59. Jahrestagung der Südwestdeutschen Gesellschaft für Urologie e.V.

Messe Offenburg-Ortenau Offenburg

06. - 09. Juni 2018

Der Übergang von BDSG zu EU-DSGVO + BDSG „neu“

Bisherige gesetzliche Regelungen

bisher

- Richtlinie 95/46/EG
- Bundesdatenschutzgesetz
- Landesdatenschutzgesetze
- Kirchliche Datenschutzgesetze
- Strafgesetzbuch
- Bürgerliches Gesetzbuch
- Sozialgesetzbuch
- Berufsordnung
- Röntgenverordnung
- weitere

Bisherige gesetzliche Regelungen

Zweck Richtlinie 95/46/EG

„…Die Datenverarbeitungssysteme stehen im Dienste des Menschen; sie haben, ungeachtet der Staatsangehörigkeit oder des Wohnorts der natürlichen Personen, deren Grundrechte und -freiheiten und insbesondere deren Privatsphäre zu achten…“

Bisherige gesetzliche Regelungen

Rechtsnatur

Als europäische Richtlinie ist sie unverbindlich.

Bisherige gesetzliche Regelungen

Zweck Bundesdatenschutzgesetz

„…Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird…“

Bisherige gesetzliche Regelungen

Rechtsnatur BDSG

- Als Bundesgesetz verbindlich innerhalb der BRD.
- Unterwirft sich anderen deutschen Gesetzen
- Unterwirft sich europäischen Verordnungen

„…Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor…“

Bisherige gesetzliche Regelungen

Aufbau BDSG

- Unterscheidung zwischen öffentlichen und nichtöffentlichen Stellen.
- Unterteilt in Abschnitte, Unterabschnitte und Paragraphen.

Bisherige gesetzliche Regelungen

Inhalt BDSG

- z. B.
- Zweck und Anwendungsbereich
- Datenvermeidung und Datensparsamkeit
- Beauftragter für den Datenschutz
- Verantwortung Verarbeiter
- Rechte Betroffener
- Technische und organisatorische Maßnahmen
- …

Bisherige gesetzliche Regelungen

Weitere Datenschutzgesetze

z. B.
- Landesdatenschutzgesetze
- Kirchliche Datenschutzgesetze

aber auch
- Strafgesetzbuch
- Bürgerliches Gesetzbuch
- …

Neue rechtliche Situation

Die EU-DSGVO

Am 25. Mai 2018 geht die EU-DSGVO nach einer zweijährigen Übergangsfrist in nationales Recht über.

Neue rechtliche Situation

Zweck DSGVO

„…Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personen-bezogener Daten…“

Neue rechtliche Situation

Rechtsnatur DSGVO

Als europäische Verordnung ist sie verbindlich.

Neue rechtliche Situation

Aufbau DSGVO

- Kapitel
- Artikel
- Erwägungsgründe

aber auch Working Paper der Artikel 29 Gruppe

Neue rechtliche Situation

Inhalt DSGVO

z. B.

- Gegenstand, Ziele, Anwendungsbereich
- Grundsätze und Rechtmäßigkeit für die Verarbeitung
- Transparenz
- Informationspflicht
- Rechenschaftspflicht
- Öffnungsklauseln

Neue rechtliche Situation

BDSG „neu“

- Zweck und Rechtsnatur wie bisher.
- Nun nur noch für den öffentlichen Bereich.

!!! Aber § 26 für Beschäftigtenverhältnisse !!!

Vergleich gesetzliche Regelungen

Auszug BDSG und DSGVO

Zweck	§ 1	Art. 1 Abs. 2
Anwendungsbereich	§ 1	Art. 2, 3
Begriffsbestimmungen	§ 3	Art. 4
Grundsätze	§ 3a	Art. 5
Verbot mit Erlaubnisvorbehalt	§ 4 Abs. 1	Art. 6
Infopflichten (Erheb. b. Betr.)	§ 4 Abs. 3	Art. 13
Einwilligung	§ 4a	Art. 7, 8

Vergleich gesetzliche Regelungen

Auszug BDSG und DSGVO

Datenschutzbeauftragter	§ 4f	Art. 37, 39
Rechte Betroffener	§ 6	Art. 12 bis 23
Techn. orga. Maßnahmen	§ 9+Anlage	Art. 24, 25, 32
Auftragsdatenverarbeitung	§ 11	Art. 28, 29, 30, 31, 32, 33
Benachrichtigung	§ 33	Art. 13, 14
Auskunft	§ 34	Art. 15
Berichtig., Lösch., Sperrung,…	§ 35	Art. 16, 17, 18, 19, 21

Wichtige Inhalte DSGVO

Anwendungsbereich – Art. 2

„…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…“

Wichtige Inhalte DSGVO

Begriffsbestimmungen – Art. 4

…„personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen;…

…„Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;…

Wichtige Inhalte DSGVO

Grundsätze – Art. 5

... auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);…

…Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“)…

Verbot m. Erlaubnisvorb. – Art. 6

…die betroffene Person hat ihre Einwilligung…für einen oder mehrere bestimmte Zwecke gegeben;…

…die Verarbeitung ist für die Erfüllung eines Vertrags…vorvertraglicher Maßnahmen erforderlich…

…die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;…

Verbot m. Erlaubnisvorb. – Art. 6

…die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;…

…die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen…sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person…überwiegen…

Einwilligung – Art. 7

…Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat…

…Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt…

Besondere Kategorien – Art. 9

Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

Absatz 1 gilt nicht in folgenden Fällen:…

Infopflichten – Art. 13

Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

Infopflichten – Art. 13

- Daten des Verantwortlichen
- Daten Datenschutzbeauftragter
- Zwecke der Verarbeitung
- Rechtsgrundlage der Verarbeitung
- ggfls. das berechtigte Interesse
- Empfänger oder Kategorien von Empfängern
- ggfls. Übermittlung an Drittland
- Aufbewahrungsfristen
- Recht Auskunft, Berichtigung, Löschung, Einschränkung
- Recht Widerruf und Beschwerde bei der Aufsichtsbehörde
- ob gestzl. oder vertragl. vorgeschrieben
- ob freiwillig und mit welchen Folgen…

Benennung DSB – Art. 37

Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn

…die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird,…

…die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung…

Benennung DSB – Art. 37

Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn

…die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder…

Aufgaben DSB – Art. 39

…Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten…

…Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften…

…Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;…

Aufgaben DSB – Art. 39

…Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung…

…Zusammenarbeit mit der Aufsichtsbehörde;…

Rechte Betroffener – Art. 12 bis 23

- Transparente Information
- Informationspflicht bei Erhebung beim Betroffenen
- Informationspflicht bei Erhebung nicht beim Betroffenen
- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung
- Recht auf Einschränkung
- Mitteilungspflicht
- Recht auf Datenübertragbarkeit
- Recht auf Widerspruch
- Automatisierte Entscheidung
- Beschränkungen

Verantwortung Verarbeit. – Art. 24

Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.

Technikgestaltung – Art. 25

Unter Berücksichtigung des Stands der Technik,… trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen…

Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden…

Sicherheit Verarbeit. – Art. 32

…diese Maßnahmen schließen unter anderem Folgendes ein:

…die Pseudonymisierung und Verschlüsselung…
…die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit…
…die Verfügbarkeit…rasch wiederherzustellen…
…ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Auftragsverarbeiter – Art. 28

Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet…

Auftragsverarbeiter – Art. 28

Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter…

Verzeichnis Verarbeitung – Art. 30

Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten…

- Name und Kontaktdaten Verantwortlicher
- Datenschutzbeauftragter
- Zwecke der Verarbeitung
- Rechtsgrundlage
- Beschreibung Kategorien personenbezogener Daten
- Kategorien von Empfängern
- Übermittlung Drittstaaten
- Aufbewahrungsfristen
- Allgemeine Beschreibung techn. organ. Maßnahmen

Umsetzung im Unternehmen

- Der Verantwortliche bekennt sich zur Umsetzung der Rechtsvorschriften – Datenschutz ist Chefsache!
- Benennung eines qualifizierten Datenschutzbeauftragten
- Bestandsanalyse
- Unterweisung der Mitarbeiter
- Beschreibung und Einführung techn. organ. Maßnahmen
  - Zutrittskontrolle
  - Zugangskontrolle
  - Zugriffskontrolle
  - Weitergabekontrolle
  - Eingabekontrolle
  - Auftragskontrolle
  - Verfügbarkeitskontrolle

Umsetzung im Unternehmen

- Sammlung Zwecke der Verarbeitung
- Sammlung Rechtsgrundlagen für die Verarbeitung
- Sammlung Auftragsverarbeiter
- Erstellung Verzeichnis Verarbeitungstätigkeiten
- Erstellung Beschreibung Verarbeitungstätigkeiten
- Erstellung Verzeichnis Auftragsverarbeiter
- Erstellung Verträge mit Auftragsverarbeiter
- Erstellung Software- und Hardwarekatalog
- Regelmäßige Pflege Datenschutzhandbuch
- Ständige Überprüfung des Datenschutzmanagement

Verzeichnis Verfahren

Allgemeine Angaben zum Verfahren	
Bezeichnung des Verfahrens	Daten an Unternehmensberater
Für dieses Verfahren verwendete Software	
Verantwortlicher für die Verfahrensbeschreibung *Name, Abteilung, Telefon, E-Mail*	
Verfahrensmeldung erstellt am	
Telefonnummer für Rückfragen	

Verzeichnis Verfahren

Angaben zur verantwortlichen Stelle	
Name oder Firma der verantwortlichen Stelle BDSG, DSGVO	
Namen der Inhaber, der Vorstände, der Geschäftsführer oder der berufenen Leiter der verantwortlichen Stelle BDSG	
Anschrift der verantwortlichen Stelle BDSG, DSGVO	
Bei verantwortlicher Stelle in Drittland: Im Inland ansässiger Vertreter BDSG	
E-Mail-Adresse der verantwortlichen Stelle DSGVO	
Telefonnummer der verantwortlichen Stelle DSGVO	
Name des gemeinsam Verantwortlichen DSGVO	
Anschrift des gemeinsam Verantwortlichen DSGVO	
E-Mail-Adresse des gemeinsam Verantwortlichen DSGVO	
Telefonnummer des gemeinsam Verantwortlichen DSGVO	

Verzeichnis Verfahren

Name des Vertreters des Verantwortlichen DSGVO	
Anschrift des Vertreters des Verantwortlichen DSGVO	
E-Mail-Adresse des Vertreters des Verantwortlichen DSGVO	
Telefonnummer des Vertreters des Verantwortlichen DSGVO	
Leiter der Datenverarbeitung BDSG	
Name des Datenschutzbeauftragten DSGVO	
Anschrift des Datenschutzbeauftragten DSGVO	
E-Mail-Adresse des Datenschutzbeauftragten DSGVO	
Telefonnummer des Datenschutzbeauftragten DSGVO	
Bei verantwortlicher Stelle in Drittland: Im Inland ansässiger Vertreter	

Verzeichnis Verfahren

Angaben zum Verfahren	
Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung BDSG, DSGVO Warum und wozu werden die Daten verarbeitet?	Erfüllung des vertraglich vereinbarten Beratungsziels. Das vereinbarte Beratungsziel ist:
Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien BDSG, DSGVO Bitte für jede Personengruppe die zugehörigen Daten/Datenkategorien angeben	
Personengruppe BDSG, DSGVO	Daten/Datenkategorie BDSG, DSGVO
Management, Mitarbeiter, Praktikanten, Bewerber, Kunden, Interessenten, Lieferanten, Handwerker, Behörden, Dienstleister sowie deren Ansprechpartner	Name, Vorname, Adressdaten, Kontaktdaten, Gehaltsdaten, Alter, Umsatzzahlen
Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können BDSG, DSGVO	Externe Unternehmensberater

Verzeichnis Verfahren

Empfänger in Drittländern DSGVO	
Empfänger in internationalen Organisationen DSGVO	
Regelfristen für die Löschung von Daten BDSG, DSGVO	10 Jahre – Jahresabschlüsse, Eröffnungsbilanzen, Handels- und Geschäftsbücher, Aufzeichnungen, Arbeitsanweisungen, Organisationsunterlagen, Rechnungen 6 Jahre – Handels- und Geschäftsbriefe sowie für sonstige Unterlagen (HGB; BGB), Buchungsbelege (HGB, AO, EStG, KStG, GewSTG, UStG, AktG, GmbHG, GenG) 4 Jahre – Überprüfung gemäß § 35 Abs. 2 Nr. 4 BDSG
Datenübermittlung in Drittstaaten geplant oder im Gange BDSG, DSGVO	ja nein
Zweck der Datenübermittlung	
Daten/Datenkategorie	
Drittland DSGVO	

Datenübermittlung an eine internationale Organisation DSGVO	ja	nein
Zweck der Datenübermittlung		
Daten/Datenkategorie		
Internat. Organisation DSGVO		
Datenübermittlung gem. Art. 49 Abs. 1 Unterabsatz 2 DSGVO	ja	nein
Dokumentation geeigneter Garantien DSGVO		
Technische und organisatorische Maßnahmen		
Die Maßnahmen entsprechen den allgemeinen technischen und organisatorischen Maßnahmen BDSG, DSGVO Die Beschreibung der allgemeinen TOMs erfolgt in einem separaten Dokument	ja	nein
Es sind für dieses Verfahren folgende abweichende/zusätzliche Maßnahmen getroffen: BDSG, DSGVO		

Zugriffsberechtigte Personen oder Personengruppen je Datenart oder Datenkategorie und deren Zugriffsrecht BDSG, DSGVO

V = Vollzugriff (beinhaltet Recht zur Berechtigungsvergabe), L = nur lesend, LS = lesend und schreibend

Datenart/Datenkategorie BDSG, DSGVO	Zugriffsberechtigte Personen(gruppe) BDSG, DSGVO	Zugriffsrecht BDSG, DSGVO

Take Home Message

- Einwilligung des Patienten
- Information zur Datenerhebung
- Verzeichnis Verfahren
- Verträge Auftragsverarbeitung
- Techn. org. Maßnahmen TOMs
- Datenschutzbeauftragter
- Verpflichtung Datengeheimnis

Ihr Datenschutzbeauftragter

Achim Wolf
Dr.-Rudolf-Eberle-Straße 8-10
76534 Baden-Baden

Telefon: +49-7223-9669-323
Fax: +49-7223-9669-6323
Mobil: +49-175-4335-701

Mail: a.wolf@be-imaging.de

Eine Dienstleistung der b.e.consult GmbH