ÄRZTEKAMMER FÜR WIEN

Häufige Fragen hinsichtlich des Datenschutzes im Ordinationsalltag

Mag.ª Alexandra Lichtenegger

Juristin

der Rechtsabteilung der Ärztekammer für Wien

Rechtsgrundlagen

Datenschutz-Grundverordnung

DSGVO

Datenschutzgesetz

DSG

Ärztegesetz 1998

ÄrzteG

Gesundheits-telematikgesetz 2012

GTelG

Allgemeine Definitionen

- Personenbezogene Daten Art. 4 Z. 1 DSGVO:
  - alle Informationen, die sich direkt oder indirekt auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen
- Verarbeiten Art. 4 Z. 2 DSGVO:
  - das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung

- Besondere Kategorien von Daten Art 9. DSGVO:
  - die rassische und ethnische Herkunft,
  - politische Meinungen,
  - religiöse oder weltanschauliche Überzeugungen,
  - die Gewerkschaftszugehörigkeit,
  - genetische Daten,
  - biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
  - Gesundheitsdaten oder
  - Daten zum Sexualleben oder der sexuellen Orientierung
- Gesundheitsdaten 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

- Verantwortlicher Art. 4 Z. 7 DSGVO:
  - 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
  - **Der*Die niedergelassene Ärzt*in ist Verantwortliche*r im Sinne der DSGVO**
- Auftragsverarbeiter Art. 4 Z. 8 DSGVO:
  - eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet
  - Bsp.: Internetanbieter, Softwarehersteller….

Unter welchen Voraussetzungen dürfen Daten verarbeitet werden?

Verarbeitung von Gesundheitsdaten

- Art. 9 DSGVO:
  - grundsätzlich gilt ein Verarbeitungsverbot für besondere Kategorien von Daten
- Ausnahmen insbesondere
  - die betroffene Person hat in die Verarbeitung der Daten für einen oder mehrere Zwecke ausdrücklich eingewilligt
  - Rechtsgrundlage, erhebliches öff. Interesse
  - Verarbeitung für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich

Häufige Fragen zum Datenschutz

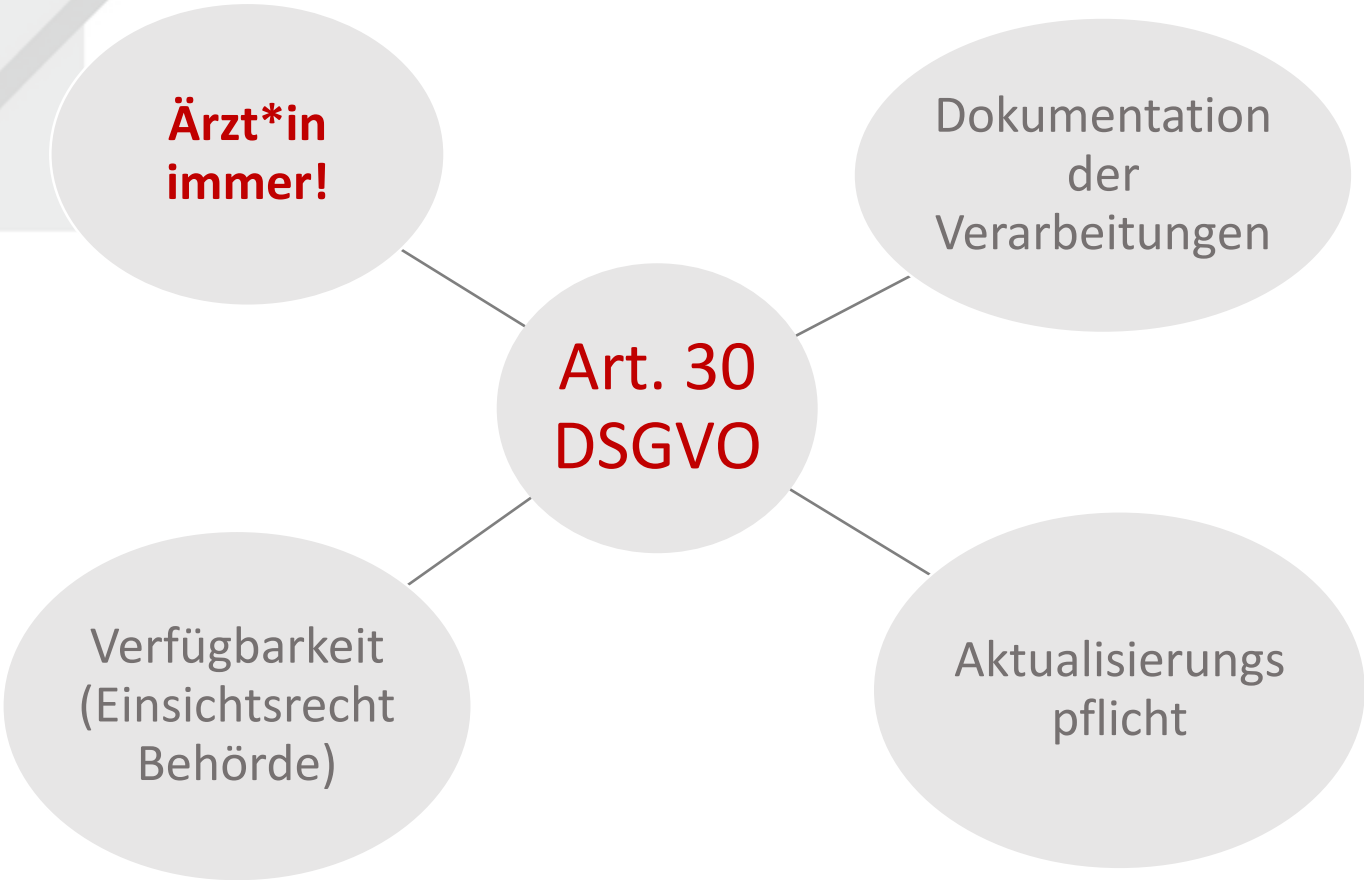
- Welche Erfordernisse der DSGVO muss ich als Ordinationsinhaber*in erfüllen?
  - Verarbeitungsverzeichnis?
  - Auftragsverarbeitervereinbarung?
  - Datenschutzbeauftragte*r?
  - Datenschutzfolgeabschätzung?
- Muss für jede Datenverarbeitung eine Einwilligung des*der Patient*in eingeholt werden?
- Wie kann ich meinem*meiner Patient*in vertrauliche Informationen übermitteln?
- Muss der*die Patient*in der Übermittlung von vertraulichen Informationen an andere Ärzt*innen bzw. Gesundheitseinrichtungen zustimmen?
- Was mache ich bei einer Datenschutzverletzung?
- Mein*e Patient*in möchte, dass ich alle Daten von ihm*ihr lösche. Ist das erlaubt?
- Mein*e Patient*in stellt ein Auskunftsbegehren, wie gehe ich hier vor?
- Welche Sanktionen sieht die Datenschutzgrundverordnung vor?

ÄRZTEKAMMER FÜR WIEN

Welche Erfordernisse muss ich als Ordinationsinhaber*in erfüllen um die DSGVO umzusetzen?

1. Verarbeitungsverzeichnis?
2. Auftragsverarbeiter-Vereinbarungen (AVV)?
3. Datenschutzbeauftragte*r?
4. Datenschutzfolgeabschätzung?

1. Verarbeitungsverzeichnis?



- Inhalt:

  - *alle Verarbeitungstätigkeiten*
  - *Namen und Kontaktdaten des*der Verantwortlichen*
  - *Zwecke der Verarbeitung*
  - *(…)*
  - *wenn möglich, die vorgesehenen Fristen für die Löschung (…)*
  - *wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (TOMs)*

→ Muster auf Homepage *www.aekwien.at*

ÄRZTEKAMMER FÜR WIEN

2. Abschluss von AVV‘s (Auftragsverarbeiter-Vereinbarungen)?

- Art. 28 DSGVO

Bedienung eines Dritten zur Datenverarbeitung

Betreuung Ordinationssoftware…

Grundvertrag + AVV

Mindestinhalte

Auskunftsrechte, SubAV…

→ Muster auf Homepage www.aekwien.at

3. Datenschutzbeauftragte*r (DSB)?

Quelle:
https://www.activemind.de/datenschutz/datenschutzbeauftragter/

- Art. 37 f. DSGVO
- DSB erforderlich, *„wenn die Kerntätigkeit des Verantwortlichen in der umfangreichen Verarbeitung besonderer Kategorien von Daten besteht“*

- → Der*die einzelne Ärzt*in ist nicht verpflichtet, DSB zu bestellen! Freiwillige Bestellung möglich
- Kriterien, ab welcher Praxisgröße DSB zu bestellen ist, nicht klar definiert
- Empfehlung bei ärztlichen Kooperationen (Gruppenpraxen, Primärversorgungseinrichtungen, Anstellung eines*einer Ärzt*in in der Einzelordination) auf das Kriterium der Patientenzahlen pro Jahr abzustellen
- durchschnittlich mehr als 5.000 Patienten pro Jahr →Bestellung eines*einer DSB!

4. Datenschutzfolgeabschätzung (DSFA)?

- Art. 35 DSGVO
- Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten, systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, Risikobewertung für die Betroffenen, wenn aus Verarbeitung hohes Risiko für Rechte und Freiheiten folgen kann
- DSFA insbesondere dann erforderlich, wenn eine *„umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten “* erfolgt

- Der einzelne Arzt ist nicht verpflichtet für die Patientenverwaltung und für die Honorarabrechnung eine DSFA durchzuführen. („Whitelist“, DSFA-V)
- Diese Ausnahme gilt nicht, falls mit einer ärztlichen Zusammenarbeit eine erhöhte Patient*innenzahl (mehr als 5000 Patient*innen pro Jahr) verbunden sind
- Empfehlung: wenn DSB bestellt werden muss
  → DSFA!
  → Muster auf Homepage *www.aekwien.at*

ÄRZTEKAMMER FÜR WIEN

Muss für jede Datenverarbeitung eine Einwilligung eingeholt werden?

- Nein
- Grundlagen der ärztlichen Datenverarbeitung:

Behandlungsvertrag

Dokumentationspflicht
§ 51 ÄrzteG

Achtung: Der Zweck der Erhebung der Daten muss dabei sehr genau eingehalten werden.

Wie kann ich meinem*meiner Patient*in vertrauliche Informationen übermitteln?

- Persönlich
- Per Post
- Per verschlüsselter Kommunikation
  - E-Mail: Ende zu Ende Verschlüsselung → Anbieterliste auf www.aekwien.at
- Per FAX?
- Per Telefon?

ÄRZTEKAMMER FÜR WIEN

Muss der*die Patient*in der Übermittlung von vertraulichen Informationen an andere Ärzt*innen bzw. Gesundheitseinrichtungen zustimmen?

- Nein – Einwilligungserklärung ist nicht erforderlich
- Soweit es zur potentielle Erweiterung des Behandlungsvertrages kommt
- Gilt auch für die Übermittlung medizinscher Proben zwecks Labordiagnostik sowie bei Über- bzw. Zuweisungen

ÄRZTEKAMMER FÜR WIEN

Was mache ich bei einer Datenschutzverletzung (Data-Breach)?

- Art. 33 DSGVO
- Bei Verletzung des Schutzes personenbezogener Daten → Meldung an Datenschutzbehörde (DSB) unverzüglich und möglichst binnen 72 Stunden
- Ausnahme: Verletzung führt zu keinem Risiko für die Rechte und Freiheiten der Betroffenen
- Bei hohem Risiko für die Rechte der Betroffenen sind diese ebenfalls über die Datenschutzverletzung zu informieren
- Dokumentation der Datenschutzverletzung!
- Meldeformular auf der Homepage der DSB (*www.dsb.gv.at*)

• Beispiele für Datenschutzverletzungen:

- jeder Vorfall, bei dem Unberechtigte Zugriff auf personenbezogene Daten erhalten
- Diebstahl/Verlust Ordinations-Laptop
- irrtümlicher Tausch oder Löschung von Befunden in der Dokumentationssoftware
- Sendung des Befundes an den falschen Patienten
- Datenschutzverletzungen durch AV
- …

Quelle: https://www.alamy.de/stockfoto-datenschutzverletzung-roten-stempel-auf-einem-weissen-hintergrund-133522744.html

ÄRZTEKAMMER FÜR WIEN

Mein*e Patient*in möchte, dass ich alle Daten von ihm*ihr lösche. Ist das erlaubt?

Quelle: https://www.privacyxperts.de/betroffenenrechte-wie-sie-mit-auskunftsersuchen-von-mitarbeitern-umgehen/

Löschung

- Art. 17 DSGVO
- Recht auf Löschung personenbezogener Daten bei Vorliegen von bestimmten aufgezählten Gründen
- Grundsätzlich Datenlöschung, wenn sie für den jeweiligen Zweck nicht mehr notwendig sind
- Darüber hinaus Aufbewahrung von Daten solange, als einfachgesetzliche Regeln die Speicherung vorsehen:

  → Ärztegesetz verpflichtet zur Aufbewahrung der Dokumentation für zumindest zehn Jahre → in diesem Zeitraum keine Löschung der Dokumentation möglich!

Wie gehe ich bei einem Auskunftsbegehren meines*meiner Patient*in vor?

- Art.15 DSGVO
- Recht auf Bestätigung ob, und wenn ja welche personenbezogenen Daten verarbeitet werden
- Inhalt der Auskunft sind die Daten selbst sowie die Beantwortung folgender Fragen:
  - *Werden personenbezogene Daten verarbeitet?*
  - *Zu welchem Zweck?*
  - *Welche Datenkategorien werden verarbeitet?*
  - *Gegenüber wem werden diese Daten offengelegt?*
  - *Aufbewahrungsdauer?*
  - *Herkunft der Daten?*
  - *Hinweis auf Beschwerderecht*
  - *Hinweis auf Betroffenenrechte*

Welche Sanktionen sieht die DSGVO vor?

- Strafdrohung bis zu EUR 20 Mio. oder 4% des weltweiten Jahresumsatzes
- Strafen primär zur Abschreckung von Datenschutzverstößen bei multinationalen Unternehmen gedacht, aber trotzdem jedenfalls empfindlichere Strafen als in der Vergangenheit
- In Österreich „Abmilderung“ im DSG: Verhältnismäßigkeit muss gewahrt werden → bei Erstverstoß meist nur Verwarnung, aber auch schon Strafe möglich!

ÄRZTEKAMMER FÜR WIEN

Vielen Dank!

Mag. Alexandra Lichtenegger

lichtenegger@aekwien.at

Tel.: 01 51501 - 1408