

# Datenschutzrechtliche Anforderungen an das Vereinsmanagement

Univ.-Ass. Mag. Žiga Škorjanc

Univ.-Ass. Mag. Felix Zopf

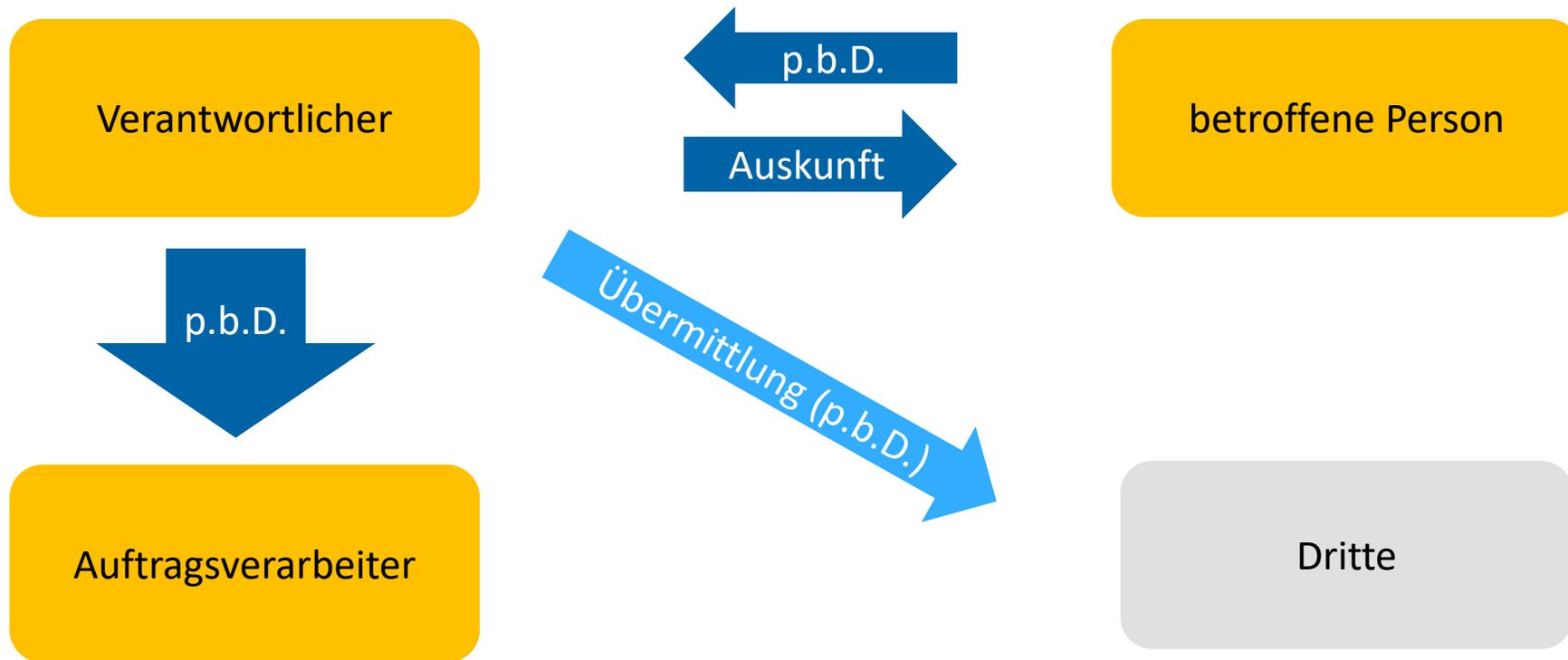


## Überblick

- Teil 1: Crashkurs Datenschutzrecht
- Teil 2: Verarbeitung von Mitgliederdaten
- Teil 3: Sanktionen bei Verstößen

# Teil 1: Crashkurs Datenschutzrecht

## Datenschutzrechtliche Rollen



## Grundsätze für die Verarbeitung personenbezogener Daten

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- **Zweckbindung**
- **Datenminimierung**
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- *Rechenschaftspflicht („accountability“)*

## Rechtsgrundlagen für die Verarbeitung der personenbezogenen Daten

- Erforderlich für die Erfüllung eines **Vertrags**, dessen Vertragspartei die betroffene Person ist
- Erforderlich zur Erfüllung einer **rechtlichen Verpflichtung** (z.B. *der Meldung zum Vereinsregister*)
- Erforderlich zur Wahrung der **berechtigten Interessen des Verantwortlichen oder eines Dritten**
  - sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen

[...]

- (ausdrückliche) Einwilligung

## Teil 2: Verarbeitung von Mitgliederdaten

## Allgemeines

- **Mitgliederdaten:** alle personenbezogenen Daten die sich auf Mitglieder beziehen
  - z.B. Name, Tatsache der Mitgliedschaft, Kontaktdaten
- Verarbeitung durch den Verein (**Verantwortlicher**)
  - Festlegung von Zwecken und Mitteln der Verarbeitung durch den Verein bzw. Vereinsorgane
  - Keine eigenständigen Zwecke der Mitglieder oder Angestellten (*ansonsten sind diese selbst Verantwortliche der jeweiligen Datenverarbeitung*)

## Führung und Weitergabe von Mitgliederverzeichnissen

- **Führung von Mitgliederverzeichnissen**
  - Erforderlich für die Erfüllung eines Vertrags (*Vereinsstatut*)
  - Einwilligung empfiehlt sich nicht
  
- **Weitergabe von Mitgliederverzeichnissen an Dritte (*externe Personen*)**
  - Eventuell erforderlich zur Wahrung der berechtigten Interessen
  - Ansonsten aber Einwilligung
  - [Eventuell erforderlich für die Erfüllung eines Vertrags]

## Verarbeitung von besonderen Kategorien personenbezogener Daten

- „*Sensitive Daten*“ betreffend z.B. **Gesundheit, politische Meinung, religiöse Überzeugung**
- **Anwendungsfälle:** z.B. politische oder religiöse Vereine, Selbsthilfevereine bei Krankheiten, Gewerkschaften, Religionsgemeinschaften
- Rechtsgrundlage:
  - Ausdrückliche Einwilligung
  - Erforderlich zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
  - **Interne Verarbeitung** der Mitglieder- und Begünstigtendaten durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Organisation ohne Gewinnerzielungsabsicht

## Spezialfall Publikumsvereine

- Zur Willensbildung im Verein sind gewisse **Stimmquoten** notwendig
- Herausgabe der **Email-Adressen** *aller Vereinsmitglieder*?
  - Vereinsrechtlicher Anspruch vs. Geheimhaltungsanspruch (?)
  - Fraglich in welcher Form: Papier oder digital?
- Rechtsgrundlage:
  - Erforderlich für die Erfüllung eines Vertrags?
  - Erforderlich zur Wahrung der berechtigten Interessen?

## Teil 3: Sanktionen bei Verstößen

## Die (vielleicht) wesentlichste Änderung im Vergleich zum DSG 2000?

- **DSB** erhielt die Befugnis, weitreichende

**Abhilfemaßnahmen** (z.B. *Verbot oder [teilweise] Beschränkung der Verarbeitung, Anordnung, Verwarnung*) mit Bescheid anzuordnen (Art 58 Abs 2 DSGVO)

- sowie die Zuständigkeit zur Verhängung von

**Geldbußen (Verwaltungsstrafen)** „zusätzlich zu oder anstelle“ von Abhilfemaßnahmen.

## Adressat der Geldbußen?

- *In Abweichung zum VStG* ist die **unmittelbare Strafbarkeit der juristischen Person** vorgesehen, ohne dass es eines verantwortlichen Beauftragten nach § 9 VStG bedarf (§ 30 DSGVO), wenn der Verstoß durch **(i)** eine *Führungsperson* begangen oder durch **(ii)** *mangelnde Überwachung oder Kontrolle* ermöglicht wurde.
- „Die Datenschutzbehörde **hat** von der Bestrafung eines Verantwortlichen [] **abzusehen**, wenn für denselben Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person verhängt wird.“  
(Keine Doppelbestrafung der juristischen und natürlichen Personen; kein Ermessen (?); § 30 Abs 3 DSGVO)

## Bemessung der Geldbußen

- **Zwei Kategorien von Verstößen:**
- Bis zu 20 000 000 EUR *oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist: Grundprinzipien der DSGVO, Unzulässig Verarbeitung, Rechte von betroffenen Personen, Nichtbefolgung einer Anweisung, Beschränkung oder eines Verbots der DSB*
- Bis zu 10 000 000 EUR *oder im Fall eines Unternehmens von bis zu 2 % seines [...] Jahresumsatzes: Keine Vereinbarung mit dem Auftragsverarbeiter, Verarbeitungsverzeichnis, DSFA...*

## Zulässigkeit der Verhängung hoher Geldstrafen durch Verwaltungsbehörden?

- Hohe Geldstrafen dürfen (auch) von Verwaltungsbehörden verhängt werden, **da im Rahmen der Überprüfung durch die Verwaltungsgerichtsbarkeit die notwendigen verfahrensrechtlichen und grundrechtlichen Garantien gegeben sind.**
- Die Judikatur zum Kernbereich der Strafgerichtsbarkeit wurde nicht aufrecht erhalten (VfGH 13.12.2017, G 408/2016, Dako 2018/10 [*Schweiger*])

## Top 5 in der EU und erste Praxiserfahrung aus Österreich

Staat	Verantwortliche	Höhe (EUR)	Verstoß
UK	British Airways	204.600.000	Unzureichende TOM (Art 32 DSGVO, data breach, Cyber-Vorfall)
UK	Marriott International, Inc	110.390.200	Unzureichende TOM (Art 32 DSGVO, data breach, Cyber-Vorfall)
FR	Google Inc.	50.000.000	Diverses (Art 4, 5f u Art 13f DSGVO; mangelnde Transparenz, unzureichende Information und mangelhafte Einwilligung zur Personalisierung von Werbeanzeigen)
AT	Österreichische Post	18.000.000	<b>Unzureichende Rechtsgrundlage für die Datenverarbeitung (Art 5 Abs 1 lit a u Art 6 u 9 DSGVO; [vermeintliche] Parteiaffinität; nicht rechtskräftig)</b>
DE (Berlin)	Deutsche Wohnen SE	14.500.000	Nichteinhaltung der Grundsätze für die Verarbeitung personenbezogener Daten (Art 5 u Art 25 DSGVO; Speicherbegrenzung, Datenminimierung)

<https://www.enforcementtracker.com/?insights>

Staat	Verantwortliche	Höhe (EUR)	Verstoß
AT	Allergie-Tagesklinik	<b>50.000</b>	Bestellung des Datenschutzbeauftragten, gesetzwidrige Einwilligung, Informationspflichten, Schwellenanalyse für DSFA; DSB-D213.692/0001-DSB/2018 vom 16.11.2018; Art 37 ff, Art 6 & Art 9, Art 12ff, Art 32 u Art 35f DSGVO.
AT	Fußballtrainer	<b>11.000</b>	Heimliche Nacktaufnahmen; 2019
AT	Berufsdetektiv	<b>6.700</b>	Verdeckte Videoüberwachung über einen Zeitraum von 15 Monaten; DSB-D550.025/0001-DSB/2019, Straferkenntnis vom 19.2.2019
AT	Wettlokal	<b>4.800</b>	Videoüberwachung Eingangsbereich; DSB-D550.038/0003-DSB/2018 vom 12.09.2018; Art 5 u Art 6 u Art 13 DSGVO § 50a DSG 2000 sowie (nunmehr) §§ 12f DSG.
AT	Privatperson	<b>2.200</b>	Videoüberwachung Mehrparteienwohnanlage; DSB-D550.037/0003-DSB/2018 vom 20.12.2018; Art 5 u Art 6 u Art 13 DSGVO § 50a DSG 2000 sowie (nunmehr) §§ 12f DSG.
AT	Betreiber eines Kebabstandes	<b>1.800</b>	Videoüberwachung; DSB- D550.048/0004-DSB/2018 vom 18.10.2018
AT	Privater Zulassungsbesitzer des Kraftfahrzeuges	<b>300</b>	Verwendung einer Dash-Cam; DSB-D550.084/0002-DSB/2018 vom 27.9.2018; Art 5 u Art 6 u Art 13 DSGVO § 50a DSG 2000 sowie (nunmehr) §§ 12f DSG.
AT	Nachbar	<b>Ermahnung</b>	Verwendung einer Übersichtskamera (zu großer Winkel zum Haus des Nachbarn); DSBD550.033/0004-DSB/2018 vom 13.11.2018

Vielen Dank für Ihre Aufmerksamkeit

Wir freuen uns auf die Diskussion



## Univ.-Ass. Mag. Žiga Škorjanc Univ.-Ass. Mag. Felix Zopf

- Institut für Innovation und Digitalisierung im Recht,  
Rechtswissenschaftliche Fakultät, Universität Wien  
A-1010 Wien

mail: [ziga.skorjanc@univie.ac.at](mailto:ziga.skorjanc@univie.ac.at)

mail: [felix.zopf@univie.ac.at](mailto:felix.zopf@univie.ac.at)

[www.univie.ac.at/id](http://www.univie.ac.at/id)

[www.linkedin.com/in/ziga-skorjanc](http://www.linkedin.com/in/ziga-skorjanc)

[www.linkedin.com/in/felix-zopf-48ba79156/](http://www.linkedin.com/in/felix-zopf-48ba79156/)