Dr. med. Christina Czeschik

Schuld ist immer der Datenschutz… oder?

Zukunftskongress
02.06.2023

Schon gehört?

Das geht nicht…

… wegen Datenschutz.

Datenschutz: eine kleine Einführung

Seit 1977 Bundesdatenschutzgesetz

Recht auf Informationelle Selbstbestimmung seit 1983 (Volkszählungsurteil)

Seit 2018 EU-Datenschutzgrundverordnung (DSGVO)

Datenschutz

= Schutz persönlicher Daten – etwa vor unbefugtem Zugriff, Missbrauch und Zweckentfremdung – mit dem Ziel, die **Privatsphäre** der betroffenen Person zu wahren.

Datenschutz bezieht sich immer auf sogenannte **personenbezogene Daten**.

Personenbezogene Daten sind Daten, die sich „auf eine identifizierte oder identifizierbare natürliche Person beziehen“ (Art. 4 Nr. 1 DSGVO).

Identifizierbar?

… ist eine Person, 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.

Beispiele für personenbezogene Daten im Gesundheitswesen?

Beispiele für personenbezogene Daten im Gesundheitswesen?

- *Namen*
- *Krankenversicherung und Versicherungsnummer*
- *Kontoverbindung*
- *Familienstand*
- *Ausbildung und Beruf*
- *Gesprochene Sprachen*
- *Essensbestellung*
- *Körperliche Untersuchungsbefunde*
- *Medizinische Anamnese*
- *Pflegeanamnese*
- *Laborergebnisse*
- *Röntgenbilder*
- *Fotos (z.B. als Wunddokumentation)*
- *DNA-Sequenzen*

Besondere Kategorien von personenbezogenen Daten

– Daten, aus denen ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder Gewerkschaftszugehörigkeit hervorgehen

– genetische Daten

– biometrische Daten

– Daten zum Sexualleben oder der sexuellen Orientierung

– Gesundheitsdaten

TOM: Technisch-organisatorische Maßnahmen

Verschlossene Türen,

Passwortschutz,

Berechtigungsmanagement,

Trennung von sensiblen und weniger sensiblen Daten

… u.v.a.

Verhältnismäßigkeitsprinzip

Persönliche Daten müssen durch TOM nicht unendlich aufwendig geschützt werden, sondern in einem Maß, das

wirtschaftlich noch sinnvoll

ist.

Datenschutzvorschriften allgemein

- Europäische Datenschutz-Grundverordnung (DSGVO)
- Bundesdatenschutzgesetz (BDSG)
- Landesdatenschutzgesetze (LDSG)
- Strafgesetzbuch (StGB)
  - Berufsgeheimnis nach § 203
  - Ärztliches Zeugnisverweigerungsrecht vor Gericht nach § 53
- Zivilprozessordnung (ZPO)
  - Ärztliches Zeugnisverweigerungsrecht vor Gericht nach § 383
- Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) und Gesetz über den Kirchlichen Datenschutz (KDG) der katholischen Kirche

Datenschutzvorschriften Gesundheitswesen

- Landesdatenschutzgesetze (LDSG): Nordrhein-Westfalen hat die landesrechtlichen Vorschriften zum Datenschutz im Gesundheitswesen in ein eigenes Gesetz ausgelagert, das Gesundheitsdatenschutzgesetz

- Sozialgesetzbücher (SGB)

- Berufsordnungen der Ärztekammern, angelehnt an die Musterberufsordnung (MBO) der Bundesärztekammer
  - Ärztliche Schweigepflicht gemäß § 9

Erlaubnisvorbehalt

Nach BDSG und DSGVO ist die Verarbeitung personenbezogener Daten grundsätzlich verboten…

Erlaubnisvorbehalt

Nach BDSG und DSGVO ist die Verarbeitung personenbezogener Daten grundsätzlich verboten…

… außer, wenn sie erlaubt ist.

Und wann ist sie erlaubt?

1. Wenn der/die Betroffene eingewilligt hat.

2. Wenn die Verarbeitung zur Erfüllung eines Vertrages (mit dem/der Betroffenen) notwendig ist.

3. Wenn die Verarbeitung notwendig zur Erfüllung einer rechtlichen Pflicht des Verantwortlichen ist.

Und wann ist sie erlaubt?

4. Wenn die Verarbeitung notwendig ist, um lebenswichtige Interessen einer Person zu schützen.

5. Wenn die Verarbeitung für die Wahrnehmung einer Aufgabe im öffentlichen Interesse ist.

6. Wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen notwendig ist.

Grundsätze für die Datenverarbeitung nach DSGVO

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Die Datenverarbeitung muss in einer rechtmäßigen und für die betroffene Person nachvollziehbaren Art und Weise erfolgen.

Grundsätze für die Datenverarbeitung nach DSGVO

Zweckbindung

Die Erhebung muss für festgelegte, eindeutige und legitime Zwecke erfolgen. Die Weiterverarbeitung darf nicht für Zwecke erfolgen, die mit diesen legitimierten Zwecken nicht übereinstimmen.

Grundsätze für die Datenverarbeitung nach DSGVO

Datenminimierung

Die erhobenen Daten müssen dem jeweiligen Zweck angemessen sein. Es dürfen nur solche Daten erhoben werden, die für die Zweckerfüllung notwendig sind (Datensparsamkeit).

Grundsätze für die Datenverarbeitung nach DSGVO

Richtigkeit

Die erhobenen Daten müssen sachlich richtig sein. Es müssen angemessene Maßnahmen getroffen werden, damit falsche Daten erkannt und berichtigt werden können.

Grundsätze für die Datenverarbeitung nach DSGVO

Speicherbegrenzung

Die erhobenen Daten dürfen nur so lange gespeichert werden, wie der Zweck es erforderlich macht bzw. die gesetzliche Grundlage es erlaubt.

(Siehe auch: „Recht auf Vergessen“)

Grundsätze für die Datenverarbeitung nach DSGVO

Integrität und Vertraulichkeit

Die erhobenen Daten müssen sicher verarbeitet werden, also so, dass unbefugter Zugriff, Zerstörung oder andere Eingriffe mit angemessener Sicherheit verhindert werden.

Fazit

Die DSGVO selbst verhindert keine Datenverarbeitung zu sinnvollen Zwecken.

„Datenschutz“ ist oft ein vorgeschobener Grund, um Dinge nicht umsetzen zu müssen.

Fazit

Aber reale Probleme sind:

- **Rechtsunsicherheit** (viele Sachverhalte sind in der DSGVO nicht klar festgelegt, sondern werden erst vor Gericht geklärt)

- Zusätzlicher Aufwand/Expertise/Kosten

Bußgelder

Bis zu **20 Millionen EUR**

oder

bis zu **4%** des weltweiten Jahresumsatzes

(je nachdem, was höher ist)

Siehe auch:

https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank/

EuGH-Urteil vom 04. Mai 2023

Schadenersatz nur bei Schaden

Wenn ein Unternehmen gegen die DSGVO verstößt, wird nur dann Schadenersatz fällig, wenn jemand tatsächlich geschädigt wurde.

Kein Schadenersatz für „Unwohlsein“ mehr.

Aber: Keine Bagatellgrenze.

(Dr. Hauke Hansen, Heise iX 06/2023)

Danke für Ihre Aufmerksamkeit!

Dr. med. Christina Czeschik
czeschik@serapion.de