
gmds
Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

# DIE EU DS-GVO – ALLES BLEIBT WIE ES IST …?

DR. BERND SCHÜTZE

T · · ·

HEALTHCARE SOLUTIONS

# DR. BERND SCHÜTZE

## Studium

- Studium Informatik (FH-Dortmund)
- Studium Humanmedizin (Uni Düsseldorf / Uni Witten/Herdecke)
- Studium Jura (Fern-Uni Hagen)

## Zusatz-Ausbildung

- Zusatzausbildung Datenschutzbeauftragter (Ulmer Akademie für Datenschutz und IT-Sicherheit)
- Zusatzausbildung Datenschutz-Auditor (TüV Süd)
- Zusatzausbildung Medizin-Produkte-Integrator (VDE Prüf- und Zertifizierungsinstitut)

## Berufserfahrung

- 10 Jahre klinische Erfahrung
- 20 Jahre IT im Krankenhäusern
- 20 Jahre Datenschutz im Gesundheitswesen

## Mitarbeit in wiss. Fachgesellschaften

- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)
- Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)
- Gesellschaft für Informatik (GI)

## Mitarbeit in Verbänden

- Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD)
- Berufsverband Medizinischer Informatiker e.V. (BVMI)
- Fachverband Biomedizinische Technik e.V. (fbmt)
- HL7 Deutschland e.V.

# ERGEBNISSE UNSERER AG

- Synopse
- Handreichung zum Umgang mit der DS-GVO (Handlungsempfehlung
- Tätigkeitsverzeichnis
- Einwilligung

# SYNOPSE

# EU DS-GVO VS. DT. RECHT

- **EU DS-GVO vorangig vor deutschem Recht anzuwenden**
- **EU DS-GVO existiert in allen Sprachen der EU**
- **Z.T. fehlerbehaftet:**
  1. Übersetzung nicht immer gut
  2. Beim Übertragen Fehler passiert
     Beispiel: Art. 20 Abs. 4:

| | |
|---|---|
| (4) | Das Recht gemäß Absatz 2 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. |

| | |
|---|---|
| 4. | The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others. |

# VORGEHEN BEI SYNOPSE

- **Synopse soll Herausarbeitung der Änderungen vom jetzigen Recht zum nachfolgenden Recht erleichtern**
- **Jetziges Recht**
  1. Deutsches Recht = BDSG
  2. EU Recht = EU Richtlinie 95/46/EG
- **Bei Interpretation der DS-GVO unbedingt zu berücksichtigen: Erwägungsgrüne**
- **Daher Gegenüberstellung BDSG, RL 95/46/EG und EU DS-GVO (dt., engl.) inkl. Erwägungsgründe**

# SYNOPSE
## (VERÖFFENTLICHT 2016-04-24)

### Kapitel I - Allgemeine Bestimmungen
(Chapter I - General Provisions)

| Richtlinie 95/46/EG | General Data Protection Regulation (GDPR) | DS-GVO | BDSG / Deutsches Recht | Erwägungsgründe |
|---|---|---|---|---|
| **Artikel 1 Gegenstand der Richtlinie** | **Article 1 Subject-matter and objectives** | **Art. 1 Gegenstand und Ziele** | | |
| Art. 1:<br>1) Die Mitgliedstaaten gewährleisten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten.<br>2) (2) Die Mitgliedstaaten beschränken oder untersagen nicht den freien Verkehr personenbezogener Daten zwischen Mitgliedstaaten aus Gründen des gemäß Absatz 1 gewährleisteten Schutzes. | Art. 1:<br>1) This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.<br>2) This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.<br>3) The free movement of personal data within the Union shall be neither restricted norprohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. | Art. 1:<br>1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.<br>2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.<br>3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden. | §1 Abs. 1 BDSG<br>(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. | 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 13 |
| **Artikel 3 Anwendungsbereich** | **Article 2 Material scope** | **Art. 2 Sachlicher Anwendungsbereich** | | |
| Art. 3:<br>1) Diese Richtlinie gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen.<br>2) Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten,<br>– die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich;<br>– die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird. | Art. 2:<br>1) This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.<br>2) This Regulation does not apply to the processing of personal data:<br>a) in the course of an activity which falls outside the scope of Union law;<br>b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;<br>c) by a natural person in the course of a purely personal or household activity;<br>d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.<br>3) For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.<br>4) This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. | Art. 2:<br>1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.<br>2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten<br>a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,<br>b) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,<br>c) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,<br>d) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.<br>3) Für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union gilt die Verordnung (EG) Nr. 45/2001. Die Verordnung (EG) Nr. 45/2001 und sonstige Rechtsakte der Union, die diese Verarbeitung personenbezogener Daten regeln, werden im Einklang mit Artikel 98 an die Grundsätze und Vorschriften der vorliegenden Verordnung angepasst.<br>4) Die vorliegende Verordnung lässt die Anwendung der Richtlinie 2000/31/EG und speziell die Vorschriften der Artikel 12 bis 15 dieser Richtlinie zur Verantwortlichkeit der Vermittler unberührt. | §1 Abs. 2,3,5 BDSG<br>2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch<br>1. öffentliche Stellen des Bundes,<br>2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie<br>a) Bundesrecht ausführen oder<br>b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,<br>3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.<br>3) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.<br>5) Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Soweit die verantwortliche Stelle nach diesem Gesetz zu nennen ist, sind auch Angaben über im Inland ansässige Vertreter zu machen. Die Sätze 2 und 3 gelten nicht, sofern Datenträger nur zum Zweck des Transits durch das | 14, 15, 16, 17, 18, 19, 20 ,21 |

# UMSETZUNGSEMPFEHLUNG

# MOTIVATION

- EU DS-GVO ändert deutsches Datenschutzrecht
- Grundsätze (Zweckbindung, Datenminimierung usw.) bleiben zwar erhalten, aber die Regelungen unterscheiden sich z.T. deutlich vom deutschen Recht
- Daher:

Gemeinsame Empfehlung bzgl. des Umgangs mit der EU Datenschutz-Grundverordnung (DS-GVO) im Gesundheitswesen

Eine Zusammenarbeit von

Bundesverband Gesundheits-IT e. V.
Arbeitsgruppe Datenschutz

bvitg
Bundesverband Gesundheits-IT

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen"

gmds

Seite 1 von 80

# HANDLUNGSEMPFEHLUNG
## (VERÖFFENTLICHT 2016-07-01)

- EU DS-GVO ändert deutsches Datenschutzrecht
- Grundsätze (Zweckbindung, Datenminimierung usw.) bleiben zwar erhalten, aber die Regelungen unterscheiden sich z.T. deutlich vom deutschen Recht
- Daher:

Gemeinsame Empfehlung bzgl. des Umgangs mit der EU Datenschutz-Grundverordnung (DS-GVO) im Gesundheitswesen

Eine Zusammenarbeit von

Bundesverband Gesundheits-IT e. V.
Arbeitsgruppe Datenschutz

bvitg
Bundesverband Gesundheits-IT

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen"

gmds

Seite 1 von 80

# HANDLUNGSEMPFEHLUNG: INHALTE

- **Allgemeines**
  - Z.B. wie interpretiere ich die DS-GVO
- **Geltungsbereich**
- **Erläuterungen zu Begrifflichkeiten**
  - Z.B. Personenbezug, Gesundheitsdaten, Öffentliches Interesse
- **Rechtsgrundlage für Verarbeitung**
  - U.a. Rahmenbedingungen aus Art. 5, Regelungen Art. 9
- **Betroffenenrechte**
  - Heraushebung Änderungen vorhandener Rechte
  - Darstellung der neuen Rechte
- **Datenverarbeitung im Unternehmen**
- **Datenschutzbeauftragter**
- **Forschung**
- **Sanktionen**

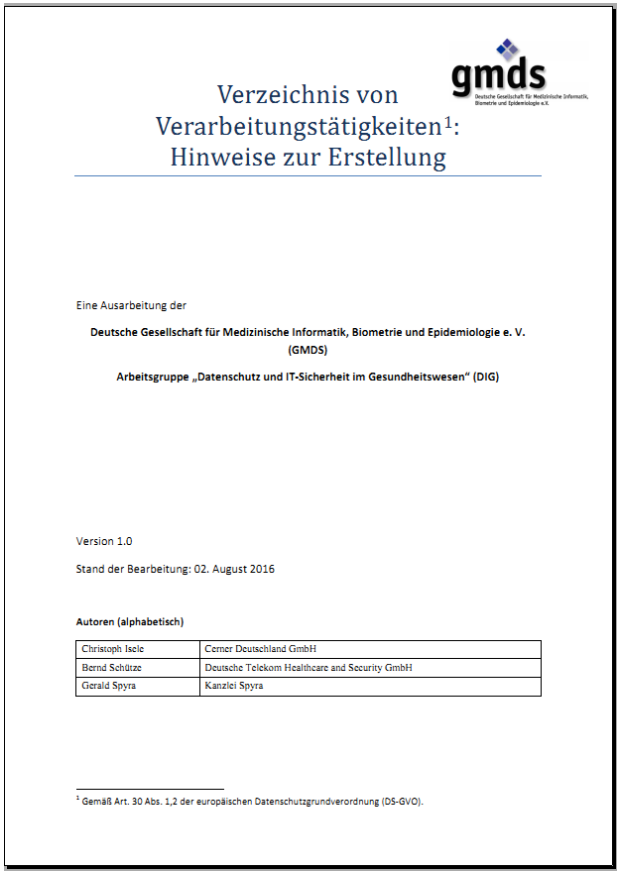
# TÄTIGKEITSVERZEICHNIS

# MOTIVATION

- **EU DS-GVO kennt Verfahrensverzeichnis nicht**
- **EU DS-GVO verlangt „Verzeichnis der Verarbeitungstätigkeiten“**
- **Dabei**
  - Vorgaben für (Mindest) Inhalte nur z.T. mit Inhalten Verfahrensverzeichnis identisch
  - DS-GVO kennt die Ausnahmetatbestände des BDSG für Verfahrensverzeichnis nicht, daher umfangreicher bzgl. „welche Tätigkeiten sind zu dokumentieren“
  - Sanktionen, wenn Tätigkeitsverzeichnis nicht vorhanden, deutlich härter als beim BDSG (BDSG nicht bußgeldbewährt, DS-GVO Bußgeld bis zu 10 Mill. Euro)

# HINWEISE ZUR ERSTELLUNG TÄTIGKEITSVERZEICHNIS
## (VERÖFFENTLICHT 2016-08-02)

- **Darstellung der Anforderungen von Art. 30 DS-GVO**
  - Z.B. Hinweise zur Interpretation von Begrifflichkeiten
- **Aufbau, Struktur des Verzeichnisses für Verantwortlichen und Auftragsverarbeiter**



Verzeichnis von Verarbeitungstätigkeiten[1]: Hinweise zur Erstellung

gmds
Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Eine Ausarbeitung der

**Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)**

**Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen" (DIG)**

Version 1.0

Stand der Bearbeitung: 02. August 2016

**Autoren (alphabetisch)**

| | |
|---|---|
| Christoph Isele | Cerner Deutschland GmbH |
| Bernd Schütze | Deutsche Telekom Healthcare and Security GmbH |
| Gerald Spyra | Kanzlei Spyra |

[1] Gemäß Art. 30 Abs. 1,2 der europäischen Datenschutzgrundverordnung (DS-GVO).

# EINWILLIGUNG

# MOTIVATION

**Wozu brauchen wir eine Einwilligung?**

- **Zur Behandlung des Patienten wird keine Einwilligung benötigt; Rechtsgrundlage ist der Behandlungsvertrag**
- **Einwilligung wird benötigt z.B. für**
  - Erhebung aktueller Gesundheitsstatus eines Patienten bei Dritten, z.B. Hausarzt
  - Externe Qualitätssicherung ohne gesetzliche Grundlage mit Einsichtnahme in Behandlungsdaten
    (Z.B. Onkozert, Deutschen Onkologie Centrum oder ISO 9001-Audits)
  - Übermittlung an Krankheitsregister ohne gesetzliche Grundlage
    (Z.B. MDS-Register)
  - Weitergabe von Patientendaten zu (externen) Forschungszwecken
  - Teilnahme von Patienten an Studien
  - Privatärztliche Abrechnung
  - ...

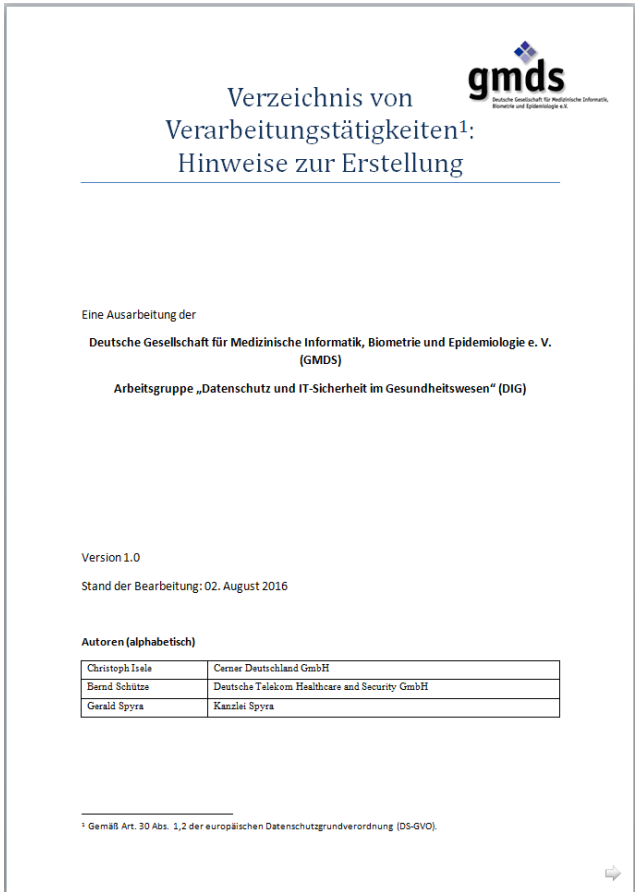
# EINWILLIGUNG

- **„Übergangsregelung“ Erwägungsgrund 171**
  - Beruhen die Verarbeitungen auf einer Einwilligung gemäß der Richtlinie 95/46/EG, so ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen dieser Verordnung entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der vorliegenden Verordnung fortsetzen kann.
  - Auf der Richtlinie 95/46/EG beruhende Entscheidungen bzw. Beschlüsse der Kommission und Genehmigungen der Aufsichtsbehörden bleiben in Kraft, bis sie geändert, ersetzt oder aufgehoben werden.
- **D.h. heute gegebene Einwilligungen, welche die Vorgaben der DS-GVO berücksichtigen, gelten für die Zukunft. Z.B. wichtig für**
  - Nachsorge in der Onkologie
  - Krankheitsregister, die nicht gesetzlich geregelt sind
  - Forschungsvorhaben

⇒ **Einwilligungen sind ab dem 25. Mai 2018 nur gültige Rechtsgrundlage für Datenverarbeitung, wenn sie den Anforderungen der DS-GVO entsprechen**

# HINWEISE ZUR ANPASSUNG EINWILLIGUNGEN
## (VERÖFFENTLICHT 2016-08-02)

- **Darstellung der Anforderungen der DS-GVO bzgl. Einwilligung**
  - Hinweis auf Besinderheit bei Kindern bzgl. Einwilligung in „Dienste der Informationsgesellschaft“
- **Checkliste zur Überprüfung von Einwilligungen**



Verzeichnis von Verarbeitungstätigkeiten[1]: Hinweise zur Erstellung

Eine Ausarbeitung der

**Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)**

**Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)**

Version 1.0

Stand der Bearbeitung: 02. August 2016

**Autoren (alphabetisch)**

| | |
|---|---|
| Christoph Isele | Cerner Deutschland GmbH |
| Bernd Schütze | Deutsche Telekom Healthcare and Security GmbH |
| Gerald Spyra | Kanzlei Spyra |

[1] Gemäß Art. 30 Abs. 1,2 der europäischen Datenschutzgrundverordnung (DS-GVO).