

LANDESFEUERWEHRSSCHULE



**FEUERWEHR**

LANDESFEUERWEHRVERBAND BURGENLAND

# Datenschutzgrundverordnung- Fortbildung

Dienstag, 12. Juni 2018 – LFS Burgenland, 7000 Eisenstadt

A blurred image of a red and white fire truck at night, with its lights on. The truck is the background for the text.

# EU-DSGVO

EU-Datenschutz-Grundverordnung

# Vorstellung

Ing. **FLORIAN D. PIFF**, MSc  
Datenschutzbeauftragter des  
LFV Burgenland

[datenschutz@LFV-Bgld.at](mailto:datenschutz@LFV-Bgld.at)

+43 664 210 95 48



# Datenschutzbeauftragter

- Der DSB kann innerhalb der Feuerwehr auch andere Aufgaben wahrnehmen. In seiner Eigenschaft als DSB ist er aber weisungsfrei zu stellen und untersteht unmittelbar der höchsten Führungsebene des Verantwortlichen, also dem jeweiligen Kommandanten (Art. 38 DSGVO, § 5 Abs. 3 DSG).

# Datenschutzbeauftragter

- Der DSB ist in alle mit personenbezogenen Daten zusammenhängenden Fragen einzubinden.
- Er informiert und berät den Verantwortlichen, den Auftragsverarbeiter, die Funktionäre und die Bediensteten.
- Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften sowie der Strategien seines Auftraggebers für den Schutz personenbezogener Daten.
- Überdies ist er die Anlaufstelle für die Datenschutzbehörde (Art. 38, 39 und 51 ff DSGVO iVm §§ 18 ff Datenschutzgesetz (DSG)).

# Überblick / Was erwartet Sie heute?

- Was ist die EU-DSGVO?
- Für wen gilt die EU-DSGVO?
- Wesentliche Inhalte/Definitionen
- FAQ des ÖBFV
- Umsetzung

# Was ist die EU-DSGVO?



Die EU-DSGVO wurde vom Europäischen Parlaments und Rat zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zur Regelung des freien Datenverkehrs kundgemacht.

Die Datenschutz-Grundverordnung trat am 25. Mai 2018 in Geltung. Die Datenschutz-Grundverordnung ist zwar als EU-Verordnung in jedem EU-Mitgliedstaat unmittelbar anwendbar, sie enthält jedoch zahlreiche Öffnungsklauseln und lässt dem nationalen Gesetzgeber gewisse Spielräume.

# Was ist die EU-DSGVO?



Zur Durchführung dieser Öffnungsklauseln und Spielräume wurde in Österreich das „Datenschutz-Anpassungsgesetz 2018“, eine Novelle des DSG 2000 (künftig: DSG) beschlossen.

# Für wen gilt EU-DSGVO?



Die EU-DSGVO richtet sich an alle – natürliche wie auch juristische – Personen, die über den Zwecke und Mittel der Verarbeitung von personenbezogener Daten entscheiden.

- Feuerwehren
- Unternehmen
- Gemeinden
- Vereine
- Etc.

# Wesentliche Inhalte / Definitionen

Personenbezogene Daten / sensible Daten

TOM: Technisch/Organisatorische Maßnahmen

Verantwortlicher

Auftragsverarbeiter

Information und Betroffenenrechte

# Personenbezogene Daten



Definitionsgemäß sind „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen.

z.B.: Name, Adresse, Geburtsdatum, Bankdaten, etc.

# „sensible Daten“



Das sind personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschafts-zugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

**z.B.: Fingerabdruck, Iris Scan, Krankengeschichte, Informationen über Straftaten etc.**



Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Diese Maßnahmen schließen unter anderem Folgendes ein:

- **Vertraulichkeit, Integrität, Verfügbarkeit**
- **Belastbarkeit der Systeme**
- **Verfügbarkeit der personenbezogenen Daten**
- **regelmäßigen Überprüfung, Bewertung und Evaluierung**

# Informationspflichten und Betroffenenrechte

Informationen und Betroffenenrechte sind ohne unangemessene Verzögerung, spätestens aber innerhalb eines Monats zu erledigen

- Auskunftsrecht (ua auch über geplante Speicherdauer)
- Recht auf Berichtigung
- Recht auf Löschung und auf „Vergessenwerden“
- Recht auf Einschränkung der Verarbeitung
- Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung an alle Empfänger
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht

# Empfänger

Als „Empfänger“ bezeichnet die DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.

Von dieser Definition ist auch der Auftragsverarbeiter erfasst, d.h. auch dieser gilt als „Empfänger“.

# Verantwortlicher

Verantwortlicher“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche bzw die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

**z.B.: Geschäftsführer, Firmeninhaber, Kommandant, etc.**

# Auftragsverarbeiter

„Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen bearbeitet.

# FAQ / Rechtliche Grundlagen

## ***Welche rechtlichen Grundlagen bestehen künftig für den Datenschutz im Feuerwehrdienst?***

- Verordnung (EU) 2016/679  
(Datenschutz-Grundverordnung – DSGVO), EU-ABl. 2016 L119/1  
(samt Erwägungen),
- Datenschutzgesetz (DSG), BGBl. I Nr. 165/1999, idgF,
- Feuerwehrspezifische Sonderregelungen in Gesetzesform (Bundes- und Landesgesetze)
- Feuerwehrinterne Regelungen in Form von Satzungen  
(„Feuerwehrordnungen“, „Dienstordnungen“)

## ***Gilt die DSGVO auch für Verstorbene?***

- Nein. Die DSGVO gilt nicht für die personenbezogenen Daten Verstorbener (vgl. Erwägung 27). Dessen ungeachtet können aber sonstige rechtliche Grundlagen für den Umgang mit den Daten Verstorbener beachtlich sein.
- Hinsichtlich der Feuerwehrmitgliedschaft gibt es jedoch keine Rechtsnachfolge. Die Mitgliedschaft ist ein höchstpersönliches Recht. Datenlöschungsanträge durch Erben sind daher nicht möglich.

## ***Ist es relevant, welche(s) Programm(e) eine Feuerwehr bzw. ein Feuerwehrverband verwendet?***

- Nein. Die rechtlichen Anforderungen an die Datenverarbeitung sind vom IT-System (insb. SyBOS und FDisk) völlig unabhängig.
- Die konkrete Datenanwendung hat sich nach den rechtlichen Grundlagen (DSGVO, nationales Recht) zu richten und nicht nach den Möglichkeiten eines EDV-Programms. Die Berechtigung zur Ermittlung von Daten ergibt sich jedenfalls nicht aus dem Umstand, dass im EDV-Programm bestimmte Datenfelder oder Funktionalitäten programmiert sind (wenn auch nicht als Pflichtfeld).

# Aufgaben und Zuständigkeiten

## ***Wer ist datenschutzrechtlicher Verantwortlicher (Art. 4 Z 7 DSGVO) für die Mitgliederverwaltung der Feuerwehren?***

- Die datenschutzrechtliche Verantwortlichkeit für die Kernaufgabe „Mitgliederverwaltung“ liegt im Wesentlichen bei den Feuerwehren. Auch der LFV erzeugt Daten und ist damit auch Verarbeiter und datenschutzrechtlicher Verantwortlicher (z.B. Lehrgangsverwaltung, Eintragung absolvierter Lehrgänge in die Stammbblätter, bestimmte Datenverarbeitungen bei höheren Feuerwehrführern und Bediensteten des LFV).

## ***Was ist ein Auftragsverarbeiter (Art. 4 Z 8 DSGVO) im Feuerwehrewesen?***

- Die LFV stellen den Feuerwehren entsprechende EDV-Programme zentral zur Verfügung. Der Betreiber des Servers ist der Auftragsverarbeiter:
- SYBOS wird von den LFV bei der Firma Solaris betrieben. Auftragsverarbeiter sind die LFV.

## *Was ist ein Verarbeitungsverzeichnis?*

- Die Meldepflichten beim Datenverarbeitungsregister entfallen künftig. Anstelle dessen bestehen künftig für alle datenschutzrechtlichen Verantwortlichen und für alle Auftragsverarbeiter verstärkte **interne Dokumentationspflichten**.

Alle Verantwortlichen und alle Auftragsverarbeiter müssen daher ein Verarbeitungsverzeichnis führen (Art. 30 Abs. 1 bzw. 2 DSGVO), in dem alle Datenverarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen, aufzulisten und zu beschreiben sind. Dieses ist auf Verlangen der Datenschutzbehörde zur Verfügung zu stellen.

## ***Welche Daten dürfen im Feuerwehrdienst verarbeitet werden?***

- Es dürfen nur jene Daten verarbeitet werden, die tatsächlich für den Feuerwehrdienst notwendig sind (Grundsatz der Datenminimierung, Art. 5 Abs. 1 lit. c DSGVO) und für die eine ausreichende rechtliche Grundlage besteht.

Beispiele:

- Nicht relevant sind z.B.: Religionsbekenntnis, Familienstand, Datum der Eheschließung.
- Identitätsdaten eines Unfallopfers (Name, Geburtsdatum, Wohnadresse) dürfen ermittelt werden (vgl. § 41 Abs. 3 Bgld. FWG 1994), weitere Daten nur bei konkreter Notwendigkeit. Daten über Art und Ausmaß von Verletzungen oder über Unfallursachen fallen nicht in die Zuständigkeit der Feuerwehr.

## ***Ist für die Datenverarbeitung der Feuerwehr eine Zustimmung des Feuerwehrmitglieds erforderlich?***

- Die Mitgliedschaft bei der Feuerwehr ist ein hoheitliches Rechtsverhältnis, das nicht der privatautonomen Ausgestaltung unterliegt. Sobald man der Feuerwehr beitrifft, akzeptiert man die für das Feuerwehrwesen geltenden Rechts- und Verwaltungsvorschriften, auf denen auch die Verarbeitung der Mitgliederdaten erfolgt.
- Es wird daher davon ausgegangen, dass – abgesehen von der Beitrittserklärung – keine (zusätzliche) Erklärung bzw. Einwilligung des Mitglieds über die Verarbeitung der einschlägigen personenbezogenen Daten erforderlich ist. Dessen ungeachtet wird empfohlen, in die Beitrittserklärung einen entsprechenden Passus über die Zustimmung zur Datenverarbeitung aufzunehmen.

## ***Welche Arten von Daten können in allen Tätigkeitsbereichen der Feuerwehr anfallen?***

Personenbezogene Daten können in allen Tätigkeitsbereichen der Feuerwehr anfallen. Das sind insbesondere:

- Mitgliederverwaltung
- Personalverwaltung der Feuerwehrverbände und Feuerwehren (für Personen in einem Dienstverhältnis)
- Alarmierungsdaten
- Alarm- und Einsatzplanung einschließlich der Sonderalarmpläne
- Einsatzdokumentation
- Einsatzberichterstattung
- Öffentlichkeitsarbeit
- Privatwirtschaftsverwaltung (wirtschaftliche Betätigung der Feuerwehr)

## ***Welche Arten von Daten werden im Rahmen der Mitgliederverwaltung benötigt?***

- Identifizierungsdaten:
  - Familien- und Vorname(n), einschl. frühere Namen,
  - Akademischer Grad oder Ingenieur-Grad
  - Geburtsdatum,
  - (Pass-)Foto des Mitglieds,
- Erreichbarkeitsdaten:
  - Wohn- und Zustelladressen,
  - E-Mail-Adressen,
  - Telefonnummern

## ■ Mitgliedschaftsdaten:

- Stammblatt- bzw. Standesbuchnummer,
- Eintritt, Austritt, Übertritt
- Frühere Mitgliedschaften,
- Status (Aktiv, Jugend, Reserve, Ehrenmitgliedschaft usw.)
- Dienstgrade,
- Funktionen,
- Auszeichnungen,

## ■ Bildung:

- Schul- und Hochschulstudium,
- Berufliche (Aus-)Bildung,
- sonstige Qualifikationen

- **Feuerwehrausbildung:**
  - Lehrgänge, Seminare u.ä.
  - Leistungsabzeichen und Leistungsprüfungen
- **Militärdienst / Zivildienst (soweit für den Feuerwehrdienst relevant)**
- **Besondere Berechtigungen und Befähigungen:**
  - Sprachkenntnisse,
  - Führerschein und spezielle Lenkberechtigungen (z.B. ADR),
  - Sprengbefugnis, usw.
- **Disziplinarmaßnahmen**
- **Bekleidung und sonstige persönliche Ausrüstung**

## ***Dürfen von der Feuerwehr Gesundheits- und Sozialversicherungsdaten verarbeitet werden?***

- Die Verarbeitung „besonderer Kategorien personenbezogener Daten“ (Art. 9 DSGVO, bisher „sensible Daten“) ist generell nur unter sehr eingeschränkten Voraussetzungen zulässig. Für die Feuerwehr sind in diesem Zusammenhang auch nur ganz wenige Daten relevant:
- **Tauglichkeitsstatus:** Die Tauglichkeit für den Feuerwehrdienst ist Grundvoraussetzung für die Mitgliedschaft. Befunde dürfen nur vom Feuerwehrarzt verarbeitet werden (Art. 9 Abs. 2 lit. h iVm Abs. 3 DSGVO).
- **Sozialversicherungsnummer:** Alle Feuerwehrmitglieder sind gemäß § 176 ASVG sozialversichert.
- **Impfdaten:** soweit diese für die Inanspruchnahme der von der AUVA zu finanzierenden Hepatitis-Impfung unbedingt erforderlich sind (§ 188b ASVG idF BGBl. I Nr. 125/2017)

***Welche personenbezogenen Daten sind für Feuerwehr typischerweise nicht relevant und dürfen daher nicht verarbeitet werden?***

- Familienstand
- Religionsbekenntnis
- Blutgruppe

## ***Welche Daten dürfen im Zuge der Einsatzdokumentation und -berichterstattung verarbeitet werden?***

- Die Feuerwehren sind öffentliche Einrichtungen, die gesetzlich festgelegte Aufgaben im Bereich der Hoheitsverwaltung erfüllen. Mit der Aufgabenerfüllung untrennbar verbunden ist die Verpflichtung der Feuerwehr, ihre Tätigkeit im erforderlichen Ausmaß nachvollziehbar zu dokumentieren.

Dazu gehören insb.:

- Einsatzort und -zeit
- Daten des/der Geschädigten (Identitätsdaten (Ausweisdokument), Erreichbarkeitsdaten),
- Daten von Verfügungsberechtigten (z.B. über Liegenschaften oder Fahrzeuge),
- eingesetzte Feuerwehrkräfte,
- Einsatzablauf (Einsatztagebuch).

- Die Verarbeitung von Daten über Art und Schwere von Verletzungen (nur für Zwecke der Dokumentation) oder über Verschuldensfragen am einsatzauslösenden Ereignis ist nicht Aufgabe der Feuerwehr.
- Für den Datenaustausch mit der Polizei gibt es in den einzelnen Feuerwehrgesetzen entsprechende Regelungen (vgl. § 41 Bgld. FWG 1994).

## ***Wie ist mit Auskunftsanfragen durch die Polizei bezüglich vorhandener Daten (z.B. Einsatzdokumentation) im Zuge der polizeilichen Ermittlungstätigkeit umzugehen?***

Für die sicherheits- und kriminalpolizeiliche Aufgabenerfüllung durch die Sicherheitsbehörden und ihre Organe gibt es spezifische gesetzliche Grundlagen (insb. das Sicherheitspolizeigesetz und die Strafprozessordnung). Bei Ersuchen der Sicherheitsorgane wird davon auszugehen sein, dass dies auf einer ausreichenden gesetzlichen Grundlage beruhen. Diesen Ersuchen wird daher grundsätzlich zu entsprechen sein. Allerdings soll die Kommunikation dabei über offizielle Wege erfolgen, nicht z.B. über die private E-Mail-Adresse des Kommandanten.

## ***Wie ist der Zugang zu personenbezogenen Daten zu regeln?***

Der Zugang zu personenbezogenen Daten ist auf ein unbedingt notwendiges Maß zu beschränken. Unbefugte sollen keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können (Art. 29 und 32 DSGVO, Erwägung 39 letzter Satz).

## ***Auf welche Daten darf eine Feuerwehr Zugriff haben?***

Jede Feuerwehr darf grundsätzlich nur Zugriff auf ihre eigenen Daten haben (auch der Administrator der Feuerwehr). Darüber hinaus darf sie Zugriff auf Daten anderer Feuerwehren und des LFV nur insoweit haben, als sie diese zur Wahrnehmung ihrer Aufgaben unbedingt benötigt.

## ***Auf welche Daten darf ein Feuerwehrmitglied Zugriff haben?***

- Der allgemeine Zugriff von Feuerwehrmitgliedern auf Daten der eigenen Feuerwehr oder anderer Feuerwehren (wie z.B. Geburtsdatum, Telefon-Nummern und E-Mail-Adressen) ist datenschutzrechtlich nicht zulässig (Art. 29 und 32 Abs. 4 DSGVO, Erwägung 39).
- Innerhalb der Feuerwehr sind Rollen für die Festlegung von Zugangsberechtigungen zu definieren: insb. für Kdt(Stv), Verwalter, Kassier, Jugendbetreuer, Gerätewart. Umfang der Lese- und Bearbeitungsberechtigung ist je nach Aufgabe/Funktion (Rolle) zu differenzieren und auf das Notwendige zu beschränken.

- Vorgesetzte (höhere Kommandanten) dürfen (nur) insoweit Zugriff auf Daten der ihnen unterstellten Feuerwehrmitglieder bzw. Feuerwehren haben, als sie diese Daten zur Ausübung ihrer Funktion brauchen (z.B. AFKdt nur auf notwendige Daten seines Abschnitts, BFKdt auf notwendige Daten seines Bezirks).

## ***Wann sind Daten zu löschen bzw. wie ist mit historischen Daten umzugehen?***

- Die DSGVO legt keine fixen Speicherfristen fest. Sofern keine innerstaatlichen Rechtsvorschriften über Speicherfristen und Löschungspflichten bestehen, sind personenbezogene Daten zu löschen, wenn sie für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind (Art. 17 DSGVO).
- Daten, die bspw. im Rahmen des Rechnungswesens der Feuerwehr verarbeitet werden, dürfen jedenfalls während der verpflichtenden Belegaufbewahrungsdauer nicht gelöscht werden. Auch Mitgliederdaten müssen nach Ende der Mitgliedschaft aus rechtsstaatlichen und historischen Gründen weiter verarbeitet werden.

- Dessen ungeachtet hat jede betroffene Person das Recht, Widerspruch gegen die Verarbeitung der sich aus ihrer besonderen Situation ergebenden personenbezogenen Daten einzulegen. Der Verantwortliche hat diesfalls zu prüfen, ob seine zwingenden berechtigten Interessen Vorrang vor den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person haben (Art. 21 DSGVO, Erwägung 69).

# Umsetzungsbeispiel

<https://www.bundesfeuerwehrverband.at/service/dsgvo>

Hinweis

**i** DIESE SEITE WIRD LAUFEND AKTUALISIERT UND ERGÄNZT, UM DEN LETZTSTAND DER INFORMATIONEN UND VORGEHENSWEISEN ZUR VERFÜGUNG STELLEN ZU KÖNNEN.

Bearbeiter: [BFR Dr. Thomas Schindler](#)

# Datenverarbeitungsverzeichnis

## FREIWILLIGE FEUERWEHR RIEDLINGSDORF

Obere Hauptstraße 1, A-7422 Riedlingsdorf

<b>Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)</b>	
<b>Organisation:</b>	
Name:	Freiwillige Feuerwehr Riedlingsdorf
Adresse:	Obere Hauptstraße 1, A-7422 Riedlingsdorf
Kontaktdaten:	<a href="mailto:kommando@ff-riedlingsdorf.at">kommando@ff-riedlingsdorf.at</a> , 0664/4659311
<b>Vertreter der Organisation (Kommandant):</b>	
Name:	HBI Stefan Zettl
Adresse:	Unteranger 18/2, A-7422 Riedlingsdorf
Kontaktdaten:	<a href="mailto:kommando@ff-riedlingsdorf.at">kommando@ff-riedlingsdorf.at</a> , 0664/4659311
<b>Datenschutzbeauftragter:</b>	
Name:	FM Ing. Florian D. Piff, MSc
Adresse:	Mühlgasse 7, A-7422 Riedlingsdorf
Kontaktdaten:	<a href="mailto:datenschutz@LFV-Bgld.at">datenschutz@LFV-Bgld.at</a> , 0664/2109548

# Datenverarbeitungsverzeichnis

ID	Anlegedatum	Enddatum	FDISK/SyBOS	Bezeichnung der Verarbeitung	Beschreibung der Verarbeitung	Rechtsgrundlage	Personenkategorien	Datenkategorien	Verarbeitung Art.9 oder 10	Datenübermittlung	Empfänger	Garantie	Löschfrist	TOM
1			Ja	Standesführung / Mitgliederverwaltung	Führen einer Mitgliederkartei, zumeist in EDV-Systemen wie FDISK/SyBOS	A1	B1	C1, C2, C3	Ja	E1	F3, F4, F6, F1	G1, G2	H1	
2			Ja	Einsatzdokumentation / Kostenersätze	Dokumentation der Einsatzfähigkeit inkl. der Verrechnung von Kostenersätzen	A1	B1, B2, B3	C1, C4	Nein	E1	F1, F13, F14	G2	H2	
3			Ja	Einsatzdokumentation	Dokumentation der Einsatzfähigkeit exkl. der Verrechnung von Kostenersätzen	A1	B1, B3, B5, B7	C1	Nein	E1	F9, F15		H1	
4			Ja	Übungs- /Ausbildungsdokumentation	Dokumentation der Übungs- und Ausbildungstätigkeit	A1	B1, B3, B5, B6 B7	C1	Nein	E1	F9, F13, F15	G2	H1	
5			Ja	Tätigkeitsdokumentation	Dokumentation sonstiger Tätigkeiten die Feuerwehr betreffend	A1	B1, B3, B5, B7	C1	Nein	E1	F9, F13, F15	G2	H1	
6				Spendenlisten / Kartenvorverkauf	Führen von Listen im Rahmen von Haussammlungen und Kartenvorverkäufen (z.B. Weiterleitung über Finanz online)	A4	B4	C1, C5	Nein	E1	F8		H2	
7			Ja	Rechnungswesen	Kassenführung, Rechnungslegung	A2, A4	B5	C1	Nein	E1, E2	F11		H2, H3	
8			Ja	Wahlen	Dokumentation von Wahlen (Funktionäre)	A1	B1, B7	C1, C3	Ja	E1	F4, F7, F13	G1, G2	H1	
9			Ja	Disziplinarwesen	Dokumentation von Disziplinarverfahren	A1	B1	C1, C3	Ja	E1	F4, F7, F13	G2	H2	
10			Ja	Tauglichkeitsuntersuchungen	Dokumentation von Tauglichkeitsuntersuchungen (z.B. Atemschutzgeräteträger)	A1	B1	C1, C2, C3	Ja	E1	F13	G2	H1	
11			Ja	Impfungen	Dokumentation/Anmeldung von Impfungen (z.B. Hepatitis A/B)	A1	B1	C1, C2, C3	Ja	E1	F13	G2	H1	
12			Ja	Aufnahmeverfahren	Erfassen von Daten im Zuge einer Bewerbung zur Feuerwehr	A1, A3	B1	C1, C2	Ja	E1	F3, F13	G2	H1	
13			Ja	Bekleidungs-/Ausrüstungskartei	Dokumentation der ausgefassten Bekleidung/Ausrüstung	A1	B1	C1, C3	Nein	E1	F13	G2	H1	
14			Ja	Unfallmeldungen	Erfassen und Versenden von Daten einen Unfall im Feuerwehrdienst betreffend	A4	B1, B3	C1, C2	Ja	E1	F4, F12, F13	G2	H1	
15				Erreichbarkeitslisten Allgemein	Verarbeitung von Erreichbarkeitsdaten (z.B. Telefonlisten)	A1	B1, B3, B4, B5, B7, B8	C1	Nein	E1	F3	G1	H1	
16				Lohnverrechnen (Hauptamtliche)	Lohnverrechnung für hauptamtliche Mitarbeiter	A4	B1	C1	Nein	E1	F8, F10, F12		H2	
17				Videoüberwachung	Aufnahme von Bildern zur Überwachung des Feuerwehrhauses	A5	B1, B3, B5, B8	C1	Nein	E1	F7		H2	

# Datenverarbeitungsverzeichnis

ID	Ja/Nein	Bezeichnung der Technisch, Organisatorischen Maßnahme (TOM)	Anmerkung zur Umsetzung
		<b>Zutrittskontrollen</b> Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	
<b>TomA</b>			
TomA1	Nein	Alarmanlage	
TomA2	Nein	Automatisches Zugangskontrollsystem (Chipkarten, Transponder, Codes, Biometrisch)	
TomA3	Ja	Manuelles Schließsystem	
TomA4	Nein	Videoüberwachung	
TomA5	Ja	Sicherheitsschlösser	
TomA6	Ja	Schlüsselregelung (Dokumentation der Schlüsselausgabe)	
TomA7	Ja	Sorgfältige Auswahl von externem Personal (z.B. Reinigungspersonal)	
		<b>Zugangskontrollen</b> Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	
<b>TomB</b>			
TomB1	Nein	Zuordnung von Benutzerrechten (Schlüsselsystem / automatisches Zugangskontrollsystem)	
TomB2	Ja	Gehäuseverriegelungen/Server	
TomB3	Ja	Authentifikation mit Benutzername / Passwort	
TomB4	Ja	Zuordnung von Benutzerprofilen zu IT-Systemen	
TomB5	Ja	Einsatz von Anti-Viren-Software	
TomB6	Nein	Einsatz einer Hardware-Firewall	
TomB7	Ja	Einsatz einer Software-Firewall	
		<b>Zugriffskontrollen</b> Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	
<b>TomC</b>			
TomC1	Nein	Erstellen eines Berechtigungskonzepts	
TomC2	Ja	Verwaltung der Rechte durch Systemadministrator	
TomC3	Ja	Anzahl der Administratoren auf das „Notwendigste“ reduziert	
TomC4	Nein	Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel	
TomC5	Nein	physische Löschung von Datenträgern vor Wiederverwendung	
TomC6	Ja	Einsatz von Aktenvernichtern	
TomC7	Nein	Protokollierung der Vernichtung	
		<b>Eingabekontrolle</b> Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	
<b>TomD</b>			
TomD1	Nein	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	

# Datenverarbeitungsverzeichnis

<b>TomE</b>		<b>Auftragskontrolle</b> Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	
TomE1	Nein	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)	
<b>TomF</b>		<b>Verfügbarkeitskontrolle</b> Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	
TomF1	Nein	Unterbrechungsfreie Stromversorgung (USV)	
TomF2	Nein	Klimaanlage in Serverräumen	
TomF3	Nein	Schutzsteckdosenleisten in Serverräumen	
TomF4	Nein	Brandmeldeanlagen	
TomF5	Ja	Erstellen eines Backup- & Recoverykonzepts	
TomF6	Nein	Testen von Datenwiederherstellung	
TomF7	Ja	Serverräume nicht unter sanitären Anlagen	
TomF8	Nein	In Hochwassergebieten: Serverräume über der Wassergrenze	
<b>TomG</b>		<b>Trennungsgebot</b> Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	
TomG1	Nein	physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern	
TomG2	Nein	Trennung von Produktiv- und Testsystem	

# Quelle(n):

<https://www.bundesfeuerwehrverband.at/service/dsgvo>

# Haben Sie Fragen?



# Appendix

# FAQ / Rechtliche Grundlagen

## *Müssen Feuerwehrgesetze geändert werden?*

- Die geltenden Feuerwehrgesetze enthalten kaum datenschutzrechtliche Regelungen. Auf Grund der DSGVO besteht aber entsprechender Bedarf nach innerstaatlicher Umsetzung, die zweckmäßigerweise in einem möglichst hohen legislatischen Standard, d.h. in Form von Gesetzen, erfolgen sollte.

## ***Für wen gilt die DSGVO?***

- Die DSGVO gilt nur für (lebende) natürliche Personen, nicht für juristische Personen (Art. 1 Abs. 1 DSGVO). Betroffen sind nur Daten, die sich auf eine identifizierte oder identifizierbare Person beziehen (Art. 4 Z 1 DSGVO).

## ***Was kann eine geeignete rechtliche Grundlage für die Verarbeitung personenbezogener Daten sein?***

- Die DSGVO
- Das Datenschutzgesetz 2000 (DSG 2000)
- Einschlägige Materiengesetze und Verordnungen (z.B. Feuerpolizei- und Feuerwehrgesetze)
- Feuerwehrsatzungen, d.h. im Rahmen der Selbstverwaltung erlassene, generelle Normen

- Eine rechtliche Grundlage für eine Datenverarbeitung muss nicht notwendigerweise ein Gesetz im formellen Sinne sein. Die entsprechende Rechtsgrundlage muss jedoch klar und präzise sein und ihre Anwendung muss für die Rechtsunterworfenen vorhersehbar sein.

# Aufgaben und Zuständigkeiten

## ***Was ist ein Auftragsverarbeiter (Art. 4 Z 8 DSGVO) im Feuerwehrewesen?***

- Die LFV stellen den Feuerwehren entsprechende EDV-Programme zentral zur Verfügung. Der Betreiber des Servers ist der Auftragsverarbeiter:
- SYBOS wird von den LFV bei der Firma Solaris betrieben. Auftragsverarbeiter sind die LFV.

## *Was ist ein Verarbeitungsverzeichnis?*

- Die Meldepflichten beim Datenverarbeitungsregister entfallen künftig. Anstelle dessen bestehen künftig für alle datenschutzrechtlichen Verantwortlichen und für alle Auftragsverarbeiter verstärkte **interne Dokumentationspflichten**.

Alle Verantwortlichen und alle Auftragsverarbeiter müssen daher ein Verarbeitungsverzeichnis führen (Art. 30 Abs. 1 bzw. 2 DSGVO), in dem alle Datenverarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen, aufzulisten und zu beschreiben sind. Dieses ist auf Verlangen der Datenschutzbehörde zur Verfügung zu stellen.

## ***Welche Daten dürfen im Rahmen der Privatwirtschaftsverwaltung der Feuerwehr verarbeitet werden?***

- Die Feuerwehren können sich im Rahmen ihrer Tätigkeiten außerhalb des gesetzlichen oder statutarischen Aufgabenbereiches nicht auf einen hoheitlichen (Sonder-)Status berufen. Sie haben daher die gleichen rechtlichen Rahmenbedingungen wie Privatpersonen zu beachten. Die Ermittlung von Daten beruht in diesem Fall ausschließlich auf Freiwilligkeit des Gegenübers.

Einschlägige Daten können sein:

- Erreichbarkeitsdaten von feuerwehrfremden Personen (Adressenverzeichnisse, Einladungsliste, Begrüßungslisten)
- Kunden- und Lieferantendaten
- Rechnungswesen

- Spenderdaten: Ist im Zusammenhang mit der Arbeitnehmerveranlagung rechtlich besonders geregelt (Sonderausgaben-Datenübermittlungsverordnung; Name, Geburtsdatum, Adressdaten)
- sonstige Daten nur mit Zustimmung der betroffenen Personen (z.B. Geburtstagsliste)