Datenschutzgrundverordnung (DSGVO)

Vier Jahre nach der Einführung

Am 25. Mai 2018 wurde die Datenschutzgrundverordnung (DSGVO) in Kraft gesetzt. Damit war viel Aufregung verbunden. Jede Firma, jede Person und jede Organisation versandte E-Mails oder Links, um von Kunden, Kollegen, Partner etc. die Bestätigung zur weiteren Speicherung personenbezogenen Daten einzuholen. Es schien, als wäre dies was komplett Neues. Dabei wurden die Grundlagen für die DSGVO bereits im Jahr 2012 von der Europäischen Kommission vorgestellt und am 15. Dezember 2015 einstimmig angenommen. Im darauffolgenden Jahr, am 24. Mai 2016, trat die Verordnung formal in Kraft. Die Mitgliedstaaten und die Firmen hatten also knapp zwei Jahre Zeit die Verordnung umzusetzen. Unabhängig davon gab es in Deutschland bereits eine gesetzliche Grundlage zum Datenschutz, das „Bundesdatenschutzgesetz“.

Bundesdatenschutzgesetz

Das Gesetz regelt, wie man personenbezogene Daten in Datenverarbeitungssystemen und auch manuell erfasst und verwaltet. Das Thema personenbezogener Daten war jedoch nicht neu. Bereits 1970 hat Hessen als erstes Bundesland (und auch als erstes Land in der Welt!) eine erste Version eines Datenschutzgesetzes in Kraft treten lassen. Dass die ersten Fassungen noch verbesserungsfähig waren, wissen wir spätestens seit dem Zeitpunkt, als das Bundesverfassungsgericht im Jahre 1983 mit seinem Urteil die Volkszählung der BRD verhinderte, so dass diese erst im Jahr 1987 stark angepasst durchgeführt werden konnte. Das Gericht hatte klargestellt, dass das Persönlichkeitsrecht an den eigenen Daten bzw. die Selbstbestimmung jeder Person über seine persönlichen Daten ein Grundrecht darstellt. Das Grundrecht der Verarbeitung von personenbezogenen Daten ist ein Verbotsrecht mit Erlaubnisvorbehalt. **Im Grundsatz ist es also gesetzlich verboten, Daten über Personen zu speichern, zu verarbeiten und weiterzugeben.**

Mit der Einführung der DSGVO änderte sich nur sehr wenig am Bundesdatenschutzgesetz. Besonderer Wert wurde bei der DSGVO allerdings auf die aktive Mitwirkung desjenigen gelegt, dessen Daten auch verarbeitet werden sollen. Man spricht hier vom sogenannten Opt-In, bei dem die Person proaktiv auswählt, ob sie ihre Daten preisgeben möchte. Eine der Umsetzung ist z. B. die Zustimmung zum Speichern von Cookies im Internet.

Im Kern bilden die Maßnahmen, die von vielen seit dem 25. Mai 2018 ergriffen wurden, seit mehr als 30 Jahren die Basis, wie in Deutschland mit personenbezogen Daten umgangen werden sollte. Die Verunsicherung durch sogenannte „Fachleute“ war enorm und die Auswirkungen waren auch in der täglichen Feuerwehrarbeit zu spüren. Von manchen Wehren hat man nicht mal den Namen des Jugendfeuerwehrwarts oder des Gerätewarts mehr erfahren - immer mit der Begründung „ich darf dies aufgrund der DSGVO nicht weitergeben“.

Der Landesfeuerwehrverband bot Informationskurse an, in denen den zahlreichen Teilnehmern in einem eintägigen Workshop die Grundlagen erklärt wurden. Im Folgenden werden die wesentlichen Punkte im Persönlichkeits- und Bildrechte kurz dargestellt, da hier nach wie vor die größten Wissensdefizite in den einzelnen Wehren und den Verbänden bestehen. Es wird gezeigt, wie man damit umgehen sollte.

Personenbezogene Daten

Das sind alle **Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen**. Wenn wir im Internet nach einem Namen „Georg“ oder „Georg Seitz“ suchen, haben wir tausende von Treffern. dabei ist es unwahrscheinlich, dass man genau den Autor identifizieren kann. Fügt man aber den Ort „Bad Düben“ hinzu, sind alle ersten Anzeigen unter Artikeln und Bildern nur vom Autor. Ab dem Zeitpunkt, in dem man eine Person identifizieren kann, ist nun die Behörde/die Firma verpflichtet, entsprechende Maßnahmen zu ergreifen, damit niemand auf diese Daten zugreifen kann.

Im Kern müssen wir uns als Feuerwehr beim **Datenschutz** kümmern, um

- die Absicherung gegen Verstöße unserer externen Dienstleister (zum Beispiel mit Geheimhaltungsverpflichtungen),
- die Minimierung von möglichen Verstößen durch Feuerwehrangehörige (zum Beispiel mit jährlichen Belehrungen),
- ein internes Datenschutzmanagement.

Zuständigkeit
In den kommunalen Einrichtungen, zu denen auch die Feuerwehr zählt, ist vereinfacht gesagt derjenige für den Datenschutz zuständig, der das Weisungsrecht hat. Somit ist es der zuständige **Bürgermeister*in**. Da wir aber auch Vereinsstrukturen (Förderverein, Kreisfeuerwehrverband, Landesfeuerwehrverband) haben, ist dort der **Vorstand oder der Leiter** der jeweiligen Stelle /Einrichtung zuständig. In Kommunen muss zwingend ein **Datenschutzbeauftragter** ernannt sein. Bei Firmen und sonstigen Organisationen wie Vereinen muss ein Datenschutzbeauftragter ab einer Anzahl von 20 Personen, die automatisiert personenbezogene Daten verarbeiten, ernannt werden.

Was darf gespeichert bzw. verarbeitet werden?
Alles, was für die Durchführung unserer Feuerwehr- und Vereinsarbeit notwendig ist darf gespeichert werden. Es gilt allgemein in allen Bereichen die **Datensparsamkeit bzw. -vermeidung.** Hilfreich ist hier, dass man für alle Attribute (Angaben), die man speichert, den Zweck erklärt. Die komplette Adresse eines Feuerwehrkamerad*in muss gespeichert sein, da man diese z. B. zur nächsten Wahl schriftlich einladen will. Darüber hinaus sind jedoch noch weitere Attribute notwendig, z. B. die G26-Untersuchung bei Atemschutzgeräteträgern, die immer wiederholt und seitens des Beauftragten überprüft werden muss. Zu denken ist etwa bei den Kinder- und Jugendfeuerwehren auch daran, dass der Verantwortliche u. a. wissen muss,

- ob das Kind allein nach Hause gehen darf oder ob es abgeholt wird,
- welche Personen im Ernstfall telefonisch zu kontaktieren sind,
- welches Schwimmabzeichen das Kind hat,
- welche besonderen Krankheiten vorliegen, auf die geachtet werden muss (z. B. bei Allergien),
- …

Was darf nicht gespeichert werden?
Dazu zählen Angaben und Daten, wie

- die politische Meinung,
- religiöse oder philosophische Überzeugungen,
- Angaben zum Sexualleben,
- ethnische Herkunft.

Wie lange dürfen Daten gespeichert werden?

- Bis zum Austritt aus der Feuerwehr (durch z. B. Umzug, altersbedingt, Tod).

Wie ist mit den Daten umzugehen?
Alle für die Tätigkeit in der Feuerwehr notwendigen Informationen dürfen also gespeichert werden. Die Frage ist, wie mit diesen Informationen umzugehen ist.

- Muss jedes Feuerwehrmitglied auf alle Daten zugreifen können?
- Wann müssen die Daten wieder gelöscht werden?
- Wo sind die Daten zu speichern?

Wichtig ist zu wissen, ob die Daten Lokal auf einen PC im Wehrleiterzimmer, das man absperren kann, oder in der Cloud auf irgendeinem Server im Internet gespeichert sind, bei dem nicht sichergestellt ist, ob er in Europa (EU) steht? Werden seitens der Feuerwehr Dienste wie z.B. WhatsApp genutzt, wo die Daten auch nach Amerika (also Drittland) übermittelt werden?

Datenspeicherung
Wenn die Daten auf einem Rechner/Netzwerk der Gemeinde/Stadt gespeichert sind, haben wir das Problem mit der Speicherung auf einem europäischen Rechner nicht. Dies muss der Datenschutzbeauftragte der Gemeinde/Stadt geklärt haben. Kritischer ist es, wenn wir personenbezogenen Daten in der Cloud speichern. Dabei muss sichergestellt sein, dass der Dienstleister seine Rechenzentren mit entsprechenden Schutzmechanismen (Zugangskontrolle, Datensicherheit etc.) ausgestattet hat, die Server in einem EU-Land stehen und die Daten nicht in ein Drittland repliziert werden können. Für uns als Feuerwehr kommt jeder Dienstleister in Frage, der seine Rechner in der EU stehen hat und im Minimum einen ISO-Standard 27001 nachweisen kann.

Welcher Personenkreis darf auf die Daten zugreifen?
Das muss innerhalb der Wehren am besten schriftlich geregelt und der dementsprechende geschützte Zugriff darauf eingerichtet werden. Als Ansatz ist zu empfehlen, alle **Führungskräfte** ab Gruppenführer zumindest auf alle Daten der aktiven Kamerad*innen zugreifen zu lassen. Hierbei sind u. a. die Daten der Sonderausbildungen wichtig, damit man die nächsten Dienste mit den entsprechend zur Verfügung stehenden Kameraden planen kann.
Auch der **Leiter der Alters- und Ehrenabteilung** sollte auf die Daten seiner Alterskamerad*innen zugreifen können. Dabei ist es für ihn z. B. wichtig, wie lange der Kamerad*in bereits in der Feuerwehr ist und welche Auszeichnungen er/sie schon erhalten hat.
Der **Jugendfeuerwehrwart** benötigt nur den Zugriff zu den Daten der Kinder und Jugendlichen, um seine Arbeiten erledigen zu können.
Jede Person hat das unabdingbare Recht

- seine Daten einzusehen,
- zu erfahren, aus welchen Quellen diese Daten stammen,
- eine Berichtigung von falschen personenbezogenen Daten zu verlangen,
- eine Übermittlung seiner persönlichen Daten an Dritte zu untersagen,
- eine Löschung (oder sofern z. B. gesetzliche Aufbewahrungsfristen vorliegen, eine Sperrung) seiner personenbezogenen Daten zu verlangen.

Letzteres kann z. B. bei einem Austritt aus der Wehr der Fall sein. Dann ist der Datensatz von allen Medien binnen einer zu definierenden Frist zu löschen. Um Diskussionen vorzubeugen, sollte in der Dokumentation der Abläufe in den Wehren z. B. folgender Satz mit eingebaut werden: ***„Bei personenbezogenen Daten wird nach Ablauf von vier Jahren zum Ende des Jahres geprüft, ob eine weitere Speicherung erforderlich ist. Sollte dies nicht der Fall sein, werden die Daten gelöscht.“***

Einwilligung zur Datenerfassung
Da die meisten Wehren heute schon Maßnahmen ergriffen haben, die persönlichen Daten der Mitglieder und Feuerwehrkameraden zu schützen, ist die Hälfte der Arbeit bereits getan. Die andere Hälfte stellt nun die Einwilligung der Kameraden*innen dar, deren Daten zu speichern sind.

Bereits bei der Aufnahme der Kamerad*innen, Jugendlichen und Kinder haben viele Wehren entsprechende Einwilligungen zum Thema des Datenschutzes und der Bildrechte mit aufgenommen. Spätestens bei unseren Alterskameraden, bei denen bei der Aufnahme in die Feuerwehr nicht über Datenschutz gesprochen wurde, müssen Einwilligungen eingeholt werden. Es gibt gesetzlich keine Unterstellung der Einwilligung der Kamerad*innen im Sinne „der wird schon einverstanden sein“. Allen Wehren ist daher folgendes zu raten:

- Macht einen Dienst zum Thema DSGVO - gekoppelt, wenn es geht, mit dem Kunsturhebergesetz zu dem Thema Bildrechten, das bei den meisten Wehren auch nicht geregelt ist.
- Zeigt beispielhaft, was über die Kameraden gespeichert ist und erklärt, zu welchem Zweck jedes Attribut gespeichert wird.
- Erklärt, wer darauf Zugriff hat und zu welchen Stellen (z. B. Gemeinde) diese Daten weitergeleitet werden.
- Zeigt an einem Beispiel auf, dass z. B. bei einem Lehrgang im Kreis oder an der Landesfeuerwehr- und Katastrophenschutzschule Nardt nur ein Teil der Informationen, also nur die für den Lehrgang relevanten Informationen, weitergegeben werden.
- Am Ende der Veranstaltung sollte jeder Kamerad*in eine personalisierten Einwilligungserklärung für seine Daten (und Bilder) unterschreiben.

Es gibt im Zusammenhang mit Datenschutz keine Mehrheitsbeschlüsse oder sonstiges, die rechtens sind, da jede Person das Recht auf seine Daten hat.

Umgang mit den sozialen Medien
Ein wesentlicher neuer Bestandteil der DSGVO widmet sich dem Umgang des Nachwuchses mit den sozialen Medien. Viele Untersuchungen haben gezeigt, dass Kinder nicht wissen und verstehen können, wie soziale Netzwerke arbeiten und was es bedeutet, dass Daten unlimitiert gespeichert werden. Deshalb wurde in der DSGVO bestimmt, dass **Jugendliche erst ab einem Alter von 16 Jahren soziale Medien wie Facebook, WhatsApp, Youtube, TikTok und Co. benutzen dürfen**.

Nachdenken lohnt sich

Seit der Einführung der DSGVO wurden schon millionenschwere Strafen an Dienstleister wie die Firma Google in Europa verhängt, da diese Medien mit persönlichen Daten (IP-Adresse des Rechners oder Handys sind nachvollziehbar) viel zu lasch umgehen. Jedem muss klar sein, dass ein Internetdienst, wie die Firma Google, mit seiner kostenlosen Suchmaschine, auch von etwas leben muss. Wenn man weiß, dass die Firma Google am Markt mehr Wert ist als das deutsche Unternehmen Siemens, sollten wir anfangen darüber nachzudenken. Letztendlich sind es unsere Daten, die automatisiert verarbeitet werden, und bei Suchen z. B. personalisierte Daten an uns sendet oder Werbeanzeigen auf dem Bildschirm ganz oben stehen.
Im Kern geht es in dem Gesetz ebenfalls um den Schutz der Kinder, denn es ist nachweisbar, dass seit der Benutzung des Internets bei Kindern eine starke Erhöhung von psychologischen Betreuungen zu verzeichnen ist.

Es ist so einfach (und wer Kinder hat und dies in den WhatsApp Gruppen z. B. in den Klassen-Chats kontrolliert) im Internet jemanden zu beschimpfen und, wer es beherrscht, dies sogar anonymisiert zu tun. Die anonymisierte Welt ermöglicht das absichtliche Beleidigen, Bedrohen, Bloßstellen oder Belästigen über einen längeren Zeitraum hinweg, was in der Fachsprache „Cybermobbing“ genannt wird.
Kinder verbreiten oder leiten ohne groß Nachzudenken Informationen, die Hass gegen Personen oder Gruppen beinhalten weiter. Gerade wir als Feuerwehren sollten darauf schauen, dass die Kommunikation mit den Kindern von diesen Attacken frei bleibt, und wenn ein derartiges Verhalten festgestellt wird, sollte sie eingreifen.