KANTON AARGAU

BEAUFTRAGTE FÜR
ÖFFENTLICHKEIT UND DATENSCHUTZ

Datenschutz – Theorie und Praxis

AZSV-Fachtagung

30. September 2024

1

Agenda

I. Rolle der Beauftragen für Öffentlichkeit und Datenschutz
II. Rechtliche Grundlagen und anwendbares Recht
III. Datenschutzrechtliche Grundsätze
IV. Bezug zur Praxis: Anwendertipps

2

I. Die ÖDB - Aufgaben

- **Aufsicht** über die Einhaltung der Vorschriften des IDAG und VIDAG
  - Datenschutz/Datensicherheit
  - Öffentlichkeitsprinzip
- **Beratung** von und **Vermittlung** zwischen Privaten und Behörden
- Stellungnahmen zu Gesetzesvorhaben und relevanten anderen Vorhaben
- Durchführung von Vorabkonsultationen
- Bewilligung von optisch-elektronischen Überwachungen (Videoüberwachung)

I. Die ÖDB - Befugnisse

- Tätigkeit von Amtes wegen oder auf Anzeige hin
- Recht auf Akteneinsicht und Auskunftserteilung bei den öffentlichen Organen (ungeachtet allfälliger Geheimhaltungspflichten)
- Erlass von Empfehlungen
- Erlass von Verfügungen, wenn die Empfehlung nicht angenommen oder nicht befolgt wird

I. Die ÖDB - Pflichten

- Behandlung von Eingaben
- Zusammenarbeit mit Datenschutzbehörden anderer Kantone, des Bundes und des Auslands
  - Zusammenarbeit insbesondere mit «privatim» – Konferenz der kantonalen Datenschutzbeauftragten
- Jahresbericht an den Grossen Rat und Regierungsrat

5

II. Rechtliche Grundlage

- Datenschutzrecht als Grundrecht in der Bundesverfassung

Art. 13 Schutz der Privatsphäre

[1] Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.

[2] Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

- Datenschutzrecht als Grundrecht in der Kantonsverfassung

§ 15 f) Recht auf persönliche Freiheit und auf Wahrung der Privatsphäre

[1] Die persönliche Freiheit ist unverletzlich. Jedermann hat das Recht auf Leben, körperliche und geistige Unversehrtheit und Bewegungsfreiheit.

[2] Die Geheim- und Intimsphäre des Privat- und Familienlebens, der Schutz vor Datenmissbrauch, die Unverletzlichkeit der Wohnung sowie das Brief- und Fernmeldegeheimnis sind gewährleistet.

[3] Vorbehalten sind im Gesetz vorgesehene Massnahmen zum Schutze der Jugend und der Gesundheit

6

II. Anwendbares Recht

Bund	Kanton	Gemeinde
Bundesgesetz über den Datenschutz (DSG)	Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG)	Datenschutzreglement
Bereichsgesetze (KVG, AHVG, SchKG,…)	Bereichsgesetze (GesG, PolG, GG, RMG,…)	Reglemente (Videoreglement, Polizeireglement, BNO,…)
Bundesbehörden	Kant. Behörden	Gemeindebehörden
Private	Private (öff. Aufgaben)	
	Landeskirchen	

II. Anwendbares Recht - Zuständigkeiten

EDÖB (Eidg. Datenschutz- und Öffentlichkeitsbeauftragter)	ÖDB (Beauftragte für Öffentlichkeit und Datenschutz)	
Bundesbehörden	Kantonale Behörden	Kantonale Behörden
	Private (mit öffentlichen Aufgaben)	
	Landeskirchen	
Private		

III. Grundsätze - Datenschutz*recht*

> **Begriffe**

Begriff	Definition	Beispiele (nicht abschliessend)
Personendaten (§ 3 Abs. 1 lit. d IDAG)	Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen.	Beatrice Müller oder Personalnummer XY
Besonders schützenswerte Personendaten (§ 3 Abs. 1 lit. k IDAG)	Daten, bei denen aufgrund ihrer Bedeutung, des Zusammenhangs, Zwecks oder Art der Datenbearbeitung, der Datenkategorie oder anderer Umstände, eine besondere Gefahr der Persönlichkeitsverletzung besteht.	Religion, Gesundheit, Massnahmen der sozialen Hilfe, strafrechtliche Verfolgungen, genetische Daten, biometrische Daten
Profiling (§ 3 Abs. 1 lit. f IDAG)	Jede Auswertung von Daten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen.	Auswertung der: Arbeitsleistung, wirtschaftl. Lage, Mobilität,…
Betroffene Personen (§ 3 Abs. 1 lit. e IDAG)	Jede natürliche Person, über die Personendaten bearbeitet werden.	Bürger:innen, Mitarbeiter:innen, Schüler:innen,…
Bearbeiten (§ 3 Abs. 1 lit. g IDAG)	Jeder Umgang mit Personendaten.	beschaffen, aufbewahren, verwenden, umarbeiten, bekanntgeben, vernichten

9

III. Grundsätze - Datenschutz*recht*

> **Prinzipien des Datenschutzes**

Prinzip / Grundsatz	Definition
Legalitätsprinzip / Rechtmässigkeit (§ 8 IDAG)	Öffentliche Organe dürfen Personendaten nur bearbeiten, wenn: - Rechtsgrundlage / gesetzliche Grundlage - Notwendig zur Erfüllung einer rechtlichen / gesetzlichen Aufgabe - Einwilligung der betroffenen Person - Hypothetische Einwilligung
Verhältnismässigkeit (§ 9 IDAG)	So viele Daten wie nötig, so wenig wie möglich. → Datenvermeidung und Datensparsamkeit
Zweckbindung (§ 11 IDAG)	Bearbeitung nur zu dem Zweck, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist
Datensicherheit (§ 12 IDAG i.V.m. § 4 VIDAG)	Personendaten müssen durch technische und organisatorische Massnahmen geschützt werden.
Richtigkeit / Korrektheit (§ 10 IDAG)	Daten müssen richtig und (soweit es der Zweck verlangt) vollständig sein. → Beweislast liegt beim öffentlichen Organ.
Transparenz / Informationspflicht (§ 13 IDAG)	Öffentliche Organe müssen über die Datenbearbeitung informieren.

10

III. Grundsätze - Datensicherheit

> **Beispiele technischer oder organisatorischer Massnahmen**

Massnahme	Beispiele
Zugangskontrolle (§ 4 Abs. 1 lit. a VIDAG)	Elektronische Zugangskontrolle (Badge, Zugangscode), Büros abgeschlossen ausserhalb Arbeitszeiten, Alarmsystem in heiklen Räumen, Protokollierung, regelmässige Überprüfung der Zutrittsrechte, physische Sicherheit
Datenträgerkontrolle (§ 4 Abs. 1 lit. b VIDAG)	Verschlüsselung von mobilen Datenträgern, Aufbewahrung unter Verschluss, technische Unterbindung, sichere Datenvernichtung
Transportkontrolle (§ 4 Abs. 1 lit. c VIDAG)	Verschlüsselung von Data in transit, Netzsicherheit, Protokollierung des Datenaustauschs
Bekanntgabekontrolle (§ 4 Abs. 1 lit. d VIDAG)	Datenempfänger identifizieren, digitale Unterschrift von Mitteilungen (Signieren)
Speicherkontrolle (§ 4 Abs. 1 lit. e VIDAG)	Verschlüsselung von Data at rest, Protokollierung, sichere Datenvernichtung, abgeschottetes Netzwerk, Aufbewahrung unter Verschluss

III. Grundsätze - Datensicherheit

> **Beispiele technischer oder organisatorischer Massnahmen**

Massnahme	Beispiel
Benutzerkontrolle (§ 4 Abs. 1 lit. f VIDAG)	MFA, VPN, Überwachung von Lieferantenzugängen
Zugriffskontrolle (§ 4 Abs. 1 lit. g VIDAG)	Rollen- und Berechtigungskonzept, regelmässige Überprüfung aller Benutzerkonten und Berechtigungen, persönliche Benutzerkonten/Adminkonten, starke Authentifizierung (MFA), Erzwingen von komplexen Passwörtern, Clean Desk, Protokollierung
Eingabekontrolle (§ 4 Abs. 1 lit. h VIDAG)	Protokollierung, Schulung von Mitarbeitenden
Wiederherstellung (§ 4 Abs. 1 lit. i VIDAG)	Backup, Kontinuitätsplan, Redundante Infrastruktur
Zuverlässigkeit, Integrität (§ 4 Abs. 1 lit. j VIDAG)	Meldung von Fehlfunktionen (Schreib- oder Lesefehler, Hitze, Feuer oder Wasser im Serverraum), Anti-Viren-Schutz, Backup

IV. Praxisbezug – Beispiele aus dem Alltag

- **Ablage von Mailkorrespondenzen in PISA:**
  - Nachvollziehbarkeit des Verwaltungshandeln:
    - Ablage geschäftsrelevanter Dokumente
  - Geschäftsrelevanz:
    - Orientierung an der zu erfüllenden Aufgabe / am Bearbeitungszweck
    - Dokumente, die für die Nachvollziehbarkeit von Entscheidungen unverzichtbar sind
- **Ablage von Arztzeugnissen in PISA:**
  - Verhältnismässigkeit / Datensparsamkeit vs. «erweiterte» Aufgabenerfüllung
- **Bekanntgabe der Zuteilungspläne an Private:**
  - Datenbekanntgabe an Private gem. § 15 IDAG (ohne Bedrohungslage):
    - Gesetzliche Pflicht 👎
    - erforderlich zur Aufgabenerfüllung 👎
    - Durchsetzung von Rechtsansprüchen 👎
    - Einwilligung ❓
  - Praktische Relevanz aufgrund der Agilität fraglich

IV. Praxisbezug – Anwendertipps zur Datensicherheit

Thema	Tipps
Starke Passwörter verwenden	Komplexität, individuelles Passwort für jeden Dienst, Passwortmanager, Multi-Faktor-Authent.
Umgang mit Hardware und Software	Clean Desk, vor unberechtigtem Zugriff schützen, zugelassene Software verwenden
Mobil unterwegs	Vorsicht mit fremden WLANs, Einsatz von VPN, Achtung vor Mitlesen/Mithören (Arbeiten in der Öffentlichkeit)
Umgang mit E-Mails	Vertrauliche Daten verschlüsseln, misstrauisch gegenüber empfangenen E-Mails
Umgang mit Daten	Klassifizierungsrichtlinie, Drucker, Zugriffe einschränken (Need-to-know)

IV. e-Learning Cybersecurity

Grundausbildung im Bereich Cybersicherheit für Behörde

www.elearningcyber.ch

15

Vielen Dank!

Katrin Gisler, MLaw, LL.M.
Beauftragte
Bahnhofplatz 13
5200 Brugg
062 835 45 60
katrin.gisler@ag.ch

Leonie Mannhart
IT-Auditorin
Bahnhofplatz 13
5200 Brugg
062 835 45 60
leonie.mannhart@ag.ch

16