IWW INSTITUT
CORPORATE PUBLISHING

White Paper (Stand: Juni 2018 | Autor: RA und FA für Medizinrecht Alexander Maur, Köln)

DSGVO: Das sollten Produktmanager in der Pharmaindistrie jetzt wissen

Nach Ablauf der zweijährigen Übergangsfrist ist am 25.05.2018 die Europäische Datenschutzgrundverordnung (DSGVO) in Kraft getreten. Gerade in den letzten Monaten wurde in den Unternehmen der Pharma- und Medizinproduktebranche fieberhaft daran gearbeitet, sich auf die Neuregelungen einzustellen. Dennoch dürfte die Diskussion um die neuen datenschutzrechtlichen Vorgaben in vielerlei Hinsicht erst nach dem Wirksamwerden beginnen. Zu weitreichend sind die Auswirkungen der Neuregelungen auf die unternehmerische Praxis.

An den Grundprinzipien des Datenschutzrechts wird festgehalten

Die neue Verordnung lässt die Grundprinzipien des in Deutschland bisher geltenden Datenschutzrechts zunächst weitgehend unberührt. Ihr Schutzbereich umfasst wie bisher personenbezogene Daten. Personenbezogen sind Daten hierbei immer dann, wenn – anders als im Falle einer Anonymisierung – die Bezugsperson identifiziert werden kann.

Auch die datenschutzrechtliche Einwilligung als der in der Praxis relevanteste Legitimationstatbestand für eine Datenverarbeitung bleibt erhalten und wird weiter gestärkt.

Gleiches gilt für die Funktion des betrieblichen Datenschutzbeauftragten als betriebsinterne Beratungs- und Kontrollinstitution.

Fokus der DSGVO: Der Datenschutz im Alltag muss sichergestellt sein

In ihren Regelungen stellt die DSGVO eine verbesserte Absicherung der beschriebenen datenschutzrechtlichen Grundprinzipien im Alltag in den Mittelpunkt. Hierzu werden vielfältige neue organisatorische Anforderungen (z. B. das Verzeichnis von Verarbeitungstätigkeiten oder die Datenschutz-Folgenabschätzung) definiert, deren Umsetzung im Unternehmen einen erheblichen Aufwand bedeutet.

Verarbeitungstätigkeiten müssen aufgelistet werden

Beim Verzeichnis der Verarbeitungstätigkeiten handelt es sich um eine umfassende Aufstellung aller Prozesse, mittels derer personenbezogene Daten verarbeitet werden. Die Auflistung soll als Basis einer unternehmerischen Reflektion dienen, mittels derer prozessindividuell Risiken identifiziert, konkretisiert und sodann geeignete technisch-organisatorische Maßnahmen zur Risikominderung definiert werden.

Primäre Intention des Verzeichnisses ist folglich, unternehmensintern ein Bewusstsein für datenschutzrelevante Prozesse zu schaffen und eine Auseinandersetzung mit Risiken und vorbeugenden Maßnahmen herbeizuführen. Sekundär dient das Verarbeitungsverzeichnis auch der Transparenz der Verarbeitungsprozesse gegenüber Aufsichtsbehörden.

Angesichts dieser Funktionen ist das Verarbeitungsverzeichnis ein integraler Bestandteil der datenschutzrechtlichen Compliance und – bei allem Aufwand – ein wichtiges unternehmensinternes Steuerungs- und Schulungsinstrument.

Bei sensiblen Prozessen ist eine Datenschutz-Folgenabschätzung erforderlich

Ergänzend zum Verzeichnis der Verarbeitungstätigkeiten sind Unternehmen verpflichtet, im Zusammenhang mit besonders sensiblen Datenverarbeitungsprozessen vorab eine sogenannte Datenschutz-Folgenabschätzung durchzuführen und das Ergebnis intern zu dokumentieren.

Besonders sensibel dürften insbesondere Datenverarbeitungsprozesse sein, die gesundheitsbezogene Daten betreffen. Kern der Datenschutzfolgenabschätzung ist die detaillierte Beschreibung des Verarbeitungsvorgangs, seines Zwecks und seiner Notwendigkeit, einhergehender Risiken sowie der zur datenschutzrechtlichen Risikominimierung geplanten Maßnahmen. Diese Darstellung muss den nachvollziehbaren Schluss erlauben, dass die Schutzstandards der Datenschutzgrundverordnung im Rahmen der Datenverarbeitung beachtet werden.

Anders als das Verarbeitungsverzeichnis ist die Folgenabschätzung damit stärker bewertender als beschreibender Natur. Auch die Datenschutz-Folgenabschätzung ist folglich ein Instrument, um das unternehmensinterne Bewusstsein für datenschutzrechtliche Belange zu schärfen und überprüfbar zu machen.

Die Betroffenenrechte sind erheblich erweitert worden

Betroffene im Sinne des Datenschutzrecht sind diejenigen, deren personenbezogene Daten gespeichert werden. Ihre Rechte werden durch die neue Verordnung erheblich gestärkt. So kann etwa jederzeit Auskunft über gespeicherte personenbezogene Daten und die Dauer der Speicherung verlangt werden. Aufbauend hierauf bestehen dann diverse Möglichkeiten, um z. B. das Löschen der Daten oder die Herausgabe der ursprünglich übermittelten Informationen zu verlangen.

Diese Rechte sind teilweise nicht neu. Die neue Verordnung bringt aber vielfältige Konkretisierungen und erleichtert die Durchsetzbarkeit der Ansprüche erheblich. Aus Unternehmenssicht ergeben sich hier häufig die komplexesten Umstellungsprobleme. Zwar sind die Ansprüche eingeschränkt, wenn sie im Zusammenhang mit einer im öffentlichen Interesse liegenden Forschung zu unverhältnismäßigen Beeinträchtigungen oder Erschwernissen führen würden, was gerade für die Pharma- und Medizinproduktebranche von großer Bedeutung ist.

Grundsätzlich ist der sachgerechte Umgang mit den erweiterten Betroffenenrechten ohne eine speziell auf die DSGVO angepasste EDV kaum vorstellbar: Insbesondere die vollständige Löschung personenbezogener Daten, die vom Betroffenen verlangt werden kann, ist in Zeiten regelmäßiger und umfangreicher Datensicherung eine technische Herausforderung, so sie denn zielgerichtet und individuell erfolgen soll. Auch die Ansprüche auf Auskunft und Herausgabe bzw. Portierung der Daten können ohne eine technische Infrastruktur, die dies sozusagen auf Knopfdruck ermöglicht, kaum sachgerecht und mit vertretbarem Zeitaufwand erfüllt werden.

Zusammenarbeit mit Drittunternehmen bedeutet Vertragsüberprüfung und -gestaltung!

Obligatorische Basis für das Hinzuziehen von Dienstleistern im Bereich der Datenverarbeitung war bereits bisher eine vertragliche Regelung der Zusammenarbeit. Hiernach wird sich prinzipiell auf Basis der DSGVO nichts ändern. Die datenschutzrechtlichen Neuerungen machen allerdings vielfach eine inhaltliche Neugestaltung der bereits geschlossenen Verträge erforderlich. Die Hintergründe hierfür sind vielfältig: Der Auftragsverarbeiter ist auf Basis der DSGVO Träger umfangreicher eigener datenschutzrechtlicher Verantwortlichkeiten. Die bisherige, etwa für den datenschutzrechtlichen Pflichtenumfang des Auftragnehmers richtungsweisende Differenzierung zwischen weisungsgebundener Tätigkeit (Auftragsdatenverarbeitung) und nicht weisungsgebundener Tätigkeit (Funktionsübertragung) findet sich in der Systematik des DSGVO nicht mehr wieder. Folglich ist z. B. die Aufteilung der Verantwortlichkeiten in den in der Vergangenheit geschlossenen

Verträgen und daran anknüpfend die Haftungsregelung vielfach nicht mehr zweckmäßig; Vertragsüberprüfungen sind sowohl aus Sicht der Dienstleister als auch aus der Perspektive des Auftraggebers dringend anzuraten.

Wearables, Social Media, Apps: Die digitale Kommunikation muss überarbeitet werden

Die DSGVO erhält diverse Regelungen, die den in den vergangenen Jahren rasant gewachsenen Markt innovativer digitaler Gesundheitsangebote via Social Media, Apps oder Wearables besonders betreffen.

Entsprechende Dienstleistungen sind zum einen so zu gestalten, dass mittels Voreinstellung personenbezogene Daten grundsätzlich nur verarbeitet werden, soweit dies erforderlich ist (privacy by default). Die Voreinstellungen der Angebote müssen hierzu insbesondere sicherstellen, dass personenbezogene Daten nicht ohne gezielte Änderung der Grundeinstellungen einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Zum anderen sind die Datenschutzgrundsätze bereits durch die Konzeption entsprechender Angebote wirksam zu schützen (privacy by design), etwa indem nicht ziellos Daten erhoben werden, die für die eigentliche Funktion des Angebots irrelevant sind.

Gerade Anbieter von Wearables und Gesundheits-Apps, die Gesundheitsdaten häufig fortlaufend und in großer Vielfalt erheben, gegebenenfalls in Clouds einbinden und/oder mit den Daten anderer Wearables quervernetzen, sind hier besonders gefordert. Vielfach ist die Diskrepanz zwischen Ist- und Soll-Zustand in diesem Bereich noch groß, ebenso wie die Aufmerksamkeit der datenschutzrechtlichen Aufsichtsbehörden, die durch den aktuellen Facebook-Datenskandal nochmals erhöht wurde.

Datenschutzrechtliche Verstöße kosten

Die Berichterstattung über die Neuerungen im Datenschutzrecht wird nahezu immer begleitet von der Diskussion um die drastisch verschärften Sanktionen. Künftig können im Falle datenschutzrechtlicher Verstöße Bußgelder bis zu 20 Mio. Euro bzw. 4 Prozent des Jahresumsatzes verhängt werden. Der Blick sollte sich aber nicht nur auf die Maximalhöhe des möglichen Bußgelds richten, die Extremfällen vorbehalten sein wird. Im Alltag viel relevanter dürfte sein, dass es voraussichtlich sehr viel häufiger als bisher zur Verhängung von Bußgeld kommen wird. Dies hat unterschiedliche Gründe:

Eine Vielzahl von Regelungen in der Verordnung sorgt dafür, dass datenschutzrechtliche Versäumnisse sichtbarer werden als bisher. Beispielsweise muss der Datenschutzbeauftragte nicht länger nur intern benannt werden, sondern auch der Landesdatenschutzbehörde mitgeteilt werden. Datenschutzrechtliche Pannen müssen ebenfalls gemeldet werden. Zudem wird ein Verbandsklagerecht eingeführt, mittels dessen Geschädigte ihre Rechte aus Datenschutzverstößen durch hierauf spezialisierte Organisationen wahrnehmen lassen können.

Zudem setzt die DSGVO auch die nationalen Behörden hinsichtlich der Sanktionierung datenschutzrechtlicher Versäumnisse unter erheblichen Druck, indem sie explizit verlangt, dass verhängte Bußgelder in jedem Fall wirksam, verhältnismäßig und abschreckend sein müssen.

All dies lässt vermuten, dass Bußgelder nicht nur höher ausfallen werden, sondern vor allem in sehr viel höherer Zahl als bisher verhängt werden. Risikoerhöhend kommt hinzu, dass die Pharmabranche per se über wenig Kredit in der öffentlichen Wahrnehmung verfügt und die von ihr vielfach verarbeiteten gesundheitsbezogenen Daten als besonders schutzwürdig einzustufen sind.

Ausblick

Die DSGVO wird das Datenschutzrecht in Europa grundlegend konkretisieren und reformieren. Entsprechend aufwendig und vielfältig sind die erforderlichen unternehmensinternen Anpassungen.

Was die von der DSGVO angestrebte Harmonisierung des Datenschutzrechts in Europa angeht, wird die Verordnung ihrem, gerade aus Sicht der typischerweise grenzüberschreitend tätigen Pharma- und Medizinprodukteindustrie sehr begrüßenswerten Anspruch leider nur teilweise gerecht: Sie lässt den Gesetzgebern in den Mitgliedstaaten vielfältige Möglichkeiten zur individuellen nationalen Konkretisierung der europäischen Vorgaben. So wird zum Inkrafttreten der Datenschutzgrundverordnung auch ein neues Bundesdatenschutzgesetz wirksam werden. Zudem wird die Auslegung der nationalen und europäischen Neuregelungen in der Praxis in Deutschland zunächst durch die einzelnen Landesdatenschutzbeauftragten erfolgen und durch deren Sichtweisen geprägt sein.

Angesichts dieser Ausgangslage dürften gerade die Monate nach Inkrafttreten der Neuerungen von der Diskussion um unterschiedliche Rechtsauslegungen keinesfalls von Harmonie geprägt sein. Vielmehr dürften gleich zu Beginn diverse Abmahnwellen sowie Verbandsklagen zu erwarten sein, auch um Präzedenzfälle zu schaffen.

Checkliste: Wichtige Aufgaben nach DSGVO

1. Verzeichnis der Verarbeitungstätigkeiten (nach Erheben, Ordnen, Anpassen, Speichern, Weiterleiten sortiert) anlegen. Dabei alle Prozesse, mittels derer personenbezogene Daten verarbeitet werden, auflisten und beschreiben. Manuelle Tätigkeiten und externe Dienstleistungen nicht vergessen!

2. Datenschutz-Folgenabschätzung durchführen.
   Eine Datenschutz-Folgenabschätzung ist bei besonders sensiblen Datenverarbeitungsprozessen (z. B. bei gesundheitsbezogenen Daten) vorab erforderlich. Diese Bewertung muss intern dokumentiert werden.

3. Technische und organisatorische Lösungen für Betroffenenrechte einrichten und dokumentieren (Datenschutzmanagement nach Art. 32 DSGVO, auch für Informationsformulare, Homepage, Wearables, Social Media, Apps etc.), z. B.:
   - Datenschutzkonzept erstellen.
   - Richtlinien für die Mitarbeiter zum Datenumgang verteilen.
   - Datenschutzerklärung auf Website und Social-Media-Seite anpassen. Betroffene umfassend über ihre Rechte nach § 13 DSGVO informieren. Dabei die Formvorgaben nach § 12 DSGVO einhalten.
   - Mittels Voreinstellung personenbezogene Daten dürfen nur verarbeitet werden, soweit dies erforderlich ist (privacy by default)
   - Die Datenschutzgrundsätze sind bereits durch die Konzeption entsprechender Angebote wirksam zu schützen (privacy by design).
   - Verlangt ein Betroffener Auskunft (z. B. über seine gespeicherten personenbezogenen Daten und die Dauer der Speicherung), die Berichtigung, das Löschen seiner Daten oder die Herausgabe bzw. Portierung der ursprünglich übermittelten Informationen, muss „auf Knopfdruck" reagiert werden können.

4. Auftragsverarbeitung durch Dienstleister überprüfen und Verträge nach Art. 28 Abs. 3 DSGVO anpassen.

5. Betrieblichen Datenschutzbeauftragten (intern oder extern) bestellen und der Landesdatenschutzbehörde melden (Art. 37 Abs. 7 DSGVO).

6. Datenverluste, Datenpannen und Hackerangriffe melden (Selbstanzeige nach Art. 32 DSGVO innerhalb von 72 Stunden gegenüber der Aufsichtsbehörde und Nachricht an den Betroffenen nach Art. 33 DSGVO).

7. Dokumentations- und Rechenschaftspflichten erfüllen (Art. 5 DSGVO). Betrifft das Einhalten aller Vorgaben der DSGVO.