____ **Uhrzeit**_____

A2) Zeitpunkt des Bekanntwerdens der Verletzung des Schutzes personenbezogener Daten **Datum**_____ **Uhrzeit**_____

A3) Begründung der Verzögerung, falls Meldung nicht binnen 72 Stunden erfolgt (Art.33 Abs.1)

_____

_____

B1) Die Verletzung des Schutzes personenbezogener Daten wurden beseitigt ☐ **ja** ☐ **nein**

B2) Wie wurde die Verletzung des Schutzes personenbezogener Daten bekannt (*festgestellt*)?

_____

_____

C1) Zeitpunkt der Benachrichtigung durch Dritte (z.B. Auftragsverarbeiter)

☐ **siehe Anlage** _____ **Datum**_____ **Uhrzeit**_____

D1) Art der Verletzung des Schutzes personenbezogener Daten (Art.33 Abs.3 lit. a,Art.4 Nr.12)

☐ **Vernichtung** ☐ **Verlust** ☐ **Veränderung** ☐ **Unbefugter Zugang**

Erläuterung zum Verstoß *(z.B. personenbezogene Daten gelöscht, Mitgliederlisten in Turnhalle vergessen, personenbezogene Daten ohne Kopie verändert, Post, E-Mail an falscher Adresse)*:

_____

_____

E1) Kategorien betroffener Daten (Art. 33 Abs. 3 lit. a)

Welche personenbezogenen Daten sind betroffen? *(bitte benennen)*

_____

_

Personenbezogene Daten sind sehr vielfältig. Beispiele, die in den Gruppen zutreffen können: Besondere Kategorie personenbezogener Daten (Gesundheitsdaten), Identität von Betroffenen (Vorname, Nachname, Geburtsdaten, Familienstand), Kontaktdaten (Telefon, E-Mail- und Postadressen, Rundschreiben nicht an BCC-Adresse), Daten zur Struktur der Gruppe (Mitgliederlisten, Protokolle), Finanzdaten, (Kontonummern, Überweisungsbeträge), Versicherungsbereich (Krankenkassendaten), Passwörter, Fotos/Videos ohne Genehmigung.

F1) Ungefähre Zahl betroffener Personen (Art. 33 Abs. 3 lit. a) **Anzahl:** _____

F2) Ungefähre Zahl betroffener Datensätze (mal Anzahl Personen) **Anzahl:** _____

Bei Rückfragen bitte direkt den Datenschutzbeauftragten kontaktieren

Ort, Datum Vorname Nachname Unterschrift