Datenschutz-Richtlinie
des Kreisfeuerwehrverbandes Limburg-Weilburg e.V.

Profil für diese Richtlinie:

Allgemein	
Kurztitel	Datenschutz-Richtlinie
Dokumenten-Nr.	DS-RL – 001
Klassifizierung	Richtlinie
Geltungsbereich	Kreisfeuerwehrverband Limburg-Weilburg e.V. (KFV)
Adressatenkreis	Alle Mitarbeitenden in den Gremien des KFV und alle Personen, die in sonstiger Weise für den KFV tätig werden.
Freigabe durch	Vorstand
Beschluss am	16.10.2018
Inkrafttreten am	16.10.2018
Gültigkeitsdauer	Bis zur Überarbeitung
Thema	Regelungen zu Datenschutz und Datensicherheit im KFV

Verantwortlichkeiten	
Ansprechpartner	Vorsitzender Thomas Schmidt verbandsvorsitzender @ kreisfeuerwehrverband.net
Dokumentenverantwortlicher	Vorstand
Beteiligte	Stv. Vorsitzender Michael Kintscher Stv. Vorsitzender Bernd Rompel Pressesprecher Yannick Silbereisen

Weitere Unterlagen	
Anlagen	Siehe Nr. 4

Änderungshistorie

Version	**Datum**	**Autor/ Ansprechpartner/in**	**Kurzbeschreibung/ Anlass**
1.0	31.08.2018	Michael Kintscher	Erstentwurf auf Basis Vorstands-beschluss vom 07.08.2018
1.1	20.09.2018	Thomas Schmidt	Zugriff auf Florix eingearbeitet
1.2	20.09.2018	Bernd Rompel	Zugriff auf KFV-Server eingearbeitet, redaktionelle Änderungen, Forma-tierung
1.3	09.10.2018	Bernd Rompel	Zusammenstellung mit Anlagen
1.4	16.10.2018	Bernd Rompel	Fertigstellung und Herausgabe nach Vorstandsbeschluss vom 16.10.2017

Inhaltsverzeichnis:

1 Einleitung ... 3
1.1 Zielsetzung ... 3
1.2 Geltungsbereich ... 3
1.3 Adressatenkreis ... 3
2 Hauptteil ... 3
2.1 Geltungsbereich/Verantwortung ... 3
2.1.1 Grundnorm und Umfang des Datenschutzes ... 3
2.1.2 Schutz der Daten ... 4
2.1.3 Verantwortlichkeiten, Datenschutzbeauftragter, Ansprechpartner/ innen für den Datenschutz ... 4
2.1.4 Belehrung neuer Mitarbeitender über den Datenschutz ... 5
2.1.5 Sonstige Personen ... 5
2.1.6 Ordnungswidrigkeiten/Strafbestimmungen ... 5
2.1.7 Datenschutz-Haftpflichtversicherung ... 6
2.2 Begriffsdefinitionen ... 6
2.2.1 Persönliche Daten ... 6
2.2.2 Interne Daten ... 6
2.2.3 Weitere Begriffsbestimmungen ... 6
2.3 Datenschutz ... 8
2.3.1 Datenerhebung ... 8
2.3.2 Datenschutzhinweis ... 8
2.4 Technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit ... 8
2.4.1 Archiv ... 8
2.4.2 Verwahrung von Unterlagen, mobilen Geräten und Datenträgern ... 8
2.4.3 Entsorgung von Unterlagen, Datenträgern und IT-Geräten ... 9
2.4.4 Datensicherheit beim Telefax / Multifunktionsgeräte ... 10
2.4.5 Sicherheitsmaßnahmen beim Einsatz der Informationstechnik ... 11
2.5 Umgang mit Bildmaterial ... 14
2.6 Inkrafttreten ... 14
3 Konsequenzen eines Verstoßes ... 14
4 Anlagen zur Richtlinie ... 15

1 Einleitung

1.1 Zielsetzung

Der KFV verfügt aufgrund seiner Aufgaben über eine Vielzahl von personenbezogenen Daten und sensiblen, schutzwürdigen Tatbeständen. Die Betroffenen sind hierbei in Teilen ihrer Persönlichkeit erfasst.

Der Vorstand des KFV hat eine gesetzliche Verantwortung bei der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten.

Datenschutz und Datensicherheit haben demzufolge beim KFV einen sehr hohen Stellenwert.

Daraus ergeben sich für den KFV die folgenden Grundsätze zum Datenschutz:

- Datenschutz ist eine gesetzliche Aufgabe und eine vereinspolitische Verpflichtung.
- Datenschutz trägt zum Erfolg der Arbeit im KFV bei und stärkt das Ansehen des KFV.
- Datenschutz ist ein Qualitätsfaktor.
- Datenschutz schafft und stärkt das Vertrauen der Betroffenen und der Mitarbeitenden.

1.2 Geltungsbereich

Rechtsgrundlagen für diese Richtlinie sind die EU-Datenschutzgrundverordnung (DSGVO), das Bundesdatenschutzgesetz (BDSG) sowie das Hessische Datenschutz- und Informationsfreiheitsgesetz (HDISG).

1.3 Adressatenkreis

Alle Mitarbeitenden in den Gremien des KFV sind verpflichtet, im Rahmen ihrer Tätigkeiten im und für den KFV die in dieser Richtlinie enthaltenen Regelungen zu beachten. Ebenfalls alle Personen, die außerhalb der Zugehörigkeit zu den Gremien des KFV für den KFV tätig werden.

2 Hauptteil

2.1 Geltungsbereich/Verantwortung

2.1.1 Grundnorm und Umfang des Datenschutzes

Jede Person hat Anspruch darauf, dass die sie betreffenden persönlichen Daten vom KFV nicht unbefugt erhoben, verarbeitet oder genutzt werden. Aus diesem Grundsatz ergeben sich zur Sicherstellung des Datenschutzes folgende Pflichten:

- Aktives Handeln zur Wahrung des Datengeheimnisses.
- Unterlassen unbefugter Erhebung, Verarbeitung und Nutzung persönlicher Daten.

- Melden von Feststellungen zu unrechtmäßig übermittelten oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangten personenbezogenen Daten.
- Korrektur von fälschlich oder missbräuchlich gespeicherten oder genutzten Daten.

Diese Pflichten des Datenschutzes gelten grundsätzlich auch für die persönlichen Daten Verstorbener.

Für die beim KFV ehrenamtlich tätigen Personen sollen alle für die Durchführung ihrer dienstlichen Aufgaben notwendigen Daten sowie Betriebs- und Geschäftsgeheimnisse zugänglich sein. Damit ist die Verpflichtung verbunden, diese Daten auch innerhalb des KFV nur bei dienstlicher Notwendigkeit an Zuständige weiterzugeben.

Eine Weitergabe von Daten ist grundsätzlich verboten. Ob ggf. im Einzelfall eine gesetzliche Auskunftspflicht an Dritte, Zeugnispflicht vor Gericht oder Pflicht zum Vorlegen oder Ausliefern von Schriftstücken, Akten und Dateien besteht, entscheidet der Vorsitzende.

Auf die datenschutzrechtlichen Kriterien zur Datenerhebung, -verarbeitung und -nutzung verweisen die entsprechenden Ausführungen in dieser Richtlinie.

Die Mitarbeitenden des KFV haben auch nach Beendigung ihrer Tätigkeit das Datengeheimnis zu wahren.

Bei einer gewollten Übertragung von Daten (Auftragsdatenverarbeitung) sind besondere Regelungen zu beachten.

2.1.2 Schutz der Daten

Beim KFV sind eine Vielzahl personenbezogener Daten vorhanden (z. B. Personaldaten, Fotos, Lieferantendaten sowie Daten von Lehrgangsteilnehmern/innen etc.). Diese Daten unterliegen den Schutzbestimmungen der Datenschutzgrundverordnung, des Bundesdatenschutzgesetzes (BDSG), des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (HDISG) sowie ggf. anderer Spezialgesetze.

2.1.3 Verantwortlichkeiten, Datenschutzbeauftragter, Ansprechpartner/innen für den Datenschutz

Die Verantwortung für die Einhaltung der Datenschutzbestimmungen nach dieser Richtlinie haben alle Mitarbeitenden des KFV für ihren jeweiligen Verantwortungsbereich. Die Verantwortung gilt auch in vollem Umfang bei der Wahrnehmung von Terminen im Auftrag des KFV sowie bei der Arbeit mit eigenen elektronischen Medien im häuslichen Bereich. Sie erfasst auch die Regelungen zur technischen Datensicherheit.

Da beim KFV weniger als 9 Personen ständigen Zugriff auf alle gespeicherten Daten haben, ist kein/e Datenschutzbeauftragter/e zu bestellen.

Verantwortlich für den Datenschutz im KFV ist der Vorsitzende Thomas Schmidt, Neunkircher Str. 12, 35799 Merenberg.

Der Vorstand wirkt durch Beratung, Kontrolle und aktive Einflussnahme, sowie durch Aufstellung von Richtlinien und fachlichen Anweisungen auf die Einhaltung der einschlägigen Datenschutz- und Datensicherheitsvorschriften hin. In allen Fragen des

Datenschutzes und der Datensicherheit sollten sich die Mitarbeitenden des KFV an den Vorstand wenden. Durch den Vorstand soll die entsprechende Unterstützung und Beratung zu den Themen Datenschutz und Datensicherheit erfolgen.

2.1.3.1 Informationspflichten bei Datenschutzmängeln, -beschwerden, -verstößen und unrechtmäßiger Kenntniserlangung von persönlichen Daten

Verstöße gegen den Datenschutz und die Datensicherheit sowie festgestellte Mängel und Beschwerden sind dem Vorstand des KFV unverzüglich zu melden.

Sollten sich beim KFV Anhaltspunkte für Verstöße oder Mängel ergeben oder wurde festgestellt, dass gespeicherte Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, ist ebenfalls unverzüglich der Vorstand des KFV zu informieren.

Der Vorstandsvorsitzende klärt in Abstimmung mit den jeweils Verantwortlichen, ob schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen und die Aufsichtsbehörden sowie die Betroffenen nach Artikel 33 und 34 DSGVO zu informieren sind. Die Entscheidung über eine Information und ggf. die Art und den Umfang der Benachrichtigung trifft der Vorstand des KFV.

Bei Verlust oder Diebstahl von Daten (Papierunterlagen oder Datenträger) ist umgehend der Vorstandsvorsitzende bzw. der Vorstand des KFV zu informieren.

Der Vorstandsvorsitzende ist in alle Vorgänge und Anfragen der/des Hessischen Datenschutzbeauftragten einzubeziehen.

2.1.4 Belehrung neuer Mitarbeitender über den Datenschutz

Alle Mitarbeitenden des KFV, die aufgrund der von ihnen wahrgenommenen Tätigkeiten dauernd oder regelmäßig personenbezogene Daten zur Kenntnis nehmen, erheben, verarbeiten oder nutzen, werden bei Beginn ihrer Tätigkeit durch den Vorstand des KFV oder dem/der Sprecher/in des jeweiligen Fachbereichs zur besonderen Verschwiegenheitspflicht belehrt und insbesondere auf die Bestimmungen der DSGVO hingewiesen (vgl. Anlage 4). Die zu unterzeichnende Verpflichtungserklärung wird digital auf dem Server des KFV abgelegt.

2.1.5 Sonstige Personen

Die Regelungen über die Verschwiegenheitspflicht und den Datenschutz gelten auch für sonstige Personen (z. B. Rechtsanwälte, Unternehmensberater, Referenten o. ä.), die für den KFV tätig werden.

2.1.6 Ordnungswidrigkeiten/Strafbestimmungen

Verstöße gegen die Datenschutzvorschriften sind ein Vertrauensbruch gegenüber den Personen, deren Daten dem KFV bekannt geworden sind und haben äußerst negative Auswirkungen auf das Ansehen des KFV in der Öffentlichkeit.

Verstöße können sowohl für den KFV, als auch für jeden einzelnen Mitarbeitenden bußgeld-, haftungs- und strafrechtliche Folgen haben. In diesem Zusammenhang wird auf die Art. 82 ff. DSGVO sowie § 203 Abs. 2 und § 353b StGB hingewiesen.

2.1.7 Datenschutz-Haftpflichtversicherung

Verletzungen der Datenschutzbestimmungen können, unabhängig von einem Verschulden,

Haftpflichtansprüche nach sich ziehen. Zur Absicherung von Ansprüchen auf Ersatz eines immateriellen Schadens wegen Verletzung des Persönlichkeitsrechts hat deshalb der KFV eine Haftpflichtversicherung abgeschlossen. Haftpflichtansprüche gegen den KFV sind unverzüglich dem Vorstandsvorsitzenden zu melden.

2.2 Begriffsdefinitionen

2.2.1 Persönliche Daten

Alle Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), die dem KFV im Rahmen seiner Aufgabenerfüllung bekannt geworden sind, verstehen sich als persönliche Daten.

Nachstehende Beispiele sollen diesen Grundsatz verdeutlichen:

- Name, Anschrift, Geburtsdatum, Beruf, Arbeitgeber, Kinderzahl, Foto, E-Mail-Adresse, Telefonnummer usw.

Dem Datenschutz unterliegen ferner Betriebs- und Geschäftsgeheimnisse von z. B. Vertragspartnern und allen anderen juristischen Personen, die vom KFV erhoben, verarbeitet oder genutzt werden.

2.2.2 Interne Daten

Hierunter sind alle Daten zu verstehen, die nicht persönliche Daten sind, z. B.:

Lieferantendaten sowie Betriebs- und Geschäftsgeheimnisse des KFV wie z. B. statistische Daten, Richtlinien, fachliche Anweisungen, Strategiepapiere, Vorstandsentscheidungen, Sitzungsprotokolle, Beschreibung spezifischer KFV-Software-Produkte, etc.

Diese Daten unterliegen der Geheimhaltung. Sie sind durch die Regelungen der §§ 203, 204 StGB besonders geschützt. Über die Herausgabe an Dritte entscheiden im Einzelfall der Vorstand oder die hierzu ermächtigten Personen.

2.2.3 Weitere Begriffsbestimmungen

Beim Umgang mit den Daten sind nachstehende, näher festgelegte Begriffe von Bedeutung:

2.2.3.1 Erheben

Ist jede Art von Beschaffen der Daten über den Betroffenen; wegen der hier zu beachtenden Kriterien vgl. Abschnitte 2.3.1 und 2.3.2.

2.2.3.2 Verarbeiten

Bedeutet das Speichern, Verändern, Übermitteln, Sperren und Löschen der Daten. Hinsichtlich der Zulässigkeit und Zweckbindung wird auf die folgenden Abschnitte verwiesen.

2.2.3.3 Nutzen

Ist jede Verwendung der Daten, soweit es sich nicht um Verarbeitung handelt, also beispielsweise auch die Kenntnisnahme durch Mitarbeitende, oder die Weitergabe innerhalb des KFV.

2.2.3.4 Pseudonymisieren

Ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

2.2.3.5 Anonymisieren

Ist das Verändern von persönlichen Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

2.2.3.6 Verantwortliche Stelle

Ist jede Person oder Stelle, die persönliche Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag (Auftragsdatenverarbeitung) vornehmen lässt.

2.2.3.7 Empfänger

Ist jede Person oder Stelle, die Daten erhält.

2.2.3.8 Dritter

Ist jede Person oder Stelle außerhalb der verantwortlichen Stelle.

2.2.3.9 Besondere Arten personenbezogener Daten

Sind Angaben über ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, o. ä.

2.2.3.10 Löschen

Ist das Unkenntlichmachen gespeicherter Daten.

2.2.3.11 Sperren

Ist das vollständige oder teilweise Untersagen der weiteren Verarbeitung oder Nutzung von Daten durch entsprechende Kennzeichnung.

2.3 Datenschutz

2.3.1 Datenerhebung

Der KFV darf persönliche Daten und besondere Arten personenbezogener Daten nur erheben und speichern, soweit dies für die satzungsmäßige Aufgabenerfüllung notwendig ist oder der/die Betroffene ausdrücklich eingewilligt hat. Angaben über die ethnische Herkunft dürfen ohne besondere Einwilligung nicht erhoben werden.

Grundsätzlich sind persönliche Daten bei dem/der Betroffenen selbst zu erheben, wobei der Erhebungszweck anzugeben ist.

Darüber hinaus gilt der allgemeine Grundsatz der Datensparsamkeit. Die Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig persönliche Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind Verfahren zur Anonymisierung, Pseudonymisierung und zur Verschlüsselung von Daten nach dem Stand der Technik vorzusehen.

2.3.2 Datenschutzhinweis

Grundsätzlich ist auf allen Briefen, Formularen, Fragebögen, Internetformularen, App-Anwendungen, die der Erhebung von Daten im Rahmen der satzungsgemäßen Aufgaben des KFV dienen, ein Datenschutzhinweis im Sinne der DSGVO an geeigneter Stelle anzubringen bzw. drucktechnisch an hervorgehobener Stelle im Text zu integrieren (siehe KFV-Muster-Briefvorlage und KFV-Muster-E-Mail-Autosignatur im jeweils neuesten Versionsstand).

2.4 Technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit

Der Vorstand des KFV hat die Entwicklung und Einführung organisatorischer und technischer Sicherheitsmaßnahmen mit sicherzustellen.

2.4.1 Archiv

Zur Gewährleistung des Datenschutzes ist eine Archivnutzung mit einzubeziehen. Archivräume sind stets abzuschließen und dürfen nur von den zutrittsbefugten Mitarbeitenden zur Erledigung ihrer übertragenen Aufgaben betreten werden.

Auf die örtlichen Gegebenheiten ist Rücksicht zu nehmen.

Es ist sicherzustellen, dass Besucher, Handwerker, Techniker usw. grundsätzlich nicht ohne Begleitung in den Räumen des Archivs verweilen.

2.4.2 Verwahrung von Unterlagen, mobilen Geräten und Datenträgern

Die Mitarbeitenden des KFV tragen für den jeweiligen Bereich die Verantwortung dafür, dass die Vertraulichkeit der Daten auch im Umgang mit den Arbeitsunterlagen stets gewahrt wird.

Sämtliche Arbeitsunterlagen mit persönlichen Daten, internen Daten sowie Betriebs- und Geschäftsgeheimnissen des KFV (siehe Abschnitte 2.1.1 und 2.2.2) sind so zu verwahren, dass jeder Zugriff oder die Einsichtnahme durch Unbefugte nach

menschlichem Ermessen ausgeschlossen ist. Als Arbeitsunterlagen verstehen sich hierbei Datenträger wie Karteien, Belege, Schriftstücke, Auflistungen, Akten und Aktensammlungen einschließlich ihrer Bestandteile.

Solche Unterlagen sind auch im häuslichen Bereich der Mitarbeitenden des KFV ausnahmslos in verschließbaren Behältnissen unterzubringen (Schränke, Schreibtische, usw.). Die Schlüssel für diese Behältnisse sind an geeigneter Stelle so aufzubewahren, dass sie Unbefugten nicht ohne weiteres zugänglich sind.

Jede einzelne Mitarbeiterin und jeder einzelne Mitarbeiter trägt hier die Verantwortung, dass diese Unterlagen nicht durch Unachtsamkeit Unbefugten (dazu gehören auch Familienangehörige) zugänglich gemacht werden.

Digitale Speichermedien (z. B. Festplatten, Speichersticks, CD-ROM, DVD und ähnliche) sind vor unberechtigten Zugriffen und vor Beschädigungen geschützt aufzubewahren.

Das Verarbeitungsverzeichnis des KFV regelt, wer personenbezogene Daten verarbeitet und wie dies digital zu geschehen hat. Werden entgegen dieser grundsätzlichen Regelung personenbezogene Daten im Einzelfall auf mobilen PC oder Datenträgern gespeichert, sind diese entsprechend den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu verschlüsseln (z. B. BitLocker, dm-crypt oder Veracrypt).

Die elektronische Archivierung (z. B. Sicherungskopie) ist in regelmäßigen Abständen durchzuführen. Die nach den einschlägigen Vorschriften vorgegebenen Aufbewahrungsfristen, sowie die Sperrung bzw. Löschung der Daten nach Ablauf dieser Aufbewahrungsfristen sind zu beachten.

2.4.3 Entsorgung von Unterlagen, Datenträgern und IT-Geräten

2.4.3.1 Papierabfälle und Altpapier

Die Mitarbeitenden des KFV haben eine sichere Behandlung von Papierabfällen und Altpapier zu gewährleisten. Eine besondere Schwachstelle bildet hier bereits der Weg vom Schreibtisch bis zur endgültigen Papiervernichtung. Papierabfälle und Altpapier sollten deshalb, je nach Sensibilität der Daten, stets zerkleinert in die vorgesehenen Behältnisse gegeben werden. Es ist zu verhindern, dass Papierabfälle mit noch lesbaren sensiblen Daten in die Müllcontainer geraten und damit unbefugten Dritten zur Kenntnis gelangen können.

2.4.3.2 Elektronische Datenträger, Elektronikschrott

Vor der Entsorgung nicht mehr benötigter oder unbrauchbar gewordener elektronischer Datenträger (Disketten, Festplatten, optische Speichermedien, Worm usw.) sind die gespeicherten Daten zu löschen. Unter Löschen ist das endgültige Unkenntlichmachen gespeicherter Daten zu verstehen. Um Daten physisch auf elektronischen Datenträgern sicher zu löschen, müssen diese mit geeigneter Software überschrieben werden. Ist dies nicht möglich, so müssen sie physisch zerstört werden. Bei der Umsetzung bzw. Aussonderung von PCs sind Löschmaßnahmen zu wählen, die eine Rekonstruktion der gelöschten Daten mit hoher Wahrscheinlichkeit ausschließen. Unterschiedliche, nicht einheitlich vorgegebene Verfahren, wie mehrfaches Überschreiben, Datenlöschung mit Magnet, Zerstörung (z. B. Schredder) bieten Datensicherheit.

Müssen Datenträger ohne die vorherige Möglichkeit des sicheren Löschens der Daten aus der Hand gegeben werden (z. B. Reparatur, Rückgabe an den Hersteller in der Garantiezeit, Austausch von Leasinggeräten), ist in Abhängigkeit von der Sensibilität der Daten auf dem Datenträger durch vertragliche Regelungen zu verhindern, dass unerwünschte Informationsflüsse stattfinden oder von Unbefugten ausgenutzt werden. In Abhängigkeit von der Sensibilität der enthaltenen Daten ist im Einzelfall ggf. auf Garantieansprüche zu verzichten.

Diese Regelungen sind auch beim Verkauf oder Austausch von Hardware mit Speichermedien zu beachten.

2.4.4 Datensicherheit beim Telefax / Multifunktionsgeräte

2.4.4.1 Sorgfaltsregeln beim Umgang mit dem Telefax

Beim Versand von Telefaxen gilt der allgemeine Grundsatz, dass der Absender/die Absenderin die Verantwortung für die vertrauliche Übertragung und den Empfang trägt.

Er/sie muss einkalkulieren, dass jemand, für den das Telefax nicht bestimmt ist, dieses aufgrund eines Bedienungs- oder eines technischen Fehlers erhält und liest.

Folgendes ist deshalb zu beachten:

- Anschlussnummer des Empfängers überprüfen
  Der Absender prüft, ob er/sie (noch) die richtige Telefaxnummer des Empfängers besitzt. Dies ist vor allem deshalb empfehlenswert, weil Telekommunikationsunternehmen die Nummer eines abgemeldeten Telefax-Anschlusses mitunter schon nach kurzer Zeit wieder an einen anderen Teilnehmer vergeben.
- Kein zeitversetztes Senden
  Das von manchen Geräten ermöglichte zeitversetzte Absenden von Telefaxen, mit dem es beispielsweise möglich ist, die am Tag vorbereiteten Sendungen in der Nacht zu übertragen, darf möglichst nicht genutzt werden, wenn die Sendung personenbezogene Daten enthält. Dies deshalb, weil der Absender/die Absenderin bei einer erkennbaren Fehlleitung die Übertragung nicht rechtzeitig abbrechen und der persönliche Empfang hierbei in der Regel nicht gewährleistet werden kann.
- Eingaben überprüfen
  Sofern der Absender/die Absenderin die gewünschte Rufnummer über die Tastatur eingibt, hat er/sie die Nummer zunächst am Display zu überprüfen, bevor er/sie durch einen Druck auf die Start-Taste dafür sorgt, dass das Telefaxgerät die eingegebene Nummer wählt.
- Nummer des erreichten Geräts überprüfen
  Wenn das Telefaxgerät nach erfolgreicher Wahl eine Verbindung aufgebaut hat, zeigt es am Display die Rufnummer an, mit der sich das angerufene Gerät meldet. Wenn diese Nummer von der eingegebenen Nummer abweicht, ist Vorsicht geboten. Der Absender/die Absender-in hat dann den Übertragungsvorgang sofort abzubrechen. Falls das Telefaxgerät bei mehr-maligen Versuchen immer die gleiche falsche Rufnummer anzeigt, ist der vorgesehene Empfänger

anzurufen, um zu erfahren, ob das Gerät eine falsche Gerätekennung aussendet oder ob eine Rufumleitung auf eine andere als die gewählte Nummer erfolgt.

- Sendebericht prüfen
  Nach dem Absenden eines Telefaxes hat der Absender/die Absenderin den Sendebericht zu überprüfen und zu kontrollieren, ob die richtige Verbindung zustande kam.
- Vorgehen bei Irrläufern
  Im Fall einer Fehlübertragung ist der Empfänger aufzufordern, den Telefax-Irrläufer sofort zu vernichten.
- Sendeberichte
  Es ist zu gewährleisten, dass es jederzeit möglich ist (z. B. anhand von Sendeberichten) festzustellen, wann welches Fax an welchen Empfänger versandt wurde.

2.4.4.2 Besonderheiten bei der Übertragung sensibler Daten

Da es bei der Telefax-Übertragung leicht zu Irrläufern kommen kann und sich empfangene Telefax-Sendungen zudem nur schwer vor unberechtigter Kenntnisnahme schützen lassen, dürfen besonders sensible Daten grundsätzlich nicht per Telefax versandt werden.

Ausnahmen davon sind nur vertretbar, wenn besondere Sicherheitsmaßnahmen ergriffen werden, die zuverlässig verhindern, dass die übertragenen Daten Dritten bekannt werden können. Einen solchen Schutz kann beispielsweise die verschlüsselte Übertragung bieten, wobei auch in diesem Fall der Absender/die Absenderin die Telefax-Übertragung in jedem einzelnen Fall telefonisch ankündigen sollte, damit der Empfänger das Telefax persönlich entgegennehmen kann.

Alternativ kommt für eilbedürftige Sendungen auch die Übertragung per verschlüsselter E-Mail in Betracht. Als weitere Alternative kann auch der Personenbezug (Anonymisierung/Pseudonymisierung) entfernt werden. Solange geeignete Verschlüsselungstechniken für den Einzelfall nicht zur Verfügung stehen oder nicht angewandt werden können, bleibt nur die Möglichkeit des Briefverkehrs.

Diese Regelungen gelten auch beim Einsatz von Fax-Servern.

2.4.4.3 Sorgfaltsregeln beim Umgang mit Multifunktionsgeräten

Multifunktionsgeräte verfügen über eine Druck-, Kopier-, Scan- und Faxfunktion. Aus datenschutzrechtlicher Sicht ist zu beachten, dass eine datenschutzgerechte Druckausgabe (Aufstellungsort, Zugriffschutz) nutzerbezogen gewährleistet sein muss, um auszuschließen, dass Ausdrucke und Kopien von unberechtigten Dritten eingesehen werden können.

2.4.5 Sicherheitsmaßnahmen beim Einsatz der Informationstechnik

2.4.5.1 Passwortverfahren und Berechtigungsvergabe

Die Zugriffsberechtigungen auf die Datenbestände des KFV sind auf die konkreten Aufgaben der Mitarbeitenden zu begrenzen. Um den erforderlichen Zugriffsschutz zu

erreichen, sind neben der technischen Unterteilung der Datenbestände in die Arbeits- und Fachgebiete für jede Mitarbeiterin und jeden Mitarbeiter eine Benutzerkennung, ein Berechtigungsprofil und ein persönliches Passwort notwendig.

Der Berechtigungsumfang ist je Mitarbeiter/in und für Externe (z. B. Systemberater o. ä.) für Abfragen, Erfassungen und PC-Anwendungen aufgaben- und fachgebietsorientiert zu definieren.

Für das Passwortverfahren gelten nachstehende allgemeine Grundsätze:

- die Benutzerkennungen sind passwortgeschützt,
- für besonders wichtige Funktionen sind Zusatzpassworte möglich.

Folgende Regelungen sind von der Benutzerin/dem Benutzer einzuhalten:

- die Benutzerin/der Benutzer hat sich durch Eingabe ihrer/seiner Benutzerkennung und eines Passwortes zu authentifizieren,
- jede Benutzerin/jeder Benutzer erhält ein persönliches Passwort,
- das Passwort darf nur der Benutzerin/dem Benutzer bekannt sein,
- die Benutzerin/der Benutzer muss sich ihr/sein Passwort selbst definieren,
- die Mindestlänge von Passworten muss 8 Zeichen betragen,
- das Passwort darf keinen Bezug auf die Passwortinhaberin/den Passwortinhaber oder ihre/seine Umgebung haben (Name, Vorname, Freund, Name der Kinder, Telefonnummer etc.),
- das Passwort muss enthalten: Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen,
- das Passwort ist sofort zu ändern, wenn der Verdacht besteht, dass andere Personen davon Kenntnis haben,
- die Weitergabe des Passwortes an andere Personen ist untersagt.

2.4.5.2 Umgang mit PCs, mobilen Systemen/Netzwerken

Hinsichtlich des Umgangs mit PCs, Notebooks, USB, PDAs, Smartphones etc. und Netzwerken wird auf die datenschutzrechtlichen Regelungen zur Verwendung auf privaten Rechnersystemen verwiesen.

2.4.5.3 Datensicherung

Die Datensicherung ist gesondert zu regeln. Bei Einsatz von PCs, mobilen Systemen und Netzwerken wird auf die datenschutzrechtlichen Regelungen zur Verwendung auf privaten Rechnersystemen verwiesen.

Sollte in Einzelfällen eine Abspeicherung von Daten auf der lokalen Festplatte von PCs notwendig sein, trägt der Benutzer/die Benutzerin die Verantwortung für die Datensicherung und deren zugriffssichere Aufbewahrung. Die Speicherung ist auf die erforderlichen Daten zu beschränken. Bei Wegfall der Notwendigkeit der lokalen Speicherung sind die Daten dort vom Benutzer/von der Benutzerin wieder zu löschen.

2.4.5.4 E-Mail

Der Nutzer/die Nutzerin muss sich über die zu beachtenden datenschutzrechtlichen Kriterien vor der Nutzung eines Mailsystems im Klaren sein und ist für deren Einhaltung verantwortlich. Verantwortlich für die Zulässigkeit der E-Mail-Nachrichten ist der Absender.

Unzulässig ist eine Nutzung, wenn für den Vorgang zwingend eine eigenhändige Unterschrift vorgesehen ist oder wenn gesetzliche Vorschriften zum Datenschutz oder dem entgegenstehen.

Die Adressierung von E-Mails ist zur Vermeidung einer fehlerhaften Zustellung stets eindeutig und besonders sorgfältig vorzunehmen.

Generell zu berücksichtigen ist, dass eine E-Mail wie eine Postkarte eine öffentlich zugängliche Nachricht ist, bei der ohne geeignete zusätzliche Sicherheitsmaßnahmen die Vertraulichkeit oder Echtheit der im Netz übermittelten Informationen nicht gewährleistet ist. Deshalb dürfen personenbezogene Daten oder sonstige vertrauliche Informationen (z. B. Betriebs- und Geschäftsgeheimnisse) nicht ohne dem aktuellen Stand entsprechender Verschlüsselungstechnik per externer E-Mail übermittelt werden.

Soll ein E-Mail an mehrere Empfänger geschickt werden, ist sicher zu stellen, dass die Empfängeradressen gegenseitig verborgen bleiben (z. B. bei Nutzung von Microsoft-Outlook ein Versand als Bcc). Der Empfängerkreis ist ohne personenbezogenen Angaben und E-Mailadresse dem Text des E-Mails voranzustellen oder am Ende der E-Mail in Form eines Verteilers aufzulisten. Ausgenommen hiervon sind E-Mails bzw. Outlook-Terminvereinbarungen zwischen den Mitarbeitenden des KFV.

Wird einer E-Mail eine Datei mit personenbezogenen Angaben angehängt, gelten auch für diese Anhänge die datenschutzrechtlichen Bestimmungen und Sicherheitshinweise. Dies bedeutet z. B.

- Verschlüsselung einer Datei mit personenbezogenen Daten mit dem Programm 7-Zip o. ä.) und Übersendung des Schlüssels per neutraler separater E-Mail bzw. per anderem Medium.
- Unabhängig vom Inhalt: Kein Versand oder Weitergabe veränderbarer Word-, Excel- oder Powerpoint-Dateien an Nichtfunktionsträger des Verbandes. Diese sind vor dem Versand ins pdf-Format zu konvertieren. Dies betrifft nicht den Versand oder die Weitergabe an Mitarbeitende des KFV (Vorstand, Verbandsausschuss, Fachbereiche, Arbeitskreise).

2.4.5.5 Nutzung von Florix bzw. des KFV Daten-Servers *(gilt nur für die berechtigten Nutzer)*

Aus Gründen, welche in der Eigenart des ehrenamtlichen Feuerwehrdienstes für den KFV (Vorstand, Verbandsausschuss, Fachbereiche, Arbeitskreise) liegen, kann eine Nutzung von PCs, welche sich nicht im Eigentum des KFV befinden (z. B. privateigene PCs), als Endgerät für feuerwehrspezifische Anwendungen sowohl organisatorisch als auch wirtschaftlich notwendig sein.

Bei einer derartigen Nutzung ist folgendes zu beachten:

- User-Accounts und Passwörter der Anwendung DellSonicWALL NetExtender sowie des weiteren Datenzugangs auf die Florix bzw. KFV-Daten sind

ausschließlich für verbandliche Zwecke zu verwenden und dürfen anderen Personen nicht zugänglich gemacht werden. Eine Speicherung von User-Account und Passwort ist nicht zulässig (Ausnahme vom BSI anerkannte Passwortsafes mit ausreichender Verschlüsselung).

Jeder Nutzer ist für die Sicherheit seines Endgerätes, mit dem auf den Florix- bzw. KFV-Server zugegriffen wird, selbst verantwortlich. Dies bedeutet, dass mindestens folgende Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) anerkannt und regelmäßig umgesetzt werden:

- Installation der regelmäßig von den jeweiligen Herstellern bereitgestellten Sicherheitsupdates für das Betriebssystem und die installierten Programme (z. B. Internet-Browser, Office, Flash Player, Adobe Reader) – idealerweise über die Funktion "Automatische Updates".
- Installation eines Virenschutzprogramms inkl. regelmäßiger Aktualisierung – idealerweise über die Funktion "Automatische Updates".
- Nutzung einer Firewall. Diese ist in den meisten modernen Betriebssystemen bereits integriert (z. B. Windows Defender) und soll den PC vor Angriffen von außen schützen. Dazu kontrolliert sie alle Verbindungen des PCs in andere Netzwerke und überprüft sowohl die Anfragen ins Internet, als auch die Daten, die aus dem Internet an den PC gesendet werden.
- Bei Nutzung eines WLAN ("Wireless LAN", drahtloses Netzwerk), sollte dies stets mittels des Verschlüsselungsstandards WPA2 verschlüsselt sein.
- Überprüfung des Sicherheitsstatus des PC in regelmäßigen Abständen.

2.5 Weitere Angaben und Regelungen

Weitere Angaben und Regelungen, z. B. die Rechte von Betroffenen, Rechtsgrundlagen, Zusammenarbeit mit Dritten, sind der Anlage 1 (siehe Nr. 4) zu entnehmen.

Weitere Übersicht von Verarbeitungstätigkeiten gem. Artikel 30 Abs. 2 DSGVO sind der Anlage 2 (siehe Nr. 4) zu entnehmen.

Weitere Angaben und Regelungen zum Umgang mit Bildmaterial, insbesondere die Veröffentlichung und die Verwendung von Bildern auf denen Personen erkennbar sind, sind der Anlage 3 (siehe Nr. 4) zu entnehmen.

2.6 Inkrafttreten

Diese Datenschutz-Richtlinie tritt zum 16.10.2018 nach dem Beschluss des Verbandsvorstandes in Kraft. Ergänzende Regelungen nach der Datenschutzgrundverordnung (DSGVO) werden ggf. in entsprechenden zusätzlichen Anlagen zu dieser Richtlinie beschrieben.

3 Konsequenzen eines Verstoßes

Verstöße gegen die Datenschutzvorschriften sind ein Vertrauensbruch gegenüber den Personen, deren Daten dem KFV bekannt geworden sind und haben äußerst negative Auswirkungen auf das Ansehen des KFV in der Öffentlichkeit.

Verstöße können sowohl für den KFV, als auch für jeden einzelnen Mitarbeitenden bußgeld-, haftungs- und strafrechtliche Folgen haben. In diesem Zusammenhang wird auf die Art. 82 ff. DSGVO sowie § 203 Abs. 2 und § 353b StGB hingewiesen.

Siehe auch Abschnitt 2.1.6.

4 Anlagen zur Richtlinie

Die nachfolgenden Dokumente sind Teil dieser Datenschutz-Richtlinie:

- Anlage 1 – Datenschutzerklärung im Internetauftritt
  (siehe https://kreisfeuerwehrverband.net/datenschutz.html)
- Anlage 2 – Verarbeitungsverzeichnis
- Anlage 3 – Umgang mit Bildmaterial
- Anlage 4 – Datenschutzerklärung für Mitarbeitende

Datenschutzerklärung
im Internetauftritt

(Anlage 1 der Datenschutz-Richtlinie
des Kreisfeuerwehrverbandes Limburg-Weilburg e.V.)

Profil:

Allgemein	
Kurztitel	Datenschutzerklärung Internetauftritt
Dokumenten-Nr.	DS-RL – 001-1
Klassifizierung	Richtlinie
Geltungsbereich	Kreisfeuerwehrverband Limburg-Weilburg e.V. (KFV)
Adressatenkreis	Alle Mitarbeitenden in den Gremien des KFV und alle Personen, die in sonstiger Weise für den KFV tätig werden
Freigabe durch	Vorstand
Beschluss am	16.10.2018
Inkrafttreten am	16.10.2018
Gültigkeitsdauer	Bis zur Überarbeitung
Thema	Regelungen zu Datenschutz und Datensicherheit im KFV

Regelungen:

Die entsprechenden Regelungen sind dem Internetauftritt zu entnehmen unter:
https://kreisfeuerwehrverband.net/datenschutz.html

Übersicht von Verarbeitungstätigkeiten gem. Artikel 30 Abs. 2 DSGVO

(Anlage 2 der Datenschutz-Richtlinie
des Kreisfeuerwehrverbandes Limburg-Weilburg e.V.)

Profil:

Allgemein	
Kurztitel	Verarbeitungsverzeichnis
Dokumenten-Nr.	DS-RL – 001-2
Klassifizierung	Übersicht
Grundlage	Umsetzung des § 18 der Verbandssatzung
Geltungsbereich	Kreisfeuerwehrverband Limburg-Weilburg e.V. (KFV)
Adressatenkreis	Alle Mitarbeitenden in den Gremien des KFV und alle Personen, die in sonstiger Weise für den KFV tätig werden
Freigabe durch	Vorstand
Beschluss am	16.10.2018
Inkrafttreten am	16.10.2018
Gültigkeitsdauer	Bis zur Überarbeitung
Thema	Regelungen zu Datenschutz und Datensicherheit im KFV

Inhaltsverzeichnis:

1 Verantwortlicher 2
2 Änderungsverzeichnis 2
3 Bezeichnung der Verarbeitung 2
3.1 Kassenverwaltung 2
3.2 Kontaktverwaltung 3
3.3 Internetauftritt 6
3.4 Terminverwaltung 7
3.5 Verwaltung 8
4 Auftragsverarbeitung 10
5 Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 DSGVO (Art. 30 Abs. 2 lit d) 11

1 Verantwortlicher

Der Vorstand hat in seiner Sitzung vom 16.10.2018 folgende Person als Verantwortlichen für Datenschutz und Datensicherheit bestimmt:

Name:	Schmidt
Vorname:	Thomas
Straße:	Neunkircher Str. 12
Postleitzahl:	35799
Ort:	Merenberg
Telefon:	0172 6924605
E-Mail-Adresse:	verbandsvorsitzender@kreisfeuerwehrverband.net

2 Änderungsverzeichnis

Änderung am	Nr.	Inhalt

3 Bezeichnung der Verarbeitung

3.1 Kassenverwaltung

3.1.1 Zweck der Verarbeitung

- Ermittlung und Verwaltung aller Einnahmen und Ausgaben

3.1.2 Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten

- Vorname
- Nachname
- Name des Unternehmens
- Rechnungsanschrift
- E-Mail-Adresse
- Telefonnummer
- Zuordnungsnummer (z. B. Kundennummer)
- Bankverbindung

- Umsatzsteueridentifikationsnummer
- Daten zu gekauften Waren oder Dienstleistungen
- Vertragsdaten
- Umsatzdaten

3.1.3 Beschreibung der Kategorien betroffener Personen

- Mitglieder
- Kunden
- überregionale Feuerwehrwehrverbände
- Sponsoren und/oder Spender

3.1.4 Kategorien von Empfängern gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offen gelegt werden

- Bankinstitute zur Durchführung von Überweisungen und Lastschriften

3.1.5 Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation

- keine

3.1.6 Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien

- Finanzbuchhaltungsdaten werden nach den Vorgaben der Abgabenordnung (AO) mindestens 10 Jahre gespeichert. Für den Beginn der Friste gilt § 147 Abs. 4 AO

3.1.7 Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DSGVO

- siehe Nr. 5

3.2 Kontaktverwaltung

3.2.1 Zweck der Verarbeitung

- Verwaltung und Bereitstellung von Kontaktmöglichkeiten von Personen, Unternehmen oder öffentlichen Stellen

3.2.2 Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten

- Vorname
- Nachname
- Name des Unternehmens
- Anschrift geschäftlich oder privat
- E-Mail-Adresse
- Telefonnummer
- Tätigkeitsbeginn und -ende für den Verband
- Abteilung des Verbandes, in dem die Tätigkeit ausgeübt wird bzw. wurde

3.2.3 Beschreibung der Kategorien betroffener Personen

- Mitglieder und deren Funktionsträger, insbesondere:
  - Stadt- und Gemeindebrandinspektoren
  - Wehrführer
  - Stadt-/Gemeindejugendfeuerwehrwarte
  - Jugendfeuerwehrwarte
  - Stadt-/Gemeindekinderfeuerwehrwarte
  - Kinderfeuerwehrwarte
  - Feuerwehrvereinsvorsitzende
  - Leiter Feuerwehrmusikgruppe
  - Musikalische Leiter Feuerwehrmusikgruppe
  - Ansprechpartner Sterbekasse
  - Ansprechpartner Ehren- und Altersabteilung
  - deren jeweilige Stellvertreter
- Funktionsträger und Mitarbeiter des Verbandes (Verbandsausschuss, Fachbereiche, Arbeitskreise)
- Lehrgangs- und Seminarteilnehmer
- Sponsoren
- Persönlichkeiten des öffentlichen Lebens
- Funktionsträger anderer Feuerwehrverbände
- Funktionsträger anderer Hilfsorganisationen
- Ehrenmitglieder

3.2.4 Kategorien von Empfängern gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offen gelegt werden

- Interne Abteilungen bzw. Personen in den Abteilungen
- STEKA Limburg-Weilburg aG
- Mitglieder oder deren Funktionsträger, sofern deren berechtigtes Interesse nachgewiesen wurde (z. B. Ausrichtung einer überörtlichen und gemeinnützigen Feuerwehrveranstaltung)
- Behörden und Körperschaften des öffentlichen Rechtes im Rahmen der gesetzlichen Erfordernisse

Über diese hinaus, den Verbandszielen widersprechende Zwecke, insbesondere zur kommerziellem Nutzung, ist eine Offenlegung der personenbezogenen Daten untersagt.

3.2.5 Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation

- keine

3.2.6 Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien

- Bei personenbezogenen Daten der Kontaktverwaltung werden nach Ablauf von vier Jahren zum Ende des jeweiligen Kalenderjahres geprüft, ob eine Speicherung noch erforderlich ist. Sollte eine Erforderlichkeit nicht bestehen, werden die Daten gelöscht.
- Funktionsträger von Mitgliedern werden gelöscht, sobald das Ausscheiden aus dem Amt bekannt geworden ist.
- Daten, die der Dokumentation der Historie des Verbandes und der heimischen Feuerwehrgeschichte dienen, werden nicht gelöscht.

3.2.7 Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DSGVO

- Kontaktdaten der Mitglieder und deren Funktionsträger, der Sponsoren, der Lehrgangs- und Seminarteilnehmer, der Persönlichkeiten des öffentlichen Lebens, der Funktionsträger anderer Verbände und Hilfsorganisationen werden auf einem zentralen Server und grundsätzlich nicht auf lokalen Datenträgern abgelegt. Die Sprecher folgender Fachbereiche pflegen die Daten ihrer Funktionsträger eigenverantwortlich und legen sie auf diesem Server in einem Bereich (Bezeichnung: DSGVO-*) ab, auf den nur sie, der Verbandsvorsitzende und dessen Stellvertreter Zugriff haben:
  - Ehren- und Altersabteilung
  - Brandschutzerziehung/-aufklärung

  - Kinderfeuerwehr
  - Jugendfeuerwehr
  - Feuerwehrvereine
  - Musik
- Kontaktdaten der Funktionsträger und Mitarbeiter des Verbandes (Verbandsausschuss, Fachbereiche, Arbeitskreise) werden grundsätzlich in FLORIX verarbeitet. Hierfür ist eine Zustimmung der Betroffenen erforderlich. Zugriff hierauf haben:
  - der Verbandsvorsitzende
  - der für die FLORIX-Bearbeitung zuständige stellvertretende Verbandsvorsitzende
  - die Kreisjugendfeuerwehrwartin (für die Mitglieder der Kreisjugendfeuerwehrleitung)
- siehe im Übrigen Nr. 5

3.3 Internetauftritt

3.3.1 Zweck der Verarbeitung

- Betrieb eines Internetauftrittes zur Außendarstellung des Verbandes
- Bereitstellung einer Art „Pin-Wand“ zur eigenen und freiwilligen Veröffentlichung personenbezogener Daten der Funktionsträger der Mitglieder des Verbandes
- Veröffentlichung von Kontaktdaten der Mitarbeitenden des KFV

3.3.2 Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten

- Vorname
- Name
- Anschrift
- Telefon-Nummer(n)
- E-Mail-Adresse
- Bestandsdaten
- Nutzungsdaten
- Inhaltsdaten

3.3.3 Beschreibung der Kategorien betroffener Personen

- Mitglieder

- Besucher

3.3.4 Kategorien von Empfängern gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offen gelegt werden

- Hosting-Provider

3.3.5 Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation

- siehe Datenschutzerklärung im Internetauftritt

3.3.6 Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien

- siehe Datenschutzerklärung im Internetauftritt

3.3.7 Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DSGVO

- siehe Datenschutzerklärung im Internetauftritt

3.4 Terminverwaltung

3.4.1 Zweck der Verarbeitung

- Planung und Verwaltung von Terminen

3.4.2 Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten

- Kontaktdaten
- Termindaten

3.4.3 Beschreibung der Kategorien betroffener Personen

- Mitglieder und deren Funktionsträger
- Funktionsträger und Mitarbeiter des Verbandes (Verbandsausschuss, Fachbereiche, Arbeitskreise)
- Lehrgangs- und Seminarteilnehmer
- Sponsoren
- Persönlichkeiten des öffentlichen Lebens

- Funktionsträger anderer Feuerwehrverbände
- Funktionsträger anderer Hilfsorganisationen
- Dritte

3.4.4 Kategorien von Empfängern gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offen gelegt werden

- Weitere Teilnehmer an Terminen

3.4.5 Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation

- keine

3.4.6 Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien

- Bei personenbezogenen Daten der Terminverwaltung wird nach Ablauf von vier Jahren zum Ende des jeweiligen Kalenderjahres geprüft, ob eine weitere Speicherung erforderlich ist. Sollte eine Erforderlichkeit nicht bestehen, werden die Daten gelöscht.
- Ausgenommen hiervon sind Daten, die als Geschäftsbriefe i. S. des HGB bzw. als buchhaltungsrelevante Daten einzuordnen sind. Hier gelten die jeweils gesetzlichen Aufbewahrungspflichten.
- Daten, die der Dokumentation der Historie des Verbandes und der heimischen Feuerwehrgeschichte dienen, werden nicht gelöscht.
- Siehe im Übrigen die Datenschutzhinweise

3.4.7 Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DSGVO

- siehe Nr. 5

3.5 Verwaltung

3.5.1 Zweck der Verarbeitung

- Allgemeine Verwaltung des Verbandes

3.5.2 Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten

- Vorname

- Nachname
- Name des Unternehmens
- Anschrift geschäftlich oder privat
- E-Mail-Adresse
- Telefonnummer
- Tätigkeitsbeginn und -ende für den Verband
- Abteilung des Verbandes, in dem die Tätigkeit ausgeübt wird bzw. wurde

3.5.3 Beschreibung der Kategorien betroffener Personen

- Mitglieder und deren Funktionsträger, insbesondere als:
  - Stadt- und Gemeindebrandinspektoren
  - Wehrführer
  - Stadt-/Gemeindejugendfeuerwehrwarte
  - Jugendfeuerwehrwarte
  - Stadt-/Gemeindekinderfeuerwehrwarte
  - Kinderfeuerwehrwarte
  - Feuerwehrvereinsvorsitzende
  - Leiter Feuerwehrmusikgruppe
  - Musikalische Leiter Feuerwehrmusikgruppe
  - Ansprechpartner Sterbekasse
  - Ansprechpartner Ehren- und Altersabteilung
  - deren jeweilige Stellvertreter
- Funktionsträger und Mitarbeiter des Verbandes (Verbandsausschuss, Fachbereiche, Arbeitskreise)
- Lehrgangs- und Seminarteilnehmer
- Sponsoren
- Persönlichkeiten des öffentlichen Lebens
- Funktionsträger anderer Feuerwehrverbände
- Funktionsträger anderer Hilfsorganisationen
- Ehrenmitglieder

3.5.4 Kategorien von Empfängern gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offen gelegt werden

- Interne Abteilungen bzw. Personen in den Abteilungen
- STEKA Limburg-Weilburg aG

- Mitglieder oder deren Funktionsträger, sofern deren berechtigtes Interesse nachgewiesen wurde (z. B. Ausrichtung einer überörtlichen und gemeinnützigen Feuerwehrveranstaltung)
- Behörden und Körperschaften des öffentlichen Rechtes im Rahmen der gesetzlichen Erfordernisse
- Überregionale Feuerwehrverbände, soweit dies für die Bearbeitung von Ehrungsanträgen erforderlich ist

3.5.5 Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation

- keine

3.5.6 Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien

- Bei personenbezogenen Daten der allgemeinen Verwaltung wird nach Ablauf von vier Jahren zum Ende des jeweiligen Kalenderjahres geprüft, ob eine weitere Speicherung erforderlich ist. Sollte eine Erforderlichkeit nicht bestehen, werden die Daten gelöscht.
- Ausgenommen hiervon sind Daten, die als Geschäftsbriefe i. S. des HGB bzw. als buchhaltungsrelevante Daten einzuordnen sind. Hier gelten die jeweils gesetzlichen Aufbewahrungspflichten.
- Daten, die der Dokumentation der Historie des Verbandes und der heimischen Feuerwehrgeschichte dienen, werden nicht gelöscht.
- Siehe im Übrigen die Datenschutzrichtlinie.

3.5.7 Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DSGVO

- siehe Nr. 5

4 Auftragsverarbeitung

- Angaben zum Auftragsverarbeiter [Unternehmen (Auftraggeber) Art. 30 Abs. 2 lit. a]
- Kategorien von Verarbeitungen, die im Auftrag durchgeführt werden (Art. 30 Abs. 2 lit. b)
- ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (Art. 30 Abs. 2 lit. c)
  - Nennung der konkreten Datenempfänger
  - Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DSGVO genannte Datenübermittlung handelt.

5 Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 DSGVO (Art. 30 Abs. 2 lit d)

- Siehe Nr. 2.4 der Datenschutzrichtlinie des Verbandes.

Umgang mit Bildmaterial

(Anlage 3 der Datenschutz-Richtlinie
des Kreisfeuerwehrverbandes Limburg-Weilburg e.V.)

Profil:

Allgemein	
Kurztitel	Umgang mit Bildmaterial
Dokumenten-Nr.	DS-RL – 001-3
Klassifizierung	Übersicht
Geltungsbereich	Kreisfeuerwehrverband Limburg-Weilburg e.V. (KFV)
Adressatenkreis	Alle Mitarbeitenden in den Gremien des KFV und alle Personen, die in sonstiger Weise für den KFV tätig werden
Freigabe durch	Vorstand
Beschluss am	16.10.2018
Inkrafttreten am	16.10.2018
Gültigkeitsdauer	Bis zur Überarbeitung
Thema	Regelungen zu Datenschutz und Datensicherheit im KFV

Inhaltsverzeichnis:

1 Allgemeines zum Recht am eigenen Bild 2
2 Rechtliche Meinung 2
3 Umsetzung im KFV 3
4 Mustertext 3

Umgang mit Bildmaterial

(Anlage 3 der Datenschutz-Richtlinie
des Kreisfeuerwehrverbandes Limburg-Weilburg e.V.)

Profil:

Allgemein	
Kurztitel	Umgang mit Bildmaterial
Dokumenten-Nr.	DS-RL – 001-3
Klassifizierung	Übersicht
Geltungsbereich	Kreisfeuerwehrverband Limburg-Weilburg e.V. (KFV)
Adressatenkreis	Alle Mitarbeitenden in den Gremien des KFV und alle Personen, die in sonstiger Weise für den KFV tätig werden
Freigabe durch	Vorstand
Beschluss am	16.10.2018
Inkrafttreten am	16.10.2018
Gültigkeitsdauer	Bis zur Überarbeitung
Thema	Regelungen zu Datenschutz und Datensicherheit im KFV

Inhaltsverzeichnis:

1 Allgemeines zum Recht am eigenen Bild 2
2 Rechtliche Meinung 2
3 Umsetzung im KFV 3
4 Mustertext 3

1 Allgemeines zum Recht am eigenen Bild

In Deutschland gilt das RECHT AM EIGENEN BILD.

Im einfachen nationalen Recht wird dies durch das Gesetz - betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie - mit dem Kurztitel „Kunsturheberrechtsgesetz“ (KunstUrhG) geregelt.

Es gibt dem Abgebildeten die Befugnis, über die Verwendung des Bildes zu bestimmen, einschließlich des Rechts, einer Veröffentlichung zu widersprechen.

Selbst das bloße Fotografieren bedarf grundsätzlich einer Genehmigung. Daher müsste diesbezüglich jede Person vor der Fertigung eines Fotos entsprechend befragt werden. Ansonsten darf das Bild auf keinen Fall veröffentlicht werden.

Allerdings gibt es auch Einschränkungen (Ausnahmen):

- Beiwerk: Wenn eine Person nicht das Hauptmotiv ist, sondern nur Beiwerk darf das Foto veröffentlicht werden.
  - Faustregel: Ist das Bild auch ohne abgebildete Person ein gutes Bild? Sollte die Person wichtiger sein, dann ist diese kein Beiwerk mehr.
    Beispiel/e: Foto von Brandenburger Tor – Bild wäre auch ohne Menschen gut und das Brandenburger Tor steht im Vordergrund.
- Menschmengen: Es ist erlaubt, Menschenmengen bei bestimmten gesellschaftlichen Ereignissen zu fotografieren, solange keine Person einzeln hervorgehoben wird.
  - Es gibt jedoch keine vorgeschrieben Personenzahl.
    Beispiel/e: Kirmes im Festzelt.
- Personen der Zeitgeschichte: Fotos von Prominenten (Politiker etc.), jedoch auch hier nur Bilder, die in Verbindung mit dem Wirken der Person stehen.
  - Absolute Person der Zeitgeschichte: Person ist immer eine Person der Zeitgeschichte.
    Beispiel/e: Politiker, Schauspieler.
  - Relative Person der Zeitgeschichte: Person ist nur für einen bestimmten Zeitpunkt Person der Zeitgeschichte.
    Beispiel/e: Feuerwehrmann, der ein Kind aus dem brennenden Haus rettet.

2 Rechtliche Meinung

Da im Zweifelsfall das Einverständnis der abgebildeten Personen auf dem veröffentlichten Bild zu beweisen ist, sollte stets ein Einverständnis - in der Regel schriftlich - eingeholt werden!

Versicherungsschutz besteht für Schäden bezüglich der Verletzung von Persönlichkeitsrechten, insoweit besteht auch Versicherungsschutz für immaterielle Schäden, nicht jedoch aus der Verletzung von Urheberrechten.

3 Umsetzung im KFV

Das bedeutet für den Kreisfeuerwehrverband Limburg-Weilburg e.V.:

- Bei Bildmaterial von Ehrungen, Auszeichnungen, etc. genügt das mündliche Einverständnis der beteiligten Personen, dass eine Verwendung im Rahmen der Presse- und Öffentlichkeitsarbeit erfolgen darf.
  Voraussetzung: Alle abgebildeten Personen sind VOLLJÄHRIG!
- Bei Fotos von Seminaren und/oder Lehrgängen des KFV o. ä. muss grundsätzlich eine schriftliche Einverständniserklärung der Teilnehmer vorliegen (siehe Mustertext im Abschnitt 4). Handelt es sich lediglich um ein Gruppenbild, kann ausnahmsweise wie im vorstehenden Fall verfahren werden.
- Bei Fotos während des Kreisjugendfeuerwehrzeltlagers und bei allen sonstigen Veranstaltungen mit Jugendlichen, bei denen ein Anmeldeprozedere erforderlich ist, ist der entsprechende Text (siehe Abschnitt 4) in die von den Erziehungsberechtigten und dem/der Teilnehmer/-in zu unterschreibende Anmeldung zu übernehmen.
- Bei allen sonstigen Veranstaltungen, bei denen kein Anmeldeprozedere erforderlich ist und an denen Minderjährige teilnehmen, wird seitens des KFV keine Öffentlichkeitsarbeit mehr geleistet. Hier obliegt die Öffentlichkeitsarbeit der kommunalen Feuerwehr.

4 Mustertext

Bei der Veranstaltung werden unter Umständen seitens der öffentlichen Presse und des Kreisfeuerwehrverband Limburg-Weilburg e.V. (KFV) Bilder und ggf. Videoaufnahmen erstellt, verarbeitet und veröffentlicht. Die Bildnisse der öffentlichen Presse unterfallen hierbei deren eigenen rechtlichen Bestimmungen.

Der KFV fertigt Bilder und Videoaufnahmen vorzugsweise zum Zwecke der Dokumentation und für die Darstellung der Historie an. Allerdings möchten der KFV die vielfältigen Tätigkeiten in den Kinder- und Jugendfeuerwehren sowie auch in den Einsatz-, Alters- und Ehrenabteilungen auch einer größeren Öffentlichkeit zugänglich machen. Daher nutzen wir einen Teil der Aufnahmen im Rahmen der Presse- und Öffentlichkeitsarbeit.

Dabei sind die agierenden Personen die wichtigsten Akteure und unser Stolz, weshalb wir um Freigabe zur Verwendung von Bildmaterial bitten. Wir bemühen uns, die Aufnahmen vorzugsweise so zu gestalten, dass möglichst nur Personengruppen aufgenommen bzw. Personen nicht allzu deutlich abgebildet werden. In manchen Fällen können jedoch auch Einzelpersonen zu erkennen sein. **Mit der Unterschrift wird daher ausdrücklich bestätigt, dass die Aufnahmen von der teilnehmenden Person kostenfrei im Rahmen der Presse- und Öffentlichkeitsarbeit veröffentlicht werden dürfen.**

In diesem Zusammenhang verweist der KFV auf die „Datenschutz-Richtlinie des KFV“ (einsehbar http://datenschutz.kreisfeuerwehrverband.net). Zudem wird ausdrücklich darauf hingewiesen, dass jeder Betroffene gemäß DSGVO insbesondere folgende Rechte in Anspruch nehmen kann: Recht auf Widerruf der Einwilligung (Art. 7, Abs. 3), auf Auskunft (Art. 15), auf Berichtigung (Art. 16), auf Löschung (Art. 17), auf Einschränkung der Verarbeitung (Art. 18), auf Datenübertragbarkeit (Art. 20), auf Widerspruch (Art. 21) sowie Beschwerderecht bei einer Aufsichtsbehörde (Art. 77).

Datenschutzerklärung für Mitarbeitende im Kreisfeuerwehrverbandes Limburg-Weilburg e. V.

(Anlage 4 der Datenschutz-Richtlinie des Kreisfeuerwehrverbandes Limburg-Weilburg e.V.)

Innerhalb des Kreisfeuerwehrverbandes Limburg-Weilburg e. V. (KFV) wird besonderer Wert auf die Vertraulichkeit im Umgang mit schutzbedürftigen Informationen gelegt.

Dabei genießen personenbezogene Daten besonderen gesetzlichen Schutz. Personenbezogene Daten sind nicht nur die Daten, die sich konkret einer bestimmten Person zuordnen lassen (wie z. B. Name, Kontaktdaten, Beruf, Aufgabe im Unternehmen etc.), sondern auch die Daten, bei denen die Person erst über zusätzliche Informationen bestimmbar gemacht werden kann.

Wir gehen im KFV im Zweifel davon aus, dass ein Personenbezug einer Information vorliegt. Für personenbezogene Daten gelten dann die jeweils einschlägigen gesetzlichen Vorschriften zum Datenschutz wie z. B. die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union.

Nach der DSGVO dürfen personenbezogene Daten nur dann verarbeitet werden, wenn es hierzu eine Rechtsgrundlage gibt oder der Betroffene eingewilligt hat. Die Daten dürfen grundsätzlich nur zu den vorgesehenen Zwecken verwendet werden. Bei der Verarbeitung der Daten ist insbesondere zu gewährleisten, dass die Integrität, Verfügbarkeit und Vertraulichkeit der personenbezogenen Daten gewährleistet ist.

Im KFV bestehen daher Vorgaben und Geschäftsprozesse für die Verarbeitung personenbezogener Daten (siehe KFV-Datenschutzrichtlinie).

Für alle Mitarbeitende bedeutet diese **Verpflichtung zur Vertraulichkeit** konkret, dass Daten nur im Rahmen unserer internen Vorgaben verwandt werden dürfen und diese gegenüber Dritten vertraulich zu behandeln sind.

Darüber hinaus sind aber auch Betriebs- und Geschäftsgeheimnisse im KFV schutzbedürftige Daten. Eine Offenlegung von Betriebs- und Geschäftsgeheimnissen soll grundsätzlich nur dann erfolgen, wenn der jeweilige Vertrags- oder Geschäftspartner zuvor auf die Vertraulichkeit verpflichtet worden ist.

Wenn hierzu Fragen sind oder wer sich im Zweifel unsicher ist, welche Regelungen zu treffen bzw. einzuhalten sind, kann sich jederzeit an unseren für den Datenschutz verantwortlichen Verbandsvorsitzenden wenden.

Darüber hinaus stellt eine unzulässige Verarbeitung von personenbezogenen Daten in bestimmten Fällen auch eine Straftat oder Ordnungswidrigkeit nach den §§ 42, 43 BDSG dar.

Ferner ist zu beachten, dass bei einer unzulässigen Verarbeitung von personenbezogenen Daten durch den KFV Geldbußen von bis zu 20 Mio. Euro möglich sind. Daher sollen alle im KFV Mitarbeitenden gemeinsam darauf achten, dass die Verarbeitung personenbezogener Daten im KFV nur in zulässiger Art und Weise erfolgt.

Diese **Verpflichtung zur Vertraulichkeit** besteht auch nach Beendigung der Mitarbeit im KFV fort.

Etwaige andere Vertraulichkeitsvereinbarungen zwischen den Mitarbeitenden und dem KFV bleiben unberührt. Diese Vertraulichkeitsverpflichtung ersetzt jedoch eine ggf. erfolgte Verpflichtung zum Datengeheimnis nach dem BDSG a. F. mit Wirkung zum 25.05.2018.

Ich stimme zur Erfüllung der Aufgaben des KFV der Erfassung folgender persönlicher Daten im ZMS-FLORIX Datenverarbeitungssystem bzw. der Veröffentlichung im KFV-Internetauftritt zu:

Florix (zur Zustimmung bitte ankreuzen)	**Webseite** (zur Zustimmung bitte ankreuzen)	**Inhalt** (bitte ausfüllen – wenn E-Mail für Website nicht freigegeben, erfolgt keine Info-Übersendung!)
(bitte ankreuzen)	(bitte ankreuzen)	Name:
(bitte ankreuzen)	(bitte ankreuzen)	Vorname:
(ggf. ankreuzen)	(entfällt)	Geburtsdatum: (Dient z. B. für Gratulationen)
(bitte ankreuzen)	(ggf. ankreuzen)	Straße:
(bitte ankreuzen)	(bitte ankreuzen)	PLZ Ort-Teilort: **(Sollte auch für die Webseite frei gegeben werden)**
(bitte ankreuzen)	(ggf. ankreuzen)	Telefon-Nr. 1: (Hier primäre Telefonnummer eingeben, z. B. Mobil- oder Festnetznummer)
(bitte ankreuzen)	(ggf. ankreuzen)	Telefon-Nr. 2:
(bitte ankreuzen)	(bitte ankreuzen)	E-Mail : (Wenn die „E-Mail“ für Website nicht freigegeben ist, erfolgt keine Aufnahme in den E-Mailverteiler für die Info-Mails und für die Kommunikation) (E-Mail-Adresse wird nicht direkt angezeigt, sondern lediglich als geschützter Link beim Namen zur Übernahme in ein Mailprogramm hinterlegt)
Derzeit in folgenden Bereichen des KFV tätig:		

Ich wurde darauf hingewiesen, dass ich auf Wunsch einen Ausdruck der im Datenverarbeitungssystem über mich erfassten Daten (Stammdatensatz) erhalten kann.

Hiermit verpflichte ich mich zur Einhaltung der vorgenannten Regelungen zur Vertraulichkeit und zur Beachtung der KFV-Datenschutzrichtlinie nebst Anlagen im Rahmen meiner Tätigkeiten im und für den KFV. Gleichzeitig erkenne ich hiermit die KFV-Datenschutzrichtlinie an.

Ort, Datum

Unterschrift des Mitarbeitenden