

eHEALTH  
SUMMIT  
AUSTRIA

 Himss Europe



In Kooperation mit



**23. – 24. MAI 2017**

Schloß Schönbrunn, Wien  
Apothekertrakt und Orangerie

# Die Folgen der neuen EU Datenschutz- Grundverordnung - Akuter Handlungsbedarf?

Dr. Waltraut Kotschy, DPCC e.U.  
on

 @ Speaker twitter handle

Präsentiert von



## DIE NEUEN REGELUNGEN

- Die neue EU Datenschutz-Grundverordnung (GVO) wird am **25. Mai 2018 in Kraft** treten
- Sie wird als EU-Verordnung in Österreich **unmittelbar gelten**

## GEGENSTAND DER UNTERSUCHUNG

Frage 1: Wie wird sich der **Umfang der zulässigen Verarbeitung** von Gesundheitsdaten **ändern**?

Frage 2: Wie **wird sich die Umsetzung** von Datenschutz durch die Auftraggeber, Dienstleister und Datenschutzbehörden **ändern**?

## VERWENDUNG VON GESUNDHEITSDATEN

- Gesundheitsdaten sind „**sensible Daten**“
- Sensible Daten unterliegen - so wie bisher - einem **strengerem Verwendungsregime** als andere personenbezogene Daten:
  - Sensible Daten dürfen **NUR** für die in Art. 9 (2) lit. b – f, h und j GVO konkret genannten Fälle verwendet werden,
  - **AUSZER** es liegt entweder vor:
    - die **ausdrückliche Zustimmung** des Betroffenen (Art. 9 (2)(a)) ODER
    - eine besondere **Rechtsvorschrift**, die wegen **erheblicher öff. Interessen** (Art. 9 (2)(g)) die Verarbeitung erlaubt

## BISHER

- **DSG (§ 9)** = Art. 8 DS-RL
- Ausdrückliche Zustimmung
- Arbeitsrecht
  
- Gesundheitsversorgung
  
- Weitere Fälle aufgrund ges. Vorschriften bei wichtigen öff. Interessen (z.B: ELGA oder § 46 DSG 2000: wiss. Forschung und Statistik)

## IN ZUKUNFT

- **GVO (Art. 9)**
- Ausdrückliche Zustimmung
- Arbeitsrecht *und Sozial(versicherungs)recht*
  
- Gesundheitsversorgung + *Versorgung auch im Sozialbereich*
- *Öffentliches Gesundheitswesen*
- *Öff. Archive, Forschung, Statistik*
- Weitere Fälle aufgrund von Unions- oder MS-Recht bei erheblichen öff. Interessen

# TATSÄCHLICHE UNTERSCHIEDE?

## Neue Verarbeitungsfälle?

**Nicht wirklich:** „neue“ Verarbeitungsfälle des Art. 9 GVO = schon bisher durch österr. Gesetze, gestützt auf Art. 8 (4) der RL 95/46, als zulässig geregelt

zB. Verwendung von Gesundheitsdaten im Sozialversicherungsbereich, im öff. Gesundheitswesen, in der wiss. Forschung etc

- **Am Umfang** der zulässigen Verarbeitung von Gesundheitsdaten **wird sich** daher **nichts ändern**: diesbezüglich entspricht die Zukunft dem status quo
- **ABER:** ergeben sich Unterschiede hinsichtlich der **näheren Bedingungen** der Verarbeitung?

## ART. 8 RL 95/46 < > ART. 9 GVO

- In Art. 9 GVO wird die Notwendigkeit des Vorhandenseins von speziellen Rechtsvorschriften, die das grundrechtskonforme Design von Verarbeitungen sichern sollen, noch konsequenter betont als bisher:
  - Nach **Art. 9 MUSS** für die Zulässigkeit der Verwendung von Gesundheitsdaten jeweils eine **Rechtsvorschrift existieren**, die besondere Vorkehrungen zum Grundrechtsschutz (iSd Art. 52 (1) der EU Grundrechte-Charta) vorsieht ( - der Mindestinhalt ist für die einzelnen Fälle unterschiedlich formuliert).

## WESSEN RECHTSVORSCHRIFT?

- Ausführende Rechtsvorschriften zu EU-Verordnungen können an sich **nur EU-Rechtsakte** sein
- Allerdings gibt es sog. „**Öffnungsklauseln**“, d.h. Klauseln in EU-Verordnung wonach, in einzelnen Punkten die Mitgliedstaaten Regelungen treffen dürfen (oder sogar müssen)
- Die GVO enthält **eine prinzipielle Öffnungsklausel** für MS-Recht **in Art. 6 Abs. 2**

## DIE ÖFFNUNGSKLAUSEL DES § 6 ABS. 2 GVO

- In Bezug auf Verarbeitungen
    - des öff. Bereichs (= Verarbeitungen für Aufgaben, die durch Gesetz übertragen wurden) UND
    - zur Erfüllung einer gesetzlichen Verpflichtung des AG, UND
    - in den im Kap. IX genannten Materien, z.B. wiss. Forschung
- DARF nationales Recht** in Form spezifischerer Bestimmungen zur Anpassung der Anwendung der GVO **aufrecht erhalten werden oder sogar neues nationales Recht geschaffen werden**

## ERGEBNIS

- Die bisherigen Verarbeitungen von Gesundheitsdaten durch Auftraggeber des öffentlichen Bereichs **dürfen auf Grundlagen von österr. Rechtsvorschriften weiter vorgenommen werden**, wenn diese jeweils den Erfordernissen der entsprechenden Bestimmung in Art. 9 entsprechen
- Dasselbe gilt für Verarbeitungen von Gesundheitsdaten, die sich aus gesetzlichen Verpflichtungen des Auftraggebers ergeben - auch wenn der AG zum privaten Bereich gehört (!) Dies gilt z.B. für elektronische Krankengeschichten, die sich aus den gesetzl. Dokumentationspflichten von niedergelassenen Ärzten und Krankenanstalten ergeben
  - **bestehende österr. Rechtsvorschriften wären daher aufrecht zu erhalten**  
(vorherige Prüfung auf GVO-Konformität notwendig, Konformität ist aber wohl regelmäßig gegeben)

## ERGEBNIS - MEDIZINISCHE FORSCHUNG

- Bisher in Österreich durch § 46 DSG 2000 geregelt
- „Forschung“ in der GVO nunmehr eigens als zulässiger Grund für die Verwendung von sensiblen Daten genannt (Art. 9 (2)(j)GVO) mit **spez. Bedingungen**: Einhaltung des Art. 89 (1) GVO
  - + Unions- oder MSRegelungen, die Grundrechtskonformität sichern
- „wissenschaftliche Forschung und Statistik“ werden im Kap. IX der GVO behandelt → **§ 46 DSG 2000 könnte aufrechterhalten werden, soweit GVO-konform !**

## DATENSCHUTZ-ANPASSUNGSGESETZ 2018, ENTWURF

- Der derzeit in Begutachtung befindliche Entwurf eines „Datenschutz-Anpassungsgesetzes 2018“ enthält einen § 25 „Verarbeitung zum Zweck der wissenschaftlichen Forschung und Statistik“, der den § 46 DSG 2000 mehr oder weniger aufrecht erhält

## ZUR 2. FRAGE: UMSETZUNG VON DATENSCHUTZ

- Neu in der GVO ist die **erhöhte Eigenverantwortung der Auftraggeber** und auch der Dienstleister für die Einhaltung der GVO
  - für Österreich wird insbesondere bei der Strafbarkeit von Datenschutzdelikten ein völliger Systemwechsel eintreten
- Die **Rechtsstellung der Betroffenen** wird in einigen Punkten **gestärkt**
  - Informationsrecht ausgeweitet und einige neue Rechte geschaffen
- Die Vollziehung von Datenschutz in Europa wird vereinheitlicht
  - **Harmonisierung von Datenschutzrecht in der EU** durch gemeinsame Vollziehung

## DS-GVO 2016 <-> DS-RL 1995?

### Die wesentlichsten Änderungen in der GVO:

- 1) Der Auftraggeber wird stärker in die Pflicht genommen; er muss
  - die Datenschutz-Risiken seiner Datenverarbeitung **selbst einschätzen und entsprechend Abhilfe schaffen** (Risikofolgenabschätzung, privacy by design, ....) UND
  - Überlegungen und Maßnahmen selbst vollständig und nachvollziehbar dokumentieren (kein Registrierungsverfahren mehr) UND
  - **Verarbeitung verantworten** → hohe Strafandrohungen: bis zu 20 Mill. € oder bis zu 4 % des weltweiten Gesamtjahresumsatzes

## DS-GVO 2016 <-> DS-RL 1995?

- 2) Auch die **Dienstleister** werden schärfer ins Visier genommen:
  - Wenn in der Union nicht niedergelassen → Vertreter bestellen
  - Inhalt des Dienstleistervertrags viel genauer festgelegt
  - Heranziehung von Sub-Dienstleistern nur mehr mit Genehmigung des Auftraggebers
  - **Eigene Dokumentationspflicht** des Dienstleisters
  - Verpflichtung, Auftraggeber hinsichtlich GVO-Konformität der Verarbeitung aktiv zu unterstützen
  - Pflicht zur **Bestellung eines DS-Beauftragten** bei gewissen Verarbeitungen...

## DS-GVO 2016 <-> DS-RL 1995?

3) Die **Rechte der Betroffenen** werden gestärkt:

- Liste der Punkte, über die informiert werden muss, erheblich ausgeweitet
- Neue Rechte geschaffen, wie das Recht auf Datenportabilität
- Hohe Strafen bei Nichtbeachtung der Betroffenen-Rechte

4) Die **Rechtsdurchsetzung** wurde gestärkt:

- **Strafen werden nunmehr von der Datenschutzbehörde verhängt**
- Popularklage?

Danke für Ihre Aufmerksamkeit!