Grundzüge der neuen europäischen Datenschutzgrundverordnung (DS-GVO)

Konsequenzen und Probleme bei der Umsetzung

Dr. Rainer Doubrawa

Vortrag anl. der MV der SABP am 27.10.2018

Vorbemerkungen zur Entstehung:

Das *weltweit erste Datenschutzgesetz war das Hessische Datenschutzgesetz 1970*
Das Datenschutzrecht hat international von Deutschland aus seinen Ursprung genommen.

Es ist heute angesichts der *rasant fortschreitenden Digitalisierung* und der immer komplexer werdenden IT- Verarbeitungsmöglichkeiten und einer immer größer werdenden Fülle verarbeitbarer personenbezogener Daten und damit des zunehmenden Datenmissbrauchs wichtiger denn je.

Bereits *Anfang 2012 legte die EU-Kommission* einen Entwurf für eine Verordnung des Europäischen Parlaments und des Rates vor
zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. *Die Datenschutz-Reform sollte gleiches Recht für alle schaffen.*

Seit dem 25.05.2016 ist die EU-DS-GVO in Kraft getreten.
Ab dem 25.05.2018 gilt sie – ohne weitere Übergangszeit.

Die EU-DSGVO soll der *Vereinheitlichung* der inzwischen zahlreichen unterschiedlichen DS-Gesetze im Gebiet der EU dienen.

Verwendete Quellen:

- EU Datenschutz-Grundverordnung EU-GVO (2016)
- EU-Datenschutzgrundverordnung – Eine Einführung. Vortrag/Folien von Hans-Hermann Schild. 2017
- Bundesdatenschutz-Gesetz BDSGneu (2017)
- 46. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten (2017)
- Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis. Dt. Ärzteblatt 09.03.2018
- Datenschutz und Datensicherheit – Update 2017 (Esturias Fachtagung)
- Datenschutz 2018. Praxis-Info der BPtK
- J. Frederichs: Besser spät als nie. Hinweise zur Datenschutz-Grundverordnung. Report Psychologie 43, 3/2018, 121-123
- Jan Philipp Albrecht: Vom Vorreiter zum Schlusslicht? Bei der Umsetzung des EU-Datenschutzes muss die Bundesregierung massiv nachbessern. BvD-News 1/2017, 5-6
- Stefan Brink: Deutscher Datenschutz: Europäisches Exportmodell oder Hemmschuh für Wirtschaft und öffentliche Sicherheit? BvD-News 1/17, 7-10
- P. Schaar: Wie viele Ausnahmen verträgt der europäische Datenschutz? BvD-News 1/17, 11-13
- Die ersten Tage mit der DSGVO …, FOCUS 22, 2018, 28-29, 37-40

Ich werde in meinem Vortrag *nur auf die wichtigsten Punkte* eingehen, die uns allgemein und als Psychologen/Psychologische Psychotherapeuten und als Angestellte in Deutschland betreffen.

Hinweise auf die jeweiligen §§ der EU-GVO oder des BDSG-neu lasse ich einfachheitshalber weg. Ich will einen kurzen Überblick geben. Dabei geht es nicht um eine Datenschützer-Schulung.

Aspekte, die den *internationalen Datentransfer* betreffen (Bereich von Wirtschaft und Handel) lasse ich dabei außen vor. (z. B. Datentransfer Deutschland/EU – USA: „Safe Harbour“ – war unsicher, stattdessen „Privacy Shield“)

Was sind „personenbezogene Daten“?

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen …
(Namen, Kennnummer, Standortdaten, Online-Kennung, physische, genetische, psychische, kulturelle, soziale Identität usw.)

Schutz der personenbezogenen Daten

Es handelt sich bei den Datenschutz-Grundrechten um einen Unterfall der *„informationellen Selbstbestimmung“*
(s. Volkszählungsurteil des BVG, Dez. 1983, Grundgesetz)

Die *Grundrechte und Freiheiten natürlicher Personen* müssen geschützt werden.

Einschränkungen sind nur zulässig bei überwiegendem Interesse der Allgemeinheit oder Dritter (natürliche oder juristische Person, Behörde …)

Die neue Rechtslage in Deutschland

Anpassung des Bundesdatenschutzgesetzes an die Vorgaben der EU DS-GVO (unter Berücksichtigung diverser Erwägungsgründe und Öffnungsklauseln):

Bundesdatenschutzgesetz-neu (2017)

neue *Datenschutzgesetze der einzelnen Bundesländer*,
z.B. Anpassung des Hessischen Datenschutzgesetzes (April 2018)

Zwecke der Datenverarbeitung (Art. 5 DS-GVO)

Die Datenverarbeitung muss für *festgelegte, eindeutige und legitime Zwecke* erfolgen
Sie muss dem Zweck angemessen und erheblich sein, sowie auf das notwendige Maß beschränkt (*Datenminimierung*)

sie *muss sachlich richtig* und erforderlichenfalls *auf dem neuesten Stand* sein und

Schutz vor unbefugter Verarbeitung, Verlust usw. gewährleisten (*Integrität und Vertraulichkeit*)

Rechtmäßigkeit der DV (Art. 6 DS-GVO)

Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im *öffentlichen Interesse* liegt oder in Ausübung *öffentlicher Gewalt* erfolgt (Art. 1)

(Die Mitgliedsstaaten können bereichsspezifische Regelungen erlassen.)

„**Verarbeitung“ von Daten**

das ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder Vorgangsreihe im Zusammenhang mit personenbezogenen Daten (Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung, Veränderung, Auslesen, Abfragen, Offenlegen durch Übermittlung, Verbreitung , Abgleich, Verknüpfung, Einschränkung, Löschung)

Der „neue“ Datenschutzbeauftragte

Der neue DSB wird nicht mehr nur auf die Beachtung der Datenschutzvorschriften hinweisen müssen.
Er hat einen *Beratungs- und Überwachungsauftrag*, unterliegt der *Rechenschaftspflicht* (Accountability) und er muss seine *Aufgaben risikoorientiert wahrnehmen*.

Es besteht **Bestellpflicht für den DSB**:
- für den *behördlichen DSB* immer
- für *betriebliche DSB*, wenn mindestens 10 Personen (BDSG neu, EU-GVO: „in jedem Fall“) ständig mit der automatisierten Verarbeitung personenbezogener Daten befasst sind.

Benennungspflicht besteht auch (das ist neu) für:

- *den **Verantwortlichen*** für den Datenschutz in der Behörde oder im Unternehmen (z. B. Vorstandsmitglied)

- *und den **Auftragsverarbeiter*** (bei Auftragsdatenverarbeitung)

DS-Beauftragter kann ein Mitarbeiter der Behörde oder des Unternehmens sein, es kann auch ein Externer sein oder auch eine externe juristische Person.

(In Hessen waren als behördliche DSB bisher keine externen Personen vorgesehen, anders als in anderen Bundesländern.)

Persönliche Anforderungen an einen DSB

1. Berufliche Qualifikation
2. Fachwissen auf dem Gebiet des Datenschutzes und der Datenschutzpraxis
3. Fähigkeit zur Erfüllung der genannten Aufgaben
4. Ein hohes Maß an persönlicher Integrität und Berufsethik

Stellung des Datenschutzbeauftragten

Der DSB hat eine unabhängige und aus der Hierarchie herausgehobene Stellung.

Wesentliche Themenkreise sind:

1. Ordnungsgemäße und frühzeitige Einbindung in die anstehenden Aufgaben
2. Erforderliche Ressourcen müssen für ihn bereit gestellt werde
3. Es gilt Weisungsfreiheit und Unabhängigkeit
4. Keine Benachteiligung: Abberufungs- und Kündigungsschutz
5. Unmittelbarer Berichtsweg zur höchsten Führungsebene
6. Anrufungsrecht der Betroffenen
7. Es dürfen keine Interessenkonflikte bestehen
8. Zusammenarbeit mit der Aufsichtsbehörde

Zu den wichtigsten Aufgaben gehören:

Verzeichnis der Verarbeitungstätigkeiten:

a) Namen und Kontaktdaten des Verantwortlichen, seines Vertreters und des DSB

b) die Zwecke der Verarbeitung

c) Beschreibung der Kategorien betr. Personen und der Kategorien personenbezogener Daten

d) die Kategorien von Empfängern …

e) ggf. Übermittlungen an Empfänger in einem Drittland …

f) vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien

g) allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Datenschutz-Folgenabschätzung

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch …

Der Verantwortliche holt bei der Durchführung einer DS-Folgenabschätzung den Rat des DSB ein …

Benennung eines Datenschutzbeauftragten

- wenn die Verarbeitung von einer *Behörde oder öffentlichen Stelle* durchgeführt wird, mit *Ausnahme von Gerichten*, die im Rahmen ihrer justiziellen Tätigkeit handeln
- wenn die *Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters* … bei umfangreichen Verarbeitungstätigkeiten und/oder Erfordernis umfangreicher regelmäßiger und systematischer Überwachung von betroffenen Personen
- wenn die Kerntätigkeit in der *umfangreichen Verarbeitung besonderer Kategorien von Daten gem. Art. 9 DS-GVO)* oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten … besteht.

Aufgaben und Pflichten des Datenschutzbeauftragten

kurzgefasst:

1. Unterrichtung und Beratung
2. Überwachung der Einhaltung des Datenschutzvorschriften
3. Sensibilisierung und Schulung
4. Beratung und Überwachung im Zusammenhang mit der DS-Folgenabschätzung (DSFA)
5. Zusammenarbeit mit der Aufsichtsbehörde
6. Tätigkeit als Anlaufstelle für die Aufsichtsbehörde

Auftragsverarbeiter

Der Auftragsverarbeiter muss hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die ***Verarbeitung im Einklang mit den Anforderungen der GVO*** erfolgt und der ***Schutz der Rechte der betroffenen Personen gewährleistet*** ist.
Die Verarbeitung erfolgt auf der ***Grundlage eines Vertrags*** …
und in dem ***Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung*, die *Art der personenbezogenen Daten*, die *Kategorien betroffener Personen* und die *Pflichten und Rechte des Verantwortlichen*** festgelegt sind.

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Berücksichtigung des ***Stands der Technik***, der *Art des Umfangs*, der ***Umstände und Zwecke der Verarbeitung***, der Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen ***Risiken*** … trifft der Verantwortliche zum Zeitpunkt der Festlegung der Mittel und des Zeitpunkts der Verarbeitung ***geeignete technische und organisatorische Maßnahmen*** (z. B. Pseudonymisierung), die dafür ausgelegt sind, die Datenschutzgrundsätze (z. B. Datenminimierung) wirksam umzusetzen.

Informationspflichten:

- Name und Kontaktdaten des Verantwortlichen

- Kontaktdaten des DSB

- Zwecke der Datenverarbeitung, ggf. Hinweis auf Erforderlichkeiten

- Empfänger(-kategorien)

- Drittlandstransfer …

- Speicherdauer

- Betroffenenrechte

Rechte der betroffenen Person:

- Transparente Information (auch über die Rechte der betroffenen Person)

- Informationspflicht bei Erhebung/Verarbeitung von personenbezogenen Daten bei der betroffenen Person (Datenschutzerklärung)

- Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden.

- Auskunftsrecht der betroffenen Person

- Recht auf Berichtigung

- Recht auf Löschung („Recht auf Vergessenwerden“)

- Recht auf Einschränkung der Verarbeitung

- Widerspruchsrecht

Haftung und Recht auf Schadenersatz, Sanktionen

- Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf *Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter*

- ***Verantwortlicher und Auftragsverarbeiter haften für Schäden bei Verstoß gegen die auferlegten Pflichten …***

- *Befreiung von der Haftung* bei Nachweis, dass Verantwortlicher oder Auftragsverarbeiter in keinerlei Hinsicht für den Umstand durch den der Schaden eingetreten ist, verantwortlich ist.

Die **Einhaltung des Datenschutzes ist unternehmerische Pflicht**, Pflicht des Verantwortlichen und des Auftragsverarbeiters, nicht in erster Linie des DSB. Unternehmen können mit **hohen Bußgeldern** (10 Mio Euro oder 2% des weltweit gesamten Umsatzes) sanktioniert werden.

Behörden und andere öffentliche Stellen sollen in Deutschland nicht mit Bußgeldern belastet werden!

Melde- und Benachrichtigungspflichten bei Datenschutzverstößen

Bei Datenpannen, Verlust von Datenträgern, Missachtung der DS-Vorschriften durch Mitarbeiter ist dies unverzüglich der Aufsichtsbehörde zu melden (innerhalb 72 Stunden). Wenn die Meldung später erfolgt, ist eine Begründung für die Verzögerung erforderlich.
Auch die betr. Person/der betr. Patient ist zu benachrichtigen. Außer, wenn wirksame Gegenmaßnahmen getroffen wurden.

Datenverarbeitung im Beschäftigungskontext

Nach Art. 88 DS-GVO können die Mitgliedsstaaten Rechtsvorschriften oder spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten … vorsehen.

In dem Art. 88 sind auch Vorschriften für Dienstvereinbarungen enthalten.

Datenschutzniveau in Krankenhäusern/Kliniken

Dies ist ein schwieriges Kapitel, vielerorts scheint die Situation im Bereich der automatisierten Patienten-Daten-Verarbeitung zumindest noch deutlich verbesserungsbedürftig. Immer wieder kommt es hier zu ***unbefugten Zugriffen auf die Daten, u. a. auf Patientendaten von Mitarbeitern und von VIPs.***

Berechtigte Zugriffe dürfen nur möglich sein für Personen, die unmittelbar dies zur Aufgabenerfüllung bei der Behandlung der Patienten benötigen. **Krankenhaus-Informations-Systeme (KIS)** sollen der Sicherheit der Patientendaten und der Zugriffs-Kontrolle dienen. Dazu ist ein **angemessenes Rollen- und Berechtigungskonzept** erforderlich**. Zugriffe müssen protokolliert werden.** Dies muss auch kontrolliert werden. So lange keine ausreichenden technischen Möglichkeiten zur Sicherung der Zugriffe gegeben sind, müssen **angemessene organisatorische Maßnahmen** in den Krankenhäusern getroffen werden.

Gesetzliche Änderungen im Bereich der ärztlichen Schweigepflicht

Bisher waren nur die „berufsmäßig tätigen Gehilfen“ der Schweigepflichtigen (Ärzte, Berufsgeheimnisträger) ohne Schweigepflichtentbindung straflos gestellt im Umgang mit Patientendaten.
Ende der letzten Legislaturperiode wurde der **§ 203 StGB (Verletzung von Privatgeheimnissen) neu gefasst**.

Die Weitergabe der Daten an externe Personen, die an der beruflichen oder dienstlichen Tätigkeit der Berufsgeheimnisträger mitwirken, ist danach (§ 203 (3) und (4)) zulässig, z. B. bei Outsourcing an Dienstleister im Gesundheitswesen (Schreibarbeiten, Rechnungswesen, Annahme von Telefonanrufen, Aktenarchivierung, Wartungsarbeiten, Bereitstellung von IT-Anlagen u.ä. – wenn erforderlich).

Ärztliche Schweigepflicht

- **Schweigepflichtentbindung** durch ausdrückliche oder konkludent erteilte ***Einwilligung des Patienten*** (am besten, aber nicht zwingend, schriftlich)

- Entbindung ***bei gesetzlichen Offenbarungspflichten***, z. B. Infektionsschutzgesetz, Krebsregistergesetze, Röntgenverordnung, Strahlenschutzverordnung, gesetzliche Unfallversicherung, Personenstandsgesetz

- ***zahlreiche Offenbarungspflichten aus dem SGB V*****,** z. B. gegenüber KVn, Prüfungsstellen (Wirtschaftlichkeit), Krankenkassen, MDK

- ***weitere Erlaubnisgründe*** (ausnahmsweise Berechtigung)

Datenschutz-Zertifizierungen

Für die Verantwortlichen und die Auftragsverarbeiter bestehen vielfältige Rechenschafts- und Nachweispflichten.
Die Zertifizierung ist eine Möglichkeit des Nachweises der Erfüllung der durch die Ds-GVO geforderten Pflichten.
Die **Zertifizierung ist freiweillig**.
Akkreditierte Zertifizierungsstellen und zuständige Aufsichtsbehörden können die Zertifikate erteilen.
Ein **Zertifikat hat maximal 3 Jahre Gültigkeit** – mit Verlängerungsmöglichkeit, aber auch Widerruf durch die Aufsichtsbehörde.
Große **Auswahl in der Zertifizierungslandschaft**: z. B. Trusted Cloud, DQS Gütesiegel Datenschutz, Standard-Datenschutz-Modell (SDM), DSZ Datenschutz-Zertifizierungsgesellschaft, TÜV.

Hinweise auf DS-Arbeitsmaterialien/Kurzpapiere

zu finden z. B. auf der Website des HDSB: datenschutz-hessen.de

Kurzpapier Nr. 1. Verzeichnis der Verarbeitungstätigkeiten
Kurzpapier Nr. 5. Datenschutz-Folgenabschätzung
Kurzpapier Nr. 6. Auskunftsrecht
Kurzpapier Nr.12. Datenschutzbeauftragte
Kurzpapier Nr.13. Auftragsdatenverarbeitung
Muster Verarbeitungsverzeichnis Auftragsverarbeiter
Muster Verarbeitungsverzeichnis Verantwortlicher

u. a.

Zum Schluss:

Fragen und Probleme bei der Umsetzung der Datenschutzvorgaben?

Diskussion – Fazit ?