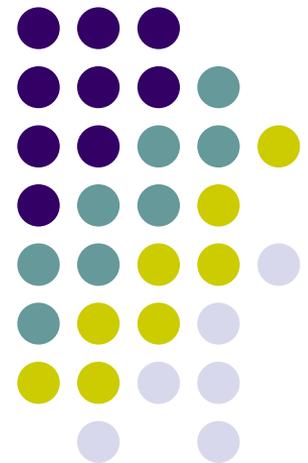


„Datenschutzgrundverordnung“ DSGVO

Datenschutz im Verein – Umsetzung
der DSGVO

RA Dr. Ronny Raith
Rechtsbeistand KFV Regen
Fachbereich 2 BFV & LFV



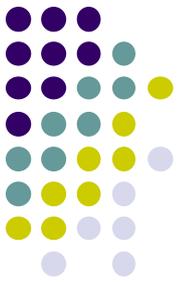
FLORIAN KOMMEN

Keine Angst vor der neuen
Datenschutz-Grundverordnung

Nr. 117 | Juni 2018

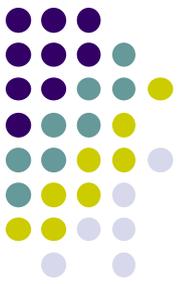


Datenschutz – was ist das?



- Datenschutz schützt nicht Daten, sondern dient dem Schutz der Privatsphäre sowie der Grundrechte und Grundfreiheiten der betroffenen Personen.
- Datenschutz ist keine moderne Erfindung, sondern gibt bereits in der Antike (z.B. im Hippokratischen Eid).
- Datenschutz ist ein Menschenrecht.
- Der Datenschutz – das Recht auf informationelle Selbstbestimmung – wurde 1983 vom BVerfG aus den Grundrechten der Art. 1 und 2 GG abgeleitet.
- Datenschutz ist bereits seit 2009 auch in der Europäischen Grundrechtscharta verankert.

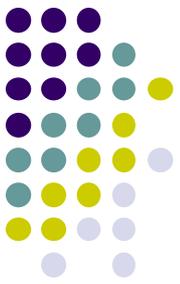
Was sind personenbezogene Daten?



Personenbezogene Daten sind gem. Art. 4 Ziff. 1 DSGVO

- „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 identifiziert werden kann, insbesondere mittels Zuordnung zu einer Kennung wie Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind“

Datenschutzgrundsätze der DSGVO



Art. 5 Abs. 1 fordert, dass personenbezogene Daten nach folgenden Grundsätzen verarbeitet werden müssen:

- „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“
- „Zweckbindung“
- „Datenminimierung“
- „Richtigkeit“
- „Speicherbegrenzung“
- „Integrität und Vertraulichkeit“

Art. 5 Abs. 2 regelt:

„Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).“

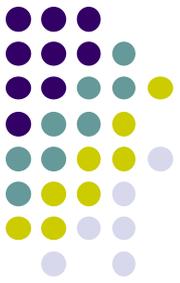
Verbot mit Erlaubnisvorbehalt (Art. 6 DSGVO)



Die Verarbeitung personenbezogener Daten ist nur „rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist“:

- **Wirksame Einwilligung der betroffenen Person**
- **Verarbeitung dient der Erfüllung eines Vertrags mit der betroffenen Person oder vorvertraglicher Maßnahmen auf Initiative der betroffenen Person**
- **Verarbeitung ist zur Erfüllung gesetzlicher Pflichten erforderlich**
- „Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen“
- „Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde“
- **„Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder einer Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen“**

Was ist neu in der DSGVO?



Vier wesentliche Änderungen sind:

- Die Dokumentationspflichten werden deutlich ausgeweitet, vgl. Art. 5 Abs. 2 DSGVO → „Nachweispflicht“ – eine Art Beweislastumkehr: Die verarbeitende Stelle muss nachweisen können, dass ihre Verarbeitung personenbezogener Daten datenschutzkonform ist.
- Die Betroffenenrechte werden deutlich ausgeweitet und es wird eine Reaktionsfrist verbindlich festgelegt, vgl. Art. 12-23 DSGVO.
- Es werden neue Bußgeldtatbestände eingeführt.
- Die Bußgelder erhöhen sich drastisch auf bis zu 20 Mio. € oder für Unternehmen auf bis zu 4% des weltweiten Jahresumsatzes, je nach dem, welcher Betrag höher ist.

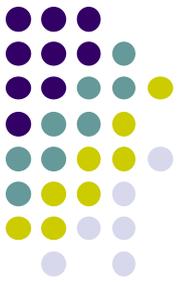
Was ist neu in der DSGVO?



Weitere wichtige Änderungen sind u.a.

- Eine Abschätzung der Risiken für die Freiheiten und Grundrechte der betroffenen Personen ist an vielen Stellen der DSGVO nötig
- Die Pflichten für Auftrags(daten)verarbeiter werden umfangreicher, u.a. müssen Auftrags(daten)verarbeiter auch ein **Verzeichnis** von Verarbeitungstätigkeiten führen.
- Bei zu ungenauer Beauftragung können Auftrags(daten)verarbeiter ebenfalls zu verantwortlichen werden.

Änderungen bei den Rechten der Betroffenen



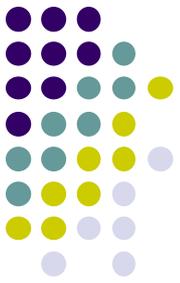
- Die Informations- und Aufklärungspflichten werden deutlich umfangreicher
- Neu sind:
 - **Recht auf „Vergessenwerden“ als Erweiterung des Rechts auf Löschung**
 - **Recht auf Datenübertragbarkeit**
- Das Widerspruchsrecht aus Art. 21 – u.a. Widerspruch gegen die Nutzung der personenbezogenen Daten für werbliche Zwecke – kann bei Internetnutzung auch durch „automatisierte Verfahren“ ausgeübt werden. D.h. etwaige von der Website- oder App.Nutzern aktivierte „Do-not-Track“-Optionen müssen berücksichtigt werden
- Es wird eine verbindliche Reaktionszeit von einem Monat eingeführt. Einmalig kann diese Frist um zwei Monate verlängert werden. Die betroffene Person ist hiervon innerhalb eines Monats unter Angabe der Gründe zu informieren.

Informationspflichten (Art. 13)



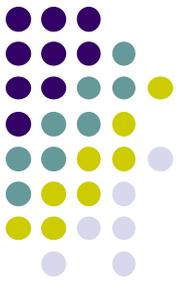
- **Name** und **Kontakt**daten des Verantwortlichen
- **Kontakt**daten des Datenschutzbeauftragten
- Die **Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung
- Wenn die Verarbeitung auf **berechtigten Interessen** (Art. 6 Abs. 1 lit. f) beruht, die vom dem Verantwortlichen oder einem Dritten verfolgt werden
- **Empfänger** oder Kategorien von Empfängern
- Die Absicht des Verantwortlichen, die personenbezogenen Daten an ein **Drittland** zu übermitteln und einen Verweis auf die geeigneten oder **angemessenen Garantien** und Möglichkeiten, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

Informationspflichten (Art. 13)



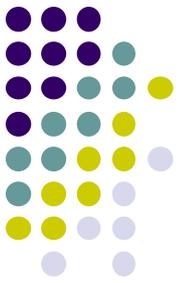
- Die **Dauer** der Speicherung
- Das Bestehen des Rechts auf **Auskunft** seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf **Berichtigung** oder **Löschung** oder **Einschränkung der Verarbeitung** oder eines **Widerspruchsrechts** gegen die Verarbeitung sowie des **Rechts auf Datenübertragbarkeit**
- Das Recht, die **Einwilligung** jederzeit **widerrufen zu können**, wenn die Verarbeitung auf Einwilligung beruht
- Das Bestehen eines **Beschwerderechts** bei einer Aufsichtsbehörde
- Ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss **erforderlich** ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen **Folgen die Nichtbereitstellung** hätte

Informationspflichten (Art. 13)



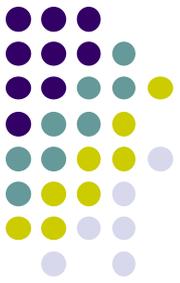
- Das Bestehen einer **automatisierten Entscheidungsfindung** einschließlich **Profiling** – zumindest in diesen Fällen – aussagekräftige Informationen über die **involvierte Logik** sowie die Tragweite und die angestrebten **Auswirkungen** einer derartigen Verarbeitung für die betroffene Person
- Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen **anderen Zweck** weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person von dieser Weiterverarbeitung Informationen **über diesen anderen Zweck** zur Verfügung.

Informationspflichten (Art. 14)



- Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zusätzlich zu den Angaben aus Art. 13 DSGVO mit:
 - aus welcher Quelle die personenbezogenen Daten stammen und ggf. ob sie aus öffentlich zugänglichen Quellen stammen.
- Diese Informationen (Art. 13 und 14) müssen nur einmalig erteilt werden, Änderungen sind aber ebenfalls mitzuteilen.

Anforderungen an die Einwilligung



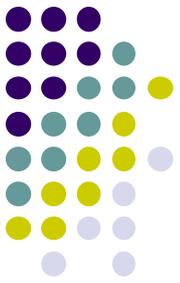
- Der Verantwortliche (z.B. der Vereinsvorsitzende) muss **nachweisen** können, dass die betroffene Person eingewilligt hat.
- Wenn die Einwilligung mit anderen Erklärungen abgegeben werden soll, „*muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist*“.
- Teile der Einwilligung, die gegen die DSGVO verstoßen sind unwirksam, vgl. Art, 7 DSGVO



Freiwilligkeit der Einwilligung

„Die Einwilligung gilt **nicht** als freiwillig erteilt,

- wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht **gesondert** eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder
- wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung **abhängig** ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist“.



Minimalumsetzung der DSGVO

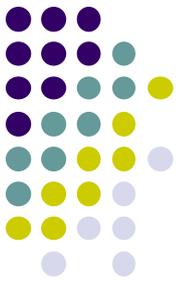
1. Erstellen Sie das Verzeichnis von Verarbeitungstätigkeiten

Dieses Verzeichnis ist Kern und Basis des Datenschutzmanagements

Hierzu gibt es vielfältige Hilfsmittel

- Leitfäden von der Bitkom und der GDD
- Muster vom Bayerischen Landesamt für Datenschutzaufsicht
- Muster des LFV
- Vorausgefüllte Muster von Datenschutzanwälten (z.B. <http://vvvt.de> oder <http://dsgvo.expert/MatV3T>)

Minimalumsetzung der DSGVO



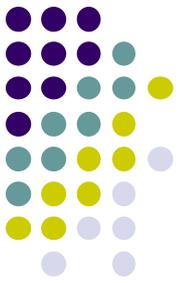
2. Benennung eines/einer Datenschutzbeauftragten

Prüfen Sie, ob Sie eine(n) Datenschutzbeauftragten benennen müssen, vgl. Art. 37 DSGVO.

Nach einhelliger Auffassung im Fachbereich 2 des LFV wird die Notwendigkeit zur Bestellung eines Datenschutzbeauftragten für die Mitgliedsfeuerwehren nicht gesehen, da die gesetzlichen Voraussetzungen nicht vorliegen dürften.

Grund hierfür ist, dass die Datenverarbeitung ersichtlich nicht Kerntätigkeit des Feuerwehrvereins bildet.

Minimalumsetzung der DSGVO



3. Erstellen Sie Datenschutzhinweise gemäß Art. 13, 14, 21 DSGVO

- Was in den Datenschutzhinweisen enthalten sein muss, ergibt sich direkt aus den Art. 13, 14 und 21 DSGVO
- Überarbeiten Sie die Datenschutzhinweise auf der Website und passen Sie insbesondere das Impressum an
- Hier sind auch die Kontaktdaten des/der Datenschutzbeauftragten anzugeben. Wenn Sie keinen benennen müssen, geben Sie dies am besten so an, das erspart Nachfragen.

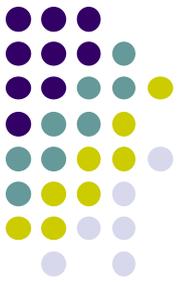


Minimalumsetzung der DSGVO

4. Legen Sie fest, wer in ihrem Verein für die Umsetzung des Datenschutzes verantwortlich ist.

- Das ist nicht der oder die Datenschutzbeauftragte!
- Der oder die Datenschutzbeauftragte berät den Verein nur und überwacht die Einhaltung des Datenschutzes
- Die für den Datenschutz verantwortliche Person kann jemand aus dem Vorstand oder der Geschäftsführung des Vereins sein.

Minimalumsetzung der DSGVO



5. Dokumentieren Sie die technischen und organisatorischen Maßnahmen zur Datensicherheit

- Aktualisieren Sie Ihre datenschutzrelevanten Dokumente auf den aktuellen Stand oder erstellen Sie diese.
- Versehen Sie diese Dokumente mit Datum und Versionsnummer
- Zu diesen Dokumenten gehören insbesondere:
 - Netzwerkübersicht, Soft- und Hardwareübersicht
 - Datenschutzrichtlinien, Arbeitsanweisungen
 - Festlegung der Verantwortlichen
 - Dokumentation der weiteren technischen und organisatorischen Maßnahmen zur Datensicherheit nach Art. 24 und 32 DSGVO – insbesondere IT-Sicherheitsmaßnahmen (Zugangsberechtigung, Passwörter u.ä.)

Minimalumsetzung der DSGVO



6. Sorgen Sie für korrekte Beauftragung Ihrer Dienstleister

- Verschaffen Sie sich einen Überblick, welche Dienstleister Sie im Zusammenhang mit der Verarbeitung personenbezogener Daten beauftragt haben (hierzu gehören auch die Akten- und Datenträgervernichtung, der Newsletterversand, etc.)
- Sorgen Sie dafür, dass Sie die Dienstleistungen, die eine Auftragsverarbeitung im Sinne des Art. 28 DSGVO sind, eine Vereinbarung zur Auftragsverarbeitung abschließen.
- Muster sind auf der Homepage des Bayerischen Landesamtes für Datenschutzaufsicht verfügbar.

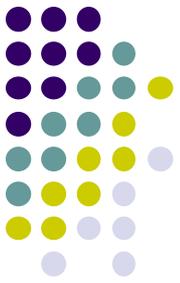
Minimalumsetzung der DSGVO



7. Prüfen bzw. Erstellen Sie Einwilligungsformulare

- Falls mit Einwilligungen gearbeitet wird, prüfen Sie, ob die Einwilligungsformulare den Anforderungen der Art. 7 und 8 DSGVO genügen
- Passen Sie die Einwilligungsformulare bei Bedarf an
- Stellen Sie sicher, dass die betroffenen Personen darüber informiert werden, in welche Art der Datenverarbeitung Sie einwilligen und zu welchem Zweck Sie die Daten erheben.
- Auf das Recht, die Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen, muss zwingend hingewiesen werden.
- Es dürfen insbesondere keine Ankreuzfelder für Einwilligungen im Voraus angekreuzt sein oder gar als Pflichtfelder gekennzeichnet sein

Minimalumsetzung der DSGVO



8. „Putzaktion“

- Räumen Sie die Mitgliederdatenbanken, die Personalakten und die sonstigen Sammlungen personenbezogener Daten auf
- Löschen Sie Daten, deren gesetzliche Aufbewahrungspflicht abgelaufen sind – oder bei denen es keine gibt – wenn es keine nachvollziehbaren Gründe gibt, warum Sie die Daten noch für die – in dem Verzeichnis von Verarbeitungstätigkeiten – festgelegten Zwecke benötigen
- Vernichten Sie Altakten, die nicht mehr benötigt werden; wenn Sie eine externe Firma beauftragen bitte auf die notwendige AV-Vereinbarung achten.
- Starten Sie ein Projekt zur Erstellung eines Lösch- und Anonymisierungskonzepts – wo angezeigt.

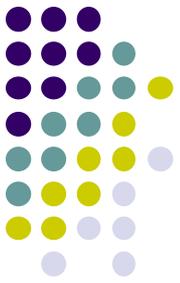


Minimalumsetzung der DSGVO

9. Folgearbeiten

- Soweit nicht alle notwendigen Schritte in einem Zug abgearbeitet werden können, erstellen Sie sich verbindlichen Zeitplan für die Umsetzung der nötigen Schritte.
- Evtl. ist es sinnvoll, eine Arbeitsgruppe einzusetzen
- Einverständniserklärungen einholen
- Vereinssatzungen anpassen

Minimalumsetzung der DSGVO



10. Regelmäßige Revision

- Prüfen Sie regelmäßig – am besten jährlich –
 - Ob die Datenschutzdokumentation noch aktuell ist,
 - Ob das Verzeichnis der Verarbeitungstätigkeiten noch aktuell und vollständig ist
 - Ob die Dienstleisterübersicht noch aktuell und vollständig ist
 - Ob die technischen und organisatorischen Maßnahmen noch ausreichen sind und noch dem – inzwischen evtl. weiterentwickelten – Stand der Technik entsprechen
 - Ob die Vereinsmitglieder eine Auffrischung oder Sensibilisierung zum Datenschutz benötigen
 - Ob die eingesetzten Ressourcen ausreichend sind



Vielen Dank für die Aufmerksamkeit!

Fragen???