Cyber-Crime

ZUNEHMENDE GEFAHR IM MEDIZINISCHEN ALLTAG!

DATENSCHUTZRECHT

16.01.2020 – RA Mag. Philip Neubauer

KSKP | RECHTSANWÄLTE

ÜBERBLICK

- Begriffe
- Sicherheit der Datenverarbeitung
- Verletzung des Schutzes von Daten
- Meldepflichten / Informationspflichten

BEGRIFFE

- **Personenbezogene Daten** (Art 4 Z 1 DSGVO)

  - *alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen;*

  - *als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.*

BEGRIFFE

- **Verarbeitung** (Art 4 Z 2 DSGVO)
  - *jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie*
    - 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;

Begriffe

- **Gesundheitsdaten** (Art 4 Z 15 DSGVO) – <u>besondere Kategorie von Daten</u>
  - *alle 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.*
  - *EuGH: Begriff ist weit auszulegen , sodass Gesundheitsdaten sich auf alle Informationen beziehen, die die Gesundheit einer Person unter allen Aspekten – körperlich wie psychisch – betreffen.*
  - *Bsp: Die Krankschreibung eines Patienten durch den Arzt mit der Mitteilung der Arbeitsunfähigkeit stellt bereits ein Gesundheitsdatum dar; auch selbst erhobene Daten durch eine betroffene Person können Gesundheitsdaten darstellen (Wearables, Gesundheits-Apps, Blutdruckmessung mit eigenen Gerät)*

SICHERHEIT DER DATENVERARBEITUNG

- **Allgemeines**

  - *Art 24 DSGVO: Programmsatz für Verantwortliche wie Ärzte, Gruppenpraxen, Kliniken etc*
    - Grundsätzliche Pflichten zur Einhaltung des Datenschutzes
    - Risiko = Eintrittswahrscheinlichkeit des (schädigenden) Ereignisses x Schwere des daraus resultierenden Schadens
    - Geeignete technische und organisatorische Maßnahmen (TOMs)

SICHERHEIT DER DATENVERARBEITUNG

- **Technische und organisatorische Maßnahmen**

  - *Pseudonymisierung*
  - *Verschlüsselung von Daten*
  - *Zutrittskontrolle (kein Zutritt von unbefugten Personen → Türsicherung, Überwachungseinrichtungen)*
  - *Zugangskontrolle (Nutzerberechtigungen, Aktivierung von Anmeldemöglichkeiten, Verwendung sicherer Passwörter, Einsatz von Malwareschutzmaßnahmen, Firewall)*
  - *Zugriffskontrolle (Need to know – Prinzip, Zugriffsprotokolle)*
  - *Weitergabekontrolle (Einsatz von elektronischen Signaturen, verschlüsselte Übertragung, sichere Gestaltung von Informationsübertragungen)*
  - *Verfügbarkeitskontrolle (Backup, USV) - Auftragskontrolle*

VERLETZUNG DES SCHUTZES VON DATEN

- **Vertraulichkeit, Integrität, Verfügbarkeit**

  - *Der Verantwortliche hat die DSB von allen Sicherheitsverletzungen zu informieren, die Auswirkungen auf die Betroffenen haben können, und muss die Betroffenen informieren, wenn für sie ein hohes Risiko besteht.*

  - *Eine Informationspflicht besteht für den Verantwortlichen nach der DSGVO dann, wenn er von einer „Verletzung des Schutzes personenbezogener Daten“ Kenntnis erlangt. Dies ist nach der DSGVO „eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von bzw zum unbefugten Zugang zu personenbezogenen Daten führt (Art 4 Z 12 DSGVO).*

VERLETZUNG DES SCHUTZES VON DATEN

- **Vertraulichkeit, Integrität, Verfügbarkeit**

  - ***Vertraulichkeit*** *– die DSGVO spricht von einer „unbefugten Offenlegung“ bzw von einem „unbefugten Zugang zu personenbezogenen Daten“.*
  - ***Integrität*** *– die DSGVO spricht von einer unbefugten „Veränderung“ der personenbezogenen Daten*
  - ***Verfügbarkeit*** *– die DSGVO spricht von der „Vernichtung“ bzw dem „Verlust“ der personenbezogenen Daten und macht damit deutlich, dass nur eine dauerhafte Kompromittierung der Verfügbarkeit erfasst ist; ein bloß vorübergehender Verlust der Verfügbarkeit (kurzer Serverausfall) stellt noch keine „Verletzung des Schutzes personenbezogener Daten“ dar.*

Erscheinungsformen von Cyber-Crime

- Data Leaks (Datenpanne oder Datenleck)
  - *E-Mail Adressen mit dazugehörigen Passwörtern von gehackten Unternehmen und Portalbetreibern werden zunehmend nicht nur im Darknet sondern auch frei erhältlich im Internet angeboten*
  - *Hacker nutzen ua bereits installierte Apps, die Schadsoftware beinhalten, für Daten- und Identitätsmissbrauch*
- „Distributed Denial of Service“ – Angriffe (DDoS-Angriffe)
  - *ein „verteilter“ DDOS-Angriff, der eine Dienstblockade darstellt*
  - *mutwillig herbeigeführte Überlastung der IT-Infrastruktur*
  - *dadurch ist ein angefragter Dienst nicht mehr bzw nur noch eingeschränkt möglich*
- Ransomsoftware (Erpressertrojaner)
  - *mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann*
- Internetbetrug
  - *Zahlreiche Modi Operandi (zB vorgetäuschte Warenlieferung)*

Quelle: Lagebericht Cybercrime 2018

Verletzung des Schutzes von Daten / Informationspflichten

	Information der DSB	Information der Betroffenen
Auslöser der Info-Pflicht	Kenntnis von der Verletzung des Schutzes personenbezogener Daten, sofern für die Betroffenen jegliches Risiko besteht	Kenntnis von der Verletzung des Schutzes personenbezogener Daten, sofern für die Betroffenen ein hohes Risiko besteht (siehe unten)
Frist	Unverzüglich (dh ohne schuldhafte Verzögerung) aber jedenfalls binnen 72 Stunden ab Kenntnis	Unverzüglich (dh ohne schuldhafte Verzögerung) ab Kenntnis
Umfang der Info	➢ Art der Sicherheitsverletzung ➢ Name und Kontaktdaten des Datenschutzbeauftragten oder sonstigen Anlaufstelle ➢ ergriffene oder vorgeschlagene reaktive Maßnahmen ➢ wahrscheinliche Folgen ➢ Kategorien und Anzahl der Betroffenen ➢ Kategorien und Anzahl der Datensätze	➢ Art der Sicherheitsverletzung ➢ Name und Kontaktdaten des Datenschutzbeauftragten oder sonstigen Anlaufstelle ➢ ergriffene oder vorgeschlagene reaktive Maßnahmen ➢ wahrscheinliche Folgen ➢ Empfehlungen zur Minderung der Folgen

Verletzung des Schutzes von Daten / Informationspflichten

	Information der DSB	Information der Betroffenen
Form der Info	per E-Mail	Per Brief, E-Mail oder sonstiger elektronischer Nachricht, sofern kein unverhältnismäßiger Aufwand entsteht – ansonsten öffentliche Bekanntmachung (zB auf der Startseite der Website, sofern diese regelmäßig von den Betroffenen besucht wird)

Verletzung des Schutzes von Daten / Praxisbeispiele

Ereignis	Informationspflicht
Laptop (ohne Festplattenverschlüsselung) mit Patientendaten im Zug vergessen	Es liegt eine Verletzung der Vertraulichkeit vor (unbefugter Zugang). Die DSB ist grds zu informieren, die Betroffenen nur, wenn aufgrund der konkreten Daten ein hohes Risiko besteht.
E-Mail zur Mahnung eines Patienten versehentlich an Geschäftspartner anstatt an den Patienten gesendet	Es liegt eine Verletzung der Vertraulichkeit vor. Die DSB ist grds zu informieren, der Betroffene nur, wenn aus der E-Mail sensible Daten ersichtlich waren und daher ein hohes Risiko vorliegt.
Einige Mitarbeiter-PCs werden durch Schadsoftware kompromittiert, die es – soweit bekannt – nicht auf die Daten abgesehen hat, die auf den PCs gespeichert sind, sondern nur dazu verwendet wird, Spam-E-Mails an Dritte zu versenden	Obwohl die PCs mit Schadsoftware befallen sind, wurde weder die Vertraulichkeit noch die Verfügbarkeit oder die Integrität der Daten verletzt. Eine Information der DSB oder Betroffenen ist daher nicht erforderlich.

KSKP | RECHTSANWÄLTE

Verletzung des Schutzes von Daten / Praxisbeispiele

Ereignis	Informationspflicht
Eine Sicherheitslücke **in Standardsoftware** wird öffentlich bekannt, die es jedermann (insb Kriminellen) ermöglicht, über das Internet auf die gesamte Kundendatenbank zuzugreifen. Die Sicherheitslücke wird innerhalb von 24 Stunden durch ein Sicherheitsupdate geschlossen. Ob in der Zwischenzeit ein unautorisierter Zugriff auf die Kundendatenbank erfolgt ist, kann nicht festgestellt werden.	Der Verantwortliche hat keine Kenntnis davon, dass es tatsächlich zu einer Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität gekommen ist. Eine Informationspflicht besteht daher nicht.
Erpresser-Schadsoftware verschlüsselt alle Patientendaten **(keine Backups vorhanden)**	Es liegt eine Verletzung der Verfügbarkeit der Daten vor. Die DSB ist allerdings nur zu informieren, wenn der Datenverlust negative Auswirkungen für die Betroffenen haben kann, die Betroffenen nur dann, wenn ein hohes Risiko vorliegt.
Erpresser-Schadsoftware verschlüsselt alle Patientendaten **(Backups vorhanden)**	Da Backups vorhanden sind und jederzeit wiederhergestellt werden können, sind die Daten weder verloren noch vernichtet. Eine Informationspflicht besteht daher grds nicht.

Verletzung des Schutzes von Daten / Strafrecht

- **Datenbeschädigung** (§ 126a StGB)
  - Schaden an automationsunterstützt verarbeiteten, übermittelten oder überlassenen Daten (Tatobjekt):
    - Daten (personenbezogene Daten, über die der Täter nicht oder nicht allein verfügen darf)
    - automationsunterstütze Daten gem § 3 DSG:
      Daten die maschinell oder programmgesteuert erfasst, gespeichert, bearbeitet, gelöscht etc werden
  - Tathandlung mit bedingtem Vorsatz
    - Handlungen, die die Daten unbrauchbar machen (auch Unterdrückungshandlungen)
    - Vermögensschaden als Schaden an Daten (zB durch Wiederherstellung der Daten)
  - Strafe
    - bis zu sechs Monaten oder Geldstrafe bis zu 360 Tagessätzen
    - Schaden übersteigt € 5.000: Freiheitsstrafe bis zu zwei Jahren
    - Beeinträchtigung von vielen Computersystemen (ab ca. 30): Freiheitsstrafe bis zu drei Jahren
    - Schaden übersteigt € 300.000: Freiheitsstrafe von sechs Monaten bis fünf Jahren

VERLETZUNG DES SCHUTZES VON DATEN

- **Entscheidungen / Judikatur**

  - DSB-D084.133/0002-DSB/2018 vom 8.8.2018: Informationspflicht an Betroffene (Verlust des Suchtmittelbuchs in Papierform – 150 Datensätze betreffend Ein- und Ausgänge Suchtmitteldepots);

  - DSB-D213.692/0001-DSB/2018 vom 16.11.2018: Sicherheitsverletzungen waren Anlass für ein amtswegiges Prüfungsverfahren betreffend Allergietagesklinik (Meldungen betreffend Sicherheitsverletzungen hatte jeweils ein Datenschutzkoordinator → aber kein Datenschutzbeauftragter vorgenommen); Ergebnis: mehrere Datenschutzverletzungen wurden von der DSB festgestellt

Kontakt KSKP Rechtsanwälte

- Kontaktdaten:
  - *Homepage: www.kskp.at*
  - *E-Mail: office@kskp.at*
  - *Hauptstandort: Am Eisernen Tor 2/II, 8010 Graz.*
  - *Telefon: 0316/8525850*

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!