Datenschutzgrundverordnung

Norbert Jirak ISDS 2018
norbert.jirak@p-k-p.at

Take Home Message

Datenschutzgrundverordung

betrifft

JEDE(N)

DSGVO

- **Neu?**
  - **die DSGVO ist am 24.5.2016 in Kraft getreten und wurde nach einer zweijährigen Übergangsfrist am 25.5.2018 unmittelbar anwendbares Recht in der EU**

DSGVO

- **Neu?**

  In Österreich gibt es (bisher weitgehend unbeachtet) das

  – **Datenschutzgesetz 2000**

  und das

  – **Gesundheitstelematikgesetz von 2012**

DSGVO

- **Neu?**

  bisher waren die „Datenanwendungen“ meldepflichtig, aber in der „Standard- und Muster-Verordnung 2004“ waren Ausnahmen definiert

DSGVO

- **Neu?**

  „§ 1. (1) Die in Anlage 1 enthaltenen Datenanwendungen gelten als nicht meldepflichtige Standardanwendungen im Sinne des § 17 Abs. 2 Z 6 DSG 2000.“

DSGVO

SA001 Rechnungswesen und Logistik

SA002 Personalverwaltung für Dienstverhältnisse

SA022 Kundenbetreuung und Marketing für eigene Zwecke

SA024 Patienten-/Klientenverwaltung und Honorarabrechnung der Gesundheitsdiensteanbieter

SA026 Verrechnung ärztlicher Verschreibungen …. durch Apotheken

SA027 Verrechnung ärztlich verordneter Heilbehelfe …

SA028 Verrechnung ärztlich verordneter Behandlungen ….

DSGVO

- **Neu!**

  Auch wenn sie nichts Anderes machen, als in diesen Standardanwendungen definiert ist, müssen sie ihre „Datenanwendungen“ jetzt dokumentieren.

DSGVO

- **Neu!**
  - **Das Datenschutz-Anpassungsgesetz 2018, trat mit 25. Mai 2018 in Kraft (parallel zum In-Geltung-Treten der EU-Datenschutz-Grundverordnung - DSGVO).**
  - **Verpflichtung zur Erstattung von DVR-Meldungen an die Datenschutzbehörde entfällt**
  - **Dokumentationspflicht**

DSGVO

Herzstück der Dokumentation zur DSGVO

- **Verzeichnis der Verarbeitungstätigkeiten (VdV)**
- **Technische und organisatorische Maßnahmen**

DSGVO

- **Verzeichnis der Verarbeitungstätigkeiten (VdV)**
  - **Wessen Daten verarbeiten wir?**
  - **Welche Daten erheben wir? (Grundsatz der Datenminimierung)**
  - **Zu welchem Zweck werden die Daten verarbeitet?**
  - **Wie kommt das Unternehmen zu den Daten**
  - **Wie lange werden die Daten aufbewahrt?**
  - **Werden Daten weitergegeben? (wenn ja: an wen und warum)**

DSGVO

- **Organisatorische Maßnahmen**
  - **Wer hat Zugang zu Daten?**
  - **Wie haben diese Personen mit den Daten umzugehen?**
  - **Wie ist bei der Verarbeitung der Daten zu verfahren?**
  - **Wie ist bei der Übermittlung von Daten vorzugehen?**
  - **etc.**

DSGVO

- **Technische Maßnahmen**
  - **Wo werden die Daten gespeichert?**
  - **Wie werden die Daten verschlüsselt?**
  - **Wie werden die Daten gesichert?**
  - **Wie werden die Zugriffsrechte verwaltet?**
  - **etc.**

DSGVO

- **Die gute Nachricht**

  Die Ärztekammer bietet unter
  http://www.aekwien.at/datenschutzgrundverordnung

  ein sehr gutes Muster an, das man „nur“ ausfüllen muss,
  (45 Seiten) um die Dokumentationspflicht zu erfüllen

  P.S.: auf der WKO-Seite können Sie sich alles in einer „Toolbox“ selber zusammensuchen, versuchen den Sinn zu erfassen, die Dokumente adaptieren und strukturieren

DSGVO

2. Datenanwendung: Finanzbuchhaltung, Rechnungswesen und Logistik

2.1. **Zweck** der Verarbeitung:
Verarbeitung und Übermittlung von Daten im Rahmen einer Geschäftsbeziehung (bzw. zur Abwicklung dieser) mit Patienten und Lieferanten einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

Beinhaltet auch: Risikomanagement, Kreditoren- und Debitorenverwaltung, Budgetierung und Kostenrechnung.

2.2. **Rechtsgrundlage** der Verarbeitung: Gesetzliche Verpflichtung

2.3. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer, Patienten, Lieferanten

2.4. Verarbeitung durch **Auftragsverarbeiter: KEINE**

2.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **Der Zugang zur Buchhaltungssoftware (BUCHSOFT) ist nur für jene Mitarbeiter möglich, die die Buchhaltung durchführen.**

Betroffene Personengruppe: Arbeitnehmer					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax, UID-Nr)	1 - 10, 14		gemäß steuerrechtlicher	
2	Bankverbindungsdaten	1 - 9			

DSGVO

- **Datenschutzgesetz**
  - **§ 1. (1) Jede natürliche Person hat Anspruch auf Geheimhaltung der sie betreffenden personenbezogenen Daten und, nach Maßgabe gesetzlicher Bestimmungen, das Recht auf Auskunft über die Verarbeitung solcher Daten sowie auf Richtigstellung unrichtiger Daten und auf Löschung unzulässigerweise verarbeiteter Daten.**
  - **§ 1.(2) Beschränkungen sind nur mit Einwilligung der betroffenen Person, in deren lebenswichtigem Interesse, ….., im berechtigten Interesse eines anderen, aufgrund eines Vertrages oder einer rechtlichen Verpflichtung zulässig. Diese Beschränkungen müssen notwendig und verhältnismäßig und …. für die betroffene Person vorhersehbar sein.**

DSGVO

- **Begriffe**
  - **Betroffene Person**
    - Natürliche Person, deren Daten verarbeitet werden
  - **Verantwortlicher**
    - Unternehmen, das Daten von natürlichen Personen verarbeitet
  - **Auftragsverarbeiter**
    - „Dritte“, die im Auftrag des „Verantwortlichen“ Daten von „Betroffenen Personen“ verarbeiten

DSGVO

- **Begriffe**
  - **„sensible Daten“**
    - **z.B. biometrische, genetische und Gesundheits-Daten**
  - **Rechtmäßigkeit**
    - **personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden**
  - **Einwilligung**
    - **freiwillige, für den bestimmten Fall, …. unmissverständlich abgegebene Willensbekundung durch die betroffene Person**

DSGVO

- **Die DSGVO findet keine Anwendung bei:**
  - **Datenverwendung im Rahmen ausschließlich persönlicher oder familiärer Tätigkeiten (private Nutzung)**
  - **Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen**
  - **Tätigkeiten im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik**
  - **Tätigkeiten der zuständigen Behörden zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit**

DSGVO

- **Die DSGVO betrifft nur personenbezogene Daten natürlicher Personen**

DSGVO

- **Damit personenbezogene Daten verarbeitet werden dürfen, bedarf es der „Rechtmäßigkeit“**
  - **Verarbeitung zur Vertragserfüllung**
  - **berechtigtes Interesse**
  - **gesetzlich erforderlich**
  - **im öffentlichen Interesse geboten**
  - **Einwilligung (dies muss laut Gesetz freiwillig, spezifisch und eindeutig durch eine bestätigende Handlung erfolgen)**

DSGVO

- **Betroffenenrechte**
  - **Auskunftsrecht**
  - **Recht auf Berichtigung**
  - **Recht auf Löschung ("Recht auf Vergessenwerden")**
  - **Recht auf Einschränkung der Verarbeitung**
  - **Recht auf Datenübertragbarkeit**
  - **Widerspruchsrecht**
  - **Recht, keiner automatisierten Entscheidung unterworfen zu werden**

DSGVO

- **Betroffenenrechte**
  - **Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person**
  - **Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden**

DSGVO

Am 20.4.2018 wurde

„Das Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl. I Nr. 165/1999, zuletzt geändert durch das Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 120/2017“ nochmals geändert

DSGVO

Die Novelle vom 20.4.2018 beinhaltet z.B. folgende Änderungen:

- **Strafen in aller Regel nur für Wiederholungstäter**
- **Öffentliche Einrichtungen sollen immer straffrei bleiben**
- **Ausnahme für Spione, die auch für ausländische Nachrichtendienste gilt ☺**
- **Erleichterungen für Videoüberwachung**

DSGVO

- **Datenschutzbeauftragter**

  Bestellung zwingend, wenn

  - **die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, welche die regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen**
  - **die Kerntätigkeit des Unternehmens in der umfangreichen Verarbeitung sensibler Daten …. besteht (z.B. Krankenanstalten)**

DSGVO

- **Datenschutzbeauftragter**
  - **Dem Sinn der DSGVO nach wäre die Bestellung eines Datenschutzbeauftragten auch für Ordinationen verpflichtend, da der „Unternehmenszweck“ nur durch Verarbeitung von „sensiblen Daten“ erreicht werden kann, und somit die Verarbeitung „sensibler Daten“ eine „Kerntätigkeit“ darstellt.**

DSGVO

- **Datenschutzbeauftragter**
  - **Lt. Ärztekammer benötigt ein einzelner Arzt keinen Datenschutzbeauftragten**
  - **Die ÄK empfiehlt ab einer Ordinationsgröße von mehr als 10 Mitarbeitern (Vollzeitäquivalent), die Zugriff auf personenbezogene Daten haben, einen Datenschutzbeauftragten zu bestellen**

DSGVO

- **Datenschutzbeauftragter**
  - **Der Datenschutzbeauftragte ist bei der Erfüllung seiner Aufgaben an keine Anweisungen bezüglich der Ausübung dieser Aufgaben gebunden.**
  - **Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden.**

DSGVO

- **Datenschutzbeauftragter**
  - **Es ist NICHT möglich, dass ein Mitglied der Geschäftsleitung bzw. der Unternehmer selbst oder der Verantwortliche für IT diese Position ausübt (Problem der Selbstkontrolle).**

DSGVO

- **Datenschutzbeauftragter Aufgaben:**
  - **Unterrichtung & Beratung der Unternehmer und Mitarbeiter hinsichtlich ihrer Pflichten nach dem Datenschutzrecht.**
  - **Die Überwachung und Überprüfung der Einhaltung der Datenschutzvorschriften und Strategien für den Schutz personenbezogener Daten, einschließlich der Zuweisung von Zuständigkeiten, Sensibilisierung und Schulung der Mitarbeiter.**
  - **Beratungen im Zusammenhang mit der Datenschutz-Folgenabschätzung und der Überwachung ihrer Durchführung.**
  - **Zusammenarbeit mit der Aufsichtsbehörde und Anlaufstelle**

DSGVO

- **Datenschutzbeauftragter Haftung**

  Eine Bestellung des Datenschutzbeauftragten als verantwortlicher Beauftragter nach dem Verwaltungsstrafgesetz ist nicht zulässig.

DSGVO

- **Datenschutzbeauftragter Haftung**

  Schadensersatzanspruch des „Verantwortlichen“ an den Datenschutzbeauftragten, wenn dieser eine fehlerhafte Beratung oder Vorabkontrolle durchgeführt hat, welche von der Aufsichtsbehörde sanktioniert wird

  (Durchsetzbarkeit?)

DSGVO

- **Auftragsverarbeiter**

  wenn sie einen Auftragsverarbeiter beschäftigen, müssen sie mit diesem einen Vertrag abschließen, in dem sie den Auftragsverarbeiter eplizit mit genau (von ihnen) definierten Verarbeitungs- Aufgaben beauftragen.

DSGVO

- **Auftragsverarbeiter**

  Beispiel Steuerberater:

  Wenn dieser auch den Jahresabschluß erstellt, können sie ihm gar nicht vorschreiben, wie er diesen zu erstellen hat

DSGVO

- **Auftragsverarbeiter**

  Beispiel IT-Betreuer:

  Hier wollen sie ja gar nicht, dass er z.B. Pateientendaten verarbeitet, er soll ja nur ihre IT-Infrastruktur am Leben halten

DSGVO

- **„Graubereiche“**

  noch fehlen manche Klarstellungen

  - ist die Weitergabe von Daten an andere Ärzte / Spitäler einwilligungspflichtig?

  (evtl. kann die ÄK eine Klarstellung herbeiführen)

DSGVO

- **„Graubereiche“**

  noch fehlen manche Klarstellungen

  - ist ein IT-Berater ein Auftragsverarbeiter?

  - ist ein Steuerberater ein Auftragsverarbeiter?

  - ist ein Provider ein Auftragsverarbeiter?

  - wer benötigt einen Datenschutzbeauftragten?

DSGVO

- „Graubereiche“

  Die Übertragung von „sensiblen Daten“ (Befunden) per FAX ist im Gesetz nicht explizit geregelt

DSGVO

- **„Graubereiche“**

  Ob eine Einwilligung zur Übertragung von „sensiblen Daten“ (Befunde) per unverschlüsseltem email „hält“ ist fraglich, weil per Gesetz eigentlich nur sichere Übertragungswege (verschlüsseltes email, VPN) erlaubt sind.

DSGVO

- **Praktische Tipps für „Verantwortliche“**

  Wenn sie einmal ein Verarbeitungsverzeichnis haben, sind Sie schon einen großen Schritt weiter

DSGVO

- **Praktische Tipps für „Verantwortliche“**

  Schaffen sie zusätzlich folgende Dokumente:

  - **Mitteilung an Mitarbeiter über die Verwendung ihrer Daten**
  - **Anweisungen an die Mitarbeiter**
    („Kopie“ der „organisatorischen Maßnahmen“)
  - **Schulungsprotokoll**
  - **Aushang (was ist zu tun wenn….)**
  - **Logbuch (Überprüfungs- und Änderungsmaßnahmen)**

DSGVO

- **Praktische Tipps für „Verantwortliche“**

  Schulen sie Ihre Mitarbeiter und lassen sie diese auch scheinbar selbstverständliche Dinge wie „der Letzte sperrt zu“ unterschreiben

DSGVO

- **Praktische Tipps für „Verantwortliche“**

  Verbannen sie Facebook, WhatsApp etc. von ihren (betrieblich genutzten) Smartphones und PCs

DSGVO

- **Praktische Tipps für „Verantwortliche“**
  - **Verzichten sie auf „Cloud“-Dienste**

DSGVO

- **Praktische Tipps für „Verantwortliche“**

  Verwende sie zur Übertragung „sensibler Daten“ gesicherte Kommunikation (DaMe) oder die eingeschriebene Post

DSGVO

- **Praktische Tipps für „Verantwortliche“**

  Bei Graubereichen:

  beziehen sie eine klare, Position, begründen sie diese und schreiben sie das in Ihrer Dokumentation nieder

DSGVO

- **Praktische Tipps für „Verantwortliche“**

  z.B.: sie meinen, ihr Steuerberater ist kein Auftragsverarbeiter:

  „die Finanzbuchhaltung und Lohnverrechnung durch <Name>, <Adresse> **stell eine Inanspruchnahme fremder Fachleistungen und keine Auftragsverarbeitung dar.“**

  Quelle: Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO der Bayerisches Landesamt für Datenschutzaufsicht vom 16.1.2018

DSGVO

- **Praktische Tipps für „Verantwortliche“**

  z.B.: sie meinen, Sie benötigen keinen Datenschutzbeauftragten:

  „für den einzelnen freiberuflichen Arzt besteht, sofern nicht mehr als zehn Mitarbeiter (Vollzeitäquivalente) Zugriff auf personenbezogene Daten/Patientenkarteien haben, keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten“

  Quelle: Rechtsmeinung der Ärztekammer

  www.aekwien.at/datenschutzgrundverordnung/einzelpraxen

DSGVO

- **Praktische Tipps für „Verantwortliche“**
  - **Lassen sie sich von ihrem IT-Betreuer eine Geheimhaltungserklärung unterschreiben**

DSGVO

- **Praktische Tipps für „Verantwortliche“**
  - **Prüfen sie regelmäßig die aktuelle Rechtslage (3 Monate)**
    es wird Klarstellungen und Musterurteile geben
  - **passen sie ggf. Ihre Umsetzung an**
  - **und tragen sie das im Logbuch ein**

Danke für ihre Aufmerksamkeit