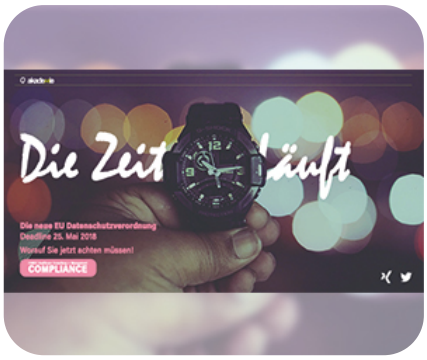

EU Datenschutzverordnung - Die Zeit Läuft!

03.05.2018 | Cornelia Piontke | Fachbeiträge

Deadline ist der 25. Mai 2018: Die neue EU-Datenschutzgrundverordnung (DSGVO) wird wirksam und ist anzuwenden. Mit der DSGVO hat die EU die Verarbeitung von personenbezogenen Daten neu geregelt und vor allem Einrichtungen im Gesundheitswesen, die mit sensiblen Daten von Patienten umgehen, müssen sich jetzt auf neue Anforderungen einstellen.

WORAUF SIE JETZT ACHTEN MÜSSEN - EINE CHECKLISTE

Deadline ist der 25. Mai 2018 | Die neue EU-Datenschutzgrundverordnung (DSGVO) wird wirksam und ist anzuwenden. Nach einer Übergangsfrist von zwei Jahren seit Inkrafttreten der DSGVO am 25. Mai 2016 sind die Tage des Abwartens gezählt. Mit der DSGVO hat die EU die Verarbeitung von personenbezogenen Daten neu geregelt und vor allem Einrichtungen im Gesundheitswesen, die mit sensiblen Daten von Patienten umgehen, müssen sich jetzt auf neue Anforderungen einstellen.

Dass die DSGVO mit ihren 99 Artikeln keine einfache, schnell durchzublätternde Rechtslektüre ist, hat sich herumgesprochen und entsprechend hoch ist die Schwelle, sich dem Werk anzunehmen. Mit unseren Informationen und der Checkliste nehmen wir Sie gern an der Hand und überspringen die Hürde, um Licht in den Dschungel der 99 Artikel der DSGVO zu bringen und die wesentlichen Punkte zu erhellen.

Warum das alles und welche Daten sind von der DSGVO eigentlich betroffen?

Hintergrund der neuen DSGVO ist die Berücksichtigung technischer Aspekte in der heutigen Zeit. Der Schutz sensibler Daten im Kontext von Themen wie Internet, moderne IT-Infrastrukturen wie Cloud-Computing, Kommunikation im Emailverkehr oder Nutzung von Online-Netzwerken sollten sich im Datenschutz wiederfinden. Ziel war es, die Rechte von Betroffenen zu stärken und datenschutzrechtliche Vorgaben an den technologischen Fortschritt anzupassen.

Die DSGVO bezieht sich daher auf die Verarbeitung personenbezogener Daten im Unternehmen oder auf der Webseite des Unternehmens. Zu den personenbezogenen Daten gehören auch Gesundheitsdaten, für die eine besondere Schutzbedürftigkeit gilt.

Was sind die wichtigsten Neuregelungen der DSGVO?

Die neue DSGVO will letztlich Unternehmen dazu zu verpflichten, persönliche Daten von Kunden und Beschäftigten besser zu schützen und somit die Rechte der Betroffenen stärken, wenn es um die Verarbeitung personenbezogener Daten geht. Die DSGVO geht mit neuen Transparenz- und Informationspflichten der Unternehmen über die bisher geltenden Regelungen des Bundesdatenschutzgesetzes hinaus. Betroffene werden in ihrem Recht auf Information, auf Auskunft und Widerspruch, auf Berichtigung und Löschung sowie Übertragbarkeit ihrer Daten gestärkt. Zudem treffen die Unternehmen weitreichende Nachweis- und Dokumentationsverpflichtungen.

WELCHE KONKRETEN AUSWIRKUNGEN HAT DIE DSGVO AUF UNTERNEHMEN?

- ***Einwilligungs- und Widerspruchserklärungen, Auskunftspflichten sowie Datenübertragbarkeit***

Die Verarbeitung von personenbezogenen Daten wie zum Beispiel Gesundheitsdaten ist grundsätzlich verboten und daher nur unter bestimmten Voraussetzungen möglich (Art. 9 DSGVO) Die Anforderungen an eine Einwilligung und Erklärungen wurden erhöht. Die Unternehmen müssen nachweisen können, dass Betroffene eine freiwillige, informierte und eindeutige Einwilligung zur Datenverarbeitung aktiv abgegeben hat oder dass andere Erlaubnistatbestände vorliegen. Die Einwilligung sollten die Unternehmen ausreichend dokumentieren.

Das Recht, die Einwilligung zur Datenverarbeitung zu widerrufen, muss jederzeit, ohne Begründung und genauso einfach Einwilligungserklärung möglich sein. Auf das Widerrufsrecht muss der Betroffene deutlich, zum Beispiel durch besondere visuelle Hervorhebung, hingewiesen werden.
Betroffene können zudem zukünftig von den Unternehmen weitergehende Informationen bezüglich ihrer Daten verlangen. Das heißt, Unternehmen sind beispielsweise verpflichtet, Informationen zur Speicherungsdauer, Verarbeitungszweck oder dessen Änderung zur Verfügung zu stellen (Art. 13 DSGVO).
Betroffene werden zukünftig auch in ihrem Recht bestärkt, ihre persönliche Daten vom Unternehmen einfordern zu können oder die Daten direkt an Dritte übermitteln zu lassen (Art. 20 DSGVO). Im Gesundheitswesen wird dies insbesondere beim Arztwechsel oder Weiterleitung von Gesundheitsdaten im Rahmen einer Behandlung interessant.

- ***Recht auf „Vergessenwerden“ und Berichtigung***

Entscheidet sich ein Betroffener, der Verarbeitung seiner Daten zu widersprechen, so muss das Unternehmen dem Verlangen umgehend nachkommen und die Daten entsprechend löschen. Entsprechende Prozesse und Zuständigkeiten sollten daher eingerichtet werden, um bei Bedarf auf Löschbegehren unverzüglich reagieren zu können. Unternehmen haben zudem dafür Sorge zu tragen, dass ihre Datenbestände aktuell sind. Das heißt auch, dass falsche Daten zu berichtigen sind.

- ***Privacy by Design und Privacy by Default***

Die Unternehmen haben im Umgang mit sensiblen Daten die Grundsätze der Datensicherheit und Datensparsamkeit einzuhalten. Das bedeutet, dass der Schutz personenbezogener Daten durch technische und organisatorische Maßnahmen sichergestellt wird. Zudem sind Voreinstellungen datenschutzfreundlich vorzunehmen, so dass so wenig wie möglich personenbezogene Daten verarbeitet werden.

- ***Datenschutzbeauftragter***

Ein Datenschutzbeauftragter (Art. 37 DSGVO) ist grundsätzlich zu benennen, wenn im Unternehmen personenbezogene

- ***Dokumentation durch das Verzeichnis von Verarbeitungstätigkeiten***

Mittels des Verzeichnisses von Verarbeitungstätigkeiten sollen die Unternehmen alle ihre Maßnahmen und Anstrengungen dokumentieren (Art. 30 DSGVO). Ein solches Verzeichnis kann in Form einer Tabelle erstellt werden, in der unter anderem aufgelistet wird, welche Daten, wann, wie, zu welchem Zweck und wie lange im Unternehmen erhoben werden. Sollte das Unternehmen wegen eines Datenschutzverstoßes angemahnt werden, kann eine gute Dokumentation im Zweifel vor Bußgeld schützen.

- ***Beauftragung Dritter mit Datenverarbeitung***

Entschließt sich ein Unternehmen externe Dritte mit der Verarbeitung personenbezogener Daten zu betrauen, so fällt dies künftig unter die neue Auftragsverarbeitung. Hierfür muss ein Auftragsvertrag geschlossen werden, der zum Beispiel regelt, um welche Daten es sich handelt und zu welchem Zweck diese verarbeitet werden, wie sie geschützt und wann sie gelöscht werden. Die Drittunternehmen sollten in der Lage sein, mit Hilfe technischer und organisatorischer Maßnahmen den Anforderungen des Datenschutzes und der Datensicherheit zu entsprechen.

- ***Datenschutz-Folgenabschätzung (Privacy Impact Assessment)***

Unternehmen, die besonders sensible Daten verarbeiten, bei denen ein hohes Risiko für die Betroffenen besteht – wie etwa im Gesundheitswesen – müssen besondere Sorgfalt walten lassen. Dateninhalte, ihr Umfang oder der Zweck für die Verarbeitung können ein hohes Risiko begründen. Unter Umständen ist dann eine so genannte Datenschutz-Folgeabschätzung (Art. 35 DSGVO) durchführen, um geeignete Schutzmaßnahmen und Sicherheitsvorkehrungen für die Rechte und Freiheiten der Betroffenen vornehmen zu können.

- ***Meldung von Verstößen und welche Sanktionen drohen bei Verstößen?***

Ist es zu einem Datenverstoß gekommen, so muss die Aufsichtsbehörde und der Betroffene darüber informiert werden. Es ist sinnvoll, im Vorfeld Prozesse und Verfahren zur Kommunikation festzulegen.
Entsprechend der DSGVO gibt es größere Haftungsrahmen und die Höhe von Bußgeldern wird nach den Umständen bestimmt. Angedroht sind bis zu 20 000 000 € oder für Unternehmens von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorigen Geschäftsjahrs pro Verstoß.

WAS IST ALSO ZU TUN?

Die Zeit für die Umsetzung der DSGVO läuft und darum ist es spätestens jetzt ratsam, eine Bestandsaufnahme zu machen. Überprüfen Sie, ob die datenschutzrechtlichen Maßnahmen im Unternehmen den Vorgaben der DSGVO entsprechen und handeln Sie gegebenenfalls. Hierfür ist es sinnvoll, die Überprüfung von Dokumenten und Prozessen mittels einer Checkliste abzuklären, die auch im Rahmen eines Compliance-Managements vorgenommen werden kann:

- ***Grundsätzliches Datenschutzmanagement (Organisation und Dokumentation, zum Beispiel: Bestellung eines Datenschutzbeauftragten)***
- ***IT-Sicherheitskonzept***
- ***Datenschutzerklärungen (Anpassung an erweiterte Informationspflichten)***
- ***Einwilligungserklärungen (Beachtung der umfangreichen formalen Vorgaben / zum Beispiel Gesundheitswesen: Patientenformulare)***
- ***Widerrufsrecht (Hinweis und Prozesse zur Umsetzung)***
- ***Datenübertragbarkeit (Prozesse zur Datensicherheit / zum Bespiel Gesundheitswesen - Krankenhausinformationssysteme / Patientendaten)***
- ***Auskunftspflichten (Prozesse zur Auskunft von Informationen)***

JOMEC GmbH
Katharinenstraße 17
10711 Berlin
+49 (0)30-32 666 124-0
info@JOMEC.de

Mit der neuen DSGVO kommen auf Unternehmen zahlreiche neue Pflichten in den Bereichen Dokumentation, Risikobewertung und Kontrolle zu. Will ein Unternehmen also nicht Gefahr laufen, durch Datenschutzverstöße mit einem Bußgeld bestraft zu werden, sollte es seine Datenschutzpraxis dringend an die Anforderungen der DSGVO anpassen und rechtskonform gestalten.

Jetzt einen unverbindlichen Beratungstermin vereinbaren

Rufen Sie uns an oder schreiben Sie uns

+49 (0)30-32 666 124-0

info@jomec.de

JOMEC GmbH
Katharinenstraße 17
10711 Berlin

+49 (0)30-32 666 124-0
info@JOMEC.de