UNIVERSITÄT SALZBURG

Die neuen EU-Datenschutz-bestimmungen und ihre Auswirkungen für Ihr Unternehmen

20. März 2018, 5. April 2018

WIFI Salzburg

Univ.-Prof. Dr. Dietmar Jahnel
Universität Salzburg
Fachbereich Öffentliches Recht
Dietmar.Jahnel@sbg.ac.at

Datenschutz-Grundverordnung

- „Allgemeines Datenschutzrecht“
- In Kraft seit 24. Mai 2016
- Geltung ab 25. Mai 2018
- Unmittelbare Verbindlichkeit und Geltung in allen Mitgliedstaaten
- Viele Kompromisslösungen
  - über 3.000 (!) Änderungsanträge nach Entwurf
- Aber: zahlreiche „Öffnungsklauseln“
  - „hinkende Verordnung“
  - DSG (2018): BGBl 120/2017
- bis dahin: DSG 2000 / DS-RL

Datenschutz-Grundverordnung

- Ganzer Titel:
- VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 **zum Schutz natürlicher Personen** bei der Verarbeitung personenbezogener Daten, **zum freien Datenverkehr** und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

Überblick

- Anwendungsbereich
- Begriffsbestimmungen
- Zulässigkeit der Verarbeitung nicht-sensibler Daten, sensibler Daten, strafrechtlich relevanter Daten
- Auftragsverarbeitung
- Die neuen Pflichten des Verantwortlichen und des Auftragsverarbeiters
  - Verzeichnisführung
  - Datenschutz-Folgenabschätzung
  - Datenschutzbeauftragter
- Betroffenenrechte
- Datenübermittlung ins Ausland
- Data Breach Notification
- Besondere Datenverarbeitungen
- Sanktionen und Rechtsschutz
- Materieller und immaterieller Schadenersatz

Sanktionen

Art 24 DS-RL / § 52 DSG 2000	Art 83, 84 DS-GVO
- Verwaltungsstrafen bis zu 25.000 Euro	- Geldbuße bis zu **10 Mio** Euro / **20 Mio** Euro oder **2 %** / **4 %** des weltweiten Umsatzes durch Aufsichtsbehörde (Verhängung durch Gericht möglich) weitere Sanktionen-> § 69 DSG: Verwaltungsstraftatbestände

Drohende Sanktionen

- „leichte“ Verstöße nach Art 83 Abs 4 DS-GVO
- Geldbuße bis 10 Mio € oder bis 2 % des Jahresumsatzes
  - Einwilligung eines Kindes
  - Pflichten nach Art 25 – 39 DS-GVO:
    - ua **Verzeichnisführungspflicht**
    - **Datenschutz-Folgenabschätzung**
    - **Datenschutzbeauftragter**
  - Zertifizierung
  - Verhaltensregeln

Drohende Sanktionen

- „schwere“ Verstöße nach Art 83 Abs 5 DS-GVO
- Geldbuße bis 20 Mio € oder bis 4 % des Jahresumsatzes
  - **Grundsätze der Datenverarbeitung**
  - **Zulässigkeitsgründe**
  - **Betroffenenrechte**
  - Datenübermittlung in ein Drittland
  - Nichtbefolgung einer Anweisung der Aufsichtsbehörde

Drohende Sanktionen

- Maßnahmen nach Art 58 Abs 2 DS-GVO
  - Abhilfebefugnisse wie **Warnung, Verwarnung, Anweisung** durch Aufsichtsbehörde
- Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt
  - bei geringfügigen Verstößen: Verwarnung anstelle einer Geldbuße (lt ErwGr 148)

Räumlicher Anwendungsbereich

- Verarbeitung im Rahmen der Tätigkeit einer Niederlassung in der Union
- Nicht in der Union niedergelassene Verantwortliche
  - wenn Waren oder Dienstleistungen an Betroffene in der Union angeboten werden
  - das Verhalten Betroffener beobachtet wird, soweit ihr Verhalten in der Union erfolgt

Persönlicher Anwendungsbereich

§ 4 Z 1 DSG 2000 / Art 2 lit a DS-RL	Art 4 Z 1 DS-GVO
- personenbezogene Daten - bestimmt - bestimmbar - indirekt personenbezogene	- personenbezogene Daten - identifiziert - Identifizierbar (direkt oder indirekt) - pseudonymisierte Daten

Persönlicher Anwendungsbereich

§ 4 Z 1 DSG 2000 / ErwGr 24 DS-RL	Art 4 Z 1 DS-GVO
- Natürliche Personen - Juristische Personen	- Natürliche Personen - ~~Juristische Personen~~ - Nationales Grundrecht: § 1 DSG 2018

Grundrecht auf Datenschutz

- Art 8 GRC
  - „Jede Person“
  - Juristische Personen, soweit deren Name natürliche Personen bestimmt
    EuGH 09.11.2010, C-92/09 (Volker und Markus Schecke und Eifert)
  - VfGH: verfassungsgesetzlich gewährleistetes Recht

Personenbezogene Daten

- alle Informationen, die sich auf eine **identifizierte** oder **identifizierbare** natürliche Person (im Folgenden „betroffene Person“) beziehen
- als identifizierbar wird eine natürliche Person angesehen, die **direkt oder indirekt**, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann

Personenbezogene Daten

- Arten von Daten
- „Normale“ = nicht-sensible Daten
  - Dietmar Jahnel
- Sensible Daten
  - Xxx ist römisch-katholisch, yyy ist an Grippe erkrankt
- Strafrechtlich relevante Daten
  - Xxx wurde wegen Diebstahls verurteilt
- pseudonymisierte Daten
  - Ziffernkombination ohne verfügbarem Schlüssel:
  - 4444 01012015
- Anonyme Daten
  - 25 % der Bevölkerung zahlen keine Einkommensteuer

Personenbezug von IP-Adressen und Cookies

- Identifizierbarkeit
- EuGH 19.10.2016, C-582/14 (Breyer)
  - Dynamische IP-Adresse bezieht sich nicht auf eine bestimmte natürliche Person
  - Identifizierbarkeit:
    - Direkt oder indirekt
    - Alle Mittel, die vernünftigerweise eingesetzt werden können (DS-RL)
    - Alle Mittel, die nach allgemeinem Ermessen wahrscheinlich genützt werden (DS-GVO)
    - Rechtliche Möglichkeiten zur Beschaffung der nötigen Informationen vom Internetanbieter zB über Behörden → hat der BGH zu prüfen

Personenbezug von IP-Adressen und Cookies

- Keine pauschalen Antworten
- Identifizierbarkeit: im konkreten Fall zu prüfen
- Neuer Begriff der „Pseudonymisierung“

Begriffsbestimmungen der DS-GVO

- Auftraggeber –> Verantwortlicher
- Dienstleister –> Auftragsverarbeiter
- Datenverwendung –> Datenverarbeitung
- Zustimmung –> Einwilligung
- Zahlreiche neue Definitionen
- Aber auch: fehlende Definitionen

Verantwortlicher / Auftragsverarbeiter

- „**Verantwortlicher**“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet
- „**Auftragsverarbeiter**“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet

Verantwortlicher / Auftragsverarbeiter

- Beispiel **Facebook**:
  - Wer ist beim Posten von Daten dritter Personen auf Facebook für die Einhaltung der rechtlichen Bestimmungen verantwortlich?
  - Abhängig vom jeweiligen Profil werden auf Facebook Werbeeinschaltungen eingeblendet. Wer ist für diese Datenverwendung verantwortlich?
- Beispiel **Rechtsanwalt**:
  - Wer ist nach Erhebung einer Mahnklage für die Auskunftserteilung zuständig. Der Rechtsanwalt oder der Kläger?
- Beispiel „**Running-App**“:
  - Welche Rolle hat der Verwender bzw der Anbieter der App, der die Daten speichert?

Auftragsdatenverarbeitung

- Art 28 DS-GVO:
  - Auftragsdatenverarbeitungsvertrag:
    - Verarbeitung nur auf Weisung des Verantwortlichen
    - Verpflichtung zur Vertraulichkeit
    - Datensicherheitsmaßnahmen
    - Subauftragsverarbeiter nur mit Genehmigung
    - Unterstützung des Verantwortlichen bei Einhaltung seiner Pflichten (zB Betroffenenrechte)
    - bei Vertragsende Löschung oder Rückgabe
  - Bei Verstoß gegen die DS-GVO gilt der AV selbst als Verantwortlicher

Gemeinsame Verantwortliche

- Art 26 DS-GVO:
  - zwei oder mehr Verantwortliche legen gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest
  - Vereinbarung, wer von ihnen welche Verpflichtung nach der DS-GVO erfüllt
  - Die betroffene Person kann ihre Rechte bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen

Gesundheitsdaten

- personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheits-dienstleistungen, beziehen **und aus denen Informationen über deren Gesundheitszustand hervorgehen**
- ErwGr 35: Dazu gehören auch […] Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren
- **Sozialversicherungsnummer**?

Pflichten des Verantwortlichen

- Die (neuen) Pflichten nach der DS-GVO (I)
  - Verzeichnisführungspflicht
    - gilt auch für den Auftragsverarbeiter!
  - Datenschutz-Folgenabschätzung
  - Datenschutzbeauftragter
    - gilt auch für den Auftragsverarbeiter!
- Wegfall der Registrierungspflicht beim DVR
  - DVR bleibt bis Ende 2019 bestehen
    - neue Exportfunktion
  - Standardverarbeitungen fallen weg

Pflichten des Verantwortlichen

- Die (neuen) Pflichten nach der DS-GVO (II)
  - Privacy by design
  - Privacy by default
  - Datensicherheitsmaßnahmen
  - Data breach notification duty
  - Zulässigkeit der Datenverarbeitung
  - Wahrung der Betroffenenrechte

Zulässigkeitsprüfung

- Dürfen für die Abwicklung eines Kaufgeschäfts über einen Online-Shop die Daten des Kunden ohne Einwilligung gespeichert werden?
- Dürfen diese Daten für eigene Werbeaussendungen verwendet werden?
- Dürfen die Arbeitszeitaufzeichnungen der Mitarbeiter gespeichert werden?
- Wie sieht es mit Bewerbungsunterlagen aus?
- Sie bestellen ihre Kontaktlinsen bei einem Online-Shop. Da man Kontaktlinsen immer wieder benötigt, ist die Funktion „Bestellung wiederholen“ besonders praktisch. Ist sie auch datenschutzrechtlich zulässig?

Zulässigkeit der Verarbeitung nicht-sensibler Daten (Art 6)

a. Einwilligung
   - jederzeitiger Widerruf
   - Nachweispflicht
b. Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist
c. Erforderlich zur Erfüllung einer rechtlichen Verpflichtung
d. Lebenswichtige Interessen
e. Aufgabe im öffentlichen Interesse, die dem Verantwortlichen übertragen wurde
f. Interessenabwägung
   - Spielraum für Argumentation
   - Judikatur: EuGH 13.5.2014, C-131/12 (Google Spain und Google)

- Mindestens **eine** dieser Bedingungen

Sensible Daten?

- Rassische und ethnische Herkunft
- Politische Meinungen
- Religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Genetische Daten
- Biometrische Daten zur eindeutigen Identifizierung
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung

Zulässigkeit der Verarbeitung sensibler Daten (Art 9)

- Grundsätzliches Verbot
- keine Interessenabwägung
- keine Vertragserfüllung
- Ausnahmen
  - Ausdrückliche Einwilligung
  - Arbeitsrechtskontext
  - Lebenswichtige Interessen
  - Kirchen, bestimmte Vereine etc
  - Offensichtlich durch Betroffenen veröffentlicht
  - Geltendmachung von Rechtsansprüchen
  - Eigene Rechtsgrundlage
  - Gesundheitsvorsorge
  - Forschung, Statistik oder Archive

Zulässigkeit der Datenverarbeitung

- Bedingungen für eine Einwilligung (Art 7 DS-GVO)
  - Definition in Art 4 Z 11: im wesentlichen unverändert
    - freiwillig für den bestimmten Fall
    - Informiert
    - unmissverständliche Willenserklärung
    - Erklärung oder konkludent
  - Nachweispflicht für den Verantwortlichen
  - In verständlicher und leicht zugänglicher Form
  - Von anderen Sachverhalten klar zu unterscheiden
  - Jederzeitige Widerrufbarkeit
  - Kriterien für die Beurteilung der Freiwilligkeit

Einwilligung

- Einwilligung von Kindern (Art 8 DS-GVO):
  - Ab 16 Jahren (Herabsetzung bis 13 Jahre möglich)
    - § 4 Abs 4 DSG (2018): **14 Jahre**
  - (nur) Dienste der Informationsgesellschaft
    - gegen Entgelt elektronisch im Fernabsatz erbrachte Dienstleistung
  - Unter der Altersgrenze: nur mit Einwilligung oder Autorisierung der Eltern (-> englische Sprachfassung)
  - Nachprüfungspflicht des Verantwortlichen: „unter Berücksichtigung der verfügbaren Technik“
  - Allgemeines Vertragsrecht bleibt unberührt

Zulässigkeit der Datenverarbeitung

- Grundsätze der Datenverarbeitung (Art 5)
  - Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
  - Zweckbindung
  - Datenminimierung
  - Richtigkeit
  - Speicherbegrenzung
  - Integrität und Vertraulichkeit
  - **Rechenschaftspflicht**

Zulässigkeit der Datenverarbeitung

- Datenverarbeitung zu einem anderen Zweck
  - Zulässigkeit bei
    - Einwilligung
    - bestehender Rechtsgrundlage
  - Kompatibilitätstest (Art 6 Abs 4)
    - Verbindung zwischen den Zwecken
    - Zusammenhang der Datenerhebung
    - Folgen der Weiterverwendung
    - Verschlüsselung oder Pseudonymisierung

Zulässigkeit der Verarbeitung strafrechtsbezogener Daten (Art 10)

- Strafrechtliche Verurteilungen
- Straftaten
- Konkreter Verdacht? (DS-GVO)
- Behördliche Aufsicht
- Eigene Rechtsgrundlage
  - § 4 Abs 3 DSG 2018
  - gesetzliche Ermächtigung oder Verpflichtung
  - gesetzliche Sorgfaltspflichten
  - Interessenabwägung

Zulässigkeitsprüfung - Antworten

- Dürfen für die Abwicklung eines Kaufgeschäfts über einen Online-Shop die Daten des Kunden ohne Einwilligung gespeichert werden?
- Dürfen diese Daten für eigene Werbeaussendungen verwendet werden?
- Dürfen die Arbeitszeitaufzeichnungen der Mitarbeiter gespeichert werden?
- Wie sieht es mit Bewerbungsunterlagen aus?
- Sie bestellen ihre Kontaktlinsen bei einem Online-Shop. Da man Kontaktlinsen immer wieder benötigt, ist die Funktion „Bestellung wiederholen“ besonders praktisch. Ist sie auch datenschutzrechtlich zulässig?

Datenübermittlung an (in) Drittländer

- Art 44 bis 50 DS-GVO:
  - Angemessenheitsbeschluss der Kommission
    - keine Genehmigung notwendig
    - Liste im Amtsblatt und Website
    - Aktueller Stand:
    - Schweiz, Argentinien, Guernsey, Insel Man, Jersey, Färöer Inseln, Andorra, Uruguay, Neuseeland, Kanada, Israel.
    - USA: EU-US-Datenschutzschild (Nachfolge von „Safe Harbor“)
    - USA: PNR-Abkommen (Fluggastdaten)

Datenübermittlung an (in) Drittländer

- Art 44 bis 50 DS-GVO:
  - Angemessene Garantien
    - keine Genehmigung notwendig
    - Standardvertragsklauseln
    - Genehmigte verbindliche interne Datenschutzvorschriften („Binding Corporate Rules“)
    - Ausnahmen in Art 49
      - ua Vertragserfüllung
      - Interessenabwägung und geeignet Garantien
      - Mitteilung an DSB
      - Kein Genehmigungsverfahren

Transparenz der Datenverarbeitung

Art 18 DS-RL / § § 17 ff DSG 2000	Art 30, 35, 37 ff DS-GVO
- Meldung beim Datenverarbeitungs-register	- Verzeichnis von Verarbeitungstätigkeiten - Datenschutz-Folgenabschätzung - Datenschutzbeauftragter

Publizität der Datenverarbeitungen

- Aktuelle Rechtslage
- Datenverarbeitungsregister (DVR) (§ 17 ff)
  - Grundsätzlich Meldepflicht
  - Ausnahmen: Nicht-meldepflichtige Datenanwendungen
    - Standardanwendungen
  - Vereinfachte Meldung
    - Musteranwendungen
- Vorabkontrolle durch die DSB (§ 18 Abs 2)
  - Sensible, strafrechtsrelevante Daten
  - Informationsverbundsystem, Bonitätsdaten
- Online-Meldung seit September 2012
  - www.dsb.gv.at

Standardanwendungen

- Standard- und Musterverordnung 2004
- Für den privaten Bereich:
  - SA001 Rechnungswesen und Logistik
  - SA002 Personalverwaltung für privatrechtliche Dienstverhältnisse
  - SA022 Kundenbetreuung und Marketing für eigene Zwecke
  - SA032 Videoüberwachung
  - SA033 Datenübermittlung im Konzern

Verzeichnisführungspflicht

- Art 30 DS-GVO
  - Namen und Kontaktdaten des Verantwortlichen
  - die **Zwecke** der Verarbeitung
  - eine Beschreibung der Kategorien betroffener Personen und der **Kategorien personenbezogener Daten**
  - die Kategorien von **Empfängern** einschließlich Empfänger in Drittländern
  - wenn möglich, die vorgesehenen **Fristen für die Löschung** der verschiedenen Datenkategorien
  - wenn möglich, eine allgemeine Beschreibung der **Datensicherheitsmaßnahmen**

Verzeichnisführungspflicht

- Art 30 Abs 2 DS-GVO: Auftragsverarbeiter
  - Namen und Kontaktdaten des Auftragsverarbeiters
  - die **Kategorien** von Verarbeitungen
  - ggf Übermittlungen in ein Drittland
  - wenn möglich, eine allgemeine Beschreibung der Datensicherheitsmaßnahmen

Verzeichnisführungspflicht

- Die „**Ausnahme**“ nach Art 30 Abs 5 DS-GVO
  - ErwGr 13: *Um der besonderen Situation der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen Rechnung zu tragen, enthält diese Verordnung eine abweichende Regelung hinsichtlich des Führens eines Verzeichnisses für Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen*
  - Ausnahme für Unternehmen mit weniger als 250 Mitarbeitern
  - Gegenausnahme („es sei denn“):
    - risikoreiche Verarbeitung, (= ODER)
    - **nicht nur gelegentliche Verarbeitung** ODER
    - sensible Daten oder strafrechtsbezogene Daten
  - **Vorsicht Falle!**

Datenschutz-Folgenabschätzung

- Art 35 DS-GVO
  - systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf **automatisierte Verarbeitung** einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen
  - Umfangreiche Verarbeitung von **sensiblen Daten** oder Strafrechtsdaten
  - systematische umfangreiche **Überwachung öffentlich zugänglicher Bereiche**
  - Positivliste durch Aufsichtsbehörde verpflichtend
    - Verordnungserlassung durch DSB
  - Negativliste fakultativ

Datenschutz-Folgenabschätzung

- Begriff „**umfangreich**“: ErwGr 91
  - Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein.

Datenschutz-Folgenabschätzung

- **Inhalt**: Art 35 Abs 7 DS-GVO
  - Beschreibung des Verarbeitungsvorgangs und der Zwecke
  - Bewertung der Notwendigkeit und Verhältnismäßigkeit
  - Risikobewertung für die Betroffenen
  - Abhilfemaßnahmen zur Bewältigung der Risiken
- Bei hohem Risiko Konsultation der Aufsichtsbehörde

Datenschutzbeauftragter

- Art 37 ff DS-GVO
  - Keine allgemeine Bestellungspflicht
  - Verpflichtend:
    - Verarbeitung von einer **Behörde** oder öffentlichen Stelle
    - Kerntätigkeit – **umfangreiche, regelmäßige und systematische Überwachung** von Betroffenen
    - Kerntätigkeit – **umfangreiche Verarbeitung sensibler** oder strafrechtlich relevanter Daten
  - freiwillige Bestellung ist möglich
  - Interner oder externer DBA möglich
  - (weitere Fälle nach nationalem Recht möglich)

Datenschutzbeauftragter

- Art 37 ff DS-GVO
  - Kerntätigkeit: ErwGr 97
    - Im privaten Sektor bezieht sich die Kerntätigkeit eines Verantwortlichen auf seine Haupttätigkeiten und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit.
  - „datengetriebenes Geschäftsmodell“?
  - Krankenanstalt erfüllt den Begriff „Kerntätigkeit“
  - nicht: unterstützende Tätigkeiten wie Lohnzahlung oder IT-Support

Datenschutzbeauftragter

- Art 37 ff DS-GVO
  - Begriff „**umfangreich**“: Beispiele (va der Art 29-Datenschutzgruppe):
  - Patientendaten eines Krankenhauses
  - Kundendatenverarbeitung von Versicherungen und Banken
    - Bei Versicherungen: regulärere Betrieb oder Profilbildung notwendig?
  - behavioural advertising durch eine Suchmaschine
  - Datenverarbeitung durch Telefon- oder Internet-Service-Provider
  - Kreditauskunftei mit Scoring
  - Cloud-Anbieter
  - Smart-Car-Anbieter, Smart Meter-Anbieter
  - Betreiber von Social Media-Plattformen
  - Betreiber von Bewertungs- und Vergleichsplattformen

Datenschutzbeauftragter

- Aufgaben: (Art 39 DS-GVO):
  - Unterrichtung und Beratung des Verantwortlichen
  - Überwachung der Einhaltung der Datenschutzvorschriften
  - Beratung bei Datenschutz-Folgenabschätzung
  - Zusammenarbeit mit der Aufsichtsbehörde
  - Anlaufstelle für die Aufsichtsbehörde
- **keine** Verantwortlichkeit nach § 9 VStG!

Datenschutzbeauftragter

- **Voraussetzungen** (Art 37 Abs 5 DS-GVO):
  - Benennung durch den Verantwortlichen
  - Aufgrund der beruflichen Qualifikationen UND
  - Insbesondere des Fachwissens
    - auf dem Gebiet des Datenschutzrechts
    - auf dem Gebiet der Datenschutzpraxis SOWIE
  - Aufgrund der Fähigkeit zur Erfüllung der in Art 39 genannten Aufgaben

Datenschutzbeauftragter

- **Voraussetzungen** (Art 29-Datenschutzgruppe):
  - Expertenwissen im Datenschutzrecht
  - Verständnis der konkreten Datenverarbeitungen
  - Verständnis über IT-Techonlogie und Datensicherheit
  - Wissen über den Wirtschaftssektor und die Organisation
  - Fähigkeit, eine Datenschutzkultur in der Organisation zu etablieren
  - Kontaktdaten: Veröffentlichung und Mitteilung an die Aufsichtsbehörde
    - Name ist nicht angeführt
  - Vorsicht mit sog „**Zertifizierungen**“

Data breach notification duty

- Art 33 und 34 DS-GVO
  - Verletzung des Schutzes personenbezogener Daten
    - Definition in Art 4 Z 12: eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden

Data breach notification duty

- Art 33 und 34 DS-GVO
  - Verletzung des Schutzes personenbezogener Daten
  - Meldung an die **Aufsichtsbehörde**
  - Binnen 72 Stunden
  - Dokumentationspflicht
  - Benachrichtigung der Betroffenen
    - bei hohem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen
    - Ausnahmen (alternativ)
      - Geeignete Sicherheitsvorkehrungen
      - Nachfolgende Maßnahmen zur Risikominimierung
      - Unverhältnismäßiger Aufwand -> öffentliche Bekanntmachung

Datensicherheit

- Art 32 DS-GVO
  - Stand der Technik
  - Schwere des Risikos
    - Skala der Schutzwürdigkeit
  - Geeignete technische und organisatorische Maßnahmen
    - Pseudonymisierung
    - …
  - „angemessenes Schutzniveau“
    - Risiko

„Risiko“

- ErwGr 75:
  - insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann
  - wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren

„Risiko“

- ErwGr 75:
  - wenn sensible Daten oder strafrechtlich relevante Daten verarbeitet werden
  - wenn persönliche Aspekte bewertet werden (Profiling)
  - wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder
  - wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft

„Hohes Risiko“

- Art 70 Abs 1 lit h (Europ. Datenschutzausschuss)
  - Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe e des vorliegenden Absatzes zu den Umständen, unter denen eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen im Sinne des Artikels 34 Absatz 1 zur Folge hat

Datensicherheit

- Organisatorische Maßnahmen:
  - Festlegung der Aufgabeverteilung
  - Zweckwidmung der Daten für die Auftragsabwicklung
  - Beschränkung der Zugriffsrechte
  - Richtlinien für Passwörter
  - Richtlinien für E-Mail-Nutzung
  - Vorgaben BYOD
  - Protokollierung von Änderungen, Abfrage und Übermittlungen
  - Geeignete Backupstrategie
  - Überprüfung der Einhaltung der Vorgaben
  - Dokumentationspflicht

Betroffenenrechte

- Informationspflicht
- Auskunftsrecht
- Recht auf Berichtigung
- Recht auf Löschung
- Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht
- Wie bisher mit einigen Erweiterungen
  - Beim Design von IT-Systemen berücksichtigen!

Informationspflicht

- Art 13: Datenerhebung bei der betroffenen Person
- Ausnahme: „wenn und soweit die betroffene Person bereits über die Informationen verfügt“
- Zum Zeitpunkt der Erhebung
- **Inhalt**
  - Name und Kontaktdaten des Verantwortlichen
  - Kontaktdaten des Datenschutzbeauftragten
  - Zweck und Rechtsgrundlage
  - Berechtigte Interessen bei Interessenabwägung
  - Empfänger oder Kategorien von Empfängern
  - Absicht einer Drittlandsübermittlung
  - Speicherdauer bzw Kriterien für die Festlegung dieser
  - Bestehen eines Rechts auf Auskunft, Löschung etc
  - Bestehen eines Widerrufsrechts bei Einwilligung
  - Bestehen eines Beschwerderechts
  - .....

Informationspflicht

- Art 14: Datenerhebung nicht bei der betroffenen Person
  - Übermittlung, Erhebung aus öffentlichen Quellen
- Ausnahmen:
  - „wenn und soweit die betroffene Person bereits über die Informationen verfügt“
  - Unmöglichkeit oder unverhältnismäßiger Aufwand
  - Regelung in Rechtsvorschriften
  - Daten unterliegen einem Berufsgeheimnis
- Zeitpunkt:
  - Spätestens 1 Monat nach Erlangung der Daten
  - Erste Mitteilung bei Kommunikation
- **Inhalt**
  - Wie bei Art 13 +
  - Die Kategorien der verarbeiteten Daten
  - Aus welcher Quelle (ev öffentlich zugänglichen) die Daten stammen

Informationspflicht

- Art 12: Art der Information
  - in präziser, transparenter, verständlicher und leicht zugänglicher Form
  - in einer klaren und einfachen Sprache
  - schriftlich
  - gegebenfalls auch elektronisch
  - unentgeltlich
  - standardisierte Bildsymbole
    - In delegierten Rechtsakten durch Kommission

Informationspflicht

SYMBOL	WESENTLICHE INFORMATIONEN	ERFÜLLT
	Es werden nicht mehr personenbezogene Daten **erhoben**, als für die spezifischen Zwecke der Verarbeitung erforderlich sind.	
	Es werden nicht mehr personenbezogene Daten **gespeichert**, als für die spezifischen Zwecke der Verarbeitung erforderlich sind.	
	Personenbezogene Daten werden nicht zu anderen als den Zwecken **verarbeitet**, für die sie erhoben wurden.	
	Es werden keine personenbezogenen Daten an gewerbliche Dritte **weitergegeben**.	
	Es werden keine personenbezogenen Daten **verkauft oder verpachtet**.	
	Es werden keine personenbezogenen Daten **unverschlüsselt** aufbewahrt.	

vorgeschlagene Symbole…

Auskunftsrecht

- Art 15 DS-GVO
  - Auskunft über die Daten
  - Verarbeitungszwecke
  - Datenkategorien
  - Empfänger von Offenlegungen
  - **Speicherdauer** (falls möglich)
  - Bestehen eines Rechts auf Berichtigung oder Löschung
  - Bestehen eines Beschwerderechts
  - Verfügbare Informationen über die Herkunft
  - Allenfalls: automatische Entscheidungsfindung oder Profiling

Auskunftsrecht

- **Auskunftserteilung**
  - Identitätsnachweis nur mehr bei begründeten Zweifeln (Art 12 Abs 6)
  - unverzüglich innerhalb von 1 Monat
  - Mitwirkungspflicht ?
  - Fristerstreckung möglich (Art 12 Abs 3)
  - Kopie der Daten
  - elektronisches Format
  - unentgeltlich (Art 12 Abs 5)
  - angemessenes Entgelt für weitere Kopien

Löschungsrecht

- Art 17 DS-GVO
  - „Recht auf Vergessenwerden“?
  - unverzüglich
  - nicht mehr für die Zwecke der Verarbeitung notwendig
  - Widerruf der Einwilligung und keine andere Rechtsgrundlage
  - Einlegen von Widerspruch
  - Verarbeitung ist unrechtmäßig
  - Löschung ergibt sich aus rechtlichen Pflichten
  - kein „absolutes“ Löschungsrecht!

Recht auf Datenübertragbarkeit

- Art 20 DS-GVO
  - Neues Betroffenenrecht
  - Daten, die die betroffene Person einem Verantwortlichen bereitgestellt hat
  - Strukturiertes, gängiges, maschinenlesbarer Format
  - Cloud-provider
  - Verpflichtung nicht für Auftragsverarbeiter

Widerspruchsrecht

- Art 21 DS-GVO
  - aus Gründen, die sich aus ihrer besonderen Situation ergeben
  - Nur bei Verarbeitungen im öffentlichen Interesse oder aufgrund einer Interessenabwägung
  - Beweislast beim Verantwortlichen
  - bei Direktwerbung jederzeit
  - Hinweispflicht

Besondere Datenverarbeitungen

- Datenverarbeitung zu privaten Zwecken
  - § 45 DSG 2000 -> keine Anwendbarkeit der DS-GVO
- Wissenschaftliche Forschung und Statistik
  - § 46 DSG 2000 -> § 25 DSG 2018
- Zurverfügungstellung von Adressen
  - § 47 DSG 2000 -> § 26 DSG 2018
- Katastrophenfall
  - § 48 DSG 2000 -> § 28 DSG 2018

Datenverarbeitung im Beschäftigungskontext

- § 11 DSG 2018:
  - ArbVG ist eine spezifische Vorschrift iSd Art 88 DS-GVO
  - Die Befugnisse des Betriebsrats bleiben unberührt
- § 6 DSG 2018
  - Datengeheimnis (wie in § 15 DSG 2000)

„Medienprivileg“

- § 9 DSG 2018
  - Für journalistische, wissenschaftliche, künstlerische oder literarische Zwecke
  - Weitgehende Ausnahmen von der DS-GVO
  - Vom DSG 2018 anwendbar:
    - § 6 (Datengeheimnis)
    - § 1 (Grundrecht auf Datenschutz)
  - Bisher: § 48 DSG 2000
    - Ausnahmen für Medienunternehmen und Mediendienste

Bildverarbeitung

- § § 12 und 13 DSG 2018:
- Bildaufnahme
  - „die durch Verwendung technischer Einrichtungen zur Bildverarbeitung vorgenommene Feststellung von Ereignissen im öffentlichen oder nicht-öffentlichen Raum **zu privaten Zwecken**“
- Erläuterungen:
  - „durch Verantwortliche im privaten Bereich“
  - Besser: nicht hoheitlich

Bildverarbeitung

- Zulässigkeit der Bildaufnahme und Übermittlung:
  - Lebenswichtiges Interesse
  - Einwilligung
  - Besondere gesetzliche Bestimmungen
  - Interessenabwägung im Einzelfall
    - Vorbeugender Schutz auf privaten Liegenschaften
    - Vorbeugender Schutz an öffentlich zugänglichen Orten mit Hausrecht
    - Privates Dokumentationsinteresse, das nicht auf die identifizierende Erfassung unbeteiligter Personen gerichtet ist (gemeint sind Freizeitkameras uÄ)

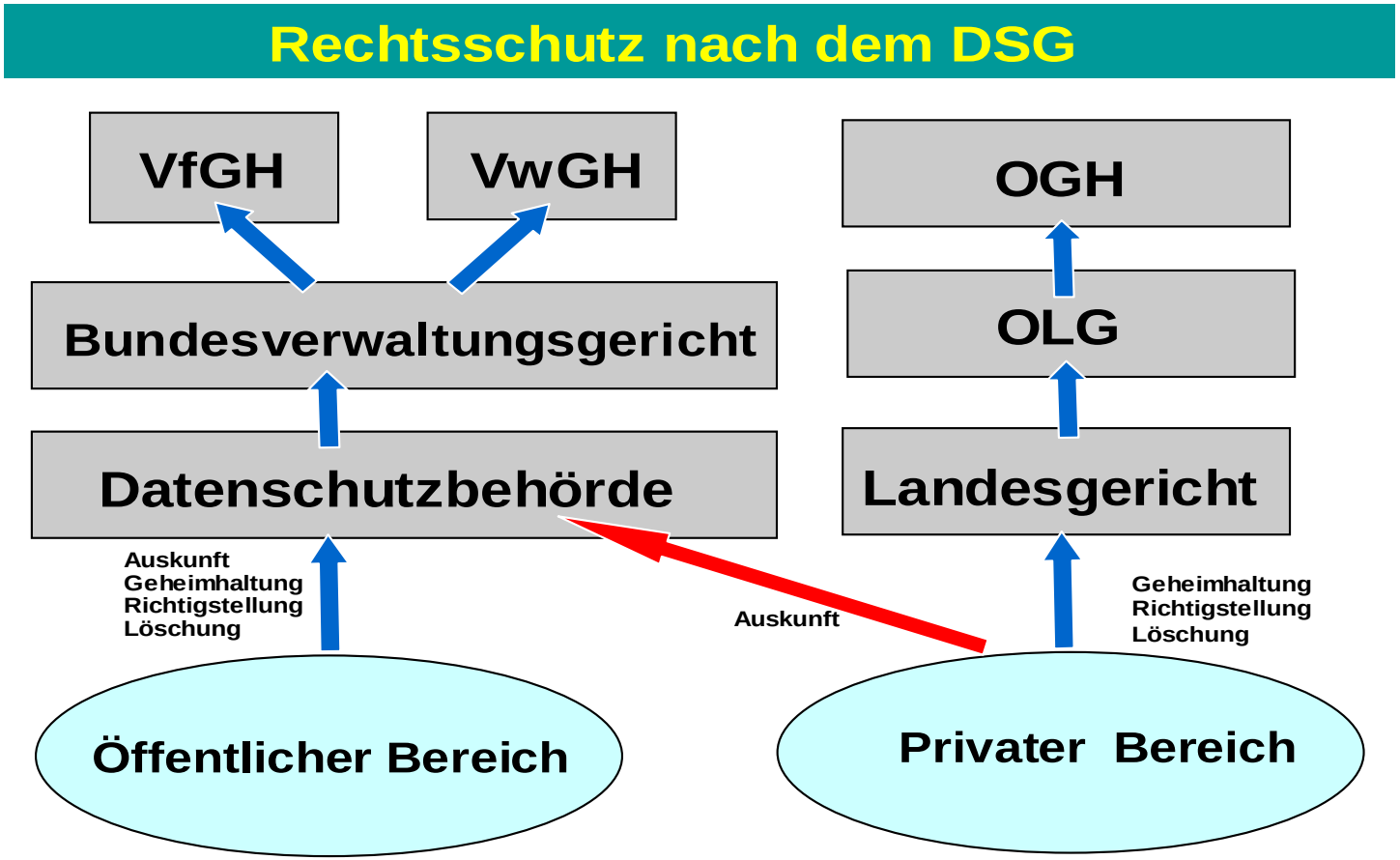
Bildverarbeitung

- Absolute Unzulässigkeit:
  - Höchstpersönlicher Lebensbereich ohne Einwilligung
  - Arbeitnehmerkontrolle
  - Automationsunterstützter Abgleich
  - Auswertung anhand von sensiblen Daten

Bildverarbeitung

- Löschungspflicht
  - 72 Stunden
  - Längere Aufbewahrung ist zu protokollieren und zu begründen
- Kennzeichnungspflicht
  - Verantwortlicher muss daraus hervorgehen

Rechtsschutz im DSG



Öffentlicher / privater Bereich

- Öffentlicher Bereich (§ 5 / § 15 DSG 2018)
  - Einrichtung in Formen des öffentlichen Rechts
    - Bund, Länder, BVB, LH, Sozialversicherungs-träger, Kammern + zB Beliehene
- Privater Bereich
  - Einrichtung in Formen des Privatrechts
    - Einzelunternehmer, OG, KG, GmbH
- Unterschied: Rechtsschutz
- § 5 Abs 4 DSG 2000

Rechtsschutz

Art 22 DS-RL / § § 30 ff DSG 2000	Art 77 - 79 DS-GVO
- Beschwerde an DSB - Gerichtliche Zuständigkeit	- Beschwerde an DSB mit gerichtlichem Rechtsbehelf dagegen - Wirksamer gerichtlicher Rechtsbehelf „unbeschadet des Rechts auf Beschwerde“

Beschwerde an die DSB

- Art 77 DS-GVO:
  - „Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs **das Recht auf Beschwerde bei einer Aufsichtsbehörde**, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, *dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt.*“

Beschwerde an die DSB

- Beschwerde an die DSB
  - Art 77 DS-GVO iVm § 13 DSG 2018
  - Gegen Verantwortliche des privaten und öffentlichen Bereichs (§ 15 DSG 2018)
  - Keine Einschränkung auf Verletzung des Auskunftsrecht im privaten Bereich
- Beschwerde an das Bundesverwaltungsgericht
  - Parteistellung für Verantwortliche des öffentlichen Bereichs
- VwGH bzw VfGH
  - Nach den allgemeinen Regeln über Revision bzw Beschwerde

Gerichtlicher Rechtsbehelf

- Art 79 DS-GVO:
  - „Jede betroffene Person hat unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Artikel 77 **das Recht auf einen wirksamen gerichtlichen Rechtsbehelf**, wenn sie der Ansicht ist, *dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.*“

Gerichtlicher Rechtsbehelf

- Klage an das nationale Gericht
  - Art 79 DS-GVO
  - „unbeschadet“ des Beschwerderechts bei der Aufsichtsbehörde
  - Neben der Beschwerde / parallel??
  - ErwGr 141:
    - Jede betroffene Person sollte das Recht haben, bei einer einzigen Aufsichtsbehörde insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthalts eine Beschwerde einzureichen **und** gemäß Artikel 47 der Charta einen wirksamen gerichtlichen Rechtsbehelf einzulegen, wenn sie sich in ihren Rechten gemäß dieser Verordnung verletzt sieht …

Gerichtlicher Rechtsbehelf

- Klage an das nationale Gericht
  - Erläuterungen zu § 69 DSG 2018:
    - „Neue Klagen können bei den ordentlichen Gerichten (§ 5 Abs. 4 DSG 2000) ab dem 25. Mai 2018 daher generell nicht mehr eingebracht werden; stattdessen ist der Antrag an die Datenschutzbehörde zu richten.“

Schadenersatzrecht (§ 33 DSG 2000)

- Immaterieller Schadenersatz
  - öffentlich zugängliche Verwendung
  - in § 18 Abs 2 Z 1 bis 3 genannte Datenarten
    - Sensible Daten
    - Strafrechtlich relevante Daten
    - Bonitätsdaten
  - Bloßstellung gemäß § 7 Abs 1 Mediengesetz

Schadenersatzrecht

- Schadenersatz (Art 82 DS-GVO / § 29 DSG 2018)
  - Materieller Schaden
  - Immaterieller Schaden
    - Wegfall der Einschränkungen des § 33 DSG 2000
    - **in allen Fällen einer Datenschutzverletzung!**
- Zuständigkeit
  - Landesgericht
  - Gewöhnlicher Aufenthalt des Klägers oder des Beklagten

Zusammenfassung

- Neu:
  - Verzeichnisführungspflicht statt Registrierung
  - (Datenschutz-Folgenabschätzung)
  - Datenschutzbeauftragter
- wie bisher mit Weiterentwicklungen und Erweiterungen:
  - Zulässigkeitsgründe für die Verarbeitung
  - Datensicherheitsmaßnahmen
  - Wahrung der Betroffenenrechte
- Neu:
  - hohe Geldbußen bei Nichtbeachtung möglich
  - Immaterieller Schadenersatz

„Fahrplan“ DS-GVO

- Vorhandene Datenverarbeitungen erfassen und analysieren
  - Zwecke feststellen
  - Rechtfertigungsgründe prüfen
- Informationspflicht erfüllen
  - Online: Datenschutzerklärung
  - Offline: Informationsblatt
- Verarbeitungsverzeichnis anlegen
- Vorbereitung auf Betroffenenrechte
  - Auskunftsrecht
  - Löschungsrecht
- …..

Literaturempfehlungen

Bergauer/Jahnel, Das neue Datenschutzrecht (Jan Sramek Verlag)

- DS-GVO und Erwägungsgründe
- DSG und Erläuterungen
- Judikatur in Leitsätzen
- 2. Auflage

Feiler/Horn, Umsetzung der DSGVO in der Praxis (Verlag Österreich)

- Fragen, Antworten, Muster
- erschienen

Zeitschriften

Dako – Datenschutz konkret (Verlag Manz)

- Kurzbeiträge

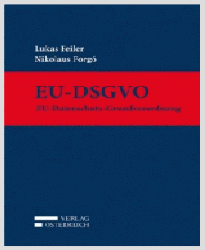
jusIT (Verlag LexisNexis)

- Aufsatzserie: DS-GVO ante portas

Jahrbuch Datenschutzrecht

- fundierte, längere Beiträge

Kommentare



Feiler/Forgó, EU-DSGVO (Verlag Österreich)

- erschienen

Gantschacher/Jelinek/Schmidl/Spanberger, Kommentar zur Datenschutz-Grundverordnung (SFU Verlag Wien)

- erschienen

Jahnel/Bergauer, DS-GVO und DSG (Jan Sramek Verlag)

- erscheint Herbst 2018

Datenschutzrecht in Online-Datenbanken

- Zeitschrift Dako im Volltext
- Jahrbuch Datenschutzrecht im Volltext ab 2010
- Textausgabe DSGVO
- *Dohr/Pollirer/Weiss/Knyrim*, DSG-Kommentar

- Zeitschrift jusIT im Volltext
- Jahrbuch Datenschutzrecht im Volltext ab 2008
- *Jahnel/Bergauer*, DS-GVO und DSG-Kommentar
- BVwG und DSB-Entscheidungen mit Leitsätzen
- auch Beiträge in Zeitschriften (Dako) und Sammelwerken suchbar (Knyrim)

- Zeitschrift jusIT im Volltext
- Jahrbuch Datenschutzrecht im Volltext ab 2014

Online-Informationssystem

Bergauer/Jahnel (Hrsg), JURnet Modul Datenschutz (Verlag Österreich)

- elektronisches Informationssystem
- richtet sich an alle „Datenschutzverantwortlichen“
- verfügbar seit Mitte September 2017
- www.jurnet.at

Datenschutzrecht

Danke fürs Zuhören!