Landkreis
Regensburg

Die neue EU-Datenschutz-Grundverordnung – was kommt auf die Vereine zu

Vereinsschule 21.11.2017

Referentin

Elisabeth Mayer

- Gemeinsame Datenschutzbeauftragte der Städte, Märkte, Gemeinden und Zweckverbände des Landkreis Regensburg sowie des Landratsamt Regensburg
- Über 10 Jahre Erfahrung im betrieblichen Datenschutz, seit Mitte 2016 beim Landratsamt Regensburg
- Langjährige Tätigkeit in Prozessmanagement und Qualitätssicherung sowie als Ausbilderin
- Sozialwissenschaftliches Studium und kaufmännische Ausbildung

Historisches zum Datenschutz

- Eid des Hippokrates (ca. 400 v. Chr)

  „Was auch immer ich bei der Behandlung oder auch unabhängig von der Behandlung im Leben der Menschen sehe oder höre, werde ich, soweit es niemals nach außen verbreitet werden darf, verschweigen … „
- Beichtgeheimnis (13. Jahrhundert)
- Berufsgeheimnisse (Rechtsanwälte, Steuerberater)
- Bankgeheimnis

Historisches zum Datenschutz

- 1970 Weltweit erstes Datenschutzgesetz in Hessen
- 1977 Erstes Bundesdatenschutzgesetz
- 1978 Erstes Bayerisches Datenschutzgesetz
- 1983 Volkszählungsurteil
- 1995 EG-Datenschutzrichtlinie
- 2016 EU-Datenschutz Grundverordnung

Grundsätzliches zum Datenschutz

- **Datenschutz** ist der Schutz personenbezogener Daten vor **Missbrauch, unberechtigter Einsicht oder Verwendung, Änderung oder Verfälschung**.
- §3 Bundesdatenschutzgesetz (BDSG) „Personenbezogene Daten sind Einzelangaben über **persönliche oder sachliche Verhältnisse** einer **bestimmten** oder **bestimmbaren natürlichen Person** (Betroffener).“

Grundsätzliches zum Datenschutz

- Art. 4 DS-GVO und § 46 BDSG
  „personenbezogene Daten“ (sind) 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, **identifiziert werden kann**

Grundsätzliches zum Datenschutz

Beispiele personenbezogener Daten

- Name
- Adresse
- Geburtsdatum
- Telefonnummer
- E-Mail-Adresse
- Autokennzeichen
- Mitgliedsnummer
- Spielernummer
- Finanzdaten
- Gesundheitliche Informationen
- Religionszugehörigkeit
- Familienstand

Grundsätzliches zum Datenschutz

Besondere Kategorien personenbezogener Daten

- Daten zur rassischen oder ethnischen Herkunft
- Daten zu politischen Meinungen
- Daten zu religiösen oder weltanschaulichen Überzeugungen
- Daten zur Gewerkschafts-zugehörigkeit
- biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person
- Gesundheitsdaten
- Daten zum Sexualleben
- Daten zur sexuellen Orientierung

Grundsätzliches zum Datenschutz

- Datenschutz ist notwendig zur **Wahrung der Persönlichkeitsrechte** aller Betroffenen und zum **Schutz der Privatsphäre.**
- Datenschutz sichert das **Grundrecht** jedes Einzelnen auf informationelle Selbst-bestimmung.
- Jeder soll davor geschützt werden, dass durch den Umgang mit seinen personenbezogenen Daten dieses Grundrecht verletzt wird.

Grundsätzliches zum Datenschutz

- Neben diesen übergeordneten Gründen gibt es weitere Gründe, warum die Datenschutz-regeln beachtet werden müssen:
  - Der Verein würde ansonsten gegen **Gesetze** verstoßen.
  - Sobald Datenschutzpannen öffentlich werden entsteht ein **Negativimage**.
  - Unter Umständen muss der Verein sogar selbst für eine **Veröffentlichung der Datenpanne** sorgen.

Grundsätzliches zum Datenschutz

Datenschutz

= **Schutz der Menschen**

≠ Schutz der Daten = Datensicherheit

Deshalb ist die Verarbeitung von personen-bezogenen Daten nur erlaubt wenn es dafür eine **Rechtsgrundlage** gibt.

Grundsätzliches zum Datenschutz

Rechtmäßigkeit der Verarbeitung

- Wirksame Einwilligung des Betroffenen
- Erforderlichkeit zur Vertragserfüllung
- Rechtliche Verpflichtung des Verantwortlichen
- Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt
- Wahrung berechtigter Interessen des Verantwortlichen
- Schutz lebenswichtiger Interessen

Grundsätzliches zum Datenschutz

Beispiel: Übermittlung von Mitgliederdaten

- An andere Vereinsmitglieder im Einzelfall bei berechtigtem Interesse und ohne schutzwürdiges Interesse der Betroffenen zulässig
- Datenweitergabe zwecks Werbung oder Direktmarketing (z. B. Sponsoren) nur mit Einwilligung
- Mitgliederwerbung mit Fremddaten nur mit Einwilligung (schutzwürdige Interessen berücksichtigen)
- Gruppenversicherung nur mit Einwilligung

Grundsätzliches zum Datenschutz

Beispiel: Übermittlung von Mitgliederdaten

- Veröffentlichungen von Vereinsdaten in der Regel zulässig, private Daten nur mit Einwilligung
  - Schwarzes Brett
  - Mitgliederzeitung
- Internet und Social Media nur mit Einwilligung (Wettkampfergebnisse u. Ä., evtl. Widerspruch)
- Bilder (z. B. Feste) nur mit Einwilligung, Risiko der Nutzung durch Dritte (Behörden, Arbeitgeber, Auskunfteien, Banken, Versicherungen)
- Beim Versand von E-Mails an mehrere Empfänger das bcc-Adressfeld nutzen

Grundsätzliches zum Datenschutz

Wo ist Datenschutz geregelt?

- Datenschutzgesetze
  - EU-Datenschutz Grundverordnung (DS-GVO) Wirkt ab 25.05.2018
  - Bundesdatenschutzgesetz BDSG
  - (Bayerisches Datenschutzgesetz BayDSG für öffentliche Stellen in Bayern)
- Fachgesetze mit Datenschutzvorschriften
  - Telemediengesetz, Telekommunikationsgesetz, Sozialgesetzbuch etc.
- Betriebsvereinbarungen

Grundsätzliches zum Datenschutz

Wer kontrolliert die Einhaltung dieser Vorschriften?

- Verantwortlich ist der Verantwortliche
- Selbstkontrolle durch Datenschutzbeauftragte (wenn vorhanden)
- Fremdkontrolle durch Aufsichtsbehörde für den Datenschutz
  - Landesamt für Datenschutzaufsicht in Ansbach https://www.lda.bayern.de/

Datenschutzbeauftragte nach DS-GVO

Benennung

- Schriftform nicht vorgeschrieben, aber empfohlen
- Pflicht nach BDSG wenn mind. 10 Personen **regelmäßig** personenbezogene Daten verarbeiten
- Pflicht nach DS-GVO wenn Kerntätigkeit **regelmäßige** und **systematische Überwachung** von betroffenen Personen in großem Umfang erfordern oder
- Kerntätigkeit **umfangreiche** Verarbeitung besonderer Kategorien von Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten.
- Externe DSB sind möglich, allerdings muss die **Erreichbarkeit** gewährleistet sein.

Datenschutzbeauftragte nach DS-GVO

Kontaktdaten der DSB (sofern vorhanden) sind zu veröffentlichen

- Mitteilung an Aufsichtsbehörde (mit Namen empfohlen)
- Auf der Webseite (Name nicht zwingend)
- Informationspflicht bei Datenerhebung
  - Ausnahmen
    - Erhebung aufgrund einer Rechtsvorschrift
    - Betroffener hat die Information schon
    - Unterrichtung unmöglich oder unverhältnismäßig aufwendig

Datenschutzbeauftragte nach DS-GVO

Aufgaben

- Unterrichtung und Beratung von Verantwortlichen und Beschäftigten
- Ansprechpartner für Betroffene
- **Überwachung** der Einhaltung der Verordnung und anderer Datenschutzvorschriften
- Zusammenarbeit mit und Anlaufstelle für Aufsichtsbehörde
- **Beratung** des Verantwortlichen bei der **Datenschutz-Folgenabschätzung** (Art. 35) und **Überwachung** der Durchführung

Datenschutzbeauftragte nach DS-GVO

Stellung und Rechte

- Berichtet unmittelbar der höchsten Managementebene
- Unterstützungspflicht des Verantwortlichen
- Frühzeitige Einbeziehung in allen datenschutz-rechtlichen Fragen
- Ressourcen für Aufgabenerfüllung und für Erhalt des Fachwissens
- Zugang zu Daten und Verarbeitungsvorgängen
- Abberufungs- und Benachteiligungsverbot
- Es dürfen keine Interessenkonflikte bestehen
- Kündigungsschutz nach BDSG

Was ändert sich

- Ab dem 25. Mai 2018 gilt die EU Datenschutz Grundverordnung.
  - Das BDSG ist bereits angepasst, ist jedoch nachrangig, ebenso die Fachgesetze (TMG, TKG etc.)
- Anwendungsbereich sind „die ganz oder teilweise automatisierte …sowie … nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“ (Art. 2 Abs. 1 DS-GVO)
  - ➢ **Auch Akten(sammlungen) fallen auch darunter.**

Was ändert sich

Neue Definitionen

- **Verantwortlicher**
  die … Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet
- **Verarbeitung**
  jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder … Vorgangsreihe im Zusammenhang mit personenbezogenen Daten (wie Erheben, Ordnen, Speichern, Übermitteln, Löschen …)

Was ändert sich

- **Auftragsverarbeiter**
  natürliche oder juristische Person… oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet
- **Einwilligung**
  der betroffenen Person ist jede **freiwillig** für den **bestimmten** Fall, in **informierter** Weise und **unmissverständlich** abgegebene Willensbekundung … mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Was ändert sich

- **Rechenschaftspflicht (Art. 5, Abs. 2)**
  - Der Verantwortliche muss die Einhaltung der Vorgaben jederzeit nachweisen können
    - Rechtmäßigkeit
    - Verarbeitung nach Treu und Glauben
    - Transparenz
    - Zweckbindung
    - Datenminimierung
    - Richtigkeit
    - Speicherbegrenzung
    - Integrität und Vertraulichkeit

Was ändert sich

Verzeichnis der Verarbeitungstätigkeiten (Art. 30)

- Löst das Verfahrensverzeichnis ab
- Ist nicht mehr allgemein einsehbar
- Nachweis der Einhaltung der Verordnung und bündelt die für die Aufsichtsbehörde nötigen Informationen
- Ist zu nicht führen bei weniger als 250 Mitarbeitern und wenn
  - die Verarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt oder
  - die Verarbeitung nicht nur gelegentlich erfolgt oder
  - keine besonderen Datenkategorien oder Daten über straf-rechtliche Verurteilungen und Straftaten verarbeitet werden

Was ändert sich

Rechte der Betroffenen

- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung und Vergessenwerden
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Recht auf Widerspruch
- Recht auf „nicht automatisierte Entscheidung“
- Recht auf Widerruf einer Einwilligung

➢ Frist für Auskunftserteilung: **4 Wochen**

Was ändert sich

Weitere neue Pflichten

- Informationspflichten
  - Namen und die Kontaktdaten des Verantwortlichen
  - Ggf. Kontaktdaten des Datenschutzbeauftragten
  - Zwecke der Verarbeitung sowie die Rechtsgrundlage
  - Ggf. die Empfänger der personenbezogenen Daten
  - Ggf. die Absicht die personenbezogenen Daten an ein Drittland zu übermitteln
  - Speicherdauer für die personenbezogenen Daten
  - Die Betroffenenrechte und jederzeitiges Widerrufsrecht einer Einwilligung
  - Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
  - Bereitstellungspflicht der Daten und mögliche Folgen der Nichtbereitstellung
- Meldung von Datenpannen
- Risikobetrachtung von Verarbeitungen

Was ändert sich

Bußgelder

- Art. 83 DS-GVO
  Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in **jedem Einzelfall wirksam, verhältnismäßig und abschreckend** ist.
- Bußgelder sind bis 20 Mio. Euro möglich!

Was ist zu tun

Konkretisierung der Satzung

- Zweck des Vereins = Zweck der Datenverarbeitung
- Klärung der Verantwortlichkeiten
- Beitragserhebung und demokratische Willensbildung gehören zum Vereinszweck
- Evtl. konkrete Benennung von Unterzwecken
- Erforderlichkeit der Datenübermittlung evtl. wegen Landes- und Bundesverbänden
- Evtl. konkrete Nennung von Daten und Verarbeitungsformen (evtl. Info + Widerspruch)
- Nicht zwingend erforderliche Daten können per Einwilligung erhoben werden (§ 4a BDSG): informiert, bestimmt, freiwillig, widerruflich, nachweisbar

Was ist zu tun

Datenschutzorganisation

- Trennung von privater und Vereins-Datenverarbeitung
- Bestimmung eines Datenschutzbeauftragten
- Ggf. Benennung eines Öffentlichkeitsverantwortlichen
- Ggf. Benennung eines IT-Verantwortlichen (Webseite)
- Ggf. Vereinbarungen zur Auftragsdatenverarbeitung
- Evtl. IT-Geräte- und Programmverzeichnis
- Evtl. Regelung des Umgangs mit Kommunikation und mit Datenträgern (E-Mail, USB, Entsorgung usw.)
- Datensparsamkeit (Anonymisierung, Pseudonymisierung, Löschung)

Was ist zu tun

Verzeichnis der Verarbeitungstätigkeiten (VVT)

- Prüfung und Dokumentation ob ein Verzeichnis erforderlich ist
- Bestandsaufnahme (Wo werden welche Daten von wem mit welchen Verfahren und Programmen verarbeitet?)
- Überprüfung und Aktualisierung bestehender Verarbeitungen

Was ist zu tun

Auftragsverarbeitung

- Bestandsaufnahme (Wo werden Daten von Dritten verarbeitet?)
- Überprüfung der geschlossenen Vereinbarungen
- Anpassung alter bzw. Abschluss neuer Vereinbarungen

Was ist zu tun

Informationspflichten sicherstellen (NEU)

- Bei Einwilligungen, auf Webseite, an Aufsichts-behörde
- Bestandsaufnahme (Wo werden Einwilligungen für die Datenverarbeitung eingeholt?)
- Umsetzung der Informationsweitergabe (an Betroffene und Aufsichtsbehörden)
- Ggf. sind neue Einwilligung einzuholen

Was ist zu tun

Sicherstellung der Betroffenenrechte

- Recht auf Auskunft (4 Wochen Zeit, Kopien, nicht Akteneinsicht)
- Umfangreiche Informationen (Verarbeitungs-zwecke, Kategorien, Empfänger, Speicher-dauer, Informationen über die Rechte des Betroffenen, Beschwerderecht, ggf. Herkunft)

Was ist zu tun

Umgang mit Datenschutzverletzungen (NEU)

- Meldung an die Aufsichtsbehörde bei Risiko für Rechte und Freiheiten der Betroffenen
- Meldung an betroffene Person bei hohem Risiko für deren Rechte und Freiheiten
- Frist: 72 Stunden ab bekannt werden

Schulung der Mitarbeiter

Was ist zu tun

Durchführung der Datenschutz Folgenab-schätzung (DSFA) (NEU)

- Prüfung und Dokumentation jeder Verarbeitung ob eine Risikobewertung (=Datenschutz Folgen-abschätzung) erforderlich ist
- Umfangreiche Risiko Bewertung (aus Sicht der Betroffenen)
- Information der Aufsichtsbehörde bei nicht beherrschbarem Risiko
- Mindestens alle drei Jahre erneute Überprüfung

Weitere Infos

- Orientierungshilfen der Datenschutzaufsichtsbehörden
- https://www.lda.bayern.de/media/info_bw_verein.pdf
- https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Vereine/Inhalt/Datenschutz_im_Verein/Datenschutz_im_Verein1.pdf
- https://www.lfd.niedersachsen.de/themen/vereine/datenschutz-im-verein-56043.html
-
- Sonstige (Datenschutz)-Webseiten
- https://www.datenschutzbeauftragter-info.de/datenschutz-im-verein/
- https://www.arag.de/auf-ins-leben/vereinsrecht/datenschutz-im-verein/
- https://www.datenschutz-praxis.de/fachartikel/jedes-mitglied-kann-die-komplette-mitgliederliste-verlangen/

Fazit

- Dokumentieren Sie Ihre Datenschutz-Maßnahmen und auch die Entscheidungs-findung.
- Erstellen Sie das Verzeichnis der Verarbeitungstätigkeiten.
- Passen Sie Ihre Aufnahmeanträge und sonstigen Einwilligungserklärungen an.
- Prüfen Sie ob ein Datenschutzbeauftragter benannt werden muss.

Vielen Dank!

Kontakt:

Elisabeth Mayer
Gemeinsame Datenschutzbeauftragte
Landkreis Regensburg

Altmühlstraße 3 - 93059 Regensburg
datenschutz@lra-regensburg.de
www.landkreis-regensburg.de

Der Vortrag gibt ausschließlich die persönliche Auffassung der Verfasserin wieder und stellt keine Rechtsberatung dar.