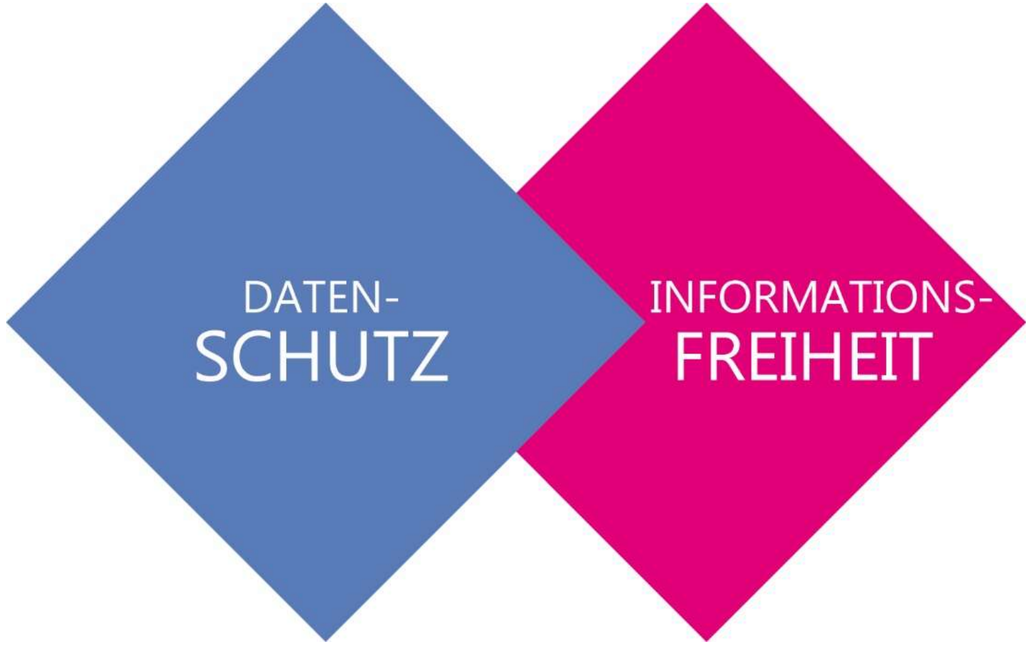

Datenschutz in sozialen Einrichtungen und Diensten

Der Paritätische Rheinland-Pfalz/Saarland

31. Oktober 2019

UNABHÄNGIGES DATENSCHUTZ ZENTRUM SAARLAND

Erste Erfahrungen aus der Praxis

Allgemein

- Größere Aufmerksamkeit für den Datenschutz
- Bürger sensibilisiert für Fragen des Datenschutzes

→ Erheblicher Anstieg an Beratungsanfragen und Beschwerden beim Unabhängigen Datenschutzzentrum

Informationspflichten

- **Grundgedanke:**

→Transparenz hinsichtlich der Existenz eines Verarbeitungs-vorgangs und dessen Zwecke

- **Form der Informationen** (Art. 12)
  - präzise, transparent
  - klare und einfache Sprache
  - leicht zugänglich
  - schriftlich oder elektronisch, mündliche Informationen als Ausnahme (Art. 12 Abs. 1 Satz 3) – ohne Medienbruch
- **Inhalt** (Art. 13 Abs. 1 und 2, Art. 14 Abs. 1 und 2)

Informationspflichten (Art. 13 DSGVO)

- Informationen zum Zeitpunkt der Erhebung bei der betroffenen Person
    - Datenschutzerklärung auf der Webseite
    - Telefonische Terminvereinbarung
- Ausnahme (Art. 13 Abs. 4)
    - alle Informationen müssen vorliegen
- Information bei Zweckänderungen (Art. 13 Abs. 3)
    - Verarbeitung zu einem anderen Zweck durch Verantwortlichen
    - Übermittlung an Dritte

Auskunftsrecht (Art. 15 DSGVO)

- Auskunft, **ob und ggf.** welche Daten vorhanden sind

  → erforderlich zur Überprüfung der Richtigkeit der vorhandenen Daten und ob Daten datenschutzkonform verarbeitet werden
- Umfang der Informationen Abs. 1 2. Hs. lit. a) bis h)
- Abs. 3: der Verantwortliche stellt eine **Kopie der personenbezogenen Daten**, die Gegenstand der Verarbeitung sind, zur Verfügung
  - Rechtsnatur und Umfang sehr umstritten

Veröffentlichung von Fotoaufnahmen zur Öffentlichkeitsarbeit

- Fotoaufnahmen zu Zwecken der Außendarstellung (in Broschüren, Internet…)
  - Rechtsgrundlage
    - Art. 6 Abs. 1 lit. f)
      - Widerspruchsrecht (Art. 21)
    - Einwilligung
  - Informationspflichten
    - Einladungsschreiben/Hinweise am Veranstaltungsort
    - Information über Veröffentlichungskanal

Verletzung des Schutzes personenbezogener Daten

Meldepflicht ggü Aufsichtsbehörde (Art. 33)

- Verletzung des Schutzes pb Daten (Art. 4 Nr. 12)
  - Vernichtung/Verlust/Veränderung (unbeabsichtigt/unrechtmäßig)
  - unbefugte Offenlegung/unbefugter Zugang
- Unverzügliche Meldung, möglichst innerhalb von 72 Stunden
  - Meldeformular
- Meldepflicht entfällt, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Pflichten der betroffenen Person führt

Verletzung des Schutzes personenbezogener Daten

Benachrichtigungspflicht der Betroffenen (Art. 34)

- wenn Verletzung des Schutzes pb Daten voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Person führt
- Ausnahmen von der Benachrichtigungspflicht (Abs. 4)
  - (präventive) geeignete technische und organisatorische Sicherheitsvorkehrungen
  - nachfolgende Maßnahmen
  - unverhältnismäßiger Aufwand, dann aber öffentliche Bekanntmachung

Facebook-Fanpage

- **Gemeinsame Verantwortlichkeit (Art. 4 Nr. 7, 26)**
  - Fanpage-Betreiber ist mitverantwortlich für die Datenverarbeitung durch Facebook (Insights-Funktion)
  - Vereinbarung nach Art. 26 DSGVO erforderlich
    - Beschreibung der tatsächlichen Funktionen und Beziehungen ggü. dem Betroffenen
    - Festlegung der jeweiligen Verpflichtungen, insbes. Informationspflichten

    → Aktuelle Nutzungsbedingungen von Facebook erfüllen die Anforderungen nicht
  - Aufsichtsbehörde kann Betreiber zur Deaktivierung verpflichten

Datenschutz in sozialen Einrichtungen

Soziale Einrichtungen und Dienste

- Häufig Umgang mit sehr sensiblen persönlichen Daten
- Breites Spektrum, daher verschiedene datenschutzrechtliche Vorgaben zu beachten, ggf. spezialgesetzliche Regelungen

Soziale Einrichtungen und Dienste

- Unterrichtung und Verpflichtung von Beschäftigten auf den Datenschutz

- ggf. auch gesetzliche Schweigepflicht zu beachten (Berufsgeheimnis nach § 203 StGB)

Datenschutzrechtliche Grundlagen

- Öffentliche Stellen im Saarland → SDSG
- Kirchliche Trägerschaft → KDG, DSG-EKD
- Nicht-öffentliche Stellen grundsätzlich DSGVO und BDSG

Datenschutzrechtliche Grundlagen

- Sozialleistungsträger → Sozialdatenschutz nach SGB

- Besonderheit: Freier Träger erfüllt Aufgabe für öffentlichen Träger oder erhält Daten von diesem → SGB

Wichtige Vorschriften aus SGB I (Allgemeiner Teil) und SGB X (Sozialverwaltungsverfahren und Sozialdatenschutz)

- § 35 SGB I – Sozialgeheimnis
- § 67 Abs. 2 SGB X – Sozialdaten

Wichtige Vorschriften aus SGB I (Allgemeiner Teil) und SGB X (Sozialverwaltungsverfahren und Sozialdatenschutz)

- § 67a SGB X – Erhebung von Sozialdaten (Grundsatz der Erforderlichkeit)
- § 78 SGB X – Zweckbindung und Geheimhaltungspflicht bei Dritten, vertragliche Vereinbarung, Hinweis Beschäftigte

Formen der Zusammenarbeit nach DSGVO

- **Gemeinsame Verantwortung** (Art. 26 DSGVO): Zwecke und Mittel der Datenverarbeitung gemeinsam festgelegt, transparente Vereinbarung bezüglich Erfüllung der Verpflichtungen gem. DSGVO (insbes. Betroffenenrechte)

- **Auftragsverarbeitung** (Art. 4 Nr. 8 i.V.m. Art. 28 DSGVO): Auftragnehmer (Auftragsverarbeiter) verarbeitet Daten auf Weisung des Auftraggebers (Verantwortlicher)

Beispiel: Jugendhilfe – SGB VIII

- §§ 3 und 4: Zusammenarbeit öffentliche und freien Jugendhilfe

- §§ 61 ff regeln Schutz von Sozialdaten in der Jugendhilfe; bei Inanspruchnahme freier Träger dort „in entsprechender Weise“ (§ 61 Abs. 3 SGB VIII)

Beispiel: Jugendhilfe – SGB VIII

- § 62 Erforderlichkeitsgrundsatz, grds. Erhebung beim Betroffenen

- Verweis auf allg. Vorgaben SGB X zum Sozialdatenschutz

Anwendung von DSGVO und BDSG

- Freier Träger autonom tätig → allg. Vorgaben aus DSGVO und BDSG; mögliche Grundlagen für Datenverarbeitung aus Art. 6 bzw. Art. 9 DSGVO hier u.a.:

  - zur „Vertragserfüllung“ erforderlich (vertragsähnliches Vertrauensverhältnis bei Beratung), Art. 6 Abs. 1 lit. b DSGVO

Anwendung von DSGVO und BDSG

- zur Versorgung im Gesundheits- oder Sozialbereich bzw. Erfüllung eines Vertrages erforderlich, Art. 9 Abs. 2 lit. h DSGVO

- Einwilligung (Art. 6 Abs. 1 lit. a bzw. Art. 9 Abs. 2 lit. a DSGVO), dann aber Art. 4 Nr. 11 und Art. 7 DSGVO zu beachten!

Anwendung von DSGVO und BDSG

Die allgemeinen Vorschriften aus DSGVO und BDSG sind daneben auch in der Personalverwaltung (§ 26 BDSG – Datenverarbeitung im Beschäftigungsverhältnis) und bei der Mitgliederverwaltung der Vereine (Art. 6 DSGVO) zu beachten.

Datenschutzbeauftragter (DSB)

Benennung eines DSB

- **Art. 37 Abs. 1 DSGVO:**
  - Verarbeitung durch Behörde oder andere öffentliche Stelle
  - **Kerntätigkeit** umfasst **umfangreiche** regelmäßige und systematische Überwachung betroffener Personen
  - **Kerntätigkeit** besteht aus **umfangreicher** Verarbeitung besonderer Kategorien von Daten (Art. 9 DSGVO) oder von Daten gemäß Art. 10 DSGVO

  -> Kriterien dürften eher nicht zutreffen
- **§ 38 Bundesdatenschutzgesetz (BDSG)**
  - in der Regel mindestens 10 (künftig 20) Personen ständig mit der automatisierten Datenverarbeitung beschäftigt

Benennung eines DSB

- Interner oder externer DSB (Art. 37 Abs. 6)
- Anforderungsprofil (Art. 37 Abs. 5)
  - Berufliche Qualifikation und Fachwissen
  - zur Erfüllung der Aufgaben in der Lage
    - Ausstattung/Persönliche Zuverlässigkeit
- Veröffentlichung der Kontaktdaten und Mitteilung der Kontaktdaten an die Aufsichtsbehörde (Abs. 7)
  - Meldeformular
- keine besondere Form der Benennung

Stellung des DSB (Art. 38)

- Frühzeitige Einbeziehung in alle Datenverarbeitungsprozesse
- Zugang zu allen Datenverarbeitungsvorgängen und Zurverfügungstellung der erforderliche Ressourcen
- Weisungsfreiheit
- Ansprechpartner für betroffene Personen
- Geheimhaltungs- und Verschwiegenheitspflicht
- kein Interessenskonflikt

Aufgaben des DSB (Art. 39)

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten
- Überwachung der Einhaltung von Datenschutzvorschriften
- Schulung und Sensibilisierung von Mitarbeitern
- Beratung bei DSFA
- Zusammenarbeit mit der Aufsichtsbehörde und Anlaufstelle für die Aufsichtsbehörde

! Verantwortung für die Einhaltung der Vorgaben der DSGVO und anderer datenschutzrechtlicher Vorschriften liegt aber beim Verantwortlichen!

Aspekte des technisch-organisatorischen Datenschutzes

Vorgaben der DSGVO

- **Art. 5 Abs. 1 lit. f:** sichere Verarbeitung einschließlich Schutz durch geeignete technische und organisatorische Maßnahmen
- **Art. 24:** Verpflichtung des Verantwortlichen, geeignete technische und organisatorische Maßnahmen umzusetzen, um Verarbeitung gem. DSGVO sicherzustellen
- **Art. 25:** Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- **Art. 32:** Sicherheit der Verarbeitung

→ Maßnahmen müssen Schutz gg. jegliche Arten einer rechtswidrigen Datenverarbeitung bieten

Gewährleistung der Datensicherheit (Art. 32)

- **Auswahlkriterien für geeignete technische und organisatorische Maßnahmen**
  - Stand der Technik
  - Kosten für die Implementierung (nicht Folgekosten)
  - Art, Umfang, Zweck und Umstände der Verarbeitung
  - Eintrittswahrscheinlichkeit und Schwere der Risiken

Geeignete Maßnahmen

- Pseudonymisierung und Verschlüsselung
- Zutrittskontrolle, Zugangskontrolle
- Zugriffskontrolle, Berechtigungskonzept für EDV-Anwendungen/Fachverfahren, aber auch Zugriff auf Papierakten regeln (z.B. abschließbare Schränke)
- Sensibilisierung der Mitarbeiter, Sorgfalt bei Postversand oder Verschicken von E-Mails
- Updates durchführen, Virenschutz und Firewall installieren, Wachsamkeit beim Öffnen von E-Mails, sichere Passwörter; Verschlüsselung von Webseiten, Back-up

Einzelfragen

- **Nutzung von WhatsApp**
  - (Meta-)Datenübermittlung in die USA und Auslesen Telefonbuch
  - bei sensiblen Daten vermeiden, nicht aktiv anbieten
- **E-Mail-Versand**
  - Transportverschlüsselung (mittlerweile Standard)
  - bei sensiblen Daten Ende-zu-Ende-Verschlüsselung (PGP-Schlüssel)
- **Nutzung von Cloud-Diensten**
  - Server-Standort relevant
  - AV-Vertrag mit Anbieter (Art. 28)

Weiterführende Informationen zur DS-GVO finden Sie unter:

https://datenschutz.saarland.de

Vielen Dank für Ihre Aufmerksamkeit

UNABHÄNGIGES DATENSCHUTZZENTRUM SAARLAND

Die Landesbeauftragte für Datenschutz
und Informationsfreiheit

Fritz-Dobisch-Straße 12 • 66111 Saarbrücken
Telefon 0681 94781-0
Fax 0681 94781-29
E-Mail: poststelle@datenschutz.saarland.de
Internet www.datenschutz.saarland.de
www.informationsfreiheit.saarland.de