

Antwort

der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Dr. Wieland Schinnenburg,
Christine Aschenberg-Dugnus, Michael Theurer, weiterer Abgeordneter und
der Fraktion der FDP
– Drucksache 19/2811 –**

Auswirkungen der Datenschutz-Grundverordnung im Gesundheits- und Pflegebereich

Vorbemerkung der Fragesteller

Am 24. Mai 2016 trat die Datenschutz-Grundverordnung (DSGVO) in Kraft, die am 25. Mai 2018 Geltung erlangt hat. Obwohl sie in vielen Bereichen keine oder nur geringe Neuregelungen trifft, sorgt sie in letzter Zeit für Aufsehen. Grund hierfür sind die Neuregelungen bei den Sanktionen, die deutlich ausgeweitet und erhöht wurden.

Ein guter Datenschutz ist in Zeiten von Datenskandalen von zentraler Bedeutung. Allerdings muss bei der Datenverarbeitung Rechtssicherheit bestehen. Eine Bürokratisierung des Datenschutzes mit immer höheren formellen Anforderungen und immer höheren Bußgeldern führt nicht unbedingt zu einem besseren Datenschutz, sondern vorwiegend zur Belastung von kleinen und mittleren Unternehmen sowie Praxen und Apotheken. Zudem besteht die Gefahr von Abmahnwellen, welche auch nicht dem eigentlichen Ziel eines besseren Datenschutzes dienen.

Im Gesundheits- und Pflegebereich werden ständig sensible persönliche Daten verarbeitet. Von Rezepten über Röntgenbildern bis zu Krankheitsdaten müssen Praxen, Kliniken, Apotheken und Krankenkassen sowie Pflegeheime zur Behandlung und Versorgung von Patienten viele Daten erheben.

Vorbemerkung der Bundesregierung

Mit der ab dem 25. Mai 2018 unmittelbar anwendbaren Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – im Folgenden DSGVO) soll der Datenschutz EU-weit harmonisiert und an die Erfordernisse des 21. Jahrhunderts angepasst werden. Die DSGVO wurde am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht und ist am 24. Mai 2016 in Kraft getreten. In Deutschland wird die DSGVO

durch das mit dem Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassung- und -Umsetzungsgesetz EU) novellierte Bundesdatenschutzgesetz (BDSG 2018) ergänzt, das im Sommer 2017 vom Deutschen Bundestag verabschiedet wurde. Die Rechtsanwender hatten zwei Jahre Zeit, um die Datenverarbeitungsvorgänge an die Bedingungen der DSGVO anzupassen.

Die wesentlichen Grundsätze der Verarbeitung von Daten ändern sich durch die DSGVO nicht. Die DSGVO enthält zudem umfangreiche Öffnungsklauseln, die den Mitgliedstaaten im Gesundheitsbereich die Möglichkeit spezifischerer Regelungen eröffnet. Im Rahmen der Anpassungsarbeiten des bereichsspezifischen Rechts an die Vorgaben der DSGVO wurde der Prämisse gefolgt, das hohe Datenschutzniveau des bereichsspezifischen Gesundheits- und Sozialdatenschutzes soweit wie möglich unter Nutzung der den Mitgliedstaaten zustehenden Gestaltungsmöglichkeiten beizubehalten. Da die DSGVO in allen EU-Mitgliedstaaten unmittelbar gilt, müssen ihre Vorgaben, soweit sie keine Öffnungsklauseln enthält, zwingend erfüllt werden.

1. Welchen Einfluss hat die DSGVO nach Auffassung der Bundesregierung auf die Übertragung von Patientendaten zwischen verschiedenen Ärzten, Kliniken, Apotheken und Pflegeeinrichtungen?
2. Welchen Einfluss hat die DSGVO nach Auffassung der Bundesregierung auf die Übertragung von Patientendaten zwischen behandelnder Stelle wie etwa einer Praxis oder Klinik und den Krankenkassen?
3. Welchen Einfluss hat die DSGVO nach Auffassung der Bundesregierung auf die Übertragung von Patientendaten zwischen Apotheken und Pflegeeinrichtungen und den Kranken- bzw. Pflegekassen?

Die Fragen 1 bis 3 werden wegen ihres Sachzusammenhangs gemeinsam beantwortet.

Artikel 9 DSGVO enthält in Bezug auf die Erlaubnistatbestände zur Verarbeitung von personenbezogenen Gesundheitsdaten durch Angehörige der Gesundheitsberufe (Artikel 9 Absatz 2 Buchstabe h DSGVO i. V. m. § 22 Absatz 1 Nummer 1 Buchstabe b BDSG 2018) keine grundsätzlichen Änderungen gegenüber der bisherigen Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Warenverkehr (Artikel 8 Absatz 3). Insofern bleiben die Möglichkeiten der Datenübermittlung zwischen Leistungserbringern sowie der Leistungserbringer an Kranken- bzw. Pflegekassen grundsätzlich bestehen. Für die Datenübermittlungen sind die Vorgaben der DSGVO, des Bundesdatenschutzgesetzes 2018 sowie spezialgesetzlicher Regelungen wie beispielsweise des Fünften und Elften Buches Sozialgesetzbuch (SGB V und SGB XI) zu beachten.

4. Welche zusätzlichen Kosten entstehen Praxen, Kliniken, Apotheken, Krankenkassen und Pflegeeinrichtungen nach Einschätzung der Bundesregierung durch die Einführung der DSGVO?
5. Welche zusätzlichen jährlichen Kosten entstehen Praxen, Kliniken, Apotheken, Krankenkassen und Pflegeeinrichtungen nach Einschätzung der Bundesregierung durch die dauerhafte Umsetzung der DSGVO?

Die Fragen 4 und 5 werden wegen ihres Sachzusammenhangs gemeinsam beantwortet.

Der Bundesregierung liegen keine Erkenntnisse darüber vor, welche zusätzlichen Kosten Praxen, Kliniken, Apotheken, Krankenkassen und Pflegeeinrichtungen durch die Einführung und durch die Umsetzung der DSGVO entstehen.

6. Sind Änderungen bei der Telematikinfrastruktur nach Auffassung der Bundesregierung notwendig, um die Datenübertragung und Speicherung DSGVO-konform umzusetzen, wenn ja, welche?

Der Sicherstellung von Datenschutz und Datensicherheit kommt in den bereichsspezifischen gesetzlichen Vorgaben für den Aufbau und die Nutzung der Telematikinfrastruktur bereits eine hohe Bedeutung zu. Das neue, durch die DSGVO und die nationalen Anpassungsgesetze geprägte Datenschutzrecht schreibt im Wesentlichen die bisherigen datenschutzrechtlichen Grundprinzipien fort. Die Grundsätze für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten bleiben bestehen. Die DSGVO hat insofern keine spezifischen Auswirkungen auf die Regelungen des SGB V im Zusammenhang mit dem Aufbau der Telematikinfrastruktur und den Anwendungen der elektronischen Gesundheitskarte. Vorgesehene Änderungen in § 291 ff. SGB V betreffen Anpassungen an die Begrifflichkeiten der DSGVO.

7. Können Patienten nach Auffassung der Bundesregierung in Zukunft Einspruch gegen die Nutzung, Speicherung und Übermittlung ihrer Behandlungsdaten einlegen, und welche Folgen hätte dies?

Die DSGVO kennt die Begriffe Widerspruch (gegen eine grundsätzlich erlaubte Datenverarbeitung) und Widerruf (der Einwilligung).

Erfolgt die Datenverarbeitung auf der Grundlage eines Erlaubnistatbestands nach der DSGVO oder nach nationalem Recht, kann ein Widerspruch nur in den in Artikel 21 DSGVO genannten Fällen erfolgen. Die Datenverarbeitung zu Behandlungszwecken fällt nicht darunter, da sie zur Erfüllung einer vertraglichen Verpflichtung gegenüber dem Betroffenen erforderlich ist (Artikel 6 Absatz 1 Buchstabe b in Verbindung mit Artikel 9 Absatz 2 Buchstabe h DSGVO in Verbindung mit § 22 Absatz 1 Nummer 1 Buchstabe b BDSG 2018).

Wird ein Widerspruch nach Artikel 21 Absatz 1 DSGVO eingelegt – etwa wenn die Datenverarbeitung ausschließlich für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt (Artikel 21 Absatz 1 in Verbindung mit Artikel 6 Absatz 1 Buchstabe e DSGVO) –, darf der Verantwortliche die personenbezogenen Daten nicht mehr verarbeiten, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Erfolgt die Datenverarbeitung nicht aufgrund eines Erlaubnistatbestands, sondern auf der Grundlage einer Einwilligung, so kann die Einwilligung, wie nach bisherigem Recht auch, jederzeit widerrufen werden mit der Folge, dass eine weitere Verarbeitung der aufgrund der Einwilligung bis zum Widerruf verarbeiteten Daten nicht mehr zulässig ist.

8. Müssen Ärzte, Krankenhäuser etc. die Behandlungsdaten nach Auffassung der Bundesregierung weiter speichern, obwohl der jeweilige Patient deren Löschung verlangt?

Artikel 17 Absatz 3 DSGVO führt die Fälle auf, bei denen trotz Löschanforderungen Daten weiterhin zu speichern sind. Dies ist u. a. der Fall, wenn die Speicherung zur Erfüllung einer gesetzlichen Verpflichtung erforderlich ist, wie beispielsweise der zehnjährigen Aufbewahrungspflicht der Patientenakte nach § 630f Absatz 3 des Bürgerlichen Gesetzbuchs (BGB).

9. Wenn weiter Behandlungsdaten gespeichert werden müssen, wie lange, und welche Maßnahmen sind nach Auffassung der Bundesregierung zu ergreifen?

Nach alter wie neuer Rechtslage sind Patientenakten grundsätzlich für die Dauer von zehn Jahren nach Abschluss der Behandlung einer bestimmten Erkrankung aufzubewahren. Dazu ist der Behandelnde gemäß § 630f Absatz 3 BGB verpflichtet. Eine entsprechende Regelung zur Aufbewahrungspflicht von ärztlichen Aufzeichnungen enthält zudem § 10 Absatz 3 der (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte, der von den Landesärztekammern in entsprechenden berufsrechtlichen Regelungen umgesetzt worden ist. Vertragsärztinnen und -ärzte werden darüber hinaus gemäß § 57 des Bundesmantelvertrages-Ärzte, der zwischen der Kassenärztlichen Bundesvereinigung und dem Spitzenverband Bund der Krankenkassen geschlossen wurde, zur entsprechenden Aufbewahrung von ärztlichen Aufzeichnungen verpflichtet.

Die Aufbewahrungszeit kann aufgrund spezieller gesetzlicher Vorgaben abweichen. Beispielsweise beträgt sie nach der Röntgenverordnung und der Strahlenschutzverordnung für bestimmte Aufzeichnungen über Röntgenbehandlungen bzw. Anwendung ionisierender Strahlungen dreißig Jahre. Auch die Krankenhausgesetze einiger Länder sehen abweichende Fristen vor.

Besondere Vorgaben zu Aufbewahrungsfristen von Behandlungsdaten sieht die DSGVO nicht vor.

10. Wird zum Austausch, zur Speicherung und zur Übermittlung von Patientendaten nach Auffassung der Bundesregierung die Zustimmung des jeweiligen Patienten benötigt?

Die für die Behandlung erforderlichen Daten können auf der Grundlage des Artikels 6 Absatz 1 Buchstabe b in Verbindung mit Artikel 9 Absatz 2 Buchstabe h DSGVO in Verbindung mit § 22 Absatz 1 Nummer 1 Buchstabe b BDSG 2018 ohne Einwilligung des jeweiligen Patienten verarbeitet werden. So ist in den gesetzlich vorgeschriebenen Fällen der Datenverarbeitung, wie beispielsweise der Speicherung gemäß § 630f BGB oder der Datenübermittlung zu Abrechnungszwecken ärztlicher Leistungen gemäß § 295 SGB V, keine Einwilligung des jeweiligen Patienten notwendig.

In den Fällen, in denen kein Erlaubnistatbestand greift, ist die Einwilligung erforderlich.

11. Benötigen nach Ansicht der Bundesregierung Praxen, Apotheken und weitere Gesundheits- und Pflegeeinrichtungen mit weniger als zehn Mitarbeitern einen Datenschutzbeauftragten oder eine Datenschutzbeauftragte?

Hinsichtlich der Notwendigkeit der Benennung eines Datenschutzbeauftragten tritt mit der DSGVO und dem BDSG 2018 in Bezug auf die Praxisgröße keine substantielle Änderung ein. Nach der seit dem 25. Mai 2018 geltenden Rechtslage ist die Benennung eines Datenschutzbeauftragten erforderlich, wenn mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden (§ 38 Absatz 1 Satz 1 BDSG 2018), d. h. wenn diese Personen mit der Datenverarbeitung nicht nur gelegentlich beschäftigt sind, sondern dies wesentlicher Teil des vereinbarten Arbeitsfeldes ist. Damit wird die bisherige Rechtslage fortgeführt, da auch schon bisher die Verpflichtung zur Bestellung eines Datenschutzbeauftragten bestand, wenn mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt wurden (§ 4f Absatz 1 BDSG in der bis zum 24. Mai 2018 geltenden Fassung).

Unabhängig von der Anzahl der mit der Datenverarbeitung Beschäftigten besteht nach § 38 Absatz 1 Satz 2 BDSG 2018 die Verpflichtung zur Benennung eines Datenschutzbeauftragten, u. a. wenn eine Datenschutz-Folgenabschätzung vorgenommen wird, sowie gemäß Artikel 37 Absatz 1 Buchstabe c DSGVO, wenn „die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 [...] besteht“.

Daraus folgt, dass nicht jeglicher Umgang mit Gesundheitsdaten oder anderen „sensiblen“ Daten im Sinne des Artikel 9 DSGVO die Pflicht zur Benennung eines betrieblichen Datenschutzbeauftragten nach Artikel 37 Absatz 1 Buchstabe c DSGVO auslöst. Der durch die DSGVO neu eingeführte Tatbestand erfordert, dass es sich um eine „umfangreiche“ Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikel 9 DSGVO handelt und dass die Verarbeitung die „Kerntätigkeit“ des Verantwortlichen oder Auftragsverarbeiters darstellt. Nach Erwägungsgrund 91 Satz 4 DSGVO sollte die Verarbeitung personenbezogener Daten nicht als umfangreich gelten, wenn die Verarbeitung personenbezogener Daten von Patienten betrifft und durch einen einzelnen Arzt oder sonstigen Angehörigen eines Gesundheitsberufs erfolgt. Es ist daher weder ein betrieblicher Datenschutzbeauftragter nach Artikel 37 Absatz 1 Buchstabe c DSGVO zu benennen noch zwingend eine Datenschutz-Folgeabschätzung nach Artikel 35 Absatz 3 Buchstabe b DSGVO durchzuführen. Nach einem Beschluss der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder zur Datenschutzbeauftragten-Bestellungspflicht nach Artikel 37 Absatz 1 Buchstabe c, Datenschutz-Grundverordnung bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs vom 26. April 2018 gilt dies auch für den Zusammenschluss von Angehörigen eines Gesundheitsberufs in Gemeinschaftspraxen.

12. Welche Qualifikation muss ein Datenschutzbeauftragter bzw. eine Datenschutzbeauftragte nach Ansicht der Bundesregierung in einer Praxis haben?

Der Datenschutzbeauftragte muss gemäß Artikel 37 Absatz 5 DSGVO insbesondere über das zur Erfüllung seiner Aufgaben erforderliche Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis verfügen. Dies entspricht dem bislang geltenden Recht (§ 4f Absatz 2 Satz 1 BDSG in der bis zum 24. Mai 2018 geltenden Fassung). Zudem sind Interessenkonflikte auszuschließen.

In Fortführung der bislang geltenden Rechtslage (§ 4f Absatz 2 Satz 2 BDSG in der bis zum 24. Mai 2018 geltenden Fassung) richtet sich das erforderliche Niveau des Fachwissens nach der Sensibilität, Komplexität und Menge der Datenverarbeitung und dem sich daraus ergebenden Schutzbedarf der personenbezogenen Daten. Je komplexer die Datenverarbeitungen und je größer die Menge sensibler Daten sind, desto höhere Anforderungen sind an das notwendige Fachwissen des Datenschutzbeauftragten zu stellen. Auf die Auslegungshinweise der unabhängigen Aufsichtsbehörden wird verwiesen.*

13. Hält die Bundesregierung es für wahrscheinlich, dass es durch die DSGVO zu einer Abmahnwelle kommen kann, die Praxen, Kliniken, Pflegeeinrichtungen und Krankenkassen betreffen würde?

Der Bundesregierung liegen keine Erkenntnisse darüber vor, dass der Gesundheitssektor von Abmahnungen stärker oder weniger stark betroffen sein könnte als andere Bereiche. Die beispielsweise aus Bremen gemeldeten Abmahnungen von Arztpraxen beziehen sich nicht auf gesundheitsspezifische Problemstellungen des Datenschutzes, sondern auf mangelhafte Datenschutzerklärungen auf der Praxis-Internetseite. Die Bundesregierung nimmt jedoch die Befürchtungen ernst, dass es im Bereich des Datenschutzes zu einer „Abmahnwelle“ kommen könnte. Im Koalitionsvertrag ist vereinbart, dass ein „Missbrauch des bewährten Abmahnrechts verhindert“ werden soll (Rz. 5819). Gegenwärtig prüft die Bundesregierung Maßnahmen in diesem Bereich.

14. Ist die Bundesregierung der Auffassung, dass Arztpraxen, Apotheken, Pflegedienste und andere Leistungserbringer im Gesundheitswesen gegen den Anspruch auf Löschung personenbezogener Gesundheitsdaten des Betroffenen diesem gegenüber einwenden können, diese Daten zur Verteidigung von Rechtsansprüchen für einen Zeitraum von 30 Jahren unter Verweis auf die absolute Verjährungsfrist (§ 199 Absatz 2 des Bürgerlichen Gesetzbuchs) nach Ende der jeweiligen Behandlung bzw. Leistungserbringung aufzubewahren?

Gemäß Artikel 17 Absatz 3 Buchstabe e DSGVO besteht ein Anspruch der betroffenen Person auf Löschung nicht, wenn die Verarbeitung zu Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Es ist deshalb nachvollziehbar, dass es aus Sicht des Leistungserbringers erforderlich sein kann, einzelne Dokumentationen bis zum Ablauf der in § 199 BGB genannten Verjährungsfristen aufzubewahren.

15. Plant die Bundesregierung Änderungen an der nationalen Umsetzung der DSGVO, um Einrichtungen im Gesundheits- und Pflegebereich zu entlasten, wenn ja, welche?

Die Bundesregierung schlägt im Rahmen des geplanten Zweiten Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU überwiegend technische Anpassungen der bereichsspezifischen Datenschutzregelungen des Bundes in den einschlägigen Gesundheits- und Pflegegesetzen an die DSGVO mit der Prämisse vor, den

* Artikel 29-Gruppe, „Leitlinien in Bezug auf Datenschutzbeauftragte“ vom 5.4. 2017 (WP 243 rev.01), S. 13f; Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, „Häufig gestellte Fragen zum Datenschutzbeauftragten (FAQ)“, Stand: Mai 2018, S. 10f; Hessischer Datenschutzbeauftragter, „Der behördliche und betriebliche Datenschutzbeauftragte nach neuem Recht“, Stand Juni 2017, S. 13f.

Status quo soweit wie möglich zu erhalten. Darüber hinaus wird unabhängig von der Umsetzung der DSGVO im Gesundheits- und Pflegebereich geprüft, ob Entlastungsmöglichkeiten von nicht erforderlichem bürokratischem Aufwand bestehen.

16. Durch welche Maßnahmen können aus Sicht der Bundesregierung Daten DSGVO-konform digital und analog zwischen Ärzten, Kliniken, Apotheken, Pflegeeinrichtungen und Krankenkassen übertragen werden?

Die Vorgaben der Artikel 24, 25 und 32 DSGVO zu technischen und organisatorischen Maßnahmen sind zu beachten. Es ist insbesondere sicherzustellen, dass Unbefugte keinen Zugriff auf Patientendaten erhalten, also etwa Dritte ein Telefongespräch nicht mithören oder Faxe nicht einsehen oder auf Bildschirmen nicht mitlesen können.

