

PDMS CONFERENCE
2015

HIMSS Europe

WILLKOMMEN | 18. Juni 2015 Schloß Schönbrunn | Wien PDMS Conference D.A.CH. 2015

Interdisziplinäre Konferenz für Patientendatenmanagementsysteme



PDMS
***Sicherheitsrelevant oder
Kostenverschwendung?***

Datenschutzbestimmungen im Vergleich D.A.CH

Österreich

Markante Phasen der Entwicklung:

- Datenschutzgesetz (1978) - Grundrecht auf Datenschutz, Definitionen (Daten, Betroffene, Auftraggeber, Verarbeiter, ...), Meldung der Verarbeitung, Auskunftsrecht, Pflicht zur Richtigstellung oder Löschung
- Datenschutzrichtlinie 95/46/EG
- Datenschutzgesetz 2000 – DSG 2000 (BGBl. I Nr. 165/1999)
- Novelle 2005 (Ergänzung Daten im Katastrophenfall – “Tsunami-Anlassgesetzgebung”)
- Novelle 2014 (Datenschutzbehörde als Kontrollstelle anstelle der Datenschutzkommission – Auflösung aller unabhängigen Verwaltungsbehörden)
- Weitere Normen (GTelG 2012, ELGA-G, SigG)
- Für KAV: weitere Regelungen zur Umsetzung des DSG 2000 (etwa Videoüberwachung, Rollen- und Berechtigungskonzepte, ...)
- (Datenschutzreform - EU-Datenschutz-Grundverordnung)

Datenschutzbestimmungen im Vergleich D.A.CH

Grundrechtsbestimmung des aktuellen DSGVO 2018:

Jedermann hat Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht.

Datenschutz für Verstorbene?

Schutzumfang:

- Ermittlungsschutz
- Recht auf Geheimhaltung
- Recht auf Auskunft
- Recht auf Richtigstellung
- Recht auf Löschung

Datenschutzbestimmungen im Vergleich D.A.CH

Dem Datenschutz unterliegt:

jede Verwendung von personenbezogenen Daten

→ elektronische Dateien und manuelle Dateien

→ von natürlichen und juristischen Personen

(=Betroffene)

Beispiel A: PatientInnen, Angehörige, KollegInnen, Nachbarn, etc.

Beispiel B: Magistrat der Stadt Wien, Firmen, Vereine, etc.

Datenschutzbestimmungen im Vergleich D.A.CH

Personenbezogene Daten = Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist

→ bestimmt: wenn aus den Angaben direkt auf einen einzelnen Menschen geschlossen werden kann

→ bestimmbar: Daten sind verschlüsselt, können aber jederzeit entschlüsselt werden (bestimmbar ist eine Person, wenn ihre Identität durch die Kombination mit Informationen ohne einen unverhältnismäßigen Aufwand feststellbar ist)

→ indirekt personenbezogene Daten: der Personenbezug ist derart, dass man die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht feststellen kann (pseudonymisiert)

→ anonymisierte Daten: die Identität des Betroffenen ist für niemanden mehr feststellbar (keine Datenschutzrelevanz)

Datenschutzbestimmungen im Vergleich D.A.CH

Rollen im Datenschutzrecht:

→ Betroffener: jede vom Auftraggeber (und vom Dienstleister) verschiedene Person, deren Daten verwendet werden

→ Auftraggeber: wer die Entscheidung getroffen hat, Daten für einen bestimmten Zweck zu verarbeiten, unabhängig davon, ob dies durch ihn selbst erfolgt oder ein anderer damit beauftragt wird (= Verantwortung über Zulässigkeit der Verwendung von Daten, Vorkehrungen zur Datensicherheit, Registrierungs-, Informations-, Auskunftspflicht, Pflicht zur Richtigstellung und Löschung)

→ Dienstleister: wer Daten, die ihm zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwendet (Werk = Aussendungen, Wartungen, Entsorgung, etc.)

Datenschutzbestimmungen im Vergleich D.A.CH

Begrifflichkeiten:

→ Verwenden (= Verarbeiten und Übermitteln) und Überlassen

→ Verarbeiten = Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen, Sperren, Löschen, Vernichten, etc.

→ Übermitteln = jede Weitergabe, ausgenommen an einen Dienstleister (=Überlassen), wie etwa Weitergabe an andere Auftraggeber oder an anderes Aufgabengebiet (Rechtsgrundlage oder Zustimmung nötig)

→ Überlassen: nötig dazu Datenschutzvertrag (auf Basis Dienstleistungsvertrag), Datenverwendung nur im Auftrag des AG, Treffen von Datensicherheitsmaßnahmen, Verschwiegenheit der MitarbeiterInnen, Subdienstleister nur mit Billigung des AG, Rückgabe der Daten bei Beendigung des Vertragsverhältnisses, Kontrollmöglichkeit für den AG

Datenschutzbestimmungen im Vergleich D.A.CH

Meldepflicht des Auftraggebers → Beispiel V056 oder V102

Name, Adresse des Auftraggebers, Aufgabengebiet, Zweck und Rechtsgrundlagen der zu registrierenden Datenanwendung, Betroffenenkreise und Datenarten, vorgesehene Übermittlungen

KAV → zusätzlich Organisationskonzept etwa OK zur V102

EDV-Bereich, Funktionsbeschreibung, Quelle der Daten, verwendende Stellen, Dauer der Aufbewahrung, Datensicherheitsmaßnahmen, Hard-, Software, Benutzergruppen, Berechtigungsumfang, datenschutzrechtliche Verpflichtung, Stand-Alone-Geräte, mobile Geräte, Nachvollziehbarkeit der Datenverwendung,

Datenschutzbestimmungen im Vergleich D.A.CH

Rechte Betroffener:

→ Auskunftsrecht (auf Antrag des Betroffenen, grundsätzlich schriftlich, der Betroffene muss seine Identität nachweisen)

Antwort binnen 8 Wochen, in allgemein verständlicher Form (verarbeitete Daten, deren Herkunft, Übermittlungsempfänger, Zweck der Datenverwendung, Rechtsgrundlagen, Dienstleister)

→ Recht auf Richtigstellung oder Löschung (durch Auftraggeber selbst oder auf Antrag - ggf. Kollision mit anderen Normen)

→ Widerspruchsrecht

Datenschutzbestimmungen im Vergleich D.A.CH

Datenschutz KAV-intern

- Datenschutzbeauftragter
- Verantwortung der Leitung der Organsiationseinheiten
- Datenverantwortliche

Dokumentation und Informationsquelle für die MitarbeiterInnen: elektronisches Datenschutzhandbuch im Intranet (Basisinformation, Berechtigungskonzepte (etwa **PDMS Rollen- und Berechtigungskonzept**), erfolgten DS-Meldungen und OK der Datenanwendungen, Protokolle der Datenschutzberatungsgruppe, DS-Verträge, Videoüberwachung, spezielle Informationen wie zu Einzelübermittlungen, telefonische Auskunft an Angehörige, ...)

Datenschutzbestimmungen im Vergleich D.A.CH

Danke für Ihr Interesse!