Vortrag
EU-Datenschutz-Grundverordnung

anlässlich der Klausurtagung
des Landesfeuerwehrverbandes Bayern e. V.

in Amberg

am Samstag, den 9. März 2019

Inhaltsübersicht

- A. Kurze Einführung in die wesentlichen Inhalte der EU-Datenschutz-Grundverordnung (DS-GVO)
- B. Praktische Auswirkungen auf die Feuerwehren und Handlungsempfehlungen, insbesondere im Hinblick auf technische und organisatorische Maßnahmen
- C. Beantwortung häufiger Fragestellungen

A. Inhalte der DS-GVO

- I. Rechtsnatur und Inkrafttreten

Zum 25.05.2018 trat die EU-Datenschutz-Grundverordnung vom 27.04.2016 europaweit in Kraft. Im Unterschied zur bisherigen Rechtslage handelt es sich nicht um eine europäische Richtlinie, die von den Mitgliedsstaaten in nationales Recht umgesetzt werden muss, sondern die in der Verordnung verankerten Regeln gelten ab diesem Zeitpunkt unmittelbar in ganz Europa.

Der deutsche Gesetzgeber hat in Ergänzung der EU-Datenschutz-Grundverordnung das Bundesdatenschutzgesetz mit Wirkung vom 25.05.2018 ebenfalls novelliert und dort ergänzende Regelungen getroffen, wo dies nach der EU-Verordnung möglich und sinnvoll war.

A. Inhalte der DS-GVO

- II. Gegenstand und Zielsetzung der DS-GVO

Es geht nicht um den Schutz der Daten, es geht um das Recht der Person auf informationelle Selbstbestimmung, sprich um den Schutz der Person = „Betroffener“. Das Schutzgut findet sich in Artikel 1 DS-GVO: Sie gilt für personenbezogene Daten und damit nur für natürliche Personen. Die bloße Bestimmbarkeit der Person aus den entsprechenden Daten reicht aber aus. Die DS-GVO gilt allerdings nicht im persönlichen oder familiären Bereich.

Die Erwägungsgründe der EU-Datenschutz-Grundverordnung sind u. a.
- Stärkung und Präzisierung der Rechte der betroffenen Personen,
- Verschärfung der Auflagen für diejenigen, die personenbezogene Daten verarbeiten und darüber entscheiden,
- gleiche Befugnisse der Mitgliedstaaten bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie gleiche Sanktionen im Falle ihrer Verletzung

A. Inhalte der DS-GVO

- III. Sachlicher Anwendungsbereich der DS-GVO

Art. 2 Abs. 1 DS-GVO:

Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Hinweis:

Auch ein strukturiertes Kartei- oder Ordnersystem, das nicht in der EDV geführt wird, ist ein „Dateisystem“ im Sinne der Verordnung!

A. Inhalte der DS-GVO

- III. Sachlicher Anwendungsbereich der DS-GVO

Verarbeitung (Art. 4 Nr. 2 DS-GVO) meint:

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

A. Inhalte der DS-GVO

- III. Sachlicher Anwendungsbereich der DS-GVO

personenbezogene Daten (Art. 4 Nr. 1 DS-GVO) sind definiert als:

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

A. Inhalte der DS-GVO

- III. Sachlicher Anwendungsbereich der DS-GVO

Personenbezogen sind demnach alle Einzelangaben, die sich auf bestimmte oder bestimmbare natürliche Personen beziehen,

z. B. persönliche Verhältnisse wie

Name, Anschrift, Geburtsdatum
Familienstand, Anzahl der Kinder
Aussehen
Fingerabdruck
Telefonnummer (priv. u. berufl.)
Arbeitgeber und Beruf
etc.

A. Inhalte der DS-GVO

- III. Sachlicher Anwendungsbereich der DS-GVO

  oder sachliche Verhältnisse wie beispielsweise

  Einkommen
  Vermögen
  Kfz-Typ
  Steuern
  Versicherungen
  Grundbesitz
  Vertragsbeziehungen
  Führen von Telefonaten
  Schreiben von E-Mails
  Umfang der Internet-Nutzung

A. Inhalte der DS-GVO

- III. Sachlicher Anwendungsbereich der DS-GVO

  besonders schutzwürdige personenbezogene Daten (Art. 9 DS-GVO)

  rassische und ethnische Herkunft
  politische Meinungen
  religiöse oder weltanschauliche Überzeugungen
  Gewerkschaftszugehörigkeit
  genetische Daten
  biometrischen Daten zur eindeutigen Identifizierung einer nat. Person
  Gesundheitsdaten
  Daten zum Sexualleben oder der sexuellen Orientierung

A. Inhalte der DS-GVO

- III. Sachlicher Anwendungsbereich der DS-GVO

besonders schutzwürdige personenbezogene Daten (Art. 9 DS-GVO)

Wichtiger Hinweis:

Auch im Bereich der Feuerwehren gehen wir – wenn auch nicht auf den ersten Blick – mit besonders schutzwürdigen personenbezogenen Daten um. Hierbei handelt es sich vor allem um Gesundheitsdaten in den beiden folgenden Fallkonstellationen:

- Tauglichkeitsuntersuchungen, insbesondere G26 für Atemschutz

- Patientenbefunde im medizinischen Bereich, z. B. First Responder

A. Inhalte der DS-GVO

- III. Sachlicher Anwendungsbereich der DS-GVO

Weil die DS-GVO nicht im persönlichen und familiären Bereich gilt, ist sie auf Behörden und Unternehmen zugeschnitten. Der Begriff des „Unternehmens“ wurde in Art. 4 Nr. 18 DS-GVO aber (zu) weit gefasst:

„Unternehmen“ ist eine natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen.

(Aus der Definition der wirtschaftlichen Tätigkeit im EU-Beihilferecht:

Auch Einheiten, die keinen Erwerbszweck verfolgen, können Waren und Dienstleistungen auf einem Markt anbieten (die Gewinnerzielungsabsicht spielt keine Rolle für die Einstufung als wirtschaftliche Tätigkeit). So können auch kirchliche, karitative und gemeinnützige Vereine oder Kultur- und Sporteinrichtungen als Unternehmen gewertet werden.)

A. Inhalte der DS-GVO

- III. Sachlicher Anwendungsbereich der DS-GVO

Zwischenergebnis:

Die Kreis- und Stadtbrandinspektionen sind als Teil des Landratsamtes als Staatsbehörde bzw. Teil der kreisfreien Stadt zur Anwendung der Datenschutzgrundverordnung als Behörde verpflichtet.

Die Kreis- und Stadtfeuerwehrverbände gelten als Unternehmen im Sinne von Art. 4 Nr. 18 DS-GVO und müssen die entsprechenden Vorschriften daher ebenfalls beachten.

A. Inhalte der DS-GVO

- IV. Grundregeln der Datenverarbeitung

Grundsätzlich handelt es sich bei den Regelungen zum Datenschutz um ein Verbot mit Erlaubnisvorbehalt, dass heißt, die Erhebung, Verarbeitung und Nutzung der Daten muss ausdrücklich erlaubt sein. Artikel 5 DS-GVO definiert hierzu die Grundsätze für die Verarbeitung personenbezogener Daten. Diese sind:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität => erfordert TOM auf technischer Ebene
- Vertraulichkeit => erfordert TOM auf technischer Ebene

A. Inhalte der DS-GVO

- IV. Grundregeln der Datenverarbeitung

Diese Grundsätze der Verarbeitung personenbezogener Daten gab es in ähnlicher Form auch schon in den bisher bestehenden Regelungen.

Neu ist jedoch die Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO betreffend die Grundsätze für die Verarbeitung personenbezogener Daten. Diese besagt, dass der Verantwortliche für die Einhaltung der Vorgaben der DSGVO nicht nur verantwortlich ist, sondern diese Einhaltung auch nachweisen können muss.

Faktisch führt das zu einer Beweislastumkehr, so dass nicht mehr der Beschwerdeführer den Verstoß gegen die Datenschutz-Grundsätze beweisen muss, sondern der Verantwortliche den Entlastungsbeweis führen muss.

A. Inhalte der DS-GVO

- IV. Grundregeln der Datenverarbeitung

1. Rechtmäßigkeit der Datenverarbeitung

Die Verarbeitung personenbezogener Daten ist nach Art. 6 DS-GVO von einigen Ausnahmen abgesehen nur dann rechtmäßig, wenn

a) die betroffene Person eine Einwilligung erteilt hat, oder
b) die Verarbeitung zur Erfüllung eines Vertrages oder einer rechtlichen Verpflichtung erforderlich ist, oder
c) die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und nicht die Interessen der betroffenen Person überwiegen, oder
d) die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen Person zu schützen.

A. Inhalte der DS-GVO

- IV. Grundregeln der Datenverarbeitung

  a) Einwilligung (Art. 7 DS-GVO)

  Die Einwilligung ist nur dann wirksam, wenn

  - sie freiwillig, ohne Zwang oder Druck, abgegeben wird
  - sie für einen bestimmten Fall abgegeben wird (also keine Einwilligung zur Datenverarbeitung zu allen gegenwärtigen und zukünftigen Zwecken)
  - der Einwilligung eine klare und verständliche Information vorausgeht
  - der Betroffene auch über die Möglichkeit des jederzeitigen Widerrufs seiner Einwilligung unterrichtet wurde
  - die Einwilligung durch eine eindeutige bestätigende Handlung erfolgt

A. Inhalte der DS-GVO

- IV. Grundregeln der Datenverarbeitung

b) Vertragserfüllung

Die Verarbeitung personenbezogener Daten ist auch dann rechtmäßig, wenn diese zur Erfüllung eines Vertrages zwischen den Parteien notwendig ist.

So erfolgt beispielsweise die Verarbeitung der Bankverbindung eines Fördermitglieds beim Lastschrifteinzug in Erfüllung dessen Beitragspflicht aus der Vereinssatzung und damit zur diesbezüglichen Erfüllung der entsprechenden Vertragspflichten, auch wenn darüber hinaus das erteilte SEPA-Lastschriftmandat im konkreten Fall als zusätzliche Einwilligung angesehen werden könnte.

A. Inhalte der DS-GVO

- IV. Grundregeln der Datenverarbeitung

c) Wahrung berechtigter Interessen

Diese Fallgruppe ist die am schwierigsten nachzuweisende Rechtsgrundlage. Denkbar ist hier zum Beispiel die Nennung der Kontaktdaten eines Pressebeauftragten auf der Internet-Homepage, damit dieser für die anfragenden Stellen auch erreichbar ist, wobei dies sicherlich nicht für alle Kommunikationsarten (Privatanschluss) gilt.

Im Vereinsbereich auch denkbar die Auswertung der Eintrittsdaten von Mitgliedern zur Ermittlung von runden Jubiläen zu Zwecken der Mitgliederpflege, auch wenn eine diesbezügliche Einwilligung nicht ausdrücklich erteilt wurde und keine vertragliche Pflicht zu Jubiläumsgeschenken besteht.

A. Inhalte der DS-GVO

- IV. Grundregeln der Datenverarbeitung

d) Schutz lebenswichtiger Interessen

Diese Erlaubnisnorm ist ein sehr enger Ausnahmetatbestand. Personenbezogene Daten sollten grundsätzlich nur dann aufgrund eines lebenswichtigen Interesses einer anderen natürlichen Person verarbeitet werden, wenn die Verarbeitung offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann. Anwendungsfall wäre beispielsweise die erste Datenerhebung und -speicherung beim Notfallpatienten, wenn dieser infolge Bewusstlosigkeit weder eine ausdrückliche Einwilligung abgeben kann, noch vorher einen Vertrag abschließen konnte. Als weitere Beispiele werden die Überwachung der Ausbreitung von Epidemien oder humanitäre Notfälle bei Naturkatastrophen angeführt.

A. Inhalte der DS-GVO

- IV. Grundregeln der Datenverarbeitung

2. Zweckbindung

Die Verarbeitung personenbezogener Daten ist, egal ob auf Basis einer Einwilligung, zur Vertragserfüllung, zur Wahrung berechtigter Interessen oder zum Schutz lebenswichtiger Interessen, nur für die vorab konkret festgelegten Zwecke zulässig.

So ist die Verarbeitung der Adressen von aktiven Mitgliedern für eine Einladung zu einer Fortbildungsveranstaltung ohne Zweifel statthaft, während beispielsweise die Weitergabe dieser Adressen an Drittanbieter (oder einen anderen Verein) – gleich ob gegen oder ohne entsprechendes Entgelt – ohne entsprechende Zweckbestimmung in der Zustimmungserklärung sicherlich unzulässig wäre.

A. Inhalte der DS-GVO

- IV. Grundregeln der Datenverarbeitung

3. Richtigkeit der Daten

Die personenbezogenen Daten müssen sachlich richtig und auf dem neuesten Stand sein, was schon im eigenen Interesse selbstverständlich sein sollte.

Die Verantwortlichen müssen daher mit angemessenem Aufwand sicherstellen, dass die Daten aktuell gehalten werden.

Auf Verlangen des Betroffenen sind die Daten unverzüglich richtig zu stellen, da die Datenschutz-Grundverordnung explizit einen entsprechenden Berichtigungsanspruch vorsieht (Art. 16 DS-GVO).

A. Inhalte der DS-GVO

- IV. Grundregeln der Datenverarbeitung

4. Datenminimierung – Datensparsamkeit

Es dürfen grundsätzlich nur diejenigen Daten erhoben und gespeichert werden, die zur Erfüllung der zulässigen Zwecke erforderlich sind (kein „Hamstern“ von Daten).

So können für den Bereich der öffentlichen Einrichtung der Feuerwehren spezifische Gesundheitsdaten bis zu einem ärztlichen Gutachten für die Frage nach der Einsatztauglichkeit erforderlich sein, während diese besonders schutzwürdigen Daten im Sinne des Art. 9 DS-GVO für die Erfüllung der Aufgaben der Feuerwehrvereine und Feuerwehrverbände offensichtlich nicht notwendig sein dürften.

A. Inhalte der DS-GVO

- IV. Grundregeln der Datenverarbeitung

4. Datenminimierung – Datensparsamkeit

Sind die personenbezogenen Daten für die Erreichung des Zwecks nicht mehr erforderlich und bestehen auch keine anderweitigen gesetzlichen Aufbewahrungsvorschriften, insbesondere handels- oder steuerrechtlicher Natur, so sind die entsprechenden Daten zu löschen, wenigstens aber zu anonymisieren.

Dem Betroffenen steht diesbezüglich auch ein entsprechendes Recht auf Löschung der Daten nach Art. 17 DS-GVO (plakativ „Recht auf Vergessenwerden“ betitelt) zu, das zum 25.05.2018 neu geschaffen wurde.

A. Inhalte der DS-GVO

- IV. Grundregeln der Datenverarbeitung

4. Datenminimierung – Datensparsamkeit

Beispiele:

a) Die personenbezogenen Daten des Bewerbers für den aktiven Feuerwehrdienst, der aufgrund entsprechend bedenklicher Einträge im Führungszeugnis vom Kommandanten nicht aufgenommen wurde, sind mangels Aufnahme in das öffentlich-rechtliche Dienstverhältnis sinnvoller Weise nach circa einem Jahr zu vernichten, da zu diesem Zeitpunkt die Klagefrist gegen den mündlich ausgesprochenen Ablehnungsbescheid (ohne Rechtsbehelfsbelehrung) verstrichen ist, und die Daten nach diesem Zeitpunkt zu keinerlei Zweck mehr benötigt werden.

A. Inhalte der DS-GVO

- IV. Grundregeln der Datenverarbeitung

4. Datenminimierung – Datensparsamkeit

Beispiele:

b) Dagegen können beispielsweise die Zahlungsverkehrsunterlagen, die die Spende eines Fördermitgliedes, dessen Bankverbindung und dessen Adressdaten beinhalten, sowie die diesbezügliche Kopie der Zuwendungsbestätigung nach § 147 AO bis zu zehn Jahre nach dem Zeitpunkt der Spende – und auch bei zwischenzeitlichem Austritt des Fördermitgliedes – aufbewahrt werden, da es sich insoweit um entsprechende Buchungsbelege handelt. Insoweit gehen die öffentlich-rechtlichen Aufbewahrungspflichten dem „Recht auf Vergessenwerden“ des einzelnen Individuums vor.

A. Inhalte der DS-GVO

- V. Verzeichnis der Verarbeitungstätigkeiten

Art. 30 Abs. 1 Satz 1 DS-GVO bestimmt hierzu:

„Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen.“

„Verantwortlicher“ ist hierbei nach Art. 4 Nr. 7 DS-GVO 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.

Das ist – jedenfalls nach Auffassung des Bayerischen Landesamtes für Datenschutzaufsicht – jeder, der mit den Daten anderer umgeht.

A. Inhalte der DS-GVO

- V. Verzeichnis der Verarbeitungstätigkeiten

Freistellung von der Verpflichtung nach Art. 30 Abs. 5 DS-GVO:

Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10.

A. Inhalte der DS-GVO

- V. Verzeichnis der Verarbeitungstätigkeiten

Meinung des bayerischen Landesamtes für Datenschutzaufsicht:

In der Praxis hat die Freistellungsregelung fast keine Bedeutung. Jedes Unternehmen oder jeder Verein, der kontinuierlich für seine Beschäftigten Lohnabrechnungen durchführt oder als Verein seine Mitgliederverwaltung auf dem Laufenden hält, ist von der Freistellung nicht mehr umfasst. Er verarbeitet die Daten nicht mehr nur gelegentlich. Unabhängig davon sollten Verantwortliche eher weniger Aufwand in die Begründung ihrer Freistellung investieren als im Zweifel lieber ein Verzeichnis ihrer Verarbeitungstätigkeiten aufzustellen. Es hilft jedem Verantwortlichen, einen Überblick darüber zu bekommen oder zu behalten, wie im eigenen Unternehmen oder Verein mit personenbezogenen Daten umgegangen wird.

A. Inhalte der DS-GVO

- V. Verzeichnis der Verarbeitungstätigkeiten

Praxishinweis:

In den Kreis- und Stadtfeuerwehrverbänden wird die Anzahl der Mitglieder in der Regel überschaubar sein und die Datenverarbeitung daher nur gelegentlich erfolgen, so dass hier eine Freistellung zumindest denkbar, wenn auch nicht empfehlenswert ist.

Im Bereich der Kreis- und Stadtbrandinspektionen ist das Verzeichnis (durch oder in Zusammenarbeit mit dem Landratsamt oder der kreisfreien Stadt) zwingend zu erstellen, da die Freistellung des Art. 30 Abs. 5 DS-GVO nur für Unternehmen, nicht aber für Behörden gilt, und zudem die Verarbeitung von Gesundheitsdaten nicht ausgeschlossen werden kann.

A. Inhalte der DS-GVO

- V. Verzeichnis der Verarbeitungstätigkeiten

  Formale Anforderungen an das Verzeichnis:

  - Führung in deutscher Sprache, schriftlich oder elektronisch
  - Verzeichnis ist grds. nicht öffentlich, dient eigener Qualitätskontrolle
  - Verzeichnis ist auf Anforderung der Aufsichtsbehörde vorzulegen
  - Verzeichnis ist regelmäßig zu aktualisieren
  - Änderungshistorie muss nachvollziehbar sein, es sind also die unterschiedlichen Versionen der Verzeichnisse für die einzelnen Zeiträume aufzuheben

A. Inhalte der DS-GVO

- V. Verzeichnis der Verarbeitungstätigkeiten

  Inhaltliche Mindestanforderungen an das Verzeichnis:

  - Namen und Kontaktdaten des Verantwortlichen
  - Zwecke der Verarbeitung
  - Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
  - Kategorien vom Empfängern von Daten einschließlich Empfänger in Drittstaaten
  - wenn möglich, vorgesehene Fristen zur Löschung

  - Praxishinweis: Muster des LDA oder des LFV verwenden!

Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten" gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf abrufbar.

Bayerisches Landesamt für Datenschutzaufsicht

Muster 1: Verein – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
TSV Waldermühl e.V.
Steinbauerstr. 45a
98123 Sonsthausen

Tel. 0981/123456-0
E-Mail: team@waldermuehler-tsv.de
Web: www.waldermuehler-tsv.de

Vorstand: Dieter Eckbauer-Düppels, geb. 03.12.1952

Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbez. Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über externen Dienstleister)	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	02.03.2018	• Auszahlung der Löhne/Gehälter • Abfuhr Sozialabgaben u. Steuern	Beschäftigte	• Name und Adressen der Beschäftigten • ggf. Religions-zugehörigkeit • Eindeutige Kennzahlen zur Steuer/ Sozialabgaben ...	Externer Dienstleister	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Mitgliederverwaltung	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	02.03.2018	Verwaltung der Vereinstätigkeiten	Mitglieder	• Name und Adressen • Eintrittsdatum • Sportbereiche ...	Keine	Keine	2 Jahre nach Beendigung der Vereinsmitgliedschaft	Siehe IT-Sicherheitskonzept
Betrieb der Webseite des Sportvereins (über Hosting-Dienstleister)	Max Meier 0981/123456-0 max@ waldmuehler-tsv.de	28.02.2018	Außendarstellung	• Mitglieder • Webseitenbesucher	IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept + HTTPS-Verschlüsselung
Veröffentlichung von Fotos der Mitglieder auf der Webseite	Max Meier 0981/123456-0 max@ waldmuehler-tsv.de	20.02.2018	Außendarstellung	Mitglieder	Fotos von Vereinstätigkeiten	Keine	Keine	Wenn Einwilligung widerrufen - unverzüglich	Siehe IT-Sicherheitskonzept
Beitragsverwaltung	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	22.02.2018	Vereinsfinanzierung	Mitglieder	Bankverbindung	Steuerberater	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
...	...	...	...	...	...	...	...	...	...

Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Automatische Updates im Betriebssystem aktivieren
- ✓ Standard-Gruppenverwaltung (z. B. in Windows)
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Aktueller Virenscanner/Sicherheitssoftware
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Standard-Shredder

A. Inhalte der DS-GVO

- VI. Auftrags(daten)verarbeitung

„Auftragsverarbeiter“ ist nach der Definition des Art. 4 Nr. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Folgende Konstellationen sind denkbar:

Der Verantwortliche gibt personenbezogene Daten an jemand außerhalb seines Unternehmens weiter (z. B. Mitarbeiterdaten an ein Lohn-Rechenzentrum) oder er ermöglicht einem Außenstehenden den Einblick auf die eigene Datenhaltung personenbezogener Daten (z. B. Wartung der eigenen IT durch externen Dienstleister, soweit hierbei auch Zugriff auf die Datenbanken besteht).

A. Inhalte der DS-GVO

- VI. Auftrags(daten)verarbeitung

Die Anforderungen an eine rechtmäßige Auftragsverarbeitung sind insbesondere in Art. 28 DS-GVO beschrieben:

- Der Auftragsverarbeiter muss hinreichende Garantien an die Einhaltung der erforderlichen Standards bieten, mithin entsprechend zuverlässig sein, Art. 28 Abs. 1 DS-GVO
- Der Auftragsverarbeiter wird für den Verantwortlichen nur auf Basis eines schriftlichen Vertrages tätig, der insbesondere das Weisungsrecht des Verantwortlichen festlegt und auch die Modalitäten der Vertragsbeendigung regelt.

Muster: https://www.lda.bayern.de/media/muster_adv.pdf

A. Inhalte der DS-GVO

- VII. Datenschutzbeauftragter

Art. 37 Abs. 1 DS-GVO bestimmt hierzu:

„Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn

- die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln,
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.“

A. Inhalte der DS-GVO

- VII. Datenschutzbeauftragter

§ 38 Abs. 1 Satz 1 BDSG (neu) bestimmt ergänzend hierzu:

Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.

Es handelt sich hierbei also um eine über die Anforderungen der DS-GVO hinausgehende nationale Regelung des deutschen Gesetzgebers.

A. Inhalte der DS-GVO

- VII. Datenschutzbeauftragter

Ergebnis für die Feuerwehr im Hinblick auf die Inspektionen und die Feuerwehrverbände:

Die Kreisverwaltungsbehörde hat als Gefahrenabwehrbehörde in jedem Fall einen Datenschutzbeauftragten zu bestellen, der (in Abstimmung mit dem Kreis-/Stadtbrandrat) die Einhaltung der entsprechenden Vorschriften nicht nur für den Bereich der Feuerwehr sicherstellen soll. Die Zuständigkeit für die Bestellung liegt beim Landrat bzw. dem Leiter der Kreisverwaltungsbehörde.

Der Feuerwehrverband benötigt in der Regel keinen Datenschutz-beauftragten, da er als privatrechtliche Organisation regelmäßig nicht mindestens zehn Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt.

B. Auswirkungen / Handlungsempfehlung

I. Dringende Maßnahmen im Hinblick auf das Inkrafttreten am 25.05.2018

1. Überprüfung des Internet-Auftritts

Bestimmte Anwaltskanzleien nahmen das Inkrafttreten der DS-GVO zum Anlass, kostenpflichtige Abmahnungen an Unternehmen und Vereine zu versenden, die die datenschutzrechtlichen Vorgaben seit dem 25.05.2018 nicht einhalten. Insbesondere der Auftritt der Feuerwehr nach außen ist deshalb entsprechen abzusichern.

Der Internet-Auftritt der Feuerwehr auf Kreisebene, der in der Regel in der Verantwortung des Kreisfeuerwehrverbandes liegt, sollte daher, soweit noch nicht geschehen, dringend auf folgende Punkte überprüft werden:

B. Auswirkungen / Handlungsempfehlung

I. Dringende Maßnahmen im Hinblick auf das Inkrafttreten am 25.05.2018

a) Tracking auf der Webseite

Der Einsatz von Tracking-Tools wie Google Analytics etc. ist erlaubt, wenn die Verarbeitung der Daten konform zu den Vorschriften der DS-GVO und des TMG abgebildet werden kann. Dies setzt voraus:

- Vertrag zur Auftragsdatenverarbeitung mit bspw. Google
- Anonymisierung der IP-Adressen
- Betroffener hat Widerspruchsrecht und ist darauf hinzuweisen
- entsprechender Hinweis in der Datenschutzerklärung notwendig
- Löschung von Altdaten, die nicht obigen Standards entsprechen

B. Auswirkungen / Handlungsempfehlung

I. Dringende Maßnahmen im Hinblick auf das Inkrafttreten am 25.05.2018

b) Kontaktformular

Bei Kontaktformularen sind, soweit diese verwendet werden, die Pflichtangaben auf das notwendige Mindestmaß zu beschränken.

Wenn mit dem Kontaktformular personenbezogene Daten wie Name, E-Mail-Adresse und andere Kontaktdaten zum Verein übertragen werden sollen, so muss die Datenübermittlung zwingend verschlüsselt erfolgen mittels einer https-geschützten Verbindung (SSL-Zertifikat). Sofern der Aufwand hierfür zu hoch erscheint, ist das Kontaktformular zu löschen und durch die Angabe von verlinkten E-Mail-Adressen des beabsichtigten Empfängers zu ersetzen, da in diesem Fall der Betroffene die Kommunikation selbst anstößt.

B. Auswirkungen / Handlungsempfehlung

I. Dringende Maßnahmen im Hinblick auf das Inkrafttreten am 25.05.2018

c) Datenschutzhinweis

Der Datenschutzhinweis war bereits nach bisheriger Rechtslage verpflichtend nach § 13 TMG und ist im Hinblick auf die mit Art. 13 der DS-GVO eingeführten Informationspflicht des Verantwortlichen gegenüber dem Betroffenen mehr denn je geboten. Anzugeben sind mindestens:

- Angaben zur verantwortlichen Stelle
- Art und Umfang der Datenverarbeitung (Server-Log, Cookies, etc.)
- Angaben zur Datenübermittlung an Dritte (z. B. durch Einbindung von PlugIns oder Tracking Tools)
- Informationen zum Widerspruchsrecht

B. Auswirkungen / Handlungsempfehlung

I. Dringende Maßnahmen im Hinblick auf das Inkrafttreten am 25.05.2018

c) Datenschutzhinweis

Aufgrund des Gebots zur transparenten Information nach Art. 12 Abs.1 Satz 1 DS-GVO ist hier unbedingt angezeigt, den Datenschutzhinweis möglichst gut ersichtlich in einen separaten Menüpunkt einzustellen, der von jedem Punkt der Homepage erreichbar sein muss:

„Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.“

B. Auswirkungen / Handlungsempfehlung

I. Dringende Maßnahmen im Hinblick auf das Inkrafttreten am 25.05.2018

d) Impressum

Die Impressumspflicht ist zwar keine Anforderung aus der DS-GVO, sondern aus § 5 TMG, dennoch sollten die Pflichtangaben im Zuge der Überprüfung der Homepage ggf. aktualisiert werden, da fehlerhafte Angaben ebenfalls eine Abmahnung nach sich ziehen können.

Pflichtangaben sind:

- Name und Anschrift des Vereins
- Rechtsform und Vertretungsberechtigter
- E-Mail-Adresse und / oder Telefonnummer zur Kontaktaufnahme
- Vereinsregisternummer und USt-ID-Nummer, soweit vorhanden

B. Auswirkungen / Handlungsempfehlung

I. Dringende Maßnahmen im Hinblick auf das Inkrafttreten am 25.05.2018

e) Newsletter-Anmeldung

Soweit die Anmeldung über ein entsprechendes Formular auf der Homepage erfolgt, ist zwingend das sogenannte „Double-Opt-In-Verfahren“ zu verwenden. Das entsprechende Häkchen darf nicht vorbelegt sein, sondern ist aktiv zu setzen, und die Anmeldung ist durch den Link in einer Bestätigungs-Mail nochmals zu aktivieren.

Dies ist eine Ausprägung der neuen Grundsätze „privacy by design“ und „privacy by default“ aus Art. 25 DS-GVO, die besagen, dass der Verantwortliche im Hinblick auf Technik und Voreinstellungen die Grundsätze des Datenschutzes möglichst umfassend umzusetzen hat.

B. Auswirkungen / Handlungsempfehlung

I. Dringende Maßnahmen im Hinblick auf das Inkrafttreten am 25.05.2018

2. Auftragsverarbeitung

Der Verantwortliche sollte – möglichst unter Zuhilfenahme des Verzeichnisses der Verarbeitungstätigkeiten – überprüfen, in welchen Bereichen eine Auftrags(daten)verarbeitung stattfindet.

Mögliche Anwendungsfälle sind insbesondere Internet-Dienstleister, soweit auf dem dortigen Server / in der Cloud auch personenbezogene Daten verarbeitet werden, sowie ausgelagerte Rechenzentren.

Auch der EDV-Systempartner, der bei der Wartung der EDV-Systeme mittels Updates, und sei es nur durch Fernzugriff, auf die Datenhaltung des Vereins zugreifen kann, ist Auftragsverarbeiter.

B. Auswirkungen / Handlungsempfehlung

I. Dringende Maßnahmen im Hinblick auf das Inkrafttreten am 25.05.2018

2. Auftragsverarbeitung

Die Abgrenzung kann im Einzelfall durchaus schwierig sein, denn die Auftragsverarbeitung ist zu unterscheiden von der Erbringung fremder Fachdienstleistungen. Wesentliches Unterscheidungskriterium ist, ob der Beauftragte ein eigenes Entscheidungsrecht hat oder die Daten nur im Auftrag des Verantwortlichen weisungsgebunden verarbeitet werden. So stellt die Durchführung der Lohnabrechnung durch ein Rechenzentrum regelmäßig eine Auftragsverarbeitung dar, während die Lohnabrechnung durch den Steuerberater im Rahmen des laufenden Mandats die Inanspruchnahme fremder Fachleistung sein kann.

Hilfestellung hierzu gibt das DSK Kurzpapier Nr. 13, abrufbar unter:
https://www.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf

B. Auswirkungen / Handlungsempfehlung

I. Dringende Maßnahmen im Hinblick auf das Inkrafttreten am 25.05.2018

2. Auftragsverarbeitung

Fällt das Ergebnis der Überprüfung dahingehend aus, dass im konkreten Fall eine Auftragsverarbeitung vorliegt, so ist mit dem Datenverarbeitungsunternehmen / EDV-Dienstleister / etc. nach Überprüfung von dessen Zuverlässigkeit eine schriftliche Vereinbarung über die Durchführung der Auftragsverarbeitung abzuschließen, da bei Nichtvorliegen der Vereinbarung die Auftragsverarbeitung und damit die Datenverarbeitung insgesamt nicht rechtmäßig ist und sowohl der Auftraggeber als auch der Auftragsverarbeiter als gemeinsame Verantwortliche für die Folgen der rechtswidrigen Datenverarbeitung haften. Der zeitnahe Abschluss eines Vertrages auf Basis des Musters des LDA ist daher dringend anzuraten.

B. Auswirkungen / Handlungsempfehlung

I. Dringende Maßnahmen im Hinblick auf das Inkrafttreten am 25.05.2018

2. Auftragsverarbeitung

Praxishinweis:

Aus den Reihen de Feuerwehren wurde bereits die Frage gestellt, ob für die Weitergabe der personenbezogenen Daten aktiver Mitglieder (gemeindlicher Datenbestand) im Rahmen der Kreisausbildung eine entsprechende Vereinbarung zur Auftragsverarbeitung mit der Kreisverwaltungsbehörde bzw. dem Kreisfeuerwehrverband abgeschlossen werden muss, damit die Daten rechtmäßig zur Verfügung gestellt werden können.

B. Auswirkungen / Handlungsempfehlung

I. Dringende Maßnahmen im Hinblick auf das Inkrafttreten am 25.05.2018

2. Auftragsverarbeitung

Lösungsansatz:

Nach Art. 19 Abs. 1 Satz 2 BayFwG hat der Kreisbrandrat für die Ausbildungsveranstaltungen Sorge zu tragen. Auch die entsprechenden Feuerwehrverbände haben im Regelfall die Ausbildung als Bestandteil in ihre satzungsgemäßen Aufgaben aufgenommen. Insoweit dürfte keine Auftragsverarbeitung, sondern die Inanspruchnahme einer „fremden“ Fachdienstleistung vorliegen, da die Lehrgangsleiter üblicherweise auch das Entscheidungsrecht über die Zulassung der Teilnehmer zu einem Lehrgang haben.

B. Auswirkungen / Handlungsempfehlung

I. Dringende Maßnahmen im Hinblick auf das Inkrafttreten am 25.05.2018

2. Auftragsverarbeitung

Lösungsansatz:

Sofern sich die Inspektion / der Feuerwehrverband zur Organisation seiner Ausbildungsveranstaltungen jedoch eines web-basierten Veranstaltungsportals bedient und auf dem Web-Server entsprechende Daten der aktiven Mitglieder verwaltet werden, wird der Anbieter dieser EDV-Lösung wohl als Auftragsdatenverarbeiter anzusehen sein, da der Betreiber des Veranstaltungsportals regelmäßig nur automatisiert ohne eigenes Entscheidungsrecht verarbeitet werden.

Eine Vereinbarung zur Auftragsdatenvereinbarung mit dem Anbieter des Web-Portals ist daher als notwendig anzusehen.

B. Auswirkungen / Handlungsempfehlung

II. Weitergehende Maßnahmen, die zeitnah vorgenommen werden sollten

1. Zunächst ist als weitergehende Maßnahme das Verzeichnis der Verarbeitungstätigkeiten zu erstellen, damit bei einer entsprechenden Anfrage der Aufsichtsbehörde dieses bereits vorgelegt werden kann und nicht noch erst aufwändig erstellt werden muss.

   Darüber hinaus liefert ein solches Verzeichnis der Verarbeitungstätigkeiten eine gute Übersicht, welche Datenverarbeitungen überhaupt stattfinden und kann daher als Basis für alle weiteren Maßnahmen dienen.

B. Auswirkungen / Handlungsempfehlung

II. Weitergehende Maßnahmen, die zeitnah vorgenommen werden sollten

2. Technische und organisatorische Maßnahmen

Wie bereits bei den Inhalten der DS-GVO aufgezeigt, sind Integrität und Vertraulichkeit bei der Verarbeitung personenbezogener Daten zwei der Grundregeln des Datenschutzes aus Art. 5 DS-GVO.

Um diese beiden Grundregeln einhalten zu können, muss der Verantwortliche diverse technische und organisatorische Maßnahmen umsetzen.

Diese Pflichten sind nicht neu, sondern galten bereits nach § 9 BDSG in seiner alten Fassung und wurden jetzt durch Art. 32 DS-GVO abgelöst und präzisiert.

B. Auswirkungen / Handlungsempfehlung

II. Weitergehende Maßnahmen, die zeitnah vorgenommen werden sollten

Unter technischen Maßnahmen werden dabei alle diejenigen Maßnahmen verstanden, die im weitesten Sinne physisch umsetzbar sind, wie

- Sicherung von Türen und Fenstern
- bauliche Maßnahmen
- Alarmanlagen,

aber auch

- Benutzerkonto mit Passworterwzingung
- Logging (Protokolldateien)

B. Auswirkungen / Handlungsempfehlung

II. Weitergehende Maßnahmen, die zeitnah vorgenommen werden sollten

Organisatorische Maßnahmen wirken hingegen durch Anweisungen, Verfahrens- und Vorgehensdokumentationen. Beispielsweise wären hier anzuführen:

- Anmeldung von fremden Personal oder Besuchern
- Arbeitsanweisungen zur Vernichtung von Fehldrucken
- Vier-Augen-Prinzip
- Regelungen zum Umgang mit fremder EDV-Hardware, Smartphones (Stichworte: BYOD Bring your own device, PUOCE Private use of company equipment, MDM Mobile device management)
- festgelegte Intervalle zu Stichprobenprüfungen

B. Auswirkungen / Handlungsempfehlung

II. Weitergehende Maßnahmen, die zeitnah vorgenommen werden sollten

Unter dem Gesichtspunkt der Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO) sind insbesondere folgende Punkte zu überprüfen:

- Zutrittskontrolle (Räume)
- Zugangskontrolle (Nutzung)
- Zugriffskontrolle (Datenzugriff)
- Trennungskontrolle (Datenbestände)

Für die Feuerwehren dürfte sich insbesondere der Punkt der Trennungskontrolle als einer der Prüfungsschwerpunkte abzeichnen, da sich die Trennung von hoheitlichen Aufgaben und Vereinsangelegenheiten auch in der Datenhaltung – gleich ob Papier oder EDV – wiederfinden sollte.

B. Auswirkungen / Handlungsempfehlung

II. Weitergehende Maßnahmen, die zeitnah vorgenommen werden sollten

Unter dem Gesichtspunkt der Integrität (Art. 32 Abs. 1 lit. b DS-GVO) sollten folgende Gesichtspunkte überprüft werden:

- Eingabekontrolle:

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, zum Beispiel durch Zugriffsprotokolle, Protokollierung der Administrationstätigkeiten und der Berechtigungsvergabe sowie Archivierung von Daten und Dokumenten.

B. Auswirkungen / Handlungsempfehlung

II. Weitergehende Maßnahmen, die zeitnah vorgenommen werden sollten

- Weitergabekontrolle

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist, zum Beispiel durch Archivierung der Übermittlung, Protokollierung, Empfangsquittung, spezielle Transportmittel, Verschlüsselung, insbesondere auch E-Mail-Verschlüsselung, Signaturen.

B. Auswirkungen / Handlungsempfehlung

II. Weitergehende Maßnahmen, die zeitnah vorgenommen werden sollten

- Weitergabekontrolle

Praxishinweis:

Besondere Bedeutung kommt in diesem Zusammenhang die Kontrolle der Weitergabe von Alarmmeldungen (Alarmfax) mit personenbezogenen Daten (insbesondere Gesundheitsdaten bei der Responder-Alarmierung, z. B. Hauptstr. 10 bei Meier Bewusstsein / vitale Bedrohung nach Hypoglykämie) an mobile Endgeräte zu. Hier sind verbindliche Vorgaben zu machen, damit sichergestellt ist, dass solche Informationen nur dem berechtigen Nutzerkreis zugänglich werden.

B. Auswirkungen / Handlungsempfehlung

II. Weitergehende Maßnahmen, die zeitnah vorgenommen werden sollten

Verschlüsselung, insbesondere auch E-Mail-Verschlüsselung, ist somit ein probates Mittel zur Erreichung der geforderten Datenintegrität als auch natürlich der Vertraulichkeit der Daten:

- Beim Betrieb eines eigenen E-Mail-Servers sind die erforderlichen Verschlüsselungseinstellungen selbst vorzunehmen; bei einem in Deutschland gehosteten Server eines Providers darf man hiervon ausgehen.
- Sofern Dateien oder Dokumente versendet werden sollen, empfiehlt sich als Lösung mit geringem Aufwand die Komprimierung der Datei in ein ZIP-Archiv und die nachfolgende Verschlüsselung des Archivs, beispielsweise mit AES-256.

B. Auswirkungen / Handlungsempfehlung

II. Weitergehende Maßnahmen, die zeitnah vorgenommen werden sollten

- Sofern die Feuerwehr ein WLAN-Netz betreibt, ist zwingend durch entsprechende Verschlüsselungsmaßnahmen sicherzustellen, dass – insbesondere wenn keine Trennung vom hausinternen Datennetz erfolgt – unbefugte Dritte keinen Zugriff auf das Netzwerk und die dort vorgehaltenen Daten erlangen.

- Bei Einwahllösungen ist eine VPN-Anbindung zwingend.

- Sofern auf mobilen Geräten, egal ob Smartphones, Tablets oder klassischen Notebooks, personenbezogene Daten verarbeitet werden können, ist neben dem Kennwort für den Nutzer-Account auch die Verwendung einer Datenträgerverschlüsselung dringend anzuraten.

B. Auswirkungen / Handlungsempfehlung

II. Weitergehende Maßnahmen, die zeitnah vorgenommen werden sollten

Zur E-Mail-Kommunikation ist ergänzend auszuführen:

E-Mails, mit denen personenbezogene Daten übermittelt werden sollen, sind ausreichend zu verschlüsseln, ggf. durch entsprechende Tools.

Da bereits die E-Mail-Adresse als solche unter den Begriff der personenbezogenen Daten fällt, stellt die Bekanntgabe der E-Mail-Adresse an einen dritten Empfänger im „An:“- oder „CC:“-Feld bereits eine Datenübermittlung dar, für die eine Rechtsgrundlage erforderlich ist. Mögliche unzulässige Datenübermittlungen sollten daher durch die Verwendung des „BCC“-Feldes vermieden werden.

B. Auswirkungen / Handlungsempfehlung

II. Weitergehende Maßnahmen, die zeitnah vorgenommen werden sollten

Praxishinweis:

Die Nutzung eines offenen E-Mail-Verteilers (cc: anstelle von bcc) durch einen Querulanten wurde unlängst vom Landesdatenschutzbeauftragten in Sachsen-Anhalt mit mehreren Bussgeldern im Gesamtumfang von 2.628 € belegt. Auch wenn dieser Fall sicherlich den besonderen Umständen des Einzelfalls geschuldet ist, sollte die Verwendung eines offenen E-Mail-Verteilers an eine große Anzahl von Empfängern definitiv nicht mehr erfolgen. Dies nicht nur aufgrund des finanziellen Risikos, sondern auch vor dem Hintergrund, dass insbesondere die Inspektionen Teil der staatlichen Behörden sind, die sich rechtskonform zu verhalten haben.

B. Auswirkungen / Handlungsempfehlung

II. Weitergehende Maßnahmen, die zeitnah vorgenommen werden sollten

Weitere Gebote des Datenschutzes sind die Verfügbarkeit und die Belastbarkeit der Daten (Art. 32 Abs. 1 lit. b DS-GVO).

Unter dem Gesichtspunkt einer Verfügbarkeitskontrolle ist durch den oder die Verantwortlichen zu überprüfen und zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Es sind nicht nur ausreichende Schutzmaßnahmen gegen Ereignisse wie Brand oder Hochwasser geboten, sondern auch gegen technische Defekte wie Stromausfall. Stark zunehmende Bedeutung hat auch eine ausreichende Absicherung gegen Befall mit Schadsoftware wie beispielsweise Ransomware sowie DoS-Attacken von außerhalb des eigenen Netzwerks.

B. Auswirkungen / Handlungsempfehlung

II. Weitergehende Maßnahmen, die zeitnah vorgenommen werden sollten

Zur Gewährleistung der notwendigen Verfügbarkeit personenbezogener Daten können daher beispielhaft folgende Maßnahmen benannt werden:

- Brandschutzvorkehrungen und automatische Löscheinrichtungen
- Unterbrechungsfreie Stromversorgung
- Klimaanlage im Serverraum
- Aufbewahrung von Datensicherungen in anderem Brandabschnitt
- Virenschutz mit regelmäßiger Prüfung und Aktualisierung
- leistungsfähige Hardware-Firewall

B. Auswirkungen / Handlungsempfehlung

III. Betroffenenrechte und Reaktionsmöglichkeiten

1. Transparente Information

Der Betroffene hat zunächst einen Anspruch darauf, transparent über die Verarbeitung seiner personenbezogenen Daten informiert zu werden. Der Verantwortliche hat zu informieren über:

- Namen und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten, soweit vorhanden
- Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen und die Rechtsgrundlagen dafür
- Interessen des Verantwortlichen, wenn er Daten auf der Basis einer Interessenabwägung verarbeiten möchte
- Empfänger der Daten, wenn der Verantwortliche sie weitergeben will

B. Auswirkungen / Handlungsempfehlung

III. Betroffenenrechte und Reaktionsmöglichkeiten

1. Transparente Information

Darüber hinaus sind auch folgende Informationen anzugeben:

- Dauer der Speicherung der Daten oder Kriterien für die Löschung
- Hinweis auf die Rechte auf Auskunft, Berichtigung, Löschung, etc.
- Hinweis, dass eine Einwilligung jederzeit grundlos widerrufen werden kann
- Hinweis auf Beschwerderecht bei der Aufsichtsbehörde

B. Auswirkungen / Handlungsempfehlung

III. Betroffenenrechte und Reaktionsmöglichkeiten

2. Auskunft

Der Betroffene hat ein Recht auf Auskunft. Diese ist nicht automatisch zu erteilen, sondern nur auf konkreten Antrag hin. Sie darf durch den Verantwortlichen nur erteilt werden, wenn er sich über die Identität des Antragstellers ausreichende Gewissheit verschafft hat. Die Auskunft ist in jedem Fall zeitnah zu erteilen; liegen von der Person, die das Auskunftsrecht geltend macht, keine Daten vor, so ist auch diese Negativ-Auskunft mitzuteilen. Die Auskunft hat nicht nur die Kategorien der Daten (Name, Ort, etc.) zu benennen, sondern auch den konkreten Inhalt der Felder mit zu umfassen, da der Antragsteller nur so prüfen kann, ob die Auskunft richtig und vollständig ist.

B. Auswirkungen / Handlungsempfehlung

III. Betroffenenrechte und Reaktionsmöglichkeiten

2. Auskunft

Darüber hinaus sind dem Antragsteller folgende Informationen mitzuteilen:

- Zweck der Verarbeitung
- Kategorien personenbezogener Daten
- Empfänger der Daten
- geplante Speicherdauer
- Hinweis auf sonstige Betroffenenrechte und Beschwerdemöglichkeit bei der Aufsichtsbehörde

B. Auswirkungen / Handlungsempfehlung

III. Betroffenenrechte und Reaktionsmöglichkeiten

2. Auskunft

Die Auskunft ist dem Antragsteller kostenfrei zu übermitteln. Selbst entsprechende Versandkosten wie Porto gehen zu Lasten des Verantwortlichen.

Etwaige Mehrausfertigungen sind dagegen nur gegen Ersatz der Kopierkosten verpflichtend.

B. Auswirkungen / Handlungsempfehlung

III. Betroffenenrechte und Reaktionsmöglichkeiten

3. Berichtigung, Löschung und Einschränkung der Verarbeitung

Es ist selbstverständlich, dass personenbezogene Daten richtig sein sollen, deshalb hat der Betroffene einen entsprechenden Anspruch auf Berichtigung.

Dem Anspruch auf Löschung muss gefolgt werden, wenn für die Erfüllung des ursprünglichen Zwecks die weitere Speicherung der Daten nicht mehr erforderlich ist, der Betroffene seine Einwilligung widerrufen hat und es keine andere Rechtsgrundlage für die weitere Speicherung der Daten gibt. Auch wenn personenbezogene Daten unrechtmäßig, also von Anfang an ohne Rechtsgrundlage erhoben und verarbeitet wurden, sind sie zu löschen.

B. Auswirkungen / Handlungsempfehlung

III. Betroffenenrechte und Reaktionsmöglichkeiten

3. Berichtigung, Löschung und Einschränkung der Verarbeitung

Besteht Streit darüber, ob die Daten richtig oder unrichtig sind, hat der Betroffene einen Anspruch auf Einschränkung der Verarbeitung. Die Daten dürfen dann zwar noch gespeichert, aber nicht mehr in sonstiger Weise verarbeitet, insbesondere nicht an Dritte weitergeleitet werden.

B. Auswirkungen / Handlungsempfehlung

III. Betroffenenrechte und Reaktionsmöglichkeiten

4. Datenübertragbarkeit

Ein wirklich neues Betroffenenrecht, das durch die DS-GVO eingeführt wurde, ist das Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO:

Der Betroffene hat das Recht, die ihn betreffenden Daten in einem strukturierten, gängigen, maschinenlesbaren Format zur Verfügung gestellt zu bekommen, und – sofern technisch möglich – auch durch den Verantwortlichen direkt an einen dritten Verantwortlichen weiterleiten zu lassen. Allerdings betrifft dies nur die Daten, die die betroffene Person selbst übermittelt hat, und nicht die Erkenntnisse daraus, die ein Verantwortlicher gezogen hat.

B. Auswirkungen / Handlungsempfehlung

III. Betroffenenrechte und Reaktionsmöglichkeiten

4. Datenübertragbarkeit

Dieses neue Betroffenenrecht könnte tatsächlich auch im Bereich der Feuerwehr relevant werden, denn damit hätte der konkrete Feuerwehrdienstleistende einen Anspruch auf Übertragung seiner personenbezogenen Daten, insbesondere wohl auch Lehrgangsdaten, von einer Feuerwehr seines bisherigen Wohnortes auf die Feuerwehr seines neuen Wohnortes.

B. Auswirkungen / Handlungsempfehlung

III. Betroffenenrechte und Reaktionsmöglichkeiten

5. Widerspruch gegen die Verarbeitung

Wird die Datenverarbeitung auf eine Interessenabwägung gestützt, hat der Betroffene ein entsprechendes Widerspruchsrecht – für die Feuerwehr nicht sonderlich relevant.

6. Recht, keiner automatisierten Entscheidung unterworfen zu werden

Für die Feuerwehr ist kein Anwendungsbereich ersichtlich.

B. Auswirkungen / Handlungsempfehlung

III. Betroffenenrechte und Reaktionsmöglichkeiten

7. Zeitnahe Reaktion

Macht ein Betroffener seine Rechte nach der DS-GVO geltend, ist eine Reaktion unverzüglich, spätestens innerhalb eines Monats, erforderlich.

Erfolgt die Reaktion nicht oder zu spät, hat der Betroffene das Recht, sich bei der Aufsichtsbehörde zu beschweren, welche das Fehlverhalten des Verantwortlichen dann entsprechend sanktionieren wird.

B. Auswirkungen / Handlungsempfehlung

IV. Verletzung des Schutzes personenbezogener Daten

1. Wann liegt eine Datenschutzverletzung überhaupt vor?

Eine „Verletzung des Schutzes personenbezogener Daten“ ist nach der Definition des Art. 4 Nr. 12 DS-GVO eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.“

Absicht ist für eine Datenschutzverletzung nicht erforderlich; sie muss auch nicht notwendiger Weise zu einem Schaden beim Betroffenen führen.

B. Auswirkungen / Handlungsempfehlung

IV. Verletzung des Schutzes personenbezogener Daten

2. Pflicht zur Meldung an die Aufsichtsbehörde

Eine Datenschutzverletzung ist unverzüglich an die Aufsichtsbehörde zu melden. Eine Ausnahme gibt es nur dann, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, was ein seltener Ausnahmefall bleiben wird.

Die Meldung an die Aufsichtsbehörde hat innerhalb von 72 Stunden zu erfolgen; das Bayerische Landesamt für Datenschutzaufsicht hat hierzu eine spezielle Online-Meldung eingerichtet:

https://www.lda.bayern.de/de/datenpanne.html

B. Auswirkungen / Handlungsempfehlung

IV. Verletzung des Schutzes personenbezogener Daten

3. Pflicht zur Benachrichtigung der betroffenen Personen

Diese Information ist nur erforderlich, wenn die Schutzverletzung „voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten“ der betroffenen Personen hat.

Diese Abschätzung ist schwierig. Es empfiehlt sich daher entweder die Beiziehung eines externen Datenschutzberaters oder Rechtsanwalts. Eine Benachrichtigung ohne vorherige Prognose sollte nicht erfolgen. Dies gilt umso mehr, als die Prognose nur dann negativ ausfallen wird, je weniger Schutzmaßnahmen im Hinblick auf beispielsweise die Verschlüsselung im Vorfeld getroffen worden sind.

C. Fragen / Diskussion

Folgende Fragen haben sich aus den bisherigen Veranstaltungen ergeben:

- Benötigen wir eine Verfahrensbeschreibung in der wir darstellen, wie bei uns Daten verarbeitet werden? Ja, ggf. Muster LDA verwenden.
- Wird eine Datenschutzerklärung für den Aufnahmeantrag neuer Mitglieder nötig sein? Ja, ggf. Muster LFV verwenden.
- Braucht es künftig eine Art von generellem „Glaubensbekenntnis“ oder Erklärung, die wir künftig auf unserer Homepage veröffentlichen müssen?

  Ja, eine Datenschutzerklärung ist auf der Homepage zu veröffentlichen.
- Wo müssen wir die Akten künftig sicher/noch sicherer lagern?

  Idealerweise in einem abschließbaren Raum mit beschränktem Zutritt und dort in abschließbaren Schränken mit nachvollziehbarem Zugang.

C. Fragen / Diskussion

Folgende Fragen haben sich aus den bisherigen Veranstaltungen ergeben:

- Sehr viele von uns haben alle Kontakte (geschäftlich, Bekannte und Freunde, Vereinsmitglieder div. Vereine) auf dem Handy und daher automatisch auch auf dem Notebook / Pad. Geht das weiterhin bzw. muss ich getrennte Verzeichnisse machen oder gar mehrere Geräte kaufen? Wie ist zu verfahren?

  Die Anschaffung mehrerer Geräte ist nicht notwendig. Allerdings ist eine getrennte Datenhaltung zwingend erforderlich. Ferner ist durch die Vergabe entsprechender Benutzerrechte und die Verwendung von Verschlüsselung sicherzustellen, dass keine unbefugten Zugriffe erfolgen.

C. Fragen / Diskussion

- Muss ich alle Mitglieder mit einer pauschalen / neutralen Info-Mail anschreiben, in der ich die Verwendung der persönlichen Daten darlege und auch die Personen, die mit diesen Daten in Verbindung kommen, angeben?

  Es ist ratsam, auch die Bestandsmitglieder eine entsprechende Einwilligung zur Datenverarbeitung, welche alle Verarbeitungszwecke umfasst, abgeben zu lassen. Sofern die Daten an Dritte außerhalb der eigenen Organisation übermittelt werden sollen, so wären auch diese Empfänger anzugeben.

- Welche Ämter / Organisationen muss ich einmalig / mehrmals über die Verwendung der Daten und den Personenkreis, der diese Daten einsehen kann, informieren?

  Im Normalfall sind keine Ämter und Organisationen über die Verwendung der Daten zu informieren. Allerdings hat im Fall einer Datenschutzverletzung innerhalb von 72 Stunden eine Meldung an das Bayerische Landesamt für Datenschutzaufsicht in Ansbach, www.lda.bayern.de, zu erfolgen.

C. Fragen / Diskussion

- Muss ich für spezielle Verwendungen der persönlichen Daten sogar schriftliche Einverständniserklärungen der Mitglieder einholen?
- Wenn ja für welche Angelegenheiten?

Sollen die personenbezogenen Daten der Mitglieder für einen speziellen Zweck verarbeitet werden, der von der ursprünglichen Einwilligung nicht umfasst ist, muss ein dahingehendes schriftliches Einverständnis eingeholt werden. Dies wird insbesondere bei der Weitergabe der Daten an Dritte der Fall sein, die ursprünglich nicht benannt worden sind, aber auch bei einer Verarbeitung der Daten für Zwecke, die nicht in der Satzung definiert sind.

C. Fragen / Diskussion

- Dürfen die Daten weiterhin auf dem PC gespeichert sein, der natürlich ans Internet angeschlossen ist, auf dem auch Google, Facebook, Whatsapp und ähnliches genutzt wird?

  Die Daten dürfen grundsätzlich auch weiterhin dort gespeichert werden, wenn sichergestellt ist, dass keine unberechtigten Zugriffe auf die Daten erfolgen.

- Wenn ich Infos an alle Mitglieder sende, so stelle ich deren Adressen sowieso in "Bcc"! Ist dies okay und ausreichend?

  Ja, die Verwendung der „Bcc“-Feldes ist aus Datenschutzgründen geboten, aber auch ausreichend.

- Wenn ich an einen "kleinen" Kreis von Personen, die ihre Adressen gegenseitig sowieso kennen, ein Mail sende, dürfen dann alle sehen, wer die Mail alles bekommen hat. Oder muss ich auch hier vorher eine "einmalige" (schriftl.) Einwilligung einholen, oder ist es sogar untersagt?

C. Fragen / Diskussion

Wenn keiner aus diesem Kreis ein schutzwürdiges Interesse an einer Geheimhaltung der Mail-Adresse geltend macht, und alle Adressen ohnehin wechselseitig bekannt sind, wird man von einer stillschweigenden Duldung ausgehen könne. Gleichwohl wäre eine Einwilligung empfehlenswert. Diese wäre allerdings immer dann zu erneuern, wenn der Teilnehmerkreis sich erweitert.

- Darf ich weiterhin Whatsapp-Gruppen haben? Ich kann ja Broadcast-Gruppen bilden, wo keiner erfährt wer noch angeschrieben ist und somit auch nicht die Adresse der anderen liest.

Die Verwendung von Whatsapp-Gruppen ist unter dem Gesichtspunkt der der DS-GVO insoweit problematisch, als Kontaktdaten ohne Zustimmung des Betroffenen auf Servern in den USA gespeichert werden, was mit den geltenden Bestimmungen derzeit nicht in Einklang zu bringen ist. Es ist eine Verlagerung der Gruppen in den privaten Bereich in Erwägung zu ziehen.

D. Weitergehende Literatur