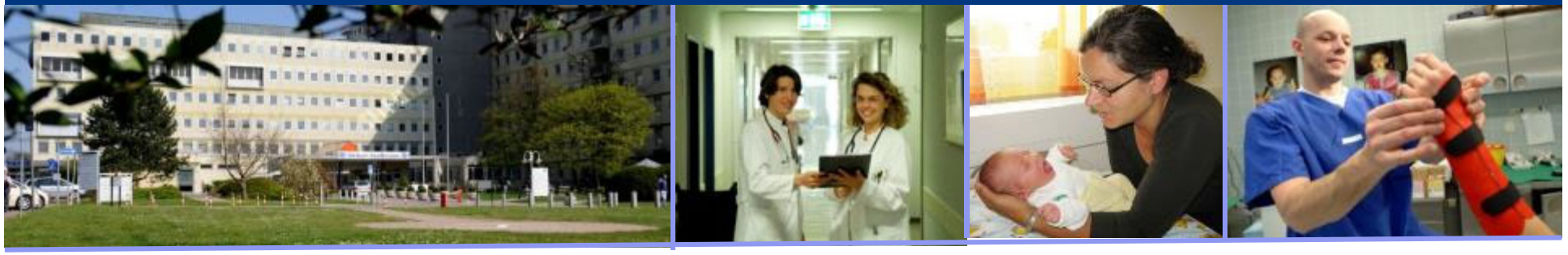
Klinikum Saarbrücken gGmbH
Akademisches Lehrkrankenhaus der Universität des Saarlandes
Ein Unternehmen der Landeshauptstadt Saarbrücken



EU-Datenschutz-Grundverordnung

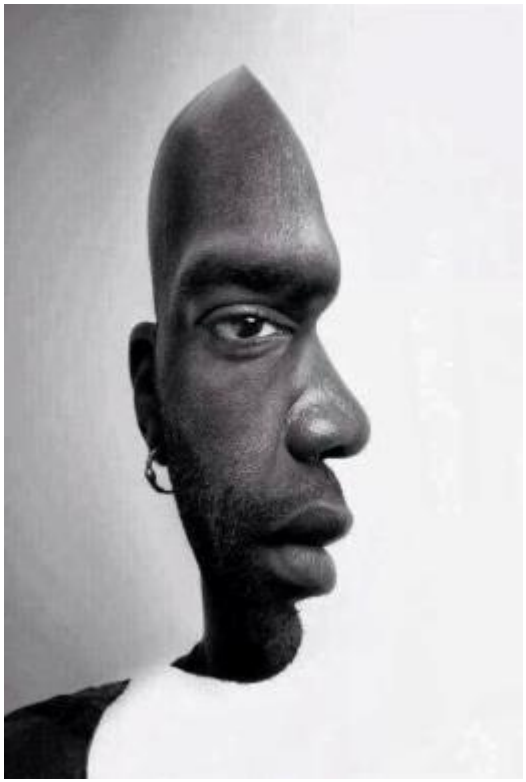
Eine Betrachtung aus Sicht eines Klinikums

Dr. med. Christian Braun M.A.

Geschäftsführer
Ärztlicher Direktor
Klinikum Saarbrücken

5. Saarländischer Medizinrechtstag
01. Dezember 2018
LÄK Saarbrücken

Vorweg zur Erläuterung



Immer wenn Sie dieses Bild sehen ist das der Hinweis, dass hier meine Sichtweise wieder gegeben ist.

Ihre Sicht der Dinge mag vielleicht punktuell eine andere sein.

Ja, sie mag an der ein oder anderen Stelle auch „lobbygefärbt“ und formaljuristisch diskussionswürdig sein, aber mein Auftrag lautet ja, eine Betrachtung aus der Sicht eines Klinikums vorzunehmen.

Um was geht es überhaupt ?

Klinikum Saarbrücken gGmbH
Akademisches Lehrkrankenhaus der Universität des Saarlandes
Ein Unternehmen der Landeshauptstadt Saarbrücken

Mit der Datenschutzgrundverordnung wurden EU-weit geltende einheitliche Datenschutzstandards eingeführt, die den Anforderungen des digitalen Wandels Rechnung tragen und den Schutz des Bürgers, seiner Privatsphäre und seiner persönlichen Daten vor Missbrauch gewährleisten sollen.

Die Verordnung löst die bislang geltende EU-Datenschutzrichtlinie aus dem Jahr 1995 ab, die noch aus den Anfangsjahren des Internets stammt, und von Cloud Computing, Big Data und mobilen Apps noch nicht die Rede war.

Die Richtlinie hatte den Mitgliedsstaaten Spielraum bei der Umsetzung in nationales Recht zugestanden. Diesen Flickenteppich soll die Verordnung beseitigen. Zudem ist die DSGVO – anders als eine Richtlinie – vom Zeitpunkt ihres Inkrafttretens an unmittelbar geltendes Recht innerhalb der EU.

„Alles nichts Neues“ oder besser „nicht alles neu“

Klinikum Saarbrücken gGmbH
Akademisches Lehrkrankenhaus der Universität des Saarlandes
Ein Unternehmen der Landeshauptstadt Saarbrücken

Das Inkrafttreten der DSGVO bedeutet nicht, dass der Datenschutz in Deutschland plötzlich von 0 auf 100 gefahren wird.

Im Gegenteil:

Deutschland hatte schon zuvor mit seinem Bundesdatenschutzgesetz (BDSG), den Landesdatenschutzgesetzen (LDSG) und weiteren Vorschriften wie etwa der beruflichen Schweigepflicht (§ 203 StGB) einen international vorbildlichen Rechtsrahmen in Sachen Datenschutz.

Statt dieser bewährten Vorschriften gilt nun nicht etwa allein die DSGVO – vielmehr mussten und müssen die vorhandenen Gesetze an die neue Datenschutz-Grundverordnung angepasst werden.

„Alles nichts Neues“ oder besser „nicht alles neu“

Klinikum Saarbrücken gGmbH
Akademisches Lehrkrankenhaus der Universität des Saarlandes
Ein Unternehmen der Landeshauptstadt Saarbrücken

Auch das galt schon vor der DSGVO:

- Datenschutz im Krankenhaus steht im engen Zusammenhang mit der ärztlichen Schweigepflicht.

- Die Krankenhäuser haben dafür zu sorgen, dass nicht jeder Beschäftigte auf alle Patientendaten zugreifen kann.

- **Es gilt das Prinzip:**

  Jeder darf nur auf solche Daten zugreifen, die er für seine Aufgaben benötigt.

Einiges ist aber schon neu ….

Klinikum Saarbrücken gGmbH
Akademisches Lehrkrankenhaus der Universität des Saarlandes
Ein Unternehmen der Landeshauptstadt Saarbrücken

Besondere Daten, besonderer Schutz ….

- Datenschutz, und insbesondere wenn es um „besondere Kategorien personenbezogener Daten“ wie Gesundheitsdaten geht, versteht sich generell als

  „Verbot mit Erlaubnisvorbehalt“

  → heißt konkret und ist nicht wirklich neu:

  Einwilligung des Patienten legitimiert die Ausnahme

- **Neu und konkretisiert:**

  Die Einwilligung darf nicht „nebenbei“ erfolgen:

  „Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt“.

  → nachweisbare Dokumentation des expliziten Einverständnisses

Transparenz und Informiertheit

Klinikum Saarbrücken gGmbH
Akademisches Lehrkrankenhaus der Universität des Saarlandes
Ein Unternehmen der Landeshauptstadt Saarbrücken

„Betroffene“ haben Anspruch auf

- eine transparente Darstellung der Verarbeitungsvorgänge in verständlicher Form
- die Erfüllung der bestehenden Informationspflichten über Verarbeitung und Zweck
- Auskunft über die geplante Dauer der Speicherung
- Berichtigung und Löschung („***Recht auf Vergessenwerden***“).
- Auskunft (grundsätzlich unentgeltlich und innerhalb eines Monats)

Jetzt wird´s bürokratisch …

Klinikum Saarbrücken gGmbH
Akademisches Lehrkrankenhaus der Universität des Saarlandes
Ein Unternehmen der Landeshauptstadt Saarbrücken

Krankenhäuser müssen, als verarbeitende Unternehmen kritisch eingestufter Gesundheitsdaten, ein

Verzeichnis aller Verarbeitungstätigkeiten

schriftlich / elektronisch führen und der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

Dies gilt für alle Verfahren mit denen personenbezogene Daten systematisch verarbeitet werden, also auch die Mitarbeiter-, Patienten- und Lieferantendaten.

Das Verzeichnis dient als Grundlage für die Nachweispflichten gegenüber der Aufsichtsbehörde, für die Auskünfte / Informationen an Betroffene, das interne Risikomanagement etc.…

Jetzt wird´s bürokratisch …

Klinikum Saarbrücken gGmbH
Akademisches Lehrkrankenhaus der Universität des Saarlandes
Ein Unternehmen der Landeshauptstadt Saarbrücken

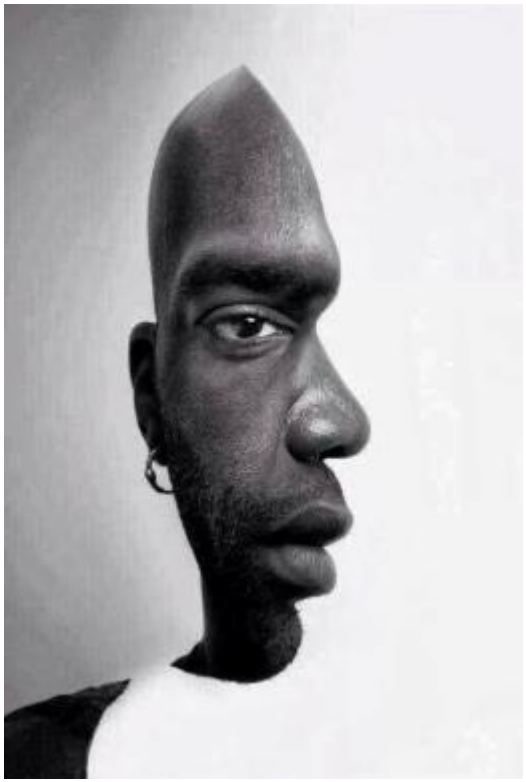
Auf Basis des vorgestellten Verzeichnisses aller Verarbeitungstätigkeiten müssen Krankenhäuser eine

Datenschutz-Folgenabschätzung

vornehmen – und dokumentieren!

Hier müssen vier Fragenbereiche beantwortet werden:

- Welche Datenverarbeitung erfolgt und zu welchen Zwecken?
- Ist sie notwendig und verhältnismäßig?
- Welche Risiken für die Rechte der Betroffenen besteht hierbei?
- Wie werden diese Risiken beherrscht (Schutzmaßnahmen: IT-Sicherheitsprozesse, Berechtigungsmanagement, etc…)?



Der bürokratische Aufwand, beginnend mit dem Verzeichnis aller Verarbeitungstätigkeiten und nicht endend mit der Datenschutz-Folgenabschätzung, ist für die Kliniken enorm.

Schon jetzt ist in vielen Kliniken das vorhandene Personal stark belastet.

Mehr Geld für Personal stehen jedoch nicht in Aussicht.

Auch für den notwendigen Ausbau der Infrastruktur, Grundvoraussetzung für eine praktische Umsetzung der DSGVO in den Krankenhäusern, fehlen die Mittel.

Krankenhausleitung - gefragt und gefordert

Durch den neuen Begriff des „Verantwortlichen“ kommt der Krankenhausleitung eine besondere Verantwortung bei der Umsetzung der DSGVO zu.

Krankenhausleitung - gefragt und gefordert

Die Verantwortung für die Einhaltung der datenschutzrechtlichen Grundlagen liegt bei der Krankenhausleitung:

- Nur diese hat die notwendigen Entscheidungsbefugnisse, um Maßnahmen umzusetzen, Aufgaben festzulegen und zu delegieren.
- Sie hat deshalb klare Regelungen für die Zuständigkeiten und Verantwortlichkeiten aufzustellen und die Mitarbeiter entsprechend dafür zu sensibilisieren.

Es wird schnell teuer …

Wer sich darauf verlässt, dass die Aufsichtsbehörden auf Konsens setzen und man sich – wie bisher – als bußfertiger Sünder exkulpieren kann, der irrt.

- In der Vergangenheit waren Bußgelder bis 50.000 EUR die Regel, und die höheren Summen bis 300.000 EUR die Ausnahme. Die DSGVO geht weit darüber hinaus, bis zu 20 Mio € oder 4% des weltweiten Jahresumsatzes eines Unternehmens

- Nach der DSGVO müssen Verstöße bestraft werden – bisher lag dies im Ermessen der Aufsichtsbehörden.

- Dies Aufsichtsbehörden werden ab jetzt zudem deutlich häufiger von Verstößen erfahren, denn es besteht eine Meldepflicht (binnen 72 h !!), die es unter dem alten BDSG nicht gab.

Die Schonfrist scheint vorbei zu sein ….

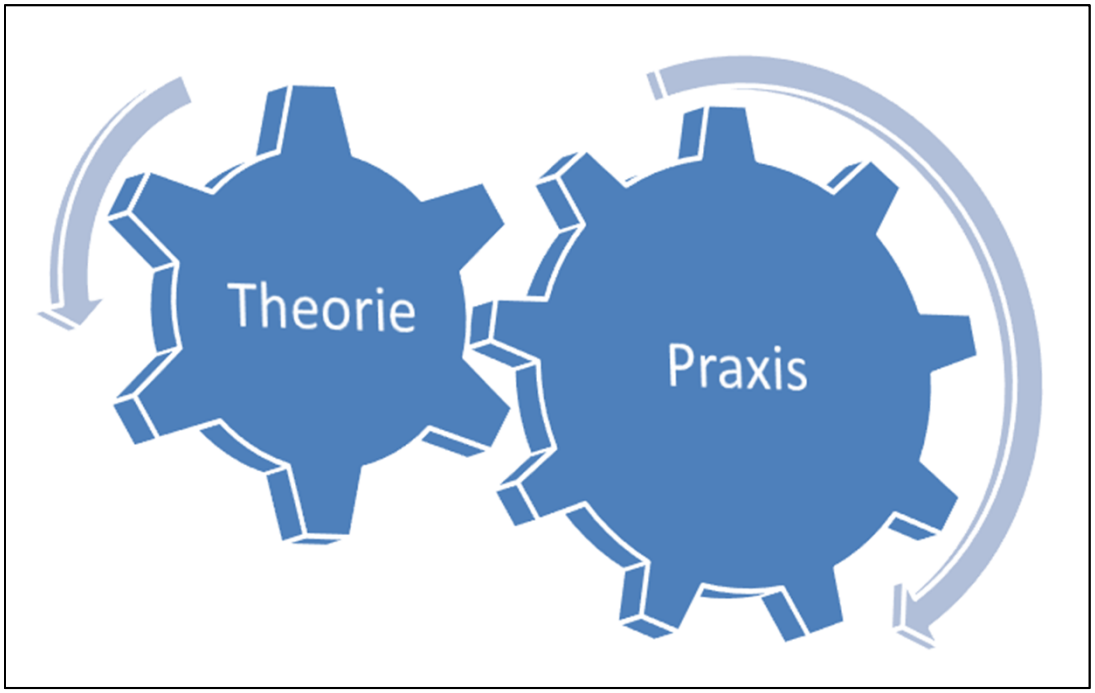
Klinikum Saarbrücken gGmbH
Akademisches Lehrkrankenhaus der Universität des Saarlandes
Ein Unternehmen der Landeshauptstadt Saarbrücken

Mittlerweile machen die Aufsichtsbehörden in ganz Europa ernst und fangen an, Verstöße beim Schutz personenbezogener Daten zu sanktionieren.

Ein portugiesisches Krankenhaus wurde zu einer Strafe von 400.000 Euro verdonnert. Die Einrichtung soll zu vielen Personen Zugriff auf Patientendaten gewährt haben. Dies erfolgte dadurch, dass dreimal so viele Benutzer mit dem Nutzungsprofil „Arzt“ in den Systemen des Krankenhauses geführt worden sind, als ursprünglich freigegeben wurde. Somit fanden Zugriffe auf Gesundheitsdaten statt, die nicht hätten passieren dürfen.

→ Klassische Nichtbeachtung des funktionsgeleiteten Berechtigungskonzepts

Nur solche Personen dürfen organisationsintern auf bestimmte Daten Zugriff haben, die sie bestimmungsgemäß für die Erledigung ihrer Aufgaben benötigen.


Theorie
Praxis

Ist das wirklich alles so gewollt ?

Ist das wirklich alles so gewollt ?

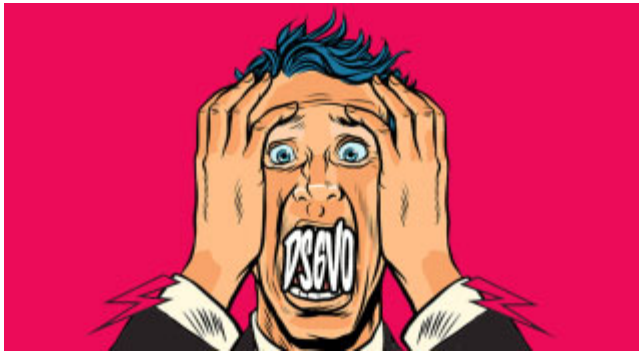
Lassen wir unsere Patienten nun Nummern ziehen, oder fragen wir jeden Patienten, ob wir ihn im Wartebereich mit Namen aufrufen dürfen und lassen uns das vorher schriftlich bestätigen ?

Ich empfehle den Praxistest…..

Ist das wirklich so gemeint ?

Klinikum Saarbrücken gGmbH
Akademisches Lehrkrankenhaus der Universität des Saarlandes
Ein Unternehmen der Landeshauptstadt Saarbrücken

Weil die deutsche Umsetzung der Datenschutz-Grundverordnung die aufwendige Dokumentation von Alltagshandlungen fordert, steht sie – zumindest an vielen Stellen - dem Grundsatz der Datensparsamkeit diametral entgegen.



In der Antike, im Mittelalter und in der frühen Neuzeit wurden Krankheiten oft mit Therapien behandelt, die schädlicher waren als die Krankheit selbst.

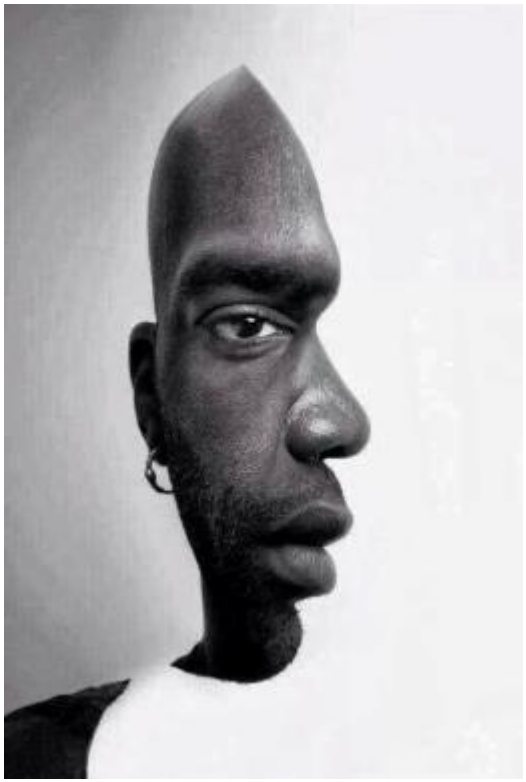
Könnte das – zumindest in Teilen - auch für die DSGVO gelten…. ?

Viel hilft viel - Hilft viel wirklich viel ?

Mehr Paragraphen zum Datenschutz

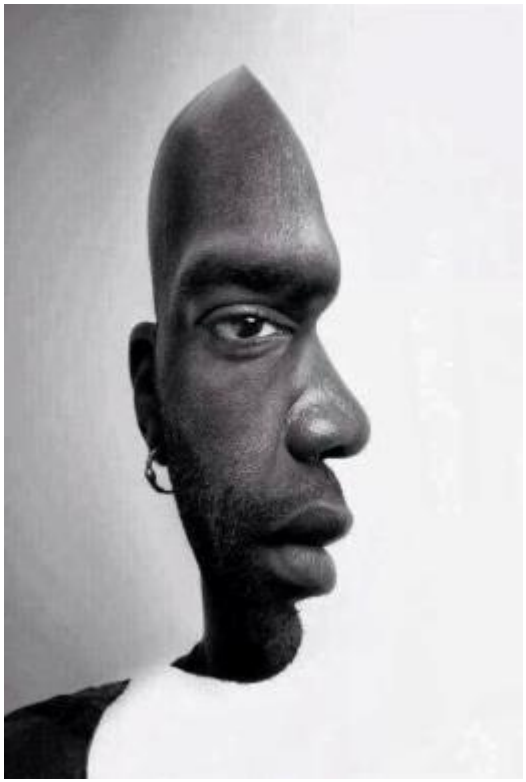
bewirken nicht zwangsläufig mehr Datenschutz!

- Kleinteiligkeit führt leicht zu einer Überregulierung
- Zu viele Pflichten bergen die Gefahr, dass diese in der Praxis nicht beachtet werden, und damit die Legitimität des Rechts insgesamt untergraben wird.
- Das hehre Ziel, Europas Bürgern die Hoheit über ihre Daten zurückgeben stets im Blick, steht doch der Nutzen in einem zumindest fragwürdigen Verhältnis zum Aufwand der Datenschutz-Grundverordnung.



Datenschutz ist gut, wichtig und richtig.

Die DSGVO geht aber an vielen Stellen weit darüber hinaus und legt ein starres Verfahren fest, das in hohem Maße Arbeitskraft und Finanzmittel in Krankenhäusern bindet, die dringend für die eigentliche Behandlung und Betreuung von Patienten gebraucht wird.



Die Klagelieder hinsichtlich einer „gesetzlich verordneten bürokratischen Überregulierung“ der DSGVO, die uns „so lähmt wie viele kleine Fesseln den Riesen Gulliver lahm gelegt haben“, sind nachvollziehbar.

Gleichwohl ruft die Gesellschaft aber ständig nach neuen Schutzrechten und noch perfekteren sozialen Sicherungssystemen, die dem Bürokratieaufbau unweigerlich Vorschub leisten ….

Danke für Ihre Aufmerksamkeit