Teil 2

Datenschutzrechtliche Fragestellungen

1. Datenschutzrechtliche Fragen (1)

Unter welchen Voraussetzungen ist ein Transfer von personenbezogenen Daten in Drittländer zulässig? Sind hiervon auch Cloud-Lösungen betroffen, wenn die Server nicht in der EU sind?

1. Datentransfer in Drittländer (2)

Herausforderung Outsourcing - Urteil Schrems II

- **EU-US Privacy Shield**
  - Angemessenheitsbeschluss der EU-Kommission
  - Regelte den Transfer von personenbezogenen Daten, die von der EU in die USA übertragen wurden
  - Mit **Urteil des EuGH vom 16.07.2020 (C-311/18 - „Schrems II“)** mit **sofortiger Wirkung für ungültig erklärt**
    - Datenschutzniveau der EU wurde nicht eingehalten
    - Übermittlung aufgrund **anderer geeigneter Garantien nach Art 46 ff DSGVO** möglich
    - Übermittlung auch unter **Einbeziehung der Standarddatenschutzklauseln** möglich

1. Datentransfer in Drittländer (3)

Herausforderung Outsourcing - Prüfpflichten

- Prüfpflichten des Verantwortlichen bei der Auswahl von Auftragsverarbeiter (Art 28 DSGVO)
- Auftragsverarbeiter müssen
  - mit hinreichend technischen und organisatorischen Maßnahmen garantieren, dass
  - Verarbeitung im Einklang mit Anforderungen des DSGVO und
  - Schutz der Rechte der betroffenen Person gewährleistet ist
- Verpflichtung für Cloud-Nutzer, sich über
  - die Einhaltung der DSGVO (**Datenschutzniveau**) und
  - die Sicherheitsbestimmungen (**Datensicherheit**)

  zu vergewissern.

1. Datentransfer in Drittländer (4)

Grundlage für zulässige Übermittlung

- Datenverarbeitung **im Inland muss den Vorgaben der DSGVO** entsprechen
- **Angemessenheitsbeschluss** gem. Art 45 DSGVO
- **Geeignete Garantien** iSd Art 46 DSGVO:
  - Verbindliche interne Vorschriften gem. Art 46 Abs 2 lit b DSGVO
  - Standarddatenschutzklauseln gem. Art 46 Abs 2 lit c und d DSGVO
  - Genehmigte Verhaltensregeln gem. Art 46 Abs 2 lit e DSGVO
  - Genehmigte Zertifizierungsmechanismen gem. Art 46 Abs 2 lit f DSGVO
  - Ad hoc Standarddatenschutzklauseln gem. Art 46 Abs 3 lit a DSGVO

1. Datentransfer in Drittländer (5)

Standarddatenschutzklauseln als geeignete Garantie

- **Durchführungsbeschluss der EU-Kommission** über **Standardvertragsklauseln** zwischen Verantwortlichen und Auftragsverarbeitern vom **04.06.2021**
  - Anforderungen des Schrems II Urteil wurden aufgenommen
  - Modularer Aufbau – alle vier Datenübertragungen wurden berücksichtigt
- Sind auf **neue Verträge ab dem 27.09.2021** anzuwenden
- **Übergangsfrist für Altverträge bis 27.12.2022**
  - **Zeitnahe Überprüfung der bestehenden Verträge empfehlenswert!**
- Downloadmöglichkeit auf der Homepage der Europäischen Kommission

1. Datentransfer in Drittländer (6)

Grundlage für zulässige Übermittlung

- Geeignete Garantien iSd Art 46 DSGVO gelten nicht uneingeschränkt!
- Datenexporteure haben
  - im **Einzelfall** und gegebenenfalls in **Zusammenarbeit mit dem Datenimporteur im Drittland zu prüfen, ob**
  - das Recht oder die Praxis des jeweiligen Drittlandes die Wirksamkeit der *„geeigneten Garantien“* iSd Art 46 DSGVO beeinträchtigt.
- Bei Beeinträchtigung sind **zusätzlich Sicherheitsgarantien** zu ergreifen bzw. zu implementieren, um Datenverarbeitung auf DSGVO-Niveau sicherzustellen!
  - EuGH lässt offen, welche Maßnahmen in einem solchen Fall zu ergreifen sind
  - Empfehlung des Europäischen Datenschutzausschusses vom 18.06.2021

2. Datenschutzrechtliche Fragen (1)

Im Zuge eines Löschungsbegehrens werden die personenbezogenen Daten durch Löschen des Datensatzes aus der Benutzeransicht entfernt. Der Administrator kann die Daten aber immer noch einsehen.

- **Handelt es sich hierbei um eine DSGVO-konforme Löschung?**
- **Haften IT-Dienstleister im Falle einer unvollständigen Löschung?**

2. Pflicht zur Löschung (2)

Allgemeines

- **Verantwortlicher** hat „*unverzüglich*“ zu löschen, wenn betroffene Person das beantragt (Löschungsbegehren)
  - **Verantwortlicher:**
    „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“ (Art 4 Z 7 DSGVO)
  - **Auftragsverarbeiter:**
    „eine natürliche oder juristische Person, Behörde, Einrichtung oder anderen Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“ (Art 4 Z 8 DSGVO)
- **Beispiel:** Der Unternehmer, der Kundendaten (von natürlichen Personen) zur Abrechnung der erbrachten Leistungen erfasst = Verantwortlicher. Die Buchhaltung des Unternehmers, welche die Rechnungsdaten erhält, ist Auftragsverarbeiter.

2. Pflichten des Auftragsverarbeiters (3)

Unterstützungspflichten

- Auftragsverarbeitung beruht regelmäßig auf **Vertrag zwischen Verantwortlichen und Auftragsverbeiter** (Schriftlichkeitsgebot!)
  - Verarbeitung personenbezogener Daten nur auf dokumentierte Weisung
- **Auftragsverarbeiter können auch Cloud-Dienste-Anbieter oder IT Datenwartungsanbieter sein**
- **Beispiel: Löschungsbegehren wird an Auftragsverarbeiter gerichtet**
  - keine ausdrückliche Pflicht zur Weiterleitung an Verantwortlichen
  - **Unterstützungspflicht** hinsichtlich Betroffenenrechte (Art 28 Abs 3 DSGVO)
  - **Unterstützungspflicht** hinsichtlich weiterer Pflichten (Art 28 Abs 3 DSGVO)
  - **Unverzügliche Weiterleitung an Verantwortlichen daher empfehlenswert!**

2. Haftung des Auftragsverarbeiters (4)

Schadenersatz & Bußgelder

- Anspruch auf Schadenersatz wenn Verstoß gegen DSGVO materiellen oder immateriellen Schaden verursacht (neben Sanktionen nach Art 83 DSGVO)
- Auftragsverarbeiter haftet bei **Verstoß gegen die ihn speziell treffenden Verpflichtungen**
  - Vernachlässigung von angemessenen und organisatorischen Maßnahmen (Art 32 DSGVO)
  - Missachtung der Anweisungen des Verantwortlichen
- Keine Haftung, wenn (nur) Verantwortlicher seine Pflichten verletzt
  - bei fehlender Rechtmäßigkeit der Verarbeitung
- Gesamtschuldnerische Haftung unter mehreren Auftragsverarbeitern möglich!
  - Regressmöglichkeit für den in Anspruch genommenen Auftragsverarbeiter (Art 82 Abs 5 DSGVO)

2. DSGVO-konforme Löschung (5)

Allgemeines

- Löschung von personenbezogenen Daten – **keine Definition!** (auch nicht in ErwGr)
- **Auswahlermessen** hinsichtlich Art & Weise der Löschung
- **Physische Löschung:**
  - Gespeicherte personenbezogene Daten werden unwiederbringlich zerstört bzw. unkenntlich gemacht -> irreversibel entfernt
  - Keine Rekonstruierung möglich (für durchschnittlichen Benutzer)
- **Logische Löschung:**
  - Zugriff auf Daten wird durch programmtechnische Maßnahmen verhindert
  - Nach Rspr. vor DSGVO: „Logisches Löschen“ nicht ausreichend (RIS Justiz RS0125838)
  - Kann Verantwortlicher auf die Daten zugreifen oder diese allenfalls rekonstruieren?

2. DSGVO-konforme Löschung (6)

Anonymisierung als Lösung?

- Anonymisierung als unumkehrbare Beseitigung des Personenbezugs
- Löschung setzt nicht zwingend eine endgültige Vernichtung voraus
- Entfernen des Personenbezuges **(„Anonymisierung“)** von personenbezogen Daten kann grundsätzlich ein **mögliches Mittel zur Löschung** iSv Art 4 Z 2 iVm Art 17 Abs 1 DSGVO sein. (DSB 05.12.2018 – DSB-D123.270/009-DSB/2018)
- Personenbezug darf weder für Verantwortlichen noch für einen Dritten ohne unverhältnismäßigen Aufwand wiederhergestellt werden können!
- Änderung der Datenorganisation – um lediglich „gezielten Zugriff“ zu vermeiden – ist nicht ausreichend! (RIS-Justiz RS0125838)
- *„Schwärzung“* – Unkenntlichmachung der personenbezogenen Daten – ausreichende Form der Löschung

3. Datenschutzrechtliche Fragen (1)

Das Design einer Software lässt eine völlige Löschung der personenbezogenen Daten nicht zu.

- **Muss das Design entsprechend abgeändert werden?**
- **Wer ist für die Änderung verantwortlich?**
- **Wer trägt die Kosten für eine nachträgliche DSGVO-konforme Adaptierung?**
- **Besteht seitens des IT-Dienstleisters eine Warnpflicht?**

3. DSGVO-Unvereinbarkeit als Mangel? (2)

Fragen der Gewährleistung

- Was war **Gegenstand der Vereinbarung**? Wurde darauf in der Vereinbarung Bedacht genommen?
- Zu welchem **Zeitpunkt wurde die Vereinbarung abgeschlossen**? Vor Inkrafttreten der DSGVO / nach Inkrafttreten der DSGVO? Macht das überhaupt einen Unterschied?
- Lässt die Software eine **Anonymisierung der Daten** (als mögliches Mittel der Löschung) zu?
- Wurde seitens des Kunden **rechtzeitig gerügt**?
- Ist die **Gewährleistungsfrist** bereits abgelaufen?

3. DSGVO-Unvereinbarkeit als Mangel? (3)

Warnpflicht bei Auftragsverarbeitung

- Ist der IT-Dienstleister auch Auftragsverarbeiter?
  - „Verkauf“ einer Software – auch einer Datenverarbeitungssoftware – ist keine Auftragsverarbeitung!
  - Bei Support oder Wartungsleistungen kann Auftragsverarbeitung vorliegen, wenn im Auftrag des Verantwortlichen personenbezogene Daten verarbeitet werden
- Besondere Warnpflicht für Auftragsverarbeiter (Art 33 Abs 2 DSGVO)
  - Dem Auftragsverarbeiter bekanntgewordene Verletzungen des Schutzes personenbezogener Daten sind unverzüglich dem Verantwortlichen zu melden.
  - Warnpflicht auch bei rechtswidrigen Anweisungen des Verantwortlichen!

3. DSGVO-Unvereinbarkeit als Mangel? (4)

Warnpflicht ohne Auftragsverarbeitung

- Softwareerstellungsvertrag als Werkvertrag
- Warnpflicht ableitbar aus den allgemeinen vor- oder nebenvertraglichen Schutz- und Aufklärungspflichten
- Erhöhter Sorgfaltsmaßstab eines Sachverständigen (§ 1299 ABGB)
- Haftung *ex contractu* bei schuldhafter Verletzung der Sorgfaltspflichten für Schäden des Werkbestellers denkbar
- Nachweisbare (schriftliche) Warnung daher jedenfalls empfehlenswert, um Haftung zu vermeiden!

4. Datenschutzrechtliche Fragen (1)

Kundenkreis Ärzte:

- **Gibt es Unterschiede hinsichtlich der datenschutzrechtlichen Vorgaben?**
- **Ist zu unterscheiden zwischen administrativer und medizinischer Kommunikation?**
- **Dürfen Patientendaten nach dem aktuellen Stand der Technik in eine EU-Cloudlösung ausgelagert werden?**

4. „Gesundheitsdaten“ nach der DSGVO (2)
besonderer Schutz?

- Besondere Kategorien personenbezogener Daten (Art 9 Abs 1 DSGVO)
  - Rassischer & ethische Herkunft
  - Politische Meinung
  - Religiöse oder weltanschauliche Überzeugung
  - Gewerkschaftszugehörigkeit
  - **Genetische Daten**
  - Biometrische Daten
  - **Gesundheitsdaten**
  - Daten zum Sexualleben oder der sexuellen Orientierung

4. „Gesundheitsdaten“ nach der DSGVO (3)
Allgemeines

- Gesundheitsdaten nach Art 9 Abs 1 DSGVO sind iSd Art 4 Z 15 DSGVO
  - „personenbezogene Daten, die sich auf die **körperliche oder geistige Gesundheit** einer **natürlichen Person**, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“
  - Informationen über Krankheiten, Behinderungen, Behandlungen oder physiologischem oder biomedizinischem Zustand der betroffenen Person – unabhängig von der Herkunft der Daten!
  - Geistige Gesundheit – maßgeblich nicht nur für Ärzte, sondern auch für Psychologen sowie Lebens- und Sozialberater
  - Begriff ist nicht weit auszulegen!
  - Auch Terminerinnerungen eines Arztes oder Protokolldaten sind hiervon erfasst

4. „Gesundheitsdaten“ nach der DSGVO (4)
Voraussetzungen für Verarbeitungen

(Einzelne) Erlaubnistatbestände des Art 9 Abs 2 DSGVO:

- Ausdrückliche Einwilligung (konkludente Einwilligung nicht ausreichend!)
  - Schriftlichkeit nicht erforderlich aber ratsam (z.B. Checkbox)
- Individuelle Versorgung im Gesundheits- und Sozialbereich (lit h)
  - gesundheitsbezogene Leistungen präventiver, diagnostischer, kurativer oder nachsorgender Natur
- Öffentliche Gesundheit (lit i)
  - Übermittlung von Gesundheitsdaten im Rahmen gesetzlicher Meldepflichten

4. Das Gesundheitstelematikgesetz (5)
Allgemeines

- Das GTelG 2012 als datenschutzrechtliche lex specialis
- Anwendungsbereich des Gesundheitstelematikgesetzes (GTelG 2012)
  - Verarbeitung (Art 4 Z 2 DSGVO) von
  - personenbezogenen elektronischen Gesundheitsdaten und genetischer Daten
  - durch Gesundheitsdiensteanbieter (iSd § 2 Z 2 GTelG 2012)
- Gesundheitsdiensteanbieter
  - Betriff ist weit auszulegen
  - Medizinproduktehersteller oder Ärzte und Notare können auch GDA sein
  - IT-Unternehmen, die im Auftrag eines GDA Gesundheitsdaten oder genetische Daten verarbeiten (weil sie Verrechnungs- oder Speicherdienstleistungen erbringen)

4. Das Gesundheitstelematikgesetz (6)

Voraussetzungen für die Übermittlung von Gesundheitsdaten

- Übermittlung zulässig nach § 9 DSVGO
- Identität der Personen, deren Daten übermittelt werden, nachgewiesen
- Identität der an Übermittlung beteiligten GDA nachgewiesen
- Rolle der an der Übermittlung beteiligten GDA nachgewiesen
- Vertraulichkeit der übermittelten Gesundheitsdaten gewährleistet
- Integrität der übermittelten Gesundheitsdaten gewährleistet

(§ 3 Abs 4 GTelG 2012)

4. Das Gesundheitstelematikgesetz (7)
Cloud Computing

- Sonderregelung für Vertraulichkeit iZm Cloud Computing (§ 6 Abs 3 GTelG 2012)
  - Verschlüsselung nach aktuellem Stand der Technik
  - Verwendung von Protokollen und Verfahren, die **vollständige Verschlüsselung** der Gesundheitsdaten bewirken **und**
  - Kryptografische Algorithmen nach der GTelV gem § 28 Abs 1 Z 2 GTelG
- Verstoß gegen Vorschriften des 2. Abschnitt des GTelG
  - Strafdrohung des Art 83 DSGVO
    - Geldstrafen bis zu 20 Millionen Euro / 4 % des weltweiten Jahresumsatzes