DATENSCHUTZ UND SOCIAL MEDIA: GRUNDLAGEN

GPMED, Patientenrekrutierung 4.0 – Die Rolle von Social Media & Co, Wien 7. Juni 2018

Mag. Markus Kastelitz, LL.M. (IT-Recht), CIPP/E
Senior Researcher | Senior Consultant
markus.kastelitz@researchinstitute.at

Research Institute AG & Co KG
Zentrum für digitale Menschenrechte

Web: https://www.researchinstitute.at

Mag. Markus Kastelitz, LL.M., CIPP/E

- Jurist mit IT-Rechts-Ausbildung
- Zertifizierter Information Privacy Professional (IAPP)
- **Senior Researcher** und **Senior Consultant**, Research Institute – Zentrum für digitale Menschenrechte
- Mitautor von Büchern zur Datenschutz-Grundverordnung
- Co-Gründer und Vorstandsmitglied **Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter – Privacyofficers.at**
- Lehrgangsbeiratsmitglied und Vortragender am Lehrgang **Datenschutz und Privacy** (Krems)
- **Erfahrungen** in:
  - Wissenschaft (Uni Hannover, Lehrstuhl Prof. Dr. Forgó)
  - Rechtsberatung (u.a. MedUni Wien, Industriekonzern, Parlamentsdirektion, RTR)
  - Datenschutzbeauftragter (MedUni Wien, Research Institute)
- **Forschungsschwerpunkte**:
  - Umsetzung der DSGVO
  - Datenschutz in der Forschung mit Schwerpunkt medizinische Forschung
  - Moderne Technologien und Datenschutz

RESEARCH INSTITUTE AG & CO KG

DIGITAL HUMAN RIGHTS CENTER

Das **Research Institute (RI)** ist ein Forschungszentrum an der Schnittstelle von **Technik, Recht** und **Gesellschaft**, das sich aus multi- und interdisziplinärer Perspektive mit der Bedeutung der Menschenrechte im digitalen Zeitalter beschäftigt.

Portfolio:

- **Forschung zu technischen** und **rechtlichen** Aspekten von **Datenschutz** und **Datensicherheit, Cybercrime, Technikfolgenabschätzung** und **Netzpolitik**
- **Smart.Rights.Consulting:** Beratung in datenschutzrechtlichen Fragen
- **Schulungen** für Privatpersonen und Mitarbeiter von Unternehmen/Organisationen
- **Maßgeschneiderte technische Lösungen** zur praktischen Umsetzung der Compliance-Prozesse (in Zusammenarbeit mit Software-Entwicklern)
- **Konzeption und Durchführung individueller und multidisziplinärer Projekte** mit renommierten Partnern auf nationaler und internationaler Ebene.

GRUNDRECHTLICHER SCHUTZ

- **Datenschutz ist ein Grundrecht**:
  - Art 8 Charta der Grundrechte der EU (GRC)
  - Art 8 Europäische Menschenrechtskonvention (EMRK)
  - § 1 Datenschutzgesetz (DSG) im Verfassungsrang
- **Datenschutz ist nicht Selbstzweck**, sondern Voraussetzung für
  - das Funktionieren einer freien demokratischen Gesellschaft und
  - die Ausübung zahlreicher anderer Grundrechte
- **Schutzgut sind nicht die Daten selbst, sondern verschiedene grundrechtlich geschützte Sphären der Menschen (insb. Privatsphäre)**
- **Grundsatz: Verarbeitung personenbezogener Daten verboten, wenn nicht ausdrücklich erlaubt**

EU-Datenschutzreform: Ergebnis und Status Quo

- **Bisher:**
  - EU: Datenschutzrichtlinie, RL 95/46/EG
  - Österreichisches Datenschutzgesetz 2000 (DSG 2000)
- **Datenschutz-Grundverordnung (DSGVO), VO 2016/679**
  - Seit 24. Mai 2016 im Rechtsbestand der EU; gilt seit 25. Mai 2018
  - Ziele und Grundsätze der DSRL gelten in der DSGVO fort
- **Nationales Datenschutzrecht**
  - Umfassende Änderung des **Datenschutzgesetzes** (DSG), BGBl I 2017/120, BGBl I 23/2018, BGBl I 24/2018
  - Zusätzlich zu beachten: spezifische dsr. Normen über viele Gesetze „verstreut“: Verschwiegenheitspflichten: § 54 ÄrzteG („Ärztegeheimnis“); § 9 KAKuG; § 16 Wr. KAG; § 11a VersVG; TKG; MPG; AMG; GesundheitstelematikG; GentechnikG etc.
  - Diese bereichsspezifischen Materiengesetze wurden bzw werden an die DSGVO angepasst:

→ z.B. zum AMG, ÄrzteG: Materien-Datenschutz-Anpassungsgesetz 2018, 2. Materien-Datenschutz-Anpassungsgesetz 2018

WAS WIRD GESCHÜTZT?

- **„Personenbezogene Daten“:** alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen, z.B.: Alter, Beruf, Anschrift, IP-Adressen (EuGH C-582/14)
- **Besonders geschützt sind dabei „sensible Daten“** (besondere Kategorien personenbezogener Daten): Daten über rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit; Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung
- **Definition Gesundheitsdaten**: 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
  - Im Schutz von Gesundheitsdaten liegt einer der historischen Ursprünge des Datenschutzrechts → **Eid des Hippokrates**

→ **In der Regel werden im Social Media-Bereich pers.bez. Daten vorliegen**

Art der Verarbeitung personenbezogener Daten

DSGVO gilt für:

- Ganz oder teilweise **elektronische** Verarbeitung personenbezogener Daten
- Verarbeitung personenbezogener Daten in Papierform, die **nach bestimmten Kriterien** geordnet sind

DSGVO gilt nicht für:

- **Unstrukturierte** Verarbeitung personenbezogener Daten in Papierform
- Weitere **Ausnahmen**
  - Tätigkeiten von natürlichen Personen zur Ausübung ausschließlich **persönlicher oder familiärer Tätigkeiten**
  - Tätigkeiten außerhalb des Unionsrechts: **Nationale Sicherheit**
  - Tätigkeiten im Anwendungsbereich von Titel V Kapitel 2 EUV: gemeinsame **Außen- und Sicherheitspolitik**
  - Tätigkeiten von Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von **Straftaten**

→ **Social Media-Nutzung unterliegt grds. der DSGVO**

Wesentliche Neuerungen der DSGVO

Verschärfung der Sanktionsmechanismen

- Strafen bis 20 Millionen EUR oder 4 Prozent des weltweiten Jahresumsatzes des betroffenen Unternehmens
- Auch für Verletzung von Handlungs-pflichten, nicht nur bei Data Breach
- Verbandsklagen zulässig
- Datenschutzbehörde wird Strafbehörde

Eigenverantwortung der „Verantwortlichen“ („Auftraggeber“)

- Dokumentationspflichten
- Rechenschaftspflicht
- Risikobasierter Ansatz
- Verpflichtende Risikoanalysen und Folgenabschätzung
- Datenschutzbeauftragter (in bestimmen Fällen)

Datenschutz-Grundverordnung (DSGVO)

Materiell-rechtliche Änderungen, zB

- Allgemeine „Data Breach Notification”
- Privacy by Design und by Default
- Entfall der Melde- und Genehmigungspflicht (DVR)
- Kein Schutz juristischer Personen mehr
- Wegfall der „indirekt personenbezogenen Daten“
- Recht auf Datenportabilität

Verstärkte Kooperation der nationalen Datenschutzbehörden

- „One-Stop-Shop“-Prinzip für Betroffene
- neues Gremium "European Data Protection Board“ (bisher: Art.-29-Gruppe)
- Konsultationsverfahren bei komplexen Risiken
- Mehr Koordination und Kohärenz

DSGVO-COMPLIANCE

- **DSGVO betont Rechenschaftspflicht des Verantwortlichen (= Unternehmen/ Institution)** für Einhaltung der VO im Unternehmen bzw. der Institution
  - Verantwortliche muss interne Maßnahmen treffen und jederzeit auch gegenüber der Datenschutzbehörde nachweisen können (**Nachweispflicht**) → interne Dokumentation erforderlich
  - **Nachweispflicht** auch für die Wirksamkeit der umgesetzten Maßnahmen

→ **Datenschutz wird zu einer kontinuierlichen Verpflichtung zur Überwachung und Verbesserung von Maßnahmen zu seiner Einhaltung**

→ **Verantwortlich dafür ist die Geschäftsleitung, die eine interne Befolgung durch MitarbeiterInnen, Geschäftspartner etc. sicherstellen muss: "Data protection must not only be done, it must be seen to be done"**

→ **Datenschutz geht alle an!**

Wichtige Rollen im Datenschutzrecht

- **„Betroffene Person“ („Betroffene/r“)**: natürliche Person, deren Daten verarbeitet werden, z.B. Patient
  - Juristische Personen nicht mehr umfasst
  - Aber natürliche Personen innerhalb von Unternehmen umfasst
- **„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
  - Wer entscheidet, welche Daten für welche Zwecke wie verarbeitet werden?
  - Auch mehrere **gemeinsam Verantwortliche** möglich (Art 26 DSGVO)

  → **Den Verantwortlichen treffen die meisten Pflichten der DSGVO („Hauptadressat“)**

- **„Auftragsverarbeiter“**: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (z.B. auch Hosting, Cloud-Dienste, etc.)

Roles in Data Protection Law

- **Sponsor**

- **CRO**

- **Trial site/**

PI, personnel

- **Patient/**

“Trial Subject”

- **<u>Between Sponsor and CRO</u>: Master Services Agreement and Work order**
- **Clinical trial agreement (CTA) between <u>Sponsor and/or CRO and Trial site</u>**
- **Personal data (health data etc.) of patients, employees (Principal Investigator, Investigators, other study personnel, monitors etc.)**
- **Roles of Sponsor, CRO and Trial site/PIs under GDPR?**

AKTUELLES VOM EUGH ODER WER IST DER VERANTWORTLICHE BEI SOCIAL MEDIA?

Gerichtshof der Europäischen Union
PRESSEMITTEILUNG Nr. 81/18
Luxemburg, den 5. Juni 2018

Presse und Information

Urteil in der Rechtssache C-210/16
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein /
Wirtschaftsakademie Schleswig-Holstein GmbH

Der Betreiber einer Facebook-Fanpage ist gemeinsam mit Facebook für die Verarbeitung der personenbezogenen Daten der Besucher seiner Seite verantwortlich

Deutschland: Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Düsseldorf, 6. Juni 2018:

- *Wer eine Fanpage besucht, muss transparent und in verständlicher Form darüber informiert werden, welche Daten zu welchen Zwecken durch Facebook und die Fanpage-Betreiber verarbeitet werden.*
- *Betreiber von Fanpages sollten sich selbst versichern, dass Facebook ihnen die Informationen zur Verfügung stellt, die zur Erfüllung der genannten Informationspflichten benötigt werden.*
- *Soweit Facebook Besucherinnen und Besucher einer Fanpage durch Erhebung personenbezogener Daten trackt, sei es durch den Einsatz von Cookies oder vergleichbarer Techniken oder durch die Speicherung der IP-Adresse, ist grundsätzlich eine Einwilligung der Nutzenden erforderlich, die die Anforderung der DS-GVO erfüllt.*
- *Für die Bereiche der gemeinsamen Verantwortung von Facebook und Fanpage-Betreibern ist in einer Vereinbarung festzulegen, wer von ihnen welche Verpflichtung der DS-GVO erfüllt. Diese Vereinbarung muss in wesentlichen Punkten den Betroffenen zur Verfügung gestellt werden, damit diese ihre Betroffenenrechte wahrnehmen können.*

Definition Social Media

„Kommunikationsplattformen im Online-Bereich, die es dem Einzelnen ermöglichen, sich Netzwerken von gleich gesinnten Nutzern anzuschließen bzw. solche zu schaffen“

(Artikel-29-Datenschutzgruppe, WP 163, 5)

- Im rechtlichen Sinne handelt es sich bei sozialen Netzwerken um einen „Dienst der Informationsgesellschaft“ iSd Artikels 1 Z 1 lit b RL 2015/1535 und § 3 Z 1 E-Commerce-Gesetz
- **FOLGEN: Informationspflichten des Diensteanbieters, insb.:**
  - **Offenlegungspflicht („Impressum“)** (§ 5 ECG; § 24 MedienG)
  - **Informationen über kommerzielle Kommunikation (Werbung, Absatzförderung)**

NEGATIVBEISPIEL

Facebook: Arzt postete Foto von Kinder-OP

Ein Kärntner Anästhesist hat auf Facebook ein Foto aus einem Operationssaal gepostet, als Beweis, dass Ärzte auch in der Nacht noch arbeiten. Was aufregt: Zu erkennen ist ein Kind auf dem OP-Tisch. Für den Arzt gibt es dienstrechtliche Konsequenzen.

Das Foto sorge für Aufregung in der Community, denn der Bub sei zu erkennen, er liegt auf dem OP-Tisch, ist intubiert, die Augen zugeklebt, betäubt, daneben sein Stofftier. Der Titel des verhängnisvollen Fotos: „Es ist 0.30, nur für die, die glauben, wir schlafen in der Nacht." Zu sehen ist auch das vierköpfige OP-Team, jeder der Gruppe wendet der Kamera den Rücken zu.

Facebook

Das Kind wurde auf dem Foto vom ORF unkenntlich gemacht.

„Nicht tolerierbar"

Juristen sahen sich das Foto bereits an und sagen, das Kind sei erkennbar. Das Foto ist zwar nicht mehr auf der Seite des Arztes zu sehen, doch es zog mittlerweile weite Kreise im Internet. Der medizinische Direktor des Klinikums Klagenfurt, Ferdinand Waldenberger, sagte gegenüber dem ORF, es gebe bereits dienstrechtliche Konsequenzen. Die Vorgehensweise des betreffenden Arztes sei nicht tolerierbar: „Er wird im Rahmen des Dienstrechts abgemahnt. Wir informieren die Mitarbeiter nochmals darüber, wie man

(Quelle: ORF.at 28.11.2014, http://kaernten.orf.at/news/stories/2681784/)

Social Media: kein rechtsfreier Raum

- **Datenschutz:**
  - **Erweiterte Informationspflichten** (Art 12 ff DSGVO) des Verantwortlichen gegenüber Betroffenen (z.B. Social Media-Nutzer); je nach Medium und Kontext: passende **Datenschutzerklärung (Website)** etc. zu erstellen, worin die Betroffenen über Datenverarbeitung (hier: „Rekrutierung von PrüfungsteilnehmerInnen“) informiert werden
  - **Rechtsgrundlage der Verarbeitung** (Art 6 Abs 1, Art 9 Abs 2 DSGVO): Für den Social Media-Auftritt: berechtigtes Interesse (Art 6 Abs 1 lit f); Tracking, Verarbeitung von sensiblen Daten (insb. Gesundheitsdaten): Einwilligung (Art 4 Z 11 iVm Art 6 Abs 1 lit a, Art 9 Abs 2 lit a) oder im Einzelfall Art 9 Abs 2 lit e: die betroffene Person hat eigene Daten offensichtlich selbst öffentlich gemacht
  - **Betroffenenrechte, Datenschutz-Folgenabschätzung, Datensicherheit** etc.
- **Weitere zu berücksichtigende Rechtsgrundlagen/soft law** (Beispiele):
  - **Arzneimittelwerberecht (AMG, MPG); Werberichtlinie u. Verhaltenskodex der Ärztekammer; Pharmig-Verhaltenscodex (VHC); IGEPHA Werbecodex etc.**
  - **E-Commerce-Gesetz, MedienG**
  - **UWG**
  - **Immaterialgüterrecht (UrhG, MarkenschutzG etc.), Persönlichkeitsschutz (§ 16 ABGB etc.)**
  - **Nutzungsbedingungen der Social Media-Plattform (insb. Werbeverbote?)**

SOCIAL MEDIA: LAST BUT NOT LEAST

- **Binden Sie die Rechtsabteilung, Ihre Rechtsberatung etc. frühzeitig in die Planung einer Social Media-Aktivität ein**
- **Achten Sie darauf, dass vertraglich vereinbart ist, wer was durchführt und wer wofür verantwortlich ist**
- **Anpassung an nationale Rechtslage**
- **Für Prüfärzte/Prüfärztinnen – erweiterte Pflichten:**

Demnächst § 36 AMG neu (idF 2. Materien-Datenschutz-Anpassungsgesetz 2018):

- *8a. die Daten (Z 8) ehestmöglich zu pseudonymisieren, die Pseudonymisierung zu dokumentieren, die Dokumentation mit äußerster Sorgfalt handzuhaben und sicherzustellen, dass die Zuordnung zu einer spezifischen betroffenen Person ausschließlich unter den im Prüfplan angegebenen Umständen erfolgt,*
- *8b. für den Sponsor die Pflichten nach Art. 13 [Infopflicht], 15 [Auskunftsrecht], 16 [Berichtigung] und 18 [Einschränkung] der Datenschutz-Grundverordnung zu erfüllen* → Recruiting als Teil der klinischen Prüfung? Falls ja, müsste sich PI um Social Media kümmern (!?)
- *8c. bei Verletzungen des Schutzes personenbezogener Daten den Prüfungsteilnehmer gemäß Art. 34 Datenschutz-Grundverordnung zu benachrichtigen und den Sponsor davon zu informieren*

Informationspflichten: Inhalt der Information

Mindestangaben zum Zeitpunkt der Erhebung zu erteilen:

- **Name** u. **Kontaktdaten** des Verantwortlichen sowie ggf. seines Vertreters
- **Kontaktdaten** des Datenschutzbeauftragten
- **Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die **Rechtsgrundlage** für die Verarbeitung
- **berechtigte Interessen,** die von dem Verantwortlichen oder einem Dritten verfolgt werden (bei Verarbeitung gem Art 6 Ab 1 lit f)
- **Empfänger oder Kategorien von Empfängern** der Daten (bei Datenübermittlung)
- beabsichtigte Datenübermittlung in ein **Drittland** /an eine **internat. Organisation** samt **Rechtsgrundlage** hierfür (s. Art 44 ff)

Zusätzliche Angaben zum Zeitpunkt der Erhebung zu erteilen:

- **Speicherdauer**; falls nicht möglich, Kriterien für die Festlegung dieser Dauer
- Bestehen von **Betroffenenrechten**
- Hinweis auf **Widerruf**, wenn die Verarbeitung auf Einwilligung basiert
- Bestehen eines **Beschwerderechts** bei einer Aufsichtsbehörde
- **Gesetzl. oder vertragl. Verpflichtung** zur Bereitstellung der Daten, ihrer Erforderlichkeit, Folgen der Weigerung d. Datenbereitstellung
- Bestehen einer **automatisierten Einzelfallentscheidung** gem. Art 22 Abs 1 u. 4 und über die involvierte Logik sowie die Tragweite
- [bei beabsichtigter **Weiterverarbeitung für andere Zwecke**: Informationen über anderen Zweck und alle anderen Informationen gem. Abs 2 → **vor** der Weiterverarbeitung zu informieren]