Höhne In der Maur & Partner
Rechtsanwälte

Die Datenschutzgrundverordnung

Mag. Markus Dörfler, LL.M.
Rechtsanwalt
20.3.2018

Markus Dörfler

1999 - 2005	Synaptic Networks
2006	Mag. iur. Universität Linz
2006 - 2007	Universitätslehrgang für Informationsrecht und Rechtsinformation, Universität Wien
2007	Master of Laws (LL.M.)
2012 - 2016	selbstständiger Rechtsanwalt - in Kooperation mit Höhne, In der Maur & Partner
2016	Partner bei Höhne, In der Maur & Partner Rechtsanwälte

Rechtsgrundlage (alt)

- Bundesgesetz über den Schutz personenbezogener Daten – Datenschutzgesetz 2000 – DSG 2000

- Richtlinie 95/46/EG vom 24.10.1995

Rechtsgrundlage (alt)

- Zweckgebundenheit
- Registrierpflicht (mit Ausnahmen)
- Datensicherheit

Rechtsgrundlage (alt)

- Verstöße:

  Verwaltungsstrafe bis zu EUR **10.000,00**

- Mein Rat:

Tun Sie nichts

Rechtsgrundlage (neu)

- Verordnung 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)
- In Kraft seit 24.5.2016 (anzuwenden ab 25.5.2018)

DSGVO

- Sanktion:
  - „wirksam, verhältnismäßig und abschreckend“
- Geldbuße:
  - bis zu EUR 10 Mio (oder 2% des weltweiten Jahresumsatzes)
  - bis zu EUR 20 Mio (oder 4% des weltweiten Jahresumsatzes)
  - zuständig: Aufsichtsbehörde

Rechtsgrundlage

- Schutzbereich:

  personenbezogene Daten

- ganz oder teilweise automatisierte Verarbeitung

Grundbegriffe

- „*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;
- **Keine** juristischen Personen
- **Keine** Daten von verstorbenen Personen
  - Achtung: Öffnungsklausel

Grundbegriffe

- Personenbezogene Daten – 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

Grundbegriffe

- 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.*“

Grundbegriffe

- 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

Grundbegriffe

- Auftragsverarbeiter (Art 4 Z 8 DSGVO):
  - Verarbeitung im Auftrag des Verantwortlichen
  - Beispiel: das Anbieten von Internetdiensten (Hosting)

Schriftliche Vereinbarung

Grundbegriffe

- Rechtmäßigkeit der Verarbeitung (Art 6 DSGVO):
  - Einwilligung
  - Erfüllung einer rechtlichen Verpflichtung
  - Lebenswichtige Interessen des Betroffenen
  - Wahrnehmung einer Aufgabe im öff. Interesse
  - Berechtige Interessen des Verantwortlichen

Grundbegriffe

- Einwilligung (Art 4 Z 11 DSGVO):
  - Zustimmung der betroffenen Person, dass personenbezogene Daten über die betroffene Person verarbeitet werden dürfen.

Nachweis der Einwilligung

Grundbegriffe

- Datensicherheit (Art 30 DSGVO):

Abzuwägen sind:

- Stand der Technik
- Implementierungskosten
- Art, Umfang, Umstände und Zweck der Verarbeitung
- Eintrittswahrscheinlichkeit und Schwere des Risikos

Zu ergreifen sind:

- geeignete technische und organisatorische **Maßnahmen**

Grundbegriffe

- Verzeichnis von Verarbeitungstätigkeiten (Art 30 DSGV) – „Verfahrensverzeichnis“
  - Anknüpfungspunkt: der Zweck der Verarbeitungstätigkeit
  - Dokumentation (auch elektronisch)
  - Jederzeitige Verfügbarkeit (Einsichtsrecht der Behörde)
  - Aktualisierungspflicht

Grundbegriffe

- Meldepflicht gegenüber der Behörde (Art 33 DSGVO)
  - Bei Verletzung des Schutzes personenbezogener Daten
  - Binnen 72 Stunden
    - außer die Verletzung führt zu keinem Risiko für die Rechte und Freiheiten der Betroffenen
    - die Meldung muss beinhalten: Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen

DSGVO

- Meldepflicht gegenüber dem Betroffenen
  - **Nicht**: bei verschlüsselten Daten
  - **Nicht**: bei hohem Aufwand
    (stattdessen: öffentliche Bekanntmachung)

Weitere Rechtsgrundlagen

- § 51 ÄrzteG
  - Aufzeichnungspflicht
  - Übermittlungsrecht
  - Aufbewahrungspflicht: mindestens 10 Jahre

Rechte der Betroffenen / Patientenrechte

- Auskunft
- Richtigstellung
- Löschung
- Widerspruch

Auskunftsrecht

- Auskunft
  - Form
  - Frist: Ein Monat
  - Kosten
  - Inhalt der Auskunft
- Einsicht in die Krankenakte (samt Kopien)
  - Aber: therapeutischer Vorbehalt
  - § 16 GTelG 2012

Praxis Prototyp

- bis zehn Ärzte
- bis zehn Mitarbeiter
- Arztsoftware (Patientenverwaltung)
- Abrechnung
- IT-Dienstleister

Wie geht es weiter?

Inhaltsverzeichnis:

B. Patientenverwaltung

10. Datenanwendung: Patientenakte

1.1. **Zweck** der Verarbeitung: Erfüllung der Dokumentationspflicht gemäß § 51 Ärztegesetz sowie die Erfassung sämtliche Leistungen) einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie zB Korrespondenz) in diesen Angelegenheiten.

Beinhaltet auch: Ausstellung von Bescheinigungen, Terminmanagement (Terminvereinbarung mit Patienten), die Wahrnehmung der Anzeige- und Meldepflicht gemäß § 54 Ärztegesetz, die Wahrnehmung der Anzeige- und Meldepflicht im Missbrauchsfall sowie Meldungen an div. Gesundheitsregister und im öffentlichen Meldewesen (Meldepflichten bei ansteckenden Krankheiten); Die Mitwirkung bei Verfahren bei der Patientenanwartschaft, der Schlichtungsstelle sowie dem Beschwerdemanagement bei der Standesvertretung und Versicherungen; Die Erstellung medizinischer Gutachten.

1.2. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage

1.3. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer, Patienten

1.4. Verarbeitung durch **Auftragsverarbeiter: [ergänzen]**

1.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[ergänzen]**

Betroffene Personengruppe: Arbeitnehmer					
Nr	**Kategorien**				
	von personenbezogenen Daten:	**an Empfängern**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl Kontaktinformationen (etwa Adresse, Tel, Mail, Fax)			gemäß der gesetzlichen Aufbewahrungspflicht (mindestens 10 Jahre)	
2	Behandlungsinformationen				

2. Muster der abgeschlossenen Vereinbarungen

AUFTRAGSVERARBEITERVERTRAG

Abgeschlossen zwischen **[Bitte Namen und Adresse ergänzen]** als ***Verantwortlicher***) und

_____

_____

_____

als ***Auftragsverarbeiter***, gemeinsam kurz: die ***Parteien***

1. Allgemeine Pflichten des Auftragsverarbeiters

1.1 Der Verantwortliche hat den Auftragsverarbeiter mit der Erbringung folgender Dienstleistungen beauftragt (im Folgenden kurz: die Datenanwendung):

1.2 Die Verarbeitung erfolgt für folgende Dauer: unbefristet / befristet bis:

1.3 Im Rahmen der Datenwendung verarbeitet der Auftragsverarbeiter folgende Datenkategorien:

1.4 Die Daten folgender Kategorien von betroffenen Personen werden im Rahmen der Datenwendung verarbeitet:

In Entsprechung dieser Verpflichtungen wird der Verantwortliche das Auskunftsrecht der betroffenen Person wie folgt handhaben:

Sobald der Betroffene einen Antrag auf Auskunft an den Verantwortlichen stellt, wird der Ansprechpartner des Verantwortlichen alle vertretbaren Mittel nutzen, um die Identität der betroffenen Person zu überprüfen. Der Antrag der betroffenen Person bedarf keiner besonderen Form und darf auch elektronisch erfolgen.

Der Antrag muss dem Verantwortlichen aber ermöglichen, die Informationen herauszufinden, die er beauskunften soll. Für die Beauskunftung ist beim Verantwortlichen **der Ansprechpartner** zuständig.

Sollte der Betroffene eine **mündliche Auskunft** verlangen, so wird der Zuständige die Identität des Betroffenen in geeigneter Weise feststellen und die Auskunft ebenso mündlich erteilen. Der Zuständige wird sämtliche Datenbestände nach Informationen, die die betroffen Person betreffen, durchsuchen und diese Informationen zusammenstellen.

Der Ansprechpartner wird sämtliche Datenbestände, in denen personenbezogene Daten über den Betroffenen zu finden sind, zusammenstellen und – sofern diese inhaltlich unübersichtlich sind – kurz erläutern.

Die Auskunft wird folgende Informationen umfassen:

- **Verarbeitete Daten:** Der Verantwortliche wird die betroffene Person darüber informieren, welche Informationen er über die Person verarbeitet.

- **Informationen:** Darüber hinaus wird der Verantwortliche der betroffenen Person folgende Informationen über die Datenverarbeitung zur Verfügung stellen:
  - die Zwecke der Verarbeitung
  - Datenkategorien
  - Empfänger und Kategorien von Empfängern

Offene Fragen

- Kommunikationsmedien
- Datenaustausch zwischen Ärzten
- Datenschutzbeauftragter

Höhne In der Maur & Partner
Rechtsanwälte

Danke für die Aufmerksamkeit

Markus Dörfler
E: markus.doerfler@h-i-p.at
T: 01/521 75-0
Höhne, In der Maur & Partner Rechtsanwälte GmbH & Co KG
Mariahilfer Straße 20, 1070 Wien
www.h-i-p.at