DSGVO

Datenschutzgrundverordnung

gültig ab

25.5.2018

Kurzeinführung von DI Karl Tschavoll
im Verein Offene Jugendarbeit Satteins
Mi 9.5.2018

Wichtige Begriffe

Verantwortliche(r)

Vorstand, (bezahlte) Mitarbeiter

Wichtige Begriffe

Auftragsverarbeiter

Plattformen, Hosting der Website etc.

Wichtige Begriffe

Betroffene

Mitglieder

Wichtige Begriffe

Dritte

Andere Mitglieder, „Fans“, Behörden

Wichtige Begriffe

Personenbezogene Daten

Alle Informationen, die sich auf
eine identifizierte oder identifizierbare **natürliche Person**
beziehen, z.B. Name, Adresse, IP, Nummernschild, ...

Wichtige Begriffe

Sensible Daten

- Rassische und ethnische Herkunft
- Politische Meinung
- Gewerkschaftszugehörigkeit
- Religiöse oder weltanschauliche Überzeugung
- Genetische und biometrische Daten
- Gesundheitsdaten zum Sexualleben oder der sexuellen Orientierung

Rechte der Mitglieder („Betroffene“)

Rechte der betroffenen Person

- Recht auf Transparenz
- Recht auf Auskunft
- Recht auf Berichtigung und Löschung
- Widerspruchsrecht

Pflichten für Vereine („Verantwortliche“)

Verfahrensverzeichnis

- Hauptteil
- Das eigentliche Verzeichnis
- Technische und organisatorische Maßnahmen (**TOMs**)

Pflichten für Vereine („Verantwortliche“)

VVZ Hauptteil

- **Anschrift** und Vertreter der verantwortlichen Stelle
- Verweis auf die **TOMs**
- Grundsätzliches **Datenlöschungskonzept** für alle Verfahren
- *Grundsätzliches Vorgehen bei Übermittlungen in Drittstaaten*

Pflichten für Vereine („Verantwortliche“)

VVZ Verfahrensbeschreibung (1)

- **Bezeichnung** des Verfahrens
- **Name** der eingesetzten Tools oder Dienstleistung
- Datum des **Beginns** der Nutzung des Verfahrens
- Datum der letzten **Überprüfung** des Verfahrens
- Name und Kontaktdaten des **Verantwortlichen** im Verein
- **Zwecke** der Verarbeitungstätigkeit

Pflichten für Vereine („Verantwortliche“)

VVZ Verfahrensbeschreibung (2)

- **Betroffenenkategorien**
- **Datenkategorien**
- **Empfängerkategorien**
- Zulässigkeit der Datenverarbeitung (**Rechtsgrundlage**)
- *Übermittlung Drittstaaten*
- Spezielle **Löschfristen**
- Spezielle technische und organisatorische Maßnahmen
- **Unterschrift** des/der Verantwortlichen

Pflichten für Vereine („Verantwortliche“)

VVZ Technische und organisatorische Maßnahmen (TOMs)

- Auflistung aller TOMs
  - Ist nicht gesetzlich vorgeschrieben, aber sinnvoll für das Datenschutzmanagement und vor allem bei Übergaben und dgl. eine wertvolle **Dokumentation**!

Beispiele für TOMs

- Neuanmeldung: Ausschließlich **Opt-in**!
- DSGVO-konforme **Datenschutzerklärung** auf der Website
- **Antiviren-Software**, Betriebssystem aktuell halten, bekannte Sicherheitslücken schnell schließen, **sichere Passwörter(!)**, **verschlüsselte Kommunikation** (Mail, Chat) und **Website** (SSL/TLS), **Festplattenverschlüsselung**, saubere Trennung bei der Hardware, verschlüsselte **Backups** der Dateien/Datenbanken mit personenbezogenen Daten.
- **E-Mail**: Keine Mail-Dienste mit Sitz außerhalb DSGVO-Raum (GMail, Hotmail etc.). Eigenes Hosting oder zu bezahlende Maildienste wie posteo.de.

Fragen und Tipps

Abläufe hinterfragen, Datenerfassung straffen

- Was ist in den **Statuten** bereits vorhanden? Was wird zur Datenerfassung vorgegeben?
- Welche Daten genau sind für eine **Aufnahme** / die **Verwaltung** von Mitgliedern notwendig?
  - Anmeldeformulare ausmisten!
  - Hinweispflicht!
- **Datenspeicherung**: Weniger ist besser.
- Welche **internen Abläufe** / **vereinsinternen Weitergaben** von Daten gibt es?

  Beispiel: Im Vereinshaus ausgehängte Mitgliederliste mit Telefon, Mail und Adresse!
- Welche Daten werden an **Dachverbände** weitergegeben? ("Dritte")

Fragen und Tipps

Auftragsverarbeiter vertraglich binden

- Auftragsverarbeitungsvertrag für **externe Dienstleister** (Auftragsverarbeiter): https://www.wko.at/branchen/handel/D_06a-Auftragsverarbeitungsvertrag-nach-Art-28-DSGVO.pdf

Fragen und Tipps

Empfehlungen

- Anmeldeformulare mit **Einverständniserklärungen** (einzeln!)
  - Zur Verarbeitung der personenbezogenen Daten im Sinne der Vereinsmitgliedschaft
  - Zur Veröffentlichung von Daten (z.B. Ergebnisse bei Sportvereinen)
  - Zur Veröffentlichung von Bildern in Vereinsmedien (Website, Vereinsaussendungen) und Regionalzeitungen.
  - Einverständnis der Eltern bei Kindern und Jugendlichen
  - Einverständnis der Eltern zur Veröffentlichung von Bildern von Kindern und Jugendlichen in Vereinsmedien (Website, Vereinsaussendungen) und Regionalzeitungen
- Einverständniserklärungen aller Mitglieder nachholen z.B. JHV

Zum Schluss

Die wichtigsten Tipps

- Ruhig bleiben
- Wichtigste Vorbereitungsschritte machen (Statutenkontrolle, Verfahrensverzeichnis, Formulare, Website)
- Verfahrensanweisung des österr. Gesetzgebers an die Datenschutzbehörde:

„*Aufklären statt Abstrafen*“

Vielen Dank!

DI Karl Tschavoll

karl.tschavoll@zeweb.at