Einführung in die DSGVO - Elternvereine

Inhalte

- Grundlagen des Datenschutzrechts
  - Rechtmäßige Datenverarbeitung
  - Informationspflichten
  - Rollen und Verantwortungen
  - Öffnungsklauseln und nationale Umsetzung
- Datenschutz und IT Compliance
  - Verfahrensverzeichnis
  - Technische und Organisatorische Maßnahmen
  - Datenschutzverletzungen
  - Der Datenschutzbeauftragte

Grundlagen des Datenschutzrechts

Änderungen durch die DSGVO

- Informationspflichten
- Einwilligung und Auskunftsrecht
- Recht auf „Vergessenwerden“
- Entfall der Meldepflicht (DVR)
- Dokumentationspflichten („Verfahrensverzeichnis“)
- Datenschutzbeauftragter
- Datensicherheit
- Datenschutz-Folgenabschätzung
- Hohe Strafen

Strafen: bis 20 Mio Euro oder 4% weltweiter Umsatz!

Begriffe

- Datenverarbeitung: jede Handhabung außer Übermittlung
- Personenbezogene Daten
  - Identifizierte oder identifizierbare Person (Namen, Kennnummer, Standort, Online-Kennung, besondere Merkmale...)
- Betroffene Person
- Verantwortlicher: entscheidet über Zwecke und Mittel
- Auftragsverarbeiter: Verarbeitet Daten im Auftrag des V.
- Empfänger: Jeder, dem Daten überlassen oder übermittelt werden
- Dritter ≠ Betroffener, Verantwortlicher, Auftragsverarbeiter

Grundsätze

- Grundsatz der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz
- Grundsatz der Zweckbindung
- **Grundsatz der Datenminimierung**
- Grundsatz der Richtigkeit
- Grundsatz der Speicherbegrenzung
- Grundsatz der Integrität und Vertraulichkeit (Datensicherheit)

- Rechenschaftspflicht des Verantwortlichen!

Verarbeitung personenbez. Daten

- Prinzip des Verbots einer Verarbeitung personenbezogener Daten mit Erlaubnisvorbehalt in folgenden Fällen:
  - die betroffene Person hat ihre Einwilligung gegeben
  - die Verarbeitung ist für die Erfüllung eines Vertrages auf Anfrage der betroffenen Person erforderlich
  - ist zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen erforderlich
  - Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person
  - Verarbeitung in öffentlichem Interesse
  - Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen/Rechte der betroffenen Person überwiegen

Besondere personenbezogene Daten

- Personenbezogene Daten zu folgenden Inhalten
  - rassische und ethnische Herkunft
  - politische Meinungen oder Gewerkschaftszugehörigkeit
  - religiöse oder weltanschauliche
  - genetischen Daten, biometrischen Daten, Gesundheits-daten
  - Daten zum Sexualleben oder der sexuellen Ori-entierung
- Dürfen nur unter folgenden Voraussetzungen verarbeitet werden:
  - ausdrückliche Zustimmung
  - rechtlich / zum Schutz erforderlich
  - Tendenzbetrieb
  - Wurden offensichtlich öffentlich gemacht
  - Gesundheitsvorsorge …

Gültige Einwilligung

- Nachweispflicht (opt in!)
- Einfach, klar, verständlich, nachweisbar
- Koppelungsverbot = kein Nachteil bei Nichterklärung
- Informationen
  - Wer ist Verantwortlicher
  - Welche Zwecke
- Widerrufsrecht

Rechte der betroffenen Person

- Transparenz
- Informationspflicht und Auskunftsrecht
- Widerrufsrecht
- Recht auf Löschung
- Recht auf Einschränkung
- Recht auf Datenübertragung

Informationspflichten

- Name des Verantwortlichen
- Zwecke und Rechtsgrundlage
  - Ggf berechtigtes Interesse
  - Ggf gesetzliche / vertragliche Notwendigkeit
- Empfänger oder Kategorien von Empfängern
- Dauer oder Kriterien für Dauer
- Rechte der betroffenen Person
- dass Daten bis Widerruf verwendet werden dürfen
- Beschwerderecht bei Aufsichtsbehörde
- Wenn von Drittem: Woher und welche Kategorien von Daten?
  - Binnen 1 Monat, jedenfalls vor Verwendung

Auskunftsrecht

- Die Verarbeitungszwecke;
- Die Kategorien verarbeiteter personenbezogener Daten;
- ggf die Empfänger oder Kategorien von Empfängern ;
- Geplante Dauer der Speicherung oder Kriterien dafür;
- Betroffenenrechte inkl. Beschwerderechts bei Aufsichtsbehörde;
- ggf Datenquelle und Kategorie von Daten

Recht auf Löschung

- Für die Zwecke nicht mehr notwendige Daten
- Widerruf einer Einwilligung
- Widerspruch gegen die Verarbeitung und keine vorrangigen berechtigten Gründe für die Verarbeitung
- Unrechtmäßige Verarbeitung
- Kind wünscht weitere Verarbeitung nach Eintritt der Volljährigkeit nicht mehr
- Empfänger müssen informiert werden!
- Keine Löschung unter bestimmten Voraussetzungen wie Recht auf Information, öffentliches Interesse, Geltendmachen von Rechtsansprüchen, gesetzliche Notwendigkeit

Recht auf Einschränkung

- Richtigkeit wird bestritten, dies wird noch geprüft
- Verarbeitung ist unrechtmäßig, doch Betroffener wählt Einschränkung statt Löschung
- Betroffener braucht Daten noch, Verantwortlicher aber nicht
- Widerspruch gegen Verarbeitung wird geprüft
- Empfänger müssen informiert werden!

Pflichten des Verantwortlichen

- Nachweis erbringen, dass DSGVO eingehalten wird
- Geeignete technische und organisatorische Maßnahmen
- Maßnahmen prüfen und aktualisieren (Audits!)

Dokumentationserfordernisse

- Nachweis über Einhaltung der Grundsätze
  - Verfahrensverzeichnis erstellen
  - Checkliste für TOMs
  - Auftragsverarbeitervertrag (zB IT Dienstleister)
- Rechtmäßigkeit benennen können
  - Woher hat der EV die Daten seiner Mitglieder?
  - Welche/r Zweck/e?
  - Einwilligung nachweisen können
  - Besondere Kategorien: Ausdrückliche Einwilligung
- Bei Kind
  - Alter feststellen (Schutzalter: 14 Jahre)
  - Vertretung durch Eltern
- Information an Betroffene bei Erhebung / Nutzung

DSG zum Recht auf Datenschutz

- Kein Anspruch, wenn Daten allgemein verfügbar oder nicht rückführbar
- Geltung für ganz / teilweise / nicht automatisierte Verarbeitung
- Berichtigung oder Löschung muss nicht unverzüglich erfolgen, wenn aus wirtschaftlichen/technischen Gründen unverhältnismäßig (betrifft Backups)
- Kindesalter: 14 Jahre
- Verpflichtendes Datengeheimnis für Verantwortlichen, Auftragsverarbeiter und deren Beschäftigte

DSG: Erlaubte Bildaufnahme

- Eine Bildaufnahme ist zulässig, wenn
  - sie im lebenswichtigen Interesse einer Person erforderlich ist,
  - die betroffene Person zur Verarbeitung ihrer personenbezogenen Daten eingewilligt hat,
  - sie durch besondere gesetzliche Bestimmungen angeordnet oder erlaubt ist, oder
  - im Einzelfall überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten bestehen und die Verhältnismäßigkeit gegeben ist.

DSG: Unzulässige Bildaufnahme

- Höchstpersönlicher Lebensbereich und keine ausdrückliche Einwilligung
- Kontrolle von Arbeitnehmern
- Abgleich mit anderen personenbezogenen Daten
- Auswertung anhand von besonderen Kategorien

Datenschutz und IT Compliance

Verfahrensverzeichnis Verantwortlicher

- Pflicht praktisch immer gegeben
  - Unternehmen mit weniger als 250 MA nicht, wenn nur gelegentliche Datenverarbeitung
  - Dies wird praktisch nach aktueller Auslegung ausgeschlossen
- Inhalte
  - Stammdatenblatt
  - Datenverarbeitungen / -zwecke
  - Detailangaben
  - Allgemeine Beschreibung TOM

Datenverarbeitungen

- Zwecke und Beschreibung
  - Geschäftsführung
  - Mitgliederverwaltung
  - Marketing
  - ....
- Datenschutz-Folgenabschätzung durchgeführt?
  - Nicht erforderlich, wenn weder Profiling noch sensible Daten in hohem Umfang noch hohe Gefahr für die Persönlichkeitsrechte – davon kann man bei einem Elternverein ausgehen.

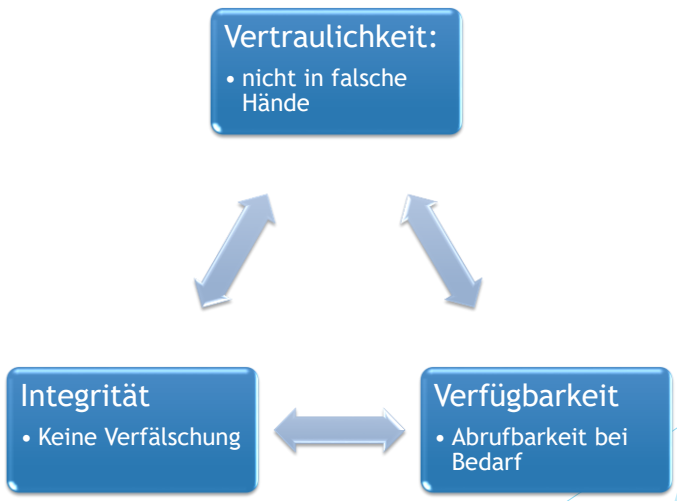
Detailangaben

- Inhalte
- Zwecke
- Kategorien betroffener Personen
  - Vereinsmitglieder, Vertragspartner, ...
- Rechtsgrundlagen
  - Rechtliche Verpflichtung, Vertragserfüllung, Einwilligung...
- Datenkategorien und Kategorien von Empfängern
  - Stammdaten, Korrespondenzdaten,...
  - Banken, IT Dienstleister ...
- Lösch- und Aufbewahrungspflichten

TOM: Sicherung von ...

- Vertraulichkeit (Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle)
- Integrität (Eingabe- und Weitergabekontrolle)
- Verfügbarkeit und Belastbarkeit
- Evaluierungsmaßnahmen

Definition von Datensicherheit



Organisatorische Maßnahmen 1

- Grundlegende Sicherheitsstrategie
  - Büro absperren bei Verlassen
  - Computer sperren
  - Bildschirmfolie verwenden bei Kundenkontakt
  - Umgang mit Emails, Links
  - Vertraulichkeitsvereinbarungen
- Einschulung und Weiterbildung, Awarenessmaßnahmen
  - Checklist erstellen
- Löschkonzept für sicheres Löschen und Entsorgen
  - Löschprotokoll führen (bei Backups)
  - Schreddern von Papier (Putzfrau!), CDs, Festplatten
- Definition von Verantwortlichkeiten und Zuständigkeiten
  - Unterschiedliche Rechte für unterschiedliche Rollen
  - Nicht jeder ist Administrator!
  - Genehmigungsprozesse, Beschaffungsprozesse

Organisatorische Maßnahmen 2

- Regeln zum Umgang mit Geräten, BYOD-Regeln
  - Verwendung privater Notebooks, Handys im Alltag?
  - Apps auf Vertraulichkeit überprüfen (Whatsapp...)
  - Inventarisierung aller IT Systeme und: Wo wird was gespeichert
- Vertragsgestaltung mit Dienstleistern
  - TOMs des Dienstleiters einfordern
  - Vertraulichkeit des Dienstleisters festlegen
- Planung und Durchführung von Überprüfungen
- Notfallkonzept entwickeln
  - Backups verwenden

Technische Maßnahmen

- Authentifizierung und Passwort-Richtlinien
  - Lange Passwörter vs. oftmaliges Ändern
- Unterschiedliche Accounts je Rolle
  - Obmann/Obfrau, Kassier, Weitere Vorstandsmitglieder
- Regelung der De/Reaktivierung von Accounts
  - Was passiert bei Ausscheiden?
- Segmentierung je nach Risikoniveau
  - Netzwerkbereiche definieren
- Absicherung (E-Mail Server, Firewall etc)
- Management von Updates
- Verschlüsselung von Datenträgern
- Datensicherung, Wiederherstellungstests, Dokumentation

Datenschutz und Website

- IP Adressen sind personenbezogene Daten, daher Verwendungszweck und Speicherdauer angeben
- Cookies erst nach Einwilligung des Besuchers
- Datenschutzerklärung:
  - Bekenntnis zum Datenschutz
  - Information über Datenanwendungen
  - Erfassung, Speicherung, Löschung der Daten
  - Info über gesetzte Cookies und Zwecke
  - Beschreibung eingesetzter Trackingtools
  - Hinweis auf Betroffenenrechte
  - Kontaktdaten

Datenschutzverletzungen

- Meldung binnen 72 Stunden an Aufsichtsbehörde, außer kein Risiko für Rechte und Freiheiten
  - Art der Datenschutzverletzung
  - Kategorie und Zahl betroffener Personen
  - Kategorie und Zahl betroffener Datensätze
  - Kontaktdaten
  - Beschreibung der wahrscheinlichen Folgen
  - Beschreibung Gegenmaßnahmen
  - Information der Betroffenen bei hohem Risiko
- Spätere Meldung muss begründet werden