Deutsches Rotes Kreuz

Datenschutz-Handbuch

für DRK-Ortsvereine und DRK-Gliederungen in Baden-Württemberg

Inhaltsverzeichnis

1 Grundlagen ... 3
1.1 Einführung ... 3
1.2 Was sind personenbezogene Daten? ... 3
1.3 Wer ist für den Datenschutz verantwortlich? ... 3
1.4 Grundsätze und Rechtsgrundlagen des Datenschutzes ... 3
1.5 Richtlinie zur Daten- /IT-Sicherheit für Mitarbeitende ... 3
1.6 Messenger Dienste (WhatsApp etc.) ... 3
1.7 Foto/ Videos ... 4
1.8 Einwilligungen ... 4
1.9 Datenpannen bzw. Datenschutzverletzungen ... 4
2 Datenschutz für Leitungskräfte ... 5
2.1 Datenschutz-Leitlinie ... 5
2.2 Datenschutzorganisation ... 5
2.3 Datenschutz-Schulung ... 5
2.4 Technische und organisatorische Maßnahmen (TOMs) ... 6
2.5 Werbung und Spendenaufrufe ... 6
2.6 Erhebung und Weitergabe von Mitglieder-/ Beschäftigtendaten und Dritten ... 6
2.7 Videoüberwachung ... 7
2.8 Sanktionen ... 7
2.9 Auskunftsrecht und Auskunftsersuchen ... 7
2.10 Auftragsdatenverarbeitung ... 8
2.11 Gemeinsame Verantwortlichkeit ... 8
2.12 Verzeichnis von Verarbeitungstätigkeiten (VVT) ... 8
2.13 Informationspflichten und Betroffenenrechte ... 8
2.14 Löschkonzept ... 8
3 Sonderthemen ... 9
3.1 Impflicht ... 9
3.2 Führerscheinkontrolle ... 9
3.3 Website (Datenschutzerklärung) ... 9
3.4 Veröffentlichungen von Daten in Aushängen, schwarzem Brett, Internet etc. ... 9
3.5 Mobiles Arbeiten mit privaten Geräten ... 10
3.6 (erweitertes) Führungszeugnis ... 10
4 DRK spezifische Einsatzfelder ... 10
4.1 Allgemeine Handlungsempfehlungen ... 10
4.2 Helfer vor Ort ... 11
4.3 Breitenausbildung/ Schulungen/ Seminare/ Gesundheitsprogramme ... 11
4.4 Jugendrotkreuz ... 11
4.5 Hundestaffel ... 11
4.6 Bergwacht/ Wasserwacht ... 11
4.7 Sanitätsdienst ... 12
4.8 Tafelläden ... 12
4.9 Kleiderläden/Kleiderkammer ... 12
4.10 Blutspendedienst ... 12

Aus Gründen der besseren Lesbarkeit wird im Folgenden auf die gleichzeitige Verwendung weiblicher und männlicher Sprachformen verzichtet und das generische Maskulinum verwendet.

Alle grün markierten Textstellen stehen als Link auf der Webseite zum Download bereit. Abkürzungen und Erläuterungen sind im Glossar zu finden.

1 Grundlagen

1.1 Einführung

Mit Einführung der Europäischen Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018 wurden alle Unternehmen, Behörden und Verbände gesetzlich verpflichtet, den Datenschutz nach den neuen Vorschriften zu betreiben. Diese Vorschriften gelten in allen Mitgliedsstaaten der Europäischen Union als unmittelbar anzuwendendes Recht. Die Mitgliedsstaaten können einen Teil der DS-GVO im nationalen Kontext präzisieren. Der deutsche Gesetzgeber hat dazu ein neues Bundesdatenschutzgesetz und verschiedene Landesdatenschutzgesetze erlassen, die ebenso seit dem 25. Mai 2018 gelten.

Die DS-GVO ist dabei stets vorrangig vor den nationalen Regelungen zu behandeln. Nationale Gesetze dürfen ihr nicht entgegenstehen, sondern sie können sie nur dort ergänzen, wo in der DS-GVO ausdrücklich eine nationale Regelung erlaubt ist. Die DS-GVO greift jedoch nur, wenn personenbezogene Daten verarbeitet werden.

1.2 Was sind personenbezogene Daten?

Personenbezogene Daten sind ein Kernbegriff des Datenschutzes. Nur wenn Daten einen Bezug zu einem Menschen aufweisen (z.B. Name, Kontaktdaten), kommt das Datenschutzrecht zur Anwendung. Daneben gibt es besonders geschützte sensible personenbezogene Daten. Diese beinhalten u.a. Daten über ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, strafrechtliche Verurteilungen sowie biometrische Daten sowie Gesundheitsdaten (Art. 9 Abs. 1 und Art. 10 DS-GVO). Angaben über Verstorbene, wie z.B. ein Nachruf eines verstorbenen Mitglieds, werden in der DS-GVO nicht geschützt.

1.3 Wer ist für den Datenschutz verantwortlich?

Die verantwortliche Stelle (i. d. R. Vorstand oder Geschäftsleitung) ist diejenige, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Unerheblich ist dabei, ob die Gliederung in das Vereinsregister mit einer eigenen Rechtspersönlichkeit eingetragen oder ein nichtrechtsfähiger Verein ist. Alle haupt-/ ehrenamtlich Beschäftigten sind jedoch verpflichtet, die datenschutzrechtlichen Regelungen einzuhalten, denn bei grob fahrlässigen Datenschutzverletzungen macht sich auch jeder Einzelne mit verantwortlich.

1.4 Grundsätze und Rechtsgrundlagen des Datenschutzes

Für jede Datenverarbeitung wird eine Rechtsgrundlage benötigt. Daneben gibt es weitere Grundsätze zur datenschutzkonformen Verarbeitung personenbezogener Daten, deren Nichtbeachten mit einem Bußgeld bedroht ist (ausführliche Informationen siehe Anlage Grundsätze des Datenschutzes).

1.5 Richtlinie zur Daten- /IT-Sicherheit für Mitarbeitende

In fast allen DRK-Gliederungen werden mittlerweile Daten elektronisch verarbeitet, wobei die Datensicherheit und besonders die IT-Sicherheit eine unverzichtbare Rolle spielt. Aus diesem Grund empfiehlt sich die Richtlinie zur Daten- /IT-Sicherheit (siehe Anlage IT-Sicherheit_Richtlinien) umzusetzen. In diesem Zusammenhang ist durch Mitglieder bzw. Mitarbeitende die Verpflichtungserklärung zum Datengeheimnis zu unterschreiben (siehe Anlage Verpflichtungserklärung zur Vertraulichkeit).

1.6 Messenger Dienste (WhatsApp etc.)

Für die geschäftliche Kommunikation dürfen nur datenschutzkonforme Messenger Dienste verwendet werde, wobei WhatsApp aktuell nicht den Datenschutzanforderungen entspricht. Datenschutzkonforme Dienste wären u. a. Threema, Signal sowie Microsoft Yammer und Microsoft Teams (siehe auch Anlage IT-Sicherheit_Richtlinien, Seite 6).

1.7 Foto/ Videos

Grundsätzlich gilt, dass jeder das Recht am eigenen Bild hat. Somit muss beim Fotografieren einer Person deren ausdrückliche Einwilligung eingeholt werden, wenn diese im Mittelpunkt des Bildes steht. Auch bei Minderjährigen ist stets eine Einwilligung aller Sorgeberechtigten einzuholen.

Öffentliche Gruppen-/ Veranstaltungsfotos von Erwachsenen dürfen ohne Einwilligung veröffentlicht werden, da der Verein ein berechtigtes Interesse hat, über das Vereinsgeschehen zu informieren. Jedoch muss der Veranstaltungscharakter im Vordergrund stehen und am Eingang der Veranstaltung ein Aushang erfolgen (siehe Anlage Veranstaltungen_Aushang_Datenschutzinformation).

Aufnahmen von vereinsinternen Aktivitäten dürfen, trotz des berechtigten Interesses, nicht veröffentlicht werden, da keine vernünftigen Erwartungen der Teilnehmenden über die Veröffentlichung vorliegen. Mit einer Einwilligung der Betroffenen und den ausgehändigten Informationspflichten wäre dies jedoch möglich. Zudem dürfen Bilder ohne Einwilligung veröffentlicht werden, bei denen die Personen als Beiwerk erscheinen. Ausführliche Informationen in (siehe Anlage Fotos/Videos) und Kapitel 1.8.

1.8 Einwilligungen

Eine Einwilligung ist nur dann wirksam, wenn sie freiwillig ohne Zwang, durch eindeutiges bestätigtes Handeln (z.B. Ankreuzen) und für einen bestimmten Zweck erfolgt. Zudem werden klare und verständliche Informationen benötigt, wer die Einwilligung für welchen Zweck möchte und der Einwilligung muss jederzeit ohne Angabe von Gründen widerrufen werden können.

Grundsätzlich gelten alte Einwilligungen vor dem 25.05.2018, weiterhin, wenn diese den Voraussetzungen der DS-GVO entsprechen. Jedoch sollte diese immer das letzte Mittel sein, um eine Rechtsgrundlage zur Datenerhebung zu schaffen, da hier vor allem das jederzeitige Widerspruchsrecht ausgeübt werden kann. Einwilligungen sollten schriftlich oder elektronisch eingeholt werden. Eine Mustereinwilligung entnehmen Sie aus der Anlage Einwilligung_Internet.

Bei Kindern und Jugendlichen ist darauf zu achten, dass alle Sorgeberechtigten und der Jugendliche ab 14 Jahre die Einwilligung unterschreiben (siehe Anlage Einwilligung_Kinder und Jugendliche).

1.9 Datenpannen bzw. Datenschutzverletzungen

Datenverlust (z. B. verlorenes Diensthandy), Offenlegung der Daten (z. B. Einsatzprotokoll liegt offen im Rettungswagen) oder unbefugter Datenzugang (z. B. USB-Stick mit Schadsoftware), all diese Vorfälle stellen Datenschutzverletzungen dar.

Kommt es zu einer Datenpanne, muss der Verantwortliche dies i. d. R. der Aufsichtsbehörde innerhalb von 72 Stunden melden. Ansonsten drohen evtl. erhebliche Bußgelder. Die Meldung erfolgt über folgenden Link: https://www.baden-wuerttemberg.datenschutz.de/datenpanne-melden/. Die Meldepflicht entfällt nur in Ausnahmen, wie z. B. wenn Personalakten schon längst hätten gelöscht werden müssen und nun bei einem Brand zerstört wurden.

Daneben müssen ggf. Betroffene benachrichtigt werden, wenn ein hohes Risiko für deren persönlichen Rechte und Freiheiten besteht. Die Risikobewertung erfolgt über zwei Kriterien:

1. Wie hoch ist die Wahrscheinlichkeit, dass der Nachteil für die Betroffenen eintritt (z. B. wie hoch ist das Interesse für unbefugte Dritte die Daten zu löschen)?
2. Wie schwer wiegt die Auswirkung für die Betroffenen (z. B. gesundheitliche/ finanzielle Folgen)?

Da 90 % der Datenpannen durch fahrlässiges Verhalten durch Mitarbeitende verursacht werden, müssen diese regelmäßig geschult und sensibilisiert werden (siehe Kapitel 2.3). Zudem können Datenpannen auch durch fehlende Richtlinien entstehen, weshalb der Verantwortliche IT-Richtlinie für Beschäftigte erstellen sollte (siehe Kapitel 1.5).

Ausführliche Informationen in folgenden Anlagen: Anlage Datenpanne_Flußdiagramm, Anlage Datenpanne_Verfahrensbeschreibung, Anlage Datenpanne_Meldebogen und Anlage Datenpanne_Benachrichtigung Betroffener.

2 Datenschutz für Leitungskräfte

Das folgende Kapitel richtet sich an alle Leitungskräfte (Vorstand, Geschäftsführung und Abteilungsleitung), die als verantwortliche Stelle die Datenschutzvorschriften in ihren Gliederungen umsetzen müssen. Als erster Schritt dient die Anlage Erste Schritte_Checkliste.

2.1 Datenschutz-Leitlinie

Eine Datenschutz-Leitlinie stellt ein „verbandsinternes Datenschutzgrundgesetz“ dar, mit dem sich die Gliederung der gesellschaftlichen Verantwortung zur Einhaltung des Datenschutzrechts verpflichtet. Eine solche Leitlinie sollte an alle Mitarbeitenden ausgehändigt und im Rahmen einer Datenschutz-Schulung kommuniziert werden (siehe auch Anlage Leitlinien).

2.2 Datenschutzorganisation

a) Einbinden des Datenschutzes in die DRK-Gliederung

Es ist wichtig, dass der Vorstand in Sachen Datenschutz voran geht und als Vorbild fungiert, um alle Mitglieder/ Mitarbeitenden „mitzunehmen“. Dabei sollten Sie folgende Punkte beachten:

3. Machen Sie die den Datenschutz zu einem wichtigen Vorstandsthema.
4. Benennen Sie Vorstandsmitglieder, die sich mit der Umsetzung des Datenschutzes beschäftigen.
5. Grundsätzlich ist der gesamte nach § 26 BGB vertretungsberechtigte Vorstand verantwortlich.
6. Berufen Sie eine Arbeitsgruppe aus den Verantwortlichen und Mitgliedern/ Mitarbeitenden, die sich der Umsetzung und Kontrolle der DS-GVO annimmt.

b) Datenschutzbeauftragter und Datenschutzkoordinator

Der Datenschutzbeauftragte (DSB) bzw. Datenschutzkoordinator (DSKO) berät die Verantwortlichen sowie Mitarbeitenden in allen Datenschutzfragen und überwacht die Einhaltung der Datenschutzvorschriften. Vertiefte Informationen in Anlage DSB/DSK_Stellung und Rolle.

c) Bestellung eines Datenschutzbeauftragten

Die DRK-Gliederung muss einen DSB bestellen, wenn mehr als 20 Personen regelmäßig mit automatisierten Daten arbeiten (siehe Anlage DSB_Checkliste Notwendigkeit DSB). Ist ein DSB zu bestellen, muss dieser der Aufsichtsbehörde online auf folgendem Link gemeldet werden: https://www.baden-wuerttemberg.datenschutz.de/dsb-online-melden/. Ortsvereine, deren Kreisverbände Datenschutz-Kunden des DRK-Landesverband Baden-Württemberg e. V. sind, können den DSB über den DRK-Landesverband benennen. Bitte bei Interesse dazu Kontakt mit dem Landesverband aufnehmen.

Achtung: Auch wenn kein DSB bestellt werden muss, ist die Gliederung trotzdem verpflichtet die DS-GVO mit den dazugehörigen nationalen Gesetzgebungen umzusetzen.

d) Unterstützung durch den DSB/ DSKO vor Ort

DSB und DSKO stimmen sich mit der jeweiligen in der DRK-Gliederung ab, welche Hilfestellungen (Beratungsgespräch, Audit, Schulungen etc.) vor Ort erfolgen sollen.

2.3 Datenschutz-Schulung

Die meisten Datenpannen sind auf Fahrlässigkeit und Unwissenheit der Beschäftigten zurückzuführen. Aus diesem Grund müssen alle Personen, die personenbezogene Daten verarbeiten, regelmäßig zum Datenschutz geschult werden.

Das DRK bietet eine Online-Schulung auf dem Lerncampus an (siehe Anlage Schulungen). Diese Schulung absolvieren alle Beschäftigten in den ersten vier Wochen ihres Dienstbeginns. Auch langjährige Mitarbeitenden müssen jährlich an einer Schulung teilnehmen. Neben der Online-Schulung ist es sinnvoll, dass Präsenzschulungen durch den DSKO erfolgen. Zudem können externe Fachleute eingeladen werden. Sollte eine Präsenzschulung nicht immer jährlich möglich sein, dann wäre zumindest die Online-Schulung vom Lerncampus in diesem Jahr zu empfehlen.

2.4 Technische und organisatorische Maßnahmen (TOMs)

Unternehmen bzw. Vereine, haben die technischen und organisatorischen Maßnahmen zu treffen, um die Vorschriften der Datenschutzgesetze zu gewährleisten (siehe Anlage Technische und organisatorische Maßnahmen_Checkliste). In Anlage Technische und organisatorische Maßnahmen_Empfehlungen sind die wichtigsten Sicherheitsmaßnahmen beschrieben, welche umzusetzen sind. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

2.5 Werbung und Spendenaufrufe

Wenn Werbung in der DRK-Gliederung durchgeführt werden, muss grundsätzlich die Informationspflichten erfüllt (siehe Kapitel 2.13 und Anlage Datenschutzinformation Fördermitglieder), das Verfahren in das Verzeichnis für Verarbeitungstätigkeiten aufgenommen (siehe Kapitel 2.12) sowie in das Löschkonzept integriert (siehe Kapitel 2.14) werden.

a) Direktwerbung Fördermitglieder: Telefon, Brief, Fax, E-Mail, SMS

Die Rechtmäßigkeit der Datenverarbeitung Rahmen der Mitgliederwerbung ergibt sich aus dem berechtigten Interesse des Verantwortlichen. Jedoch müssen die Betroffenen zum Zeitpunkt der Datenerhebung datenschutzrechtlich informiert werden und die Möglichkeit haben, der Datennutzung zu widersprechen.

Der Verein kann auch eine Firma beauftragen, solche Werbemaßnahmen durchzuführen. Dabei ist die externe Firma zu verpflichten, sowohl die vom Verein überlassenen, als auch die bei der Werbeaktion erhobenen Daten nicht für eigene oder andere Zwecke zu nutzen und sämtliche Daten nach Abschluss der Aktion vollständig an den Verein abzuliefern.

Es ist noch nicht eindeutig geregelt, inwieweit die Direktwerbung gegen das Gesetz gegen unlauteren Wettbewerb (UWG) verstößt. Daher sollte im Mitgliedsantrag darauf hingewiesen werden, dass das Mitglied jederzeit das Recht hat gegen die Datennutzung für Werbezwecke zu widersprechen.

b) Direktwerbung Dritte: Brief

Zulässig ist auch, Werbung an Postadressen zu versenden, die in allgemein zugänglichen Verzeichnissen wie Telefonbüchern oder Online-Adressverzeichnissen stehen (nicht Adressdaten aus Webseiten). Jedoch hat der adressierte Empfänger das Recht, der Datennutzung zu Werbezwecken jederzeit zu widersprechen. Der werbende Verein muss den Empfänger in jedem Werbebrief ausdrücklich auf dieses Widerspruchsrecht hinweisen.

c) Direktwerbung Dritte: Telefon, Fax, E-Mail, SMS

Die Durchführung von Werbung per Telefon, Fax, E-Mail oder SMS ohne Einwilligung des Betroffenen stellt laut UWG eine unzumutbare Belästigung dar und ist damit verboten.

d) Datentransfer an Sponsoren und Firmen zu Werbezwecke

Der Datentransfer ohne Einwilligung ist grundsätzlich verboten, wenn weder in der Satzung oder durch Mitgliederbeschluss die Datenweitergabe legitimiert ist.

2.6 Erhebung und Weitergabe von Mitglieder-/ Beschäftigtendaten und Dritten

a) Mitgliederdaten

Mitgliederdaten dürfen erhoben werden, wenn diese dem Vereinsziel dienen und für die Mitgliederverwaltung notwendig sind. Jedoch muss der Grundsatz der Datenminimierung berücksichtigt werden, so darf z. B. der Vorstand auf alle Mitgliederdaten zugreifen, jedoch benötigt der Kassierer nur Bankdaten. Werden Versicherungsverträge für die Mitglieder abgeschlossen, dann ist die Datenerhebung möglich, sofern durch die Versicherung Risiken für den Verein abgedeckt sind.

Die Datenweitergabe an den Dachverband geht nur mit einer Einwilligung oder wenn bereits im Mitgliedsantrag auf die Datenweitergabe an den Dachverband hingewiesen wird und ein berechtigtes Interesse des Betroffenen besteht (z.B. Mitgliederversicherung über den Dachverband).

Der Verein darf auch Mitgliederdaten erheben, auch wenn diese Erhebung nicht dem Vereinsziel bzw. Vereinsverwaltung dient, sofern der Verein an der Datenerhebung ein berechtigtes Interesse hat. Bei dieser Datenerhebung dürfen aber nicht die schutzwürdigen Interessen der Betroffenen überwiegen (z. B. Betroffener ist unter 16 Jahre alt und er kann voraussichtlich sein Handeln und Tun nicht angemessen einschätzen).

b) Dritte

Die Datenerhebung von Dritten (z. B. Gäste) ist möglich, sofern nicht die schutzwürdigen Interessen der Betroffenen eingeschränkt sind. Die Daten dürfen nur für den Zweck genutzt werden, für welchen die Daten erhoben wurden. Werden Mitgliederdaten an andere Mitglieder übermittelt, dann ist dies grundsätzlich nur mit einer Einwilligung zulässig, da das andere Mitglied als „Dritter" angesehen wird. Eine Ausnahme könnte sein, wenn die Satzung z. B. für die außerordentliche Mitgliederversammlung eine Mindestanzahl von Mitgliedern vorsieht.

c) Datenweitergabe an Behörden und Versicherungen

Behörden dürfen Daten anfordern, um Leistungen zu überprüfen, da hierbei ein berechtigtes Interesse des Vereins (Zuschüsse) und der Behörde (Kontrolle) vorliegt. Eine Datenübermittlung an Versicherungen und Arbeitgeber wegen eines Unfalls sind zulässig, um evtl. Regressansprüche einzufordern (berechtigtes Interesse), sofern nicht die Interessen der Betroffenen überwiegen.

d) Erhebung von Personaldaten

Im § 26 BDSG in Verbindung mit Art. 88 DS-GVO ist geregelt, dass sämtliche personenbezogene Daten, welche zur Begründung eines Arbeitsverhältnisses notwendig sind, erhoben werden dürfen. Ausführliche Informationen zu finden in Anlage Personal_Basiswissen, Anlage Personal_Bewerbung und Anlage Datenschutzinformation Beschäftigte.

2.7 Videoüberwachung

Das Unternehmen kann sich bei dem Einsatz von Videosystemen auf die Wahrung der berechtigten Interessen berufen, wenn die Interessen oder Grundrechte der Betroffenen nicht überwiegen. Folglich müssen die Interessen der DRK-Gliederung gegen die Grundrechte der Betroffenen abgewogen werden. Ein berechtigtes Interesse wäre, wenn eine Gefahrenlage besteht oder die Aufzeichnungen der Beweissicherung dienen sollen (z. B. es gab mehrere Einbrüche). Um der Transparenzpflicht nachzukommen, müssen in einem solchen Fall Hinweisschilder angebracht werden, die von den Betroffenen eindeutig gesehen werden (siehe Anlage Video_Hinweisschild).

2.8 Sanktionen

Der Verantwortliche ist verpflichtet, datenschutzkonform zu arbeiten, indem die Vorgaben der DS-GVO umgesetzt und dokumentiert werden. Durch geeignete Maßnahmen (Umsetzung von Richtlinien, Sensibilisierung der Mitarbeitenden, dokumentiertes Löschkonzept etc.) können Datenpannen und somit Sanktionen vermieden werden.

Wenn der Datenschutz nicht eingehalten wird, kann die Aufsichtsbehörden wirksame, abschreckende und verhältnismäßige Geldbußen verhängen (bis zum 20 Mio. Euro oder 4 % des Umsatzes). Zudem können Betroffene Schadensersatz für materiellen und immateriellen Schaden fordern.

2.9 Auskunftsrecht und Auskunftsersuchen

Betroffene haben das Recht, mit einem formlosen Antrag und ohne Begründung, Auskunft über ihre gespeicherten personenbezogenen Daten zu verlangen (siehe Anlage Auskunftsersuchen Basiswissen). Es ist ratsam, rechtzeitig organisatorische Vorkehrungen für zügige und korrekte Auskunftserteilungen zu treffen (siehe Anlage Auskunftsersuchen_Musterbrief zur Beantwortung). Dabei ist die 4-Wochenfrist zu beachten. Vor Datenherausgabe muss die Identität des Auskunftsersuchenden überprüft werden (z. B. persönliches Vorlegen des Personalausweises).

Es kommt immer wieder vor, dass z. B. Angehörige oder Behörden (Polizei, Staatsanwaltschaft) ein Auskunftsersuchen stellt. Ausführliche Informationen zur Auskunftsersuche durch Dritte sind in der

Anlage Auskunftsersuchen_Verfahrensbeschreibung und in der Anlage Auskunftsersuchen_Checkliste zu finden.

2.10 Auftragsdatenverarbeitung

Selten erledigen Vereine ihre gesamten Aufgaben ohne fremde Hilfe. Häufig werden Dienstleister eingeschalten, die z.B. für das Unternehmen die IT-Einrichtung warten. Von einer Auftragsverarbeitung wird dann gesprochen, wenn ein externes Unternehmen im Auftrag des Verantwortlichen Daten verarbeitet. Das heißt, dass der Verantwortliche Daten an jemanden nach außen gibt und Einblick auf die eigenen Daten ermöglicht. Für alle Auftragsverarbeitungsverhältnisse muss ein Vertrag abgeschlossen werden (siehe Anlage Auftragsdatenverarbeitungsvertrag_Mustervertrag). Beispiele:

- Bei Dienstleistungen eines Buchhaltungsbüros (Lohnbuchhaltung bzw. Finanzbuchhaltung) liegt eine Auftragsverarbeitung vor.
- Bei Dienstleistungen eines Steuerberaters liegt i. d. R. wegen der Inanspruchnahme fremder Fachleistungen keine Auftragsverarbeitung vor, sondern eine Datenübermittlung an einen Dritten.
- Die Beauftragung von Rechtsanwälten, Wirtschaftsprüfer oder externe Datenschutzbeauftragte (Berufsgeheimnisträger) stellt i. d. R. keine Auftragsverarbeitung dar, da die Erbringung einer fremdem Fachleistung im Vordergrund steht.

2.11 Gemeinsame Verantwortlichkeit

Wenn mehrere Verantwortliche gemeinsam über die Zwecke und Mittel der Datenverarbeitung entscheiden, liegt eine gemeinsame Verantwortlichkeit vor, wie z. B. die Anwendung „mein.DRK.team“. In der Anwendung nutzen Landesverband, Kreis- und Ortsverbände unabhängig voneinander die Daten, weshalb ein Vertrag abgeschlossen werden muss (siehe Anlage Gemeinsame Verantwortung_Mustervertrag).

2.12 Verzeichnis von Verarbeitungstätigkeiten (VVT)

Für sämtliche datenschutzrelevante Prozesse muss ein Verzeichnis von Verarbeitungstätigkeit mit den gesetzlichen Vorgaben schriftlich erstellt werden. Je nach Umfang und Größe der Gliederung ist davon auszugehen, dass zwischen 5 und 10 Verarbeitungstätigkeiten dokumentiert werden müssen. Aus der Dokumentation muss hervorgehen, welche personenbezogene Daten die einzelne Gliederung mit Hilfe welcher Verfahren auf welche Weise verarbeitet. In den VVT_Vorlagen ist ein Excel Muster mit Löschprotokoll hinterlegt. Dort sind all gängigen Verarbeitungstätigkeiten aufgeführt.

2.13 Informationspflichten und Betroffenenrechte

Die DS-GVO stärkt die Betroffenenrechte und hat bei der Datenverarbeitung eine ausgeweitete Transparenzpflicht. Demnach müssen Betroffenen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache informiert werden, was zu welchem Zweck mit ihren Daten gemacht wird. Diese Informationen müssen zum Zeitpunkt der Datenerhebung bereitgestellt werden. In manchen Situationen können die Informationspflichten nicht unmittelbar zur Verfügung gestellt werden (z.B. Postkarte für Gewinnspiel). In einem solchen Fall kann ein Medienbruch vorgenommen werden, d. h. dem Betroffenen kann ein Link zu der Datenschutzinformation auf der Webseite zur Verfügung gestellt werden. Muster-Informationspflichten sind in Anlagen Datenschutzinformationen_Vorlagen zu finden.

2.14 Löschkonzept

Personenbezogene Daten müssen gelöscht werden, wenn keine Aufbewahrungsfristen dem entgegenstehen (siehe Anlage Aufbewahrungsfristen). Durch die gesetzliche Verpflichtung der Datenlöschung sollte ein Löschkonzept entwickelt und auf Grund der Nachweispflicht ein Löschprotokoll verwendet werden (siehe Anlage Löschkonzept und Anlage Löschprotokolle).

3 Sonderthemen

3.1 Impflicht

Aufgrund des Grundsatzes der Datenminimierung und der Sensibilität von Gesundheitsdaten sollte auf eine Kopie des Impfausweises verzichtet werden. Es empfiehlt sich dagegen bei Vorlage des Impfnachweises in der Personalabteilung einen Vermerk anzufertigen, dass der Beschäftigte über die notwendige Impfung verfügt und diesen Vermerk in der Personalakte abzulegen. Der Vermerk kann durch zwei Personen, die mit Personalangelegenheiten betraut sind, per Unterschrift dokumentiert werden (4-Augen-Prinzip).

3.2 Führerscheinkontrolle

Bevor DRK-Gliederungen einem Mitarbeitenden ein Fahrzeug überlassen, müssen diese prüfen, ob er über die erforderliche Fahrerlaubnis verfügt. Wird dies versäumt und bei einer Polizeikontrolle festgestellt, dass die Fahrerlaubnis fehlt, drohen dem Arbeitgeber strafrechtliche Konsequenzen. Die Führerscheinkontrolle sollte je nach Einsatzgebiet in regelmäßigen Abständen geprüft werden (z. B. bei Beschäftigten in der Verwaltung alle sechs Monate, beim Führen von Einsatzfahrzeugen monatlich).

Es wird empfohlen, dass eine beauftragte Person Einsicht in den Original Führerschein nimmt (keine Kopie anfertigen) und Name, Termin der Einsichtnahme und die Person, die Einsicht genommen hat, dokumentiert. Die alten Daten müssen nach erneuter Prüfung gelöscht werden.

In der prüfungsfreien Zeit ist der Arbeitnehmer verpflichtet, Veränderungen in Bezug auf das Führen von Fahrzeugen (z. B. Verlust des Führerscheines) dem Arbeitgeber unverzüglich zu melden. Damit der Arbeitnehmer dies zur Kenntnis genommen hat, muss er eine Verpflichtungserklärung unterschreiben (siehe Führerschein_Kontrollbogen).

3.3 Website (Datenschutzerklärung)

Eine Datenschutzerklärung muss immer dann auf einer Internetseite vorhanden sein, wenn beim Besuch der Seite personenbezogene Daten erfasst werden. Da in der Regel immer die IP-Adresse und Verweildauer auf der Website verarbeitet werden, benötigt fast jede Website eine Datenschutzerklärung (siehe Anlage Webseite_Muster Datenschutzerklärung). Die Webseite und das Impressum sollten regelmäßig (alle sechs Monate) auf die Datenschutzkonformität hin überprüft werden.

3.4 Veröffentlichungen von Daten in Aushängen, schwarzem Brett, Internet etc.

a) Aushänge auf dem Vereinsgelände bzw. Vereinspublikationen

Personenbezogene Daten (z. B. Ein-/Austritte, Jubiläen, Geburtstage) dürfen nur veröffentlicht werden, wenn dies für die Erreichung des Vereinszwecks erforderlich ist oder der Verein ein berechtigtes Interesse daran hat und die schutzwürdigen Interessen der Betroffenen nicht überwiegen.

Es ist ratsam, dass bereits im Mitgliedsantrag aufgeführt wird, welche Ereignisse veröffentlicht werden und dass das neue Mitglied dem widersprechen kann. Informationen aus dem persönlichen Lebensbereich (Geburt von Kindern, Schulabschluss etc.), Höhe der Spende und Kontaktdaten dürfen nur veröffentlicht werden, wenn der Betroffene eingewilligt hat.

b) Interne Aushänge

Häufig finden sich auf dem internen schwarzen Brett, Intranet oder Dienstplan sensible Daten wie z.B. „krank“. Damit soll ein uneingeschränkter Betriebsablauf sichergestellt und die Kollegen über die Abwesenheit informieren werden. Jedoch macht es für Mitarbeitenden keinen Unterschied, ob der Kollege krank oder im Urlaub ist. Aus diesem Grund dürfen betriebsöffentliche Aushänge ausschließlich mit der allgemeinen Form wie z.B. „abwesend“ aufgeführt werden.

c) Internet und Intranet

Grundsätzlich ist die Veröffentlichung von Daten im Internet ohne Einwilligung verboten, da die Daten für alle zugänglich sind, auf Dauer gespeichert und verfälsch bar sind. Hingegen dürfen Daten (Name, Kontaktdaten) von Funktionsträgern (z. B. Vorstand) auch ohne Einwilligung veröffentlicht werden.

Das Intranet ist passwortgeschützt und besitzt individuelle Zugriffsrechte, dadurch haben unberechtigte Dritte keinen Zugriff. Mitglieder dürfen aber nur auf die Daten Zugriff haben, welche im Rahmen der Mitgliedschaft für sie notwendig sind. Ein Funktionsträger kann erweiterte Zugriffsrechte haben.

d) Presse und sonstige Medien

Die Veröffentlichung ist nur zulässig, wenn die personenbezogenen Daten im öffentlichen Interesse sind (z. B. Jubiläen). Hier muss darauf geachtet werden, dass die schutzwürdigen Belange der Betroffenen beachtet werden. Zudem ist zu berücksichtigen, ob die Veranstaltung einen öffentlichen Charakter hat oder nicht. Wenn z. B. der betroffene Jubilar wusste, dass dies eine öffentliche Veranstaltung war, dann muss er auch damit rechnen, dass z. B. sein Foto in der Zeitung erscheint.

3.5 Mobiles Arbeiten mit privaten Geräten

Wenn Beschäftigte mit privaten Geräten arbeiten, ist zu beachten, dass der Zugriff auf dienstliche E-Mails nur über eine Webmail-Oberfläche und auf Unternehmensressourcen nur über eine VPN-Verbindung erfolgt. Alle dienstlichen Daten müssen verschlüsselt sein, wie z. B. Verschlüsselung der Festplatte im Rechner über ein Bitlocker. Bei der Nutzung eines Familien-PC muss ein eigenes Nutzerkonto für dienstliche Zwecke eingerichtet werden. Zudem muss auf dem Betriebssystem immer die aktuellen Sicherheitsupdates eingespielt und ein aktueller Virenscanner installiert sein.

Eine große Schwierigkeit bei der Nutzung privater IT-Geräte ist, dass der Arbeitgeber die Geräte nicht ohne Weiteres untersuchen kann. Um den Kontrollverlust zu vermeiden und dennoch nicht den Privatbereich der Beschäftigten zu tangieren, muss eine Betriebsvereinbarung (siehe Anlage Vorlage Betriebsvereinbarung mobiles Arbeiten) und eine individuelle Vereinbarung (siehe Anlage Vorlage individuelle Vereinbarung mobiles Arbeiten) abgeschlossen werden. Ein individueller Zusatz ist nötig, da der Betriebsrat nicht für die Einzelnen einwilligen kann, was in deren privaten Besitz ist.[1]

3.6 (Erweitertes) Führungszeugnis

Im Hauptamt darf der Arbeitgeber das (erweiterte) Führungszeugnis z. B. in der Personalakte aufbewahren. Im Neben-/ Ehrenamt darf nicht ohne Einwilligung des Betroffenen das gesamte (erweiterte) Führungszeugnis gespeichert werden, sondern nur drei Informationen: (1) die Tatsache, dass Einsicht genommen wurde, (2) das Datum des Führungszeugnisses und (3) ob die betreffende Person wegen einer Straftat rechtskräftig verurteilt wurde. Die Daten sind nach Ausscheiden des Betroffenen unverzüglich zu löschen.

4 DRK spezifische Einsatzfelder

4.1 Allgemeine Handlungsempfehlungen

Für alle DRK spezifischen Arbeitsfelder müssen folgende Punkte beachtet bzw. umgesetzt werden:

1. Umsetzung der Informationspflichten (siehe Kapitel 2.13)
2. Aufnahme jedes Einsatzfelds in das Verzeichnis für Verarbeitungstätigkeiten (siehe Kapitel 2.12)
3. Aufnahme jedes Einsatzfelds in das Löschkonzept – Aufbewahrungsfristen (siehe Kapitel 2.14)
4. Es ist immer darauf zu achten, dass nur die Daten erhoben werden, die für den Erhebungszweck notwendig sind (Grundsatz der Datenminimierung).
5. Darauf achten, dass Daten von dem Zugriff und der Einsicht von unberechtigten Dritten geschützt sind (u. a. verschließbare Schränke/ Räume; Passwortschutz) (siehe Kapitel 1.5).
6. Sensible Daten (z. B. Gesundheitsdaten) dürfen nur als verschlüsselte E-Mail übertragen werden.
7. Mails an mehrere Empfänger, müssen diese in bcc versendet werden. Bei Arbeitsgruppen ist dies nicht notwendig, da die Gruppenmitglieder sich gegenseitig kennen.

[1] *Quelle: Gerling (2020): Mobiles Arbeiten: Bring your own Device revisited. WEKA MEDIA GmbH & Co. KG.*

4.2 Helfer vor Ort

Technisch kann die Alarmierung per SMS aufs Handy oder über Funkmeldeempfänger erfolgen. Eine SMS ist grundsätzlich relativ sicher, jedoch ist ein digitaler verschlüsselter Funkmeldeempfänger die sichere Variante. Die Leitstelle darf nur personenbezogene Daten versenden, die für den Einsatz notwendig sind. Zudem dürfen bei der Datenübermittlung keine unberechtigte Dritte Einsicht erlangen.

Bei der Erstversorgung eines Patienten ist darauf zu achten, dass zum Zeitpunkt der Datenerhebung die Datenschutzinformationen dem Betroffenen (sofern möglich) übergeben werden. Das analoge Patientenprotokoll ist bis zur Übergabe an die Verantwortliche sicher aufzubewahren, so dass kein unberechtigter Dritte Dateneinsicht hat (z. B. verschließbare Mappe). Sollte das analoge Patientenprotokoll nach dem Einsatz aufbewahrt werden, dann ist auf die datenschutzkonforme Aufbewahrung bis zur Löschung zu achten. Bei der digitalen Erfassung ist darauf zu achten, dass das Endgerät vor einem unberechtigten Zugriff durch ein datenschutzkonformes Passwort gesichert ist.

4.3 Breitenausbildung/ Schulungen/ Seminare/ Gesundheitsprogramme

Bei externen Angeboten werden Teilnehmerdaten erfasst. Diese Daten sollten nicht über eine Teilnehmerliste erfasst werden, bei der Einzelne die anderen Teilnehmerdaten einsehen kann. Eine Ausnahme wäre, wenn alle Teilnehmenden einwilligen, dass die Anderen diese einsehen dürfen. Eine andere Möglichkeit ist, dass man pro Teilnehmer/in eine Teilnahmebescheinigung auslegt.

Werden hingegen interne Veranstaltungen, d.h. innerhalb einer DRK-Gliederung durchgeführt, dann ist es grundsätzlich möglich eine Teilnehmerliste für alle Teilnehmenden zu erstellen. Das gleiche gilt für Projektgruppen, die aus verschiedenen Personen aus den einzelnen DRK-Gliederungen zusammengesetzt sind.

Namensschilder für den Tisch sind grundsätzlich unproblematisch, da die Namen im Laufe einer Veranstaltung genannt werden. Jedoch müssen diese nach der Veranstaltung geschreddert werden.

4.4 Jugendrotkreuz

Im Bereich JRK ist zu empfehlen, dass Fotos und Videos für Kinder und Jugendliche bis 16 Jahren nur mit schriftlicher Einwilligung der sorgeberechtigten Personen veröffentlicht werden dürfen. Es ist darauf zu achten, ob Alt-Einwilligungen (vor dem 25.05.2018) noch datenschutzkonform sind, ansonsten müssten diese angepasst werden (siehe Kapitel 1.7). Fotos und Videos sind in regelmäßigen Abständen zu löschen bzw. zu archivieren. Die Archivierung muss durch eine Zweckbindung legitimiert werden. Sobald der Erhebungszweck weggefallen ist, sind die Bilder zu löschen. Die Archivierung erfolgt revisionssicher und es haben nur die Personen mit einem berechtigten Interesse Zugriff.

4.5 Hundestaffel

Einsatzleitung der Hundestaffel erhält i. d. R. alle einsatzrelevanten Daten von der einsatzauslösenden Stelle (i. d. R. Polizeibehörde). Neben Stammdaten werden auch besonders schützenswerte Daten (z. B. Fotos; Gesundheitsdaten) übergeben. Diese Daten müssen nach dem Einsatz unverzüglich datenschutzkonform gelöscht werden. Die erhaltenen personenbezogenen Daten müssen bis zur Löschung durch geeignete technische und organisatorische Maßnahmen geschützt werden, so dass unberechtigte Dritte keinen Zugriff auf die Daten bekommen können.

Das Einsatzprotokoll sollte keine personenbezogenen Daten enthalten bzw. nur solche Datenkategorien (z. B. Geschlecht) enthalten, die keinen Rückschluss zu dem Betroffenen zulassen. Wenn keine personenbezogenen Daten erhoben werden, sind keine weiteren Maßnahmen durchzuführen. Sollte ein Einsatz des Rettungsdienstes notwendig sein, dann muss die Datenerhebung durch den Rettungsdienst/die Leistelle erfolgen.

4.6 Bergwacht/ Wasserwacht

Personenbezogene Daten werden von der einsatzauslösenden Stelle an die Berg-/Wasserwacht übermittelt. Das Einsatzprotokoll bleibt mit Durchschlag bei der Berg-/Wasserwacht. Ein Durchschlag erhält der Patient und ein Durchschlag erhält ggf. der Rettungsdienst zur weiteren Behandlung. Es

sind Maßnahmen zu ergreifen, die gewährleisten, dass das Einsatzprotokoll datenschutzkonform aufbewahrt wird, d. h., dass unberechtigten Dritten keine Einsicht erhalten. Das Abrechnungsformular wird über eine Cloud mit datenschutzkonformem Zugang an den DRK Landesverband transferiert.

Die Betroffenen sind über ihre Rechte zum Zeitpunkt der Datenerhebung zu informieren, sofern dies möglich ist. Daher sollten die Datenschutzinformationen bei den Einsätzen mitgeführt werden und ggf. an den Betroffenen ausgehändigt werden.

4.7 Sanitätsdienst

Bei der Versorgung eines Patienten ist darauf zu achten, dass zum Zeitpunkt der Datenerhebung die Datenschutzinformationen der betroffenen Person (sofern möglich) übergeben werden. Das analoge Patientenprotokoll ist bis zur Übergabe an die Verantwortliche Person sicher aufzubewahren, so dass kein unberechtigter Dritte die personenbezogenen Daten einsehen kann (z. B. verschließbare Mappe). Sollte das analoge Patientenprotokoll nach dem Einsatz aufbewahrt werden, dann ist auch hier auf die datenschutzkonforme Aufbewahrung bis zur Löschung zu achten. Bei der digitalen Erfassung der Patientendaten ist darauf zu achten, dass das Endgerät vor einem unberechtigten Zugriff durch ein datenschutzkonformes Passwort.

4.8 Tafelläden

Bedürftige erhalten in Tafelläden Essen in Tafelläden, die die Bedürftigkeit nachweisen müssen (z. B. Sozialausweis). Die Daten (i. d. R. Name, Vorname, Wohnort und Anzahl der Familienmitglieder) werden entweder digital oder analog erfasst. Datenerhebung weiterer Kategorien wie z. B. Status ist nicht zulässig, da diese Datenkategorie nicht notwendig ist. Wichtig ist, den Tafelausweis zu pseudonymisieren z. B. durch Nummernvergabe und nur die Daten erheben, die notwendig sind.

4.9 Kleiderläden/Kleiderkammer

Kleiderläden erheben keine personenbezogenen Daten von Bedürftigen. Die Bedürftigkeit wird anhand eines Sozialausweises nachgewiesen.

4.10 Blutspendedienst

Die Geschäftsführung der Blutspendedienst gGmbH und nicht die jeweilige DRK-Gliederung ist für den Datenschutz verantwortlich. Die Sensibilisierung der Ehrenamtlichen der DRK-Gliederung über die datenschutzkonforme Datenverarbeitung liegt in der Verantwortung des Blutspendedienstes.