Die neue EU-Datenschutz-Grundverordnung (DSGVO) und das neue Bundesdatenschutzgesetz (BDSG)

mit Schwerpunkt Pharmazie

Einleitung

Die neue EU-Datenschutz-Grundverordnung (DSGVO) wurde erlassen, um eine einheitliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten in allen EU-Mitgliedsstaaten zu schaffen. Sie tritt am 25. Mai 2018 in Kraft und enthält deutlich strengere Auflagen zum Datenschutz als die frühere Datenschutzrichtlinie. Gleichzeitig treten die auf die neue Verordnung angepassten nationalen Datenschutz-Bestimmungen in Kraft. Für Deutschland ist dies unter anderem das neue Bundesdatenschutzgesetz (BDSG). Es wurde im April 2017 vom Bundeskabinett verabschiedet und im Juli 2017 im Bundesanzeiger veröffentlicht.

Die neue DSGVO schließt Lücken in der alten Regelung, vor allem in Bezug auf digitale Technologien und enthält völlig neue Vorgaben wie die „Datenschutz-Folgenabschätzung“ oder die „Privacy by Design“. Für Unternehmen bedeuten sie eine erhebliche Ausweitung ihrer Informations- und Dokumentationspflicht, die zahlreiche Änderungen im eigenen Betrieb mit sich bringen.

Wer die neuen Auflagen nicht einhält, riskiert empfindliche Bußgelder und womöglich einen wirtschaftlich fatalen, öffentlichen Reputationsverlust.

Dieses Whitepaper gibt einen Überblick über die wichtigsten Neuerungen der DSGVO und des BDSG und welche Konsequenzen sie für die Unternehmen haben. Dabei werden die Gesetzesgrundlagen, die speziell für die Pharmazie von Interesse sind, besonders ausführlich betrachtet. Diese betreffen u. a. den Umgang mit Patientendaten sowie den Datenschutz für Ärzte sowie die Neuregelung des § 203 im Strafgesetzbuch, der die Verschwiegenheitspflicht reguliert.

Die neuen Gesetze bringen nicht nur Nachteile mit sich. Für forschende Unternehmen eröffnen sich in den Bereichen Datenerhebung und -analyse Möglichkeiten, die es ihnen erlauben, Forschungsprojekte schneller und effektiver durchzuführen und zum Abschluss zu bringen.

Wichtiger Hinweis: Die Schlussfolgerungen bzgl. der einzelnen Gesetzestexte entspringen der persönlichen Auffassung und Interpretation des Autors und sind nicht rechtsverbindlich. Ihre Prüfung unterliegt der Verantwortung der einzelnen Unternehmen.

Inhaltsverzeichnis

Die neue Europäische Datenschutz-Grundverordnung DSGVO

Das Ziel der neuen europäischen Datenschutz-Grundverordnung[1] war eine Vereinheitlichung beim Umgang mit personenbezogenen Daten innerhalb der EU. Das ist allerdings nur teilweise geglückt, weil es viele so genannte „Öffnungsklauseln" gibt. Sie gewähren den einzelnen Ländern einen Ermessungsspielraum bei ihren nationalen Datenschutzgesetzen. Dazu gehören z. B. der Beschäftigungsdatenschutz und Ausnahmen bei der normalerweise zwingenden Einwilligung in die Datenverarbeitung und Datenspeicherung. Im Zweifelsfall hat die DSGVO immer Vorrang vor den nationalen Gesetzen.

Insgesamt ist die neue DSGVO umfangreicher als die vorherige EU-Datenschutzrichtlinie 95/46/EG[2] und sorgt für einen besseren Schutz der betroffenen Bürger. Beispielsweise werden die Löschung personenbezogener Daten sowie die Datenportabilität erleichtert.

Unternehmen haben viel umfangreichere Transparenz- und Informationspflichten als bisher, müssen in bestimmten Fällen eine Datenschutz-Folgenabschätzung (Risikoanalyse) vorweisen und haben bei Einwilligungen stärkere Auflagen. Bei Nichtbeachtung der Vorschriften gibt es zudem wesentlich höhere Bußgelder.

Auch digitale Technologien werden stärker berücksichtigt, was sich in strengeren Vorschriften zur Datensicherheit von Social Media-Kanälen ausdrückt. Um ständige Neuerungen und Erweiterungen der DSGVO in der nahen Zukunft zu vermeiden, wurde in den entsprechenden Gesetzestexten die Formulierung „Unter Berücksichtigung des Stands der Technik" gewählt, um zukünftige Änderungen bei der digitalen Verarbeitung einzuschließen. Trotzdem ist eine Evaluierung der DSGVO vorgesehen und Konkretisierungen wird es fortlaufend durch den Datenschutz geben.

Ab wann und für wen gilt die neue Datenschutz-Grundverordnung?

Die neue europäische Datenschutzverordnung tritt am 25. Mai 2018 in Kraft. Alle Unternehmen sind ab diesem Tag an sie gebunden, egal wie groß sie sind, welche Rechtsform sie haben oder welcher Branche sie angehören. Für Einrichtungen der öffentlichen Hand sind zusätzlich Bundesland spezifische Gesetze zu beachten.

Die neuen Gesetze gelten nicht nur für europäische Firmen, sondern auch für ausländische Unternehmen, die Daten von europäischen Bürgern erfassen und für Nicht-EU-Angehörige, die sich in der EU aufhalten. Wenn Drittstaaten, die generell kein angemessenes Datenschutzniveau

---

[1] Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, Amtsblatt der Europäischen Union, Abl. L 119/1

[2] Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt der Europäischen Union, Abl. L 281/31

besitzen, personenbezogene Daten abrufen, bleibt dies weiterhin kritisch.

Welche Folgen hat eine Nichtbeachtung?

Kommt es zu einem Verstoß gegen die Datenschutzgrundverordnung, sind die Bußgelder beträchtlich. Sie betragen jetzt bis zu 20 Millionen Euro bzw. bei weltweit tätigen Firmen bis zu vier Prozent des erwirtschafteten Jahresumsatzes.[3]

Deutsche Gesetzgebung beim Datenschutz: das neue BDSG

Das Bundesdatenschutzgesetz ist grundsätzlich ein Verbotsgesetz mit Erlaubnisvorbehalt. Daran ändert auch die DSGVO nichts. Die Datenerfassung und Datenspeicherung ist mit wenigen in Artikel 6 definierten Ausnahmen nur dann erlaubt, wenn die Einwilligung des Betroffenen vorliegt. Zusätzlich sind entsprechende organisatorische und prozessuale Vorkehrungen seitens der Unternehmen zu treffen, da sie einerseits Informationspflicht den Betroffenen gegenüber haben, andererseits damit die Betroffenen gegenüber den Unternehmen ihre Rechte auf Information, Löschung, Berichtigung oder Sperrung ausüben können.

Allerdings hat der Gesetzgeber Ausnahmen festgelegt, beispielsweise wenn die allgemeine Ordnung und Sicherheit des Landes in Gefahr sind.[4] Das lässt die Speicherung personenbezogener Angaben von Straftätern oder – gerade aktuell – als „Gefährder" eingeschätzten Personen ohne deren Einwilligung zu. Das neue BDSG bietet darüber hinaus auch für die medizinische Forschung interessante Ausnahmen (davon später mehr). Außerdem gibt es noch Spezialgesetze wie das Geldwäsche-, das Telekommunikations- oder das IT-Sicherheitsgesetz.

In Deutschland ist die Durchführung der Datenschutzbestimmungen komplizierter als in anderen EU-Mitgliedsstaaten. Hier gibt es neben der DSGVO und dem BDSG noch die Gesetzgebung der einzelnen Länder für die öffentliche Hand, die allerdings zumeist die Informationsübermittlung an die Behörden und die Rolle der Datenschutzaufsicht betrifft. Bei Verstößen mit erheblichen Auswirkungen auf die Betroffenenrechte ist die Aufsichtsbehörde des Bundeslandes zu informieren.

Die wichtigsten Neuerungen der DSGVO kurz zusammengefasst

Richtigkeit der Daten

Nach Art. 5 Abs. 1 (d) DSGVO müssen personenbezogene Daten erforderlichenfalls auf dem neuesten Stand sein. Datensammler müssen danach nicht nur zu Beginn, sondern während der gesamten Laufzeit der Datenspeicherung und -verarbeitung die Richtigkeit der Angaben sicherstellen. Sie sind auch ohne Aufforderung dazu verpflichtet z. B. eine falsche Adresse zu löschen oder zu korrigieren.

---

[3] Vgl. Art. 83 Abs. 5 DSGVO

[4] Vgl. Art. 23 Erwägungsgrund 73 sowie § 23 BDSG

Rechenschaftspflicht

„Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).“ [5]
Unternehmen müssen nicht nur – wie bisher – bei einer Prüfung die Einhaltung der Datenschutzgesetze nachweisen. Sie sind verpflichtet, datenschutzrechtlich relevante Vorgänge und ihre Funktionsfähigkeit zu dokumentieren und aktiv nachzuweisen. Dazu gehören ein Datenschutz-Konzept bzgl. der Umsetzung, die Überwachung und die Korrektur der Daten. Die dadurch notwendigen strukturellen Anpassungen erfordern einen hohen bürokratischen Aufwand.

Die „Hacker-Regelung“

Verletzungen des Schutzes personenbezogener Daten müssen unverzüglich innerhalb von 72 Stunden der jeweiligen Aufsichtsbehörde mitgeteilt werden.[6] Betroffene müssen ebenfalls unverzüglich informiert werden, wenn „die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat“. [7] Sollte dies mit einem unverhältnismäßigen Aufwand verbunden sein, ist „stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden“.[8]

Recht auf „Datenportabiliät“

Art. 20 befasst sich mit dem neuen „Recht auf Datenübertragbarkeit“. Unternehmen müssen Betroffenen ihre personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zukommen lassen und sind verpflichtet sie – soweit technisch möglich – an einen anderen „Verantwortlichen“ zu übertragen. Diese Pflicht zur Datenübertragung betrifft jede Firma, da auch Daten von Mitarbeitern unter diese Regelung fallen.[9]

„Privacy by Design“ – Datenschutz durch datenfreundliche Voreinstellungen

Unternehmen müssen ihre Produkte datenschutzfreundlich gestalten und die Erlaubnis zur Datennutzung ausdrücklich einholen.[10] Dafür sind Maßnahmen erforderlich, die „den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun“. Das gilt auch für ausländische Unternehmen wie Facebook und Co.

---

[5] Vgl. Art. 5 Abs. 2 DSGVO

[6] Vgl. Art. 33 DSGVO

[7] Vgl. Art. 34 Abs. 1 DSGVO

[8] Vgl. Art. 34 Abs. 3 (c) DSGVO

[9] Vgl. Art. 20 DSGVO

[10] Vgl. Art. 25 DSGVO

Welche Datenschutz-Gesetze betreffen speziell die Pharmabranche?

Die Datenschutz-Grundverordnung hält viele Neuerungen für die Pharmabranche bereit. Sie betreffen vorwiegend forschende Unternehmen, die Daten von Patienten verarbeiten. Sie greift aber auch bei Daten von Nutzern medizinischer Apps und bei Daten, die über Ärzte erhoben werden und für die Organisation des pharmazeutischen Außendienstes unerlässlich sind. Im Falle von Patientendaten kann es sich um rein statistische Analysen für die zukünftige Entwicklung von Medikamenten, aber auch in Auftrag gegebene klinische Studien handeln.

Recht auf „Vergessenwerden“

Betroffene können ihre Daten leichter – und vollständig – löschen lassen.[11] Für das Recht auf Löschung der Daten gibt es jedoch Ausnahmen. Zum Beispiel bei Daten, die für „im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke“ genutzt werden.[12] Weitere Ausnahmen bilden zum Beispiel sie steuerliche Aufbewahrungspflicht oder vorgegebene Fristen im Arzeneimittelgesetz und im Gendiagnostikgesetz.

[11] Vgl. Art. 17 DSGVO

[12] Vgl. Art. 89 DSGVO

Die Datenschutz-Folgenabschätzung

Zwar musste die Datenverarbeitung schon unter den alten Gesetzen bei besonderen Risiken zuerst geprüft werden, doch jetzt wird diese Regelung ausgeweitet und gesetzlich verankert.

Die Folgenabschätzung wird vorab zwingend erforderlich, wenn die Verwendung neuer Technologien oder die Art, der Umfang und der Zweck ein voraussichtlich hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge hat.[13] Die Aufsichtsbehörden müssen zudem eine Liste der Verarbeitungsvorgänge erstellen, für die eine Folgenabschätzung notwendig wird.

Was alles vorab geprüft, kontrolliert, untersucht und nachgewiesen werden muss, wurde im Gesetz genauestens festgelegt. Die Liste ist recht umfangreich und zwingt Unternehmen bereits vor einer geplanten Datenerfassung zu umfangreichen Dokumentationen und Analysen. Sie beinhaltet

- eine genaue Beschreibung der Daten-Verarbeitung,
- ihren Zweck,
- die Notwendigkeit und Verhältnismäßigkeit in Bezug auf diesen Zweck,
- die Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen,
- die „geplanten Abhilfemaßnahmen zur Bewältigung der Risiken, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren".[14]

Gesundheitsdaten sind natürlich hochsensibel und bedürfen eines besonderen Schutzes. Deshalb ist eine Folgenabschätzung für sie unverzichtbar. Der bürokratische Aufwand für ihre Durchführung ist enorm und bedarf einer genauen Planung und Umsetzung.

Optionen bei der Einwilligung zur Datenerhebung

Die DSGVO unterscheidet zwischen Einwilligungen, die für einen oder mehrere Zwecke gegeben werden und solchen, die für einen eindeutigen festgelegten Zweck sind. Dies muss bei der Einwilligung beachtet werden.

Der Erwägungsgrund 33 zum Art. 7 DSGVO erlaubt die Einwilligung zur wissenschaftlichen Forschung.

„Oftmals kann der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden. Daher sollte es betroffenen Personen erlaubt sein, ihre Einwilligung **für bestimmte Bereiche wissenschaftlicher Forschung** zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Die betroffenen Personen sollten Gelegenheit erhalten, ihre Einwilligung nur für bestimme

[13] Vgl. Art. 35 DSGVO

[14] https://www.datenschutz-notizen.de/datenschutz-grundverordnung-datenschutz-folgenabschaetzung-konsultation-1414608/ (16.10.2017)

Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen.“ [15]

Abhilfe könnte nur ein Gesetz schaffen, dass die Rechte der Patienten komplett aushebelt – zum Wohle der Gesellschaft.

Das neue Bundesdatenschutzgesetz scheint diesen Weg zu gehen, wie der folgende Abschnitt deutlich macht:

Vorteile der neuen Datenschutzgesetze für Pharma-Unternehmen

Die neuen Datenschutzgesetze bringen auch Vorteile. Im Bereich der medizinischen Forschung, ergeben sich neue Möglichkeiten, weil die Rechte der Patienten im Bundesdatenschutzgesetz erheblich eingeschränkt werden.

Das Forschungsprivileg des neuen BDSG

Die Verarbeitung von Daten für wissenschaftliche und historische Forschungszwecke unterliegt dem zwingenden Grundsatz der Datenminimierung. Um die Rechte und Freiheiten der betroffenen Personen zu gewährleisten, sollen diese im besten Fall anonymisiert werden. Wenn dies dem Forschungsziel widerspricht, kann Pseudonymisierung eine Maßnahme sein, die aber auch nur eingesetzt werden kann, wenn sie dem Forschungszweck nicht wiederspricht.[16]

Noch wichtiger ist Absatz 2: Wenn personenbezogene Daten zu wissenschaftlichen und historischen Forschungszwecken oder zu statistischen Zwecken verarbeitet werden, können Ausnahmen von den Rechten aus den Artikeln 15 (Auskunftsrecht der Betroffenen, 16 (Recht auf Berichtigung), 18 (Recht auf Einschränkung der Verarbeitung) und 21 (Widerspruchsrecht) vorgesehen werden. Und zwar dann, wenn sie die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen.[17]

Hier haben die einzelnen Länder bei ihrer Gesetzgebung einen Gestaltungsspielraum und können die Ausnahmen selbst festlegen. Die Kommission prüft, ob der deutsche Gesetzgeber diesen Spielraum nicht überschritten hat.

Deutsche Gesetze zum Forschungsprivileg – zu großzügig?

Im § 27 Abs. 1 des neuen BDSG wird die Verarbeitung **personenbezogener Daten auch ohne Einwilligung (!) für wissenschaftliche oder historische Forschungszwecke zugelassen**,

[15] Vgl. DSGVO, Erwägungsgrund 33

[16] Vgl. Art. 89 Abs. 1 DSGVO

[17] Vgl. Art. 89 Abs. 2 DSGVO

wenn sie für den Zweck erforderlich ist und die Interessen des Verantwortlichen erheblich überwiegen.[18] [19]
→ Dieses Gesetz bietet mehr Freiheit für die klinische Forschung, denn ein Interesse der Öffentlichkeit wird nicht gefordert.[20] [21]

§ 27 Abs. 2 beschränkt die Rechte der betroffenen Personen, wenn diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und für deren Erfüllung notwendig ist. Außerdem haben sie **kein Recht auf Auskunft, wenn die Daten für die Zwecke der wissenschaftlichen Forschung erforderlich sind** und die Auskunftserteilung einen unverhältnismäßig hohen Aufwand erfordern würde.
→ Der Wegfall der Auskunftspflicht bei unverhältnismäßigen Aufwand ist eine erhebliche Erleichterung für forschende Unternehmen.

§ 27 Abs. 3 ist nicht neu, sondern behält die Regelung des bisherigen BDSG. Er bestimmt, dass Daten dann zu anonymisieren sind, sobald dies nach dem Forschungs- und Statistikzweck möglich ist. Bis dahin müssen Merkmale, die einer bestimmten Person zugeordnet werden können, getrennt gespeichert werden. Zunächst klingt das nach einer Einschränkung. Jedoch dürfen sie nur mit den Einzelangaben zusammengeführt werden, wenn es der Forschungs- oder Statistikzweck erfordert.
→ Das bedeutet, dass persönliche Daten wie die ethnische Zugehörigkeit zum Zweck der Forschung gespeichert werden dürfen, wenn sie für das Forschungsziel relevant sind.[22]

Alle Regelungen sind im Kapitel 1: Rechtsgrundlagen der Verarbeitung personenbezogener Daten im BDSG aufgeführt. Verbraucher- und Datenschützer sehen in diesen Regelungen eine Absenkung des hohen Schutzniveaus der Betroffenenrechte im Vergleich zur EU-Datenschutzgrundverordnung und somit einen Verstoß gegen die vorrangige DSGVO. Über Gerichtsurteile wollen sie Änderungen erzwingen.[23]
Auf Grund dieser Kritik und auch in Anbetracht der drohenden Bußgelder, sollten alle Regelungen zur Verarbeitung personenbezogener Daten penibel und konsequent beachtet werden.

Es bleibt also spannend bzgl. der Datenschutzrechte von Patienten. Doch wie sieht es mit den personenbezogenen Daten von Ärzten aus, die mit Pharmaunternehmen zusammenarbeiten?

---

[18] Vgl. § 27 Abs. 1 und Abs. 2 BDSG

[19] https://www.dsb-ratgeber.de/artikel/bdsg-neu-datenverarbeitung-fuer-forschungszwecke-das-hat-sich-geaendert.html (26.10.2017)

[20] Vgl. § 27 Abs. 3 BDSG

[21] https://www.pressebox.de/inaktiv/gen-ethisches-netzwerk-ev-gen-berlin-mitte/Stellungnahme-zum-Entwurf-des-Datenschutz-Anpassungs-und-Umsetzungsgesetzes-EU-DSAnpUG-EU-der-Bundesregierung/boxid/849063 (26.10.2017)

[22] Vgl. § 27 Abs. 3 BSDG

[23] https://netzpolitik.org/2017/kommentar-das-neue-bundesdatenschutzgesetz-ein-postfaktisches-gesetz (26.10.2017)

Was ändert sich beim Datenschutz für Ärzte?

Die neuen Gesetzesgrundlagen beinhalten für die Erhebung arztbezogener Daten eine Reihe wichtiger Änderungen. Diese betreffen beispielsweise auch die Erfassung persönlicher Daten auf Veranstaltungen, in der Marktforschung und beim Management der Key Opinion Leader. Von diesen vielen Punkten, welche die Zusammenarbeit mit Ärzten beeinflussen, möchten wir hier den EFPIA Transparenzkodex als Beispiel betrachten:

EFPIA Transparenzkodex

2013 erfolgte die Einführung des „Transparenzkodex" durch die *European Federation of Pharmaceutical Industries and Associations* (EFPIA). Er verpflichtet alle Mitgliedsunternehmen zur Offenlegung der finanziellen und geldwerten Zuwendungen an Fachkreise (z. B. an Ärzte oder Apotheker) und fordert die eindeutige Identifizierung der Leistungsempfänger mit Namen, Adresse und – bei Ärzten – der Arztnummer. Gleichzeitig wird auf den geltenden Datenschutz hingewiesen.[24]

In den neuen Gesetzen hat das Recht der Ärzte auf Persönlichkeitsschutz weiterhin Vorrang vor dem öffentlichen Interesse. Deshalb ist eine Veröffentlichung ihrer personenbezogenen Daten nach wie vor nur möglich, wenn sie ausdrücklich und schriftlich zugestimmt haben.

Viele Unternehmen haben in der Vergangenheit Angehörige medizinischer Fachkreise bereits freiwillig umfassend informiert. In Zukunft ist dies jedoch auch gesetzlich vorgeschrieben.[25]

Zu den Informationen, die jedem Arzt vor seiner Einwilligung mitgeteilt werden müssen, gehören unter anderem:

- Name und Kontaktdaten des Verantwortlichen im Unternehmen
- Name des zuständigen Datenschutzbeauftragten
- Die Angabe für welchen Zweck die Datenerhebung erfolgt
- Die Angabe, an wen die Daten womöglich weitergeleitet bzw. wo sie veröffentlicht werden
- Der Hinweis auf das Recht zum Widerruf der Einwilligungserklärung[26]

Das kommt konkret auf die Unternehmen zu

Um die zahlreichen Neuerungen rechtzeitig umzusetzen, müssen sich die Unternehmen beeilen. Es gilt, die gesamte Datenschutzpolitik auf den Prüfstand zu stellen, Änderungen vorzunehmen und

[24] http://www.kodexkonform.com/deutsch/news-und-infos/fsa-und-efpia.html (26.10.2017)

[25] http://www.chemanager-online.com/themen/sicherheit/von-folgeabschaetzung-bis-nachweispflicht (26.10.2017)

[26] Vgl. § 32 BDSG

neu zu organisieren. Alleine die erforderlichen technischen Veränderungen der Prozesse nehmen Monate in Anspruch.

Dabei dürfen auch kleine Änderungen nicht übersehen werden, zum Beispiel neue Datenschutzvorgaben für die Mitarbeiter oder die Installation einer neuen Sicherheitssoftware auf einem Rechner. Sie kosten zwar für sich alleine betrachtet relativ wenig Zeit, mutieren aber in ihrer Masse zu einer Mammutaufgabe. Hier können Firmen schnell den Überblick verlieren und sich verzetteln.

Pharmaunternehmen haben durch die Folgenabschätzung einen noch höheren Aufwand, denn die Risikoanalyse und ihre Dokumentation sind sehr zeit- und kostenintensiv.

Liste der erforderlichen Datenschutz-Maßnahmen

Die folgende Aufzählung ist nur beispielhaft, vermittelt aber bereits einen ersten Eindruck über die zwingend notwendigen Vorbereitungen zur Einhaltung der neuen Datenschutzgesetze:

- Treffen Sie alle erforderlichen technischen Maßnahmen, um personenbezogene Daten ausreichend zu schützen (neueste Software, Firewall, gesicherte Seiten etc.).
- Stellen Sie sicher, dass personenbezogene Daten komplett gelöscht werden können – in Akten, auf Datenträgern und in der Cloud.
- Erarbeiten Sie ein Konzept zu Ihrer Auskunftspflicht.
- Planen Sie bereits jetzt die Umsetzung Ihrer zukünftigen Dokumentationspflichten (Rechenschaftspflicht, Datenschutz-Folgenabschätzung).
- Erstellen Sie einen Handlungsleitfaden für den Fall eines Missbrauchs der personenbezogenen Angaben.
- Sorgen Sie für die technischen Voraussetzungen, um das Recht auf Datenübertragung (Datenportabilität) zu gewährleisten.
- Passen Sie Ihre Prozesse den neuesten technischen Möglichkeiten zum Datenschutz an.
- Sorgen Sie für eine ausreichende Schulung Ihres Datenschutzbeauftragten.
- Führen Sie mit Ihren Mitarbeitern Fortbildungen zu den neuen Datenschutzgesetzen durch.
- Stellen Sie sicher, dass Ihre IT-Beauftragten die neuen Vorgaben umsetzen.
- Überlegen Sie, wie Sie die erforderlichen Umstellungen organisieren, ohne den Betriebsablauf empfindlich zu stören.

Und last but not least:

- Prüfen Sie, wie viel Zeit Sie für die Umstellungen tatsächlich brauchen und welches Budget Sie dafür einplanen müssen.

Probleme bei der Umsetzung der neuen Gesetze

In einer Umfrage im Mai 2017 unter 750 CIOs und IT-Managern aus Frankreich, Deutschland und Großbritannien befürchteten 70 Prozent, dass ihre Organisation die Umstellung nicht rechtzeitig schafft. Sie gaben auch an, dass ein umfassendes Verständnis der DSGVO-Zusammenhänge fehlt, die Verantwortlichkeit für die Einhaltung der gesetzlichen Vorgaben im Umgang mit Daten nicht immer klar ist und die Vorbereitung auf die DSGVO nur langsam vorankommt.[27] „Laut einer Studie von Veritas sind von den befragten Unternehmen nur zwei Prozent wirklich auf die neuen Datenschutzbestimmungen vorbereitet." [28] [29]

Da Pharma-Unternehmen wesentlich umfangreichere Dokumentationspflichten haben als Firmen anderer Branchen, ist bei ihnen die Gefahr, die Umstellung nicht rechtzeitig zu schaffen, besonders groß.

Fazit

Die neue EU-Datenschutz-Grundverordnung führt zu einer besseren einheitlichen Regelung innerhalb der EU. Doch teilweise sind die neuen Bestimmungen zu schwammig formuliert und lassen verschiedene Interpretationen zu. Außerdem gestattet die neue DSGVO den einzelnen Ländern immer noch einen zu großen Spielraum bzgl. ihrer nationalen Gesetzgebung.

Neben den vielen Nachteilen der neuen Gesetzgebung, zu denen in erster Linie die umfangreichen Dokumentations- und Rechenschaftspflichten sowie die Folgenabschätzung gehören, bietet das Bundesdatenschutzgesetz mit seinen Auslegungsspielräumen zur Patienteneinwilligung forschenden Pharma-Unternehmen einen nie dagewesenen Spielraum für ihre zukünftigen Projekte. Dieses Forschungsprivileg könnte allerdings wieder revidiert werden, falls es nachweislich mit der übergeordneten DSGVO kollidiert. Absolute Klarheit dürfte nur anhand zukünftiger Gerichtsurteile möglich sein, doch könnten auch Orientierungshilfen von Aufsichtsbehörden dazu kommen und Auslegungshilfen des EU-Datenausschusses.

Bis dahin herrscht eine gewisse Rechtsunsicherheit. Sie stellt Unternehmen vor eine schwierige Entscheidung: Sollen sie die Bestimmungen großzügig auslegen und dadurch hohe Bußgelder und Imageverlust riskieren? Oder sollen sie die Rechtsvorschriften aus Vorsicht sehr eng interpretieren, was einen hohen Arbeits- und Kostenaufwand nach sich zieht? Das Beste wäre wahrscheinlich die goldene Mitte. Um sie zu finden, ist die Unterstützung durch spezialisierte Rechtsanwälte unverzichtbar.

---

[27] http://www.netapp.com/de/company/news/press-releases/news-rel-20170508-842365.aspx (26.10.2017)

[28] https://www.heise.de/ix/meldung/Studie-Unternehmen-glauben-nur-auf-neuen-Datenschutz-vorbereitet-zu-sein-3784634.html (26.10.2017)

[29] https://www.veritas.com/de/de/news-releases/2016-12-15-veritas-study-reveals-over-half-of-businesses-are-unprepared-for-gdpr (26.10.2017)

Die größte Herausforderung – vor allem für Pharma-Unternehmen – scheint die rechtzeitige Umsetzung der neuen Datenschutzgesetze im eigenen Betrieb zu sein. Viele Firmen haben den Arbeitsaufwand völlig unterschätzt und liegen in ihrem Zeitplan weit zurück.

Die neue EU-DSGV und das BDSG-neu treten – ohne Wenn und Aber – am 25. Mai 2018 in Kraft, womit die Übergangszeit von 2 Jahren endet.

Wer jetzt nicht umgehend handelt und den Datenschutz in seinem Unternehmen zügig auf den neuesten Stand bringt, riskiert Abmahnungen und hohe Strafzahlungen.

Empfehlung

Um die neue DSGVO und das neue Bundesdatenschutzgesetz rechtzeitig umzusetzen, ist eine Hilfe von außen sehr empfehlenswert.

Die Mitarbeiter der MMM Consulting GmbH unterstützen Ihr Unternehmen ganzheitlich bei der Umsetzung der neuen datenschutzrechtlichen Vorgaben für Ihre Geschäfts- und IT-Prozesse – fristgerecht und unternehmensweit.

Unsere praxisgeschulten Experten erstellen nach der Analyse des Ist-Zustands klare Konzepte und Strategien und übernehmen auf Wunsch als Projektleiter ihre praktische Umsetzung. Dafür setzen sie ihre langjährige Erfahrung bei der Optimierung von Prüfprozessen und ihre Fachkompetenz bei der Anpassung bestehender CMR- oder anderer IT-Systeme ein. Die Konsolidierung der Datenquellen sowie die Schaffung einheitlicher skalierbarer Standards gehören ebenso zu ihrem Angebot wie die Minimierung operativer Risiken.

Die MMM Consulting GmbH zeichnet sich durch einen umfangreichen Service und hohe Flexibilität aus. Wir sind dort, wo Sie uns brauchen – und zwar genau dann, wenn Sie uns brauchen.

MMM Consulting GmbH

Köthener Straße 38
D-10963 Berlin

Telefon +49 (0)30 26 39 80 60
Fax +49 (0)30 26 39 80 61

E-Mail office@mmm-consulting.de
Web www.mmm-consulting.de