Blickpunkt Brüssel

Die neue Datenschutz-Grundverordnung (DSGVO): Konsequenzen für den Kleinunternehmer (Arztpraxen etc.) und Rechtsfolgen eines Verstoßes

Elaine Jatta

Mai

2019

Blickpunkt Brüssel

Sie sind medizinische Fachangestellte in einer Arztpraxis. Vor Ihnen steht ein minderjähriger Analphabet mit Migrationshintergrund. Sie erklären ihm die DSGVO. Wenn Sie wissen, wie das geht, brauchen Sie nicht auf „mehr" zu klicken.

Die neue DSGVO – Was wird tatsächlich von Kleinunternehmern wie zum Beispiel Arztpraxen verlangt, um sich rechtskonform zu verhalten? Die wichtigsten Fragen und Antworten auf einen Blick.

1. Einleitung

Durch die im Mai 2018 in Kraft getretene EU-Verordnung gilt ein europaweit einheitliches Datenschutzrecht. EU-Verordnungen müssen im Gegensatz zu EU-Richtlinien nicht noch in nationales Recht umgesetzt werden. Sie gelten automatisch wie nationales Recht in allen Mitgliedsstaaten. Folge der Einführung der neuen DSGVO sind unter anderem viel detailliertere Informationspflichten für jeden Unternehmer, jede Organisation und jeden anderen Gewerbebetreiber, der personenbezogene Daten speichert. Die Auswirkungen sind nicht nur für Großkonzerne, sondern auch für Kleinunternehmer wie Arztpraxen, ehrenamtliche Organisationen oder andere Selbstständige spürbar.

Was für Folgen drohen jedoch bei einem Verstoß gegen die neue DSGVO? Gesetzesgrundlage hierfür ist das neue Bundesdatenschutzgesetz (**BDSG**) in Verbindung mit **Art. 83 DSGVO**, der für Aufsichtsbehörden festlegt, welcher Verstoß gegen den Datenschutz mit Wirksamkeit der DSGVO sanktioniert werden muss. Hierbei bleibt den Aufsichtsbehörden nur ein sehr geringer Ermessensspielraum von einer Sanktion abzusehen, z.B. wenn es sich um natürliche Personen handelt oder der Verstoß durch einen Mitarbeiter erfolgt ist. Ansonsten soll laut der Vorschrift u.a. zu Abschreckungszwecken jeder Verstoß mit der Verhängung von Geldbußen sanktioniert werden.

Warum kam die EU überhaupt zu dem Entschluss, eine Harmonisierung der Datenschutzregelung auf EU-Ebene durchzuführen?

Bis Mai 2018 oblag die Regelung des Datenschutzes den Mitgliedsstaaten selbst, in Deutschland z.B. durch das Bundesdatenschutzgesetz (BDSG). Da Daten jedoch

grenzüberschreitend übermittelt werden können und die Gesetzeslage in der Vergangenheit in den verschiedenen Mitgliedsstaaten zum Teil erheblich voneinander abwich, sollte durch die Harmonisierung ein einheitlicher Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten erreicht werden.

Dieser Beitrag zeigt die Problematik der neuen DSGVO für den Kleinunternehmer am Beispiel einer Arztpraxis auf und liefert einen Überblick über typische Fragen, die in diesem Zusammenhang bei Selbstständigen aufkommen.

2. Die Problematik am Beispiel einer Hausarztpraxis

Täglich kommen bis zu 80 Patienten in eine Praxis für Allgemeinmedizin. Je nach Lage haben viele von ihnen einen Migrationshintergrund und sprechen kein (oder wenig) Deutsch. Es gibt Minderjährige, die ohne Eltern kommen oder Analphabeten. Problematisch wird es zusätzlich, wenn es sich bei dem Patienten um eine Einzelperson handelt, die sich an niemanden zur Erklärung wenden kann. Die neue DSGVO betrifft ausnahmslos jeden. Die medizinischen Fachangestellten müssen ungeachtet problematischer Fälle jeden Patienten über die Erhebung personenbezogener Daten informieren. Zwar schreibt **Art. 13 DSGVO** nur eine Informationspflicht des Datenerhebers vor und nicht die Pflicht zur Einholung einer Einwilligung. Der Patient muss lediglich durch Unterschrift die Kenntnisnahme dokumentieren. Neben einem zeitlichen Aufwand ist für den Praxisbetrieb mitunter schwierig zu beantworten „Wie erkläre ich einem Patienten, der kaum Deutsch versteht und noch nie von der DSGVO gehört hat, wieso er nur weiter behandelt werden kann, wenn er von diesem Dokument Kenntnis nimmt?“. Trotz erheblicher Thematisierung der neuen DSGVO in den Medien gibt es dennoch eine große Anzahl an in Deutschland lebenden Menschen, die bei ihrem Praxisbesuch zum ersten Mal mit der Thematik konfrontiert werden. Bevor den Patienten Gelegenheit zur Kenntnisnahme ihrer Rechte gegeben wird, müssen die Praxismitarbeiter/innen erklären, dass auf dem Chip der Krankenversichertenkarte ein Mindestsatz an Informationen als Referenzdaten gespeichert werden muss (Name, Geburtstag, Anschrift). Diese Referenzdaten werden wiederum automatisch auf jedes Schriftstück gedruckt, das die Praxis für den Patienten ausstellt, z.B. Überweisungen, Arbeitsunfähigkeitsbescheinigungen oder einfache Rezepte. Durch die neue DSGVO besteht unter anderem diese Aufklärungspflicht seitens des Unternehmens, das die personenbezogenen Daten erhebt und ggfs. weiterleitet. Es handelt sich somit im ersten Schritt um eine Pflicht zur Aufklärung über die Rechte des Dateninhabers in Bezug auf seine personenbezogenen Daten. Bereits die Unterlassung dieser Aufklärung jedes Patienten, der die Praxis seit der Einführung der neuen DSGVO betritt, stellt jeweils

einen Verstoß gegen die DSGVO dar. Egal wie groß die zeitliche Belastung für den Praxisbetrieb ist, um sich rechtmäßig zu verhalten, muss jeder Patient aufgeklärt werden, bevor eine Behandlung stattfinden kann und darf. Im Gegenzug darf der Arzt zwar selbstverständlich im Falle einer Verweigerung der Einwilligung auch die Behandlung verweigern. Dies könnte im Ernstfall aber zu einem erheblichen Gewissens- und sogar Berufspflichtenkonflikt führen.

Wer kann einen Verstoß wem melden?

Jeder Dateninhaber kann sich selbstständig bei dem Verdacht eines Verstoßes gegen die neue DSGVO an die zuständige Aufsichtsbehörde wenden und den Verstoß melden. Hierzu rufen diese auf ihren Webseiten sogar auf. Wer sind die zuständigen Aufsichtsbehörden?

Gemäß **Art. 51 DSGVO** sieht jeder Mitgliedstaat vor, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Verordnung zuständig sind. Damit werden die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt und der freie Verkehr personenbezogener Daten in der Union erleichtert. In Deutschland hat jedes Bundesland seine eigene Datenschutzaufsichtsbehörde, deren örtliche Zuständigkeit sich nach dem Sitz der nicht-öffentlichen Stelle richtet. Die Datenschutzbeauftragten der Bundesländer sind mit Ausnahme von Bayern sowohl für den nicht-öffentlichen als auch für den öffentlichen Bereich zuständig. Informationen zu einzelnen **Landesdatenschutzbeauftragten** sind im Internet zu finden, z.B. für das Land NRW unter https://www.ldi.nrw.de/mainmenu_Ueberuns/index.php.

Für Unternehmen, deren Hauptaktivität die Datenerhebung und Datenverarbeitung von natürlichen Personen ist, muss es einen **betrieblichen Datenschutzbeauftragten** geben und auf Bundesebene gibt es eine gesonderte **Bundesdatenschutzbeauftragte**.

Wie sieht es mit minderjährigen Patienten aus?

Auch im Bereich Datenschutz gelten für Minderjährige und nicht voll geschäftsfähige Personen Besonderheiten. Die Bedingungen für die Einwilligung Minderjähriger in die Verarbeitung ihrer personenbezogenen Daten regelt **Art. 8 DSGVO**. Demnach muss ein Minderjähriger, der das **sechzehnte Lebensjahr** vollendet hat, selbstständig in die Verarbeitung personenbezogener Daten einwilligen. Bis zu dieser Altersgrenze bedarf

ein Minderjähriger zur Einwilligung in die Verarbeitung personenbezogener Daten der Zustimmung der gesetzlichen Vertreter. Für den Fall der Arztpraxis ist dies jedoch nicht von Bedeutung, da – wie oben dargestellt – nur die Gelegenheit zur Kenntnisnahme gegeben werden und eben keine Einwilligung gemäß Art. 8 DSGVO eingeholt werden muss.

Eine Harmonisierung auf EU-Ebene soll bei den Mitgliedsstaaten nur gesetzliche Mindeststandards garantieren, wie dies auch zum Beispiel 2013 mit der Einführung der EU-Asylverfahren-Richtlinie geschah. Ziel dieser Richtlinie war, die Gewährleistung eines Mindestschutzes und Verfahrensgarantien in allen Mitgliedstaaten für Personen zu erreichen, die internationalen Schutz benötigen, sowie gleichzeitig die Verhinderung von Asylmissbrauch, welcher der Glaubwürdigkeit des Systems schadet. Darüber hinaus darf jedoch weiterhin jeder Mitgliedsstaat seine eigene Asylpolitik regeln, solange sie nicht mit den europäischen Gesetzesgrundlagen kollidiert.

Vergleichbar verhält es sich im Umgang mit der neuen DSGVO und Minderjährigen: Gemäß Art. 8 Abs. 1 S. 3 DSGVO ist es den EU-Mitgliedsstaaten überlassen, die durch die Vorschrift festgelegte Altersgrenze von sechzehn Jahren bis auf das dreizehnte Lebensjahr herabzusetzen. In Deutschland ist die Altersgrenze das sechzehnte Lebensjahr.

Was ist Ziel der neuen DSGVO und welche Kernkriterien muss eine Datenschutzerklärung enthalten?

Durch die neue DSGVO soll dem Einzelnen mehr Autorität und Mitspracherecht in Bezug auf die Erhebung und Speicherung seiner personenbezogenen Daten verliehen werden. Die folgenden vier Kriterien sind Kernpunkte der neuen Verordnung:

- **Stärkung der Einwilligung der Person (Art. 4 DSGVO) –** Das bedeutet im Wesentlichen, dass eine ausdrückliche Zustimmung der betroffenen Personen zur Erhebung personenbezogener Daten eingeholt werden muss. Lediglich die Information hierüber (z.B. in den Allgemeinen Geschäftsbedingungen) ist nicht mehr ausreichend.

- **„Recht auf Löschung" bzw. das „Recht auf Vergessenwerden" (Art. 17 DSGVO)** liefert in Absatz 1 Ziffer a)-f) sechs Gründe, bei dessen Vorliegen eine Person die Löschung ihrer personenbezogenen Daten vom betroffenen Unternehmen verlangen kann. Hierzu gehört beispielsweise auch der Widerruf

der Einwilligung, falls das Unternehmen keine Rechtsgrundlage für die Verarbeitung der Daten aufweisen kann.

- **Recht auf Datenübertragbarkeit (Art. 20 DSGVO) –** Das heißt, die betroffene Person hat gegenüber dem Unternehmen ein Recht auf Übertragung der verarbeiteten Daten, soweit dies technisch möglich ist, falls beispielsweise die Verarbeitung mithilfe automatisierter Verfahren erfolgt ist.

- **Einheitliche Aufsichtsbehörde des eigenen Mitgliedsstaates, egal wo ein Verstoß passiert** – Um es betroffenen Personen einfacher zu machen, einen Verstoß zu melden, gibt es eine Aufsichtsbehörde als Ansprechpartner. Wenn beispielsweise im Frankreichurlaub ein behandelnder Arzt keine Information zur Verarbeitung der personenbezogenen Daten vor der Behandlung aushändigt, kann der Deutsche diesen Verstoß nach seiner Rückkehr bei der für ihn zuständigen deutschen Aufsichtsbehörde melden.

Gilt eine Unterschrift, wenn ich nicht verstehe, was ich unterschreibe?

Grundsätzlich gilt im deutschen Recht, dass eine Erklärung nur Rechtswirkung entfalten kann, wenn der Erklärende neben einem **Handlungs- und Erklärungswillen auch einen sog. Rechtsbindungswillen** hat. Da gemäß **Art. 13 DSGVO** jedoch nur die Informationspflicht vorgeschrieben ist und eben nicht die Einholung einer schriftlichen Einverständniserklärung, dürfte ein Verstoß in den obengenannten Problemfällen nicht nachweisbar sein, da ein Hinweis in der Akte, dass der Patient über die Erhebung der personenbezogenen Daten informiert wurde, den Aufsichtsbehörden ausreicht. Dabei ist es tatsächlich unerheblich, wie viel er von dem, was er unterschreibt, dem Sinn nach versteht.

3. Die Rechtsfolgen eines Verstoßes

a. Ordnungswidrigkeiten gemäß § 43 Bundesdatenschutzgesetz (BDSG)

Der Bußgeldkatalog des § 43 BDSG, der die Ordnungswidrigkeiten regelt, unterscheidet zwischen zwei Bußgeldstufen:

- Einem Verstoß gegen die Meldepflicht, die Auskunftspflicht, die Zweckbindung oder unzulässige Erhebung von personenbezogenen Daten entgegen den Willen des Betroffenen und
- Fälle der unbefugten Datenerhebung von nicht allgemein zugänglichen personenbezogenen Daten, Erschleichung einer Datenübermittlung, Nutzung personenbezogener Daten zu Werbezwecken trotz Widerruf des Betroffenen und Verstößen gegen die Informationspflicht bei Kenntnis unrechtmäßiger Datenerhebung.

Die Obergrenze für Verstöße der ersten Kategorie liegt bei **50.000 Euro** und für die zweite Kategorie bei **300.000 Euro**. Die Höhe der Geldbuße richtet sich nach dem Jahresumsatz des betroffenen Unternehmens (in der Regel ca. 2-4% je nach Schwere des Verstoßes des (weltweiten) Jahresumsatzes).

b. Verstöße mit strafrechtlicher Relevanz

Erfolgt der Verstoß vorsätzlich und mit der Absicht der Bereicherung oder gegen Entgelt, kann es sogar zu einer Freiheitsstrafe von bis zu 3 Jahren kommen. Für den Kleinunternehmer, der lediglich seinen Informationspflichten pflichtwidrig nicht nachgekommen ist, sollte dieser Tatbestand jedoch nicht von Bedeutung sein. Falls man überhaupt ins Visier der Behörden geraten sollte, müssen deren Maßnahmen immer verhältnismäßig sein, weshalb in der Regel bei kleinen Verstößen, die aus Unkenntnis resultieren, Beratung statt Bestrafung stattfindet. Gegen den Kleinunternehmer, der aus Unkenntnis gehandelt hat, wird es in aller Regel bei einem Erstverstoß keine Strafe geben, sondern eine Ermahnung mit Hinweisen, wie das Problem abgestellt werden kann.

Die Höhe der Sanktionen soll jedoch zeigen, dass der mit der neuen DSGVO verfolgte Schutz von personenbezogenen Daten dem Gesetzgeber äußerst wichtig ist und z.B. für Wiederholungstäter, die mit Vorsatz und Gewinnerzielungsabsicht besonders viele Daten rechtswidrig verarbeiten, hohe Strafen zu befürchten sein können.