DERRA, MEYER & PARTNER
Rechtsanwälte PartGmbB

DS-GVO „Readiness Check“ –

Das sind die Herausforderung für das Unternehmen

Am 25.05.2016 ist die EU-Datenschutz-Grundverordnung (DS-GVO) in Kraft getreten. Die DS-GVO gestaltet den Datenschutz in Deutschland grundlegend neu. Es wird nicht nur der Bußgeldrahmen um etwa den Faktor 60 erhöht, sondern auch die Anforderungen an die Organisation und die Dokumentation im Datenschutz grundlegend erweitert. Ab dem 25.05.2018 gilt, dass jede Verarbeitung personenbezogener Daten entweder den Anforderungen der DS-GVO entspricht oder rechtswidrig ist. Die Zeitspanne muss daher dazu genutzt werden, die Verarbeitung personenbezogener Daten an diesen neuen Vorgaben auszurichten!

Für welche Fälle gelten die Anforderungen der DS-GVO?

Wie bereits heute im Datenschutzrecht ist auch für die DS-GVO entscheidend, ob personenbezogene Daten verarbeitet werden. Das sind mit anderen Worten alle Informationen, die auf einen Menschen beziehbar sind.

Auf der Hand liegt, dass damit Menschen als Kunden und Beschäftigte erfasst sind. Aber im Unternehmensalltag gilt das häufig auch für sonstige Kunden, Lieferanten und Geschäftsbeziehungen. Denn der Vertragspartner mag eine juristische Person sein, aber typischerweise werden dazu auch Daten von Menschen (Ansprechpartner, Geschäftsführer, etc.) gespeichert.

Reine Maschinendaten sind ausgenommen. Das ist bedeutend für das Thema Industrie 4.0. Dabei darf aber nicht übersehen werden, dass auch dort die DS-GVO gilt, wenn mittelbar auch eine Aussage über einen Menschen getroffen wird (bspw. die Begleitperson der Maschine). Auch die Digitalisierung und Smart- bzw. Big-Data kommen nie an einer Datenschutzprüfung vorbei.

Kurzum: Es gibt kaum einen Bereich des Unternehmens, den der Datenschutz nicht erfasst.

Warum die Umstellung auf die DS-GVO nicht verpasst werden darf!

Vorstehendes ist nicht neu. Neu ist allerdings das Aufdeckungs- und Sanktionsrisiko bei Verstößen.

Der Bußgeldrahmen wird durch die DS-GVO um etwa den Faktor 60 erhöht! Der Bußgeldrahmen wird je nach Verstoß auf 10 Mio./20 Mio. EURO (bzw. 2%/4% des weltweiten Vorjahresumsatzes) erhöht. Das führt zwangsläufig zu signifikant höheren Bußgeldern.

Ihr Ansprechpartner: Rechtsanwalt Dr. Jens Eckhardt, Derra, Meyer & Partner, Düsseldorf, Ulm, Berlin,
Fachanwalt für IT-Recht, Datenschutz-Auditor (TÜV), Compliance-Officer (TÜV),
eckhardt@derra-d.de, Tel.: +49 211 17520660

Das ist aber nur der vordergründige Aspekt der Verschärfung. Grundlegender ist, dass die DS-GVO dem Ansatz „Datenschutz durch Dokumentation und Organisation“ folgt. Das bedeutet für die Unternehmenspraxis:

- Die DS-GVO hat drei grundlegende „Stellschrauben“ zur Dokumentation und Organisation:

  1. Das Unternehmen muss durch Dokumentation nachweisen, dass es die Vorgaben der Datenschutzgrundverordnung einhält (Art. 5 Abs. 2 DS-GVO).
  2. Das Unternehmen muss durch nachweisbare Maßnahmen die Einhaltung des Datenschutzrechts sicherstellen (Art. 24 DS-GVO).
  3. Durch dokumentierte Maßnahmen muss ebenfalls sichergestellt sein, dass der umfangreiche Katalog der Betroffenenrechte erfüllt werden kann (Art. 12 DS-GVO).

  Allein mit diesen Schlagworten können Sie natürlich so noch nichts anfangen und wissen auch nicht, was zu tun ist. Aber Sie können erkennen, dass die DS-GVO von Ihnen mehr und anderes verlangt als das bisherige Datenschutzrecht.

- Derjenige, dessen Daten verwendet werden, ist zukünftig viel umfassender proaktiv (!) über den Umgang mit seinen Daten zu informieren. Die Erweiterung der Informationspflicht geht so weit, dass auch die Rechtsgrundlage genannt werden muss, die zur Datenerhebung berechtigt. Ein Verstoß hiergegen ist leicht feststell- und damit sanktionierbar.

- Die vorstehende Informationspflicht bedeutet damit auch, dass der Datenverarbeiter für jede Verarbeitung die Zulässigkeit prüfen muss, um die Rechtsgrundlage benennen zu können.

- Kommt es zu einer Datenpanne – sprich insbesondere Verlust, Offenlegung der Daten oder Fremdzugriff – ist die Aufsichtsbehörde und der Betroffene zu informieren.

- Bei risikobehafteten Datenverarbeitungen muss eine Folgenabschätzung durchgeführt werden und gegebenenfalls sogar die Datenschutzaufsichtsbehörde verpflichtend zur geplanten Datenverarbeitung befragt werden.

Dieser Effekt der Pflicht zur Befassung und Mehraufwand ist durch die DS-GVO sehr wohl gewollt. Denn die DS-GVO will die Unternehmen geradezu dazu zwingen, sich mit der Datenverarbeitung auseinanderzusetzen. Das zeigt sich auch darin, dass allein schon der Verstoß gegen die vorgenannten Dokumentations- und Organisationspflichten zu Bußgeldern und zur Haftung führen kann. Sie müssen daher ernst genommen werden.

Für die Unternehmenspraxis machen vor allem die „Stellschrauben“ einen weiteren Aspekt deutlich: Das Unternehmen und damit die Unternehmensleitung ist für die Einhaltung des Datenschutzes verantwortlich. Die DS-GVO gestaltet den Datenschutz als Management-Aufgabe aus. Die DS-GVO macht deutlicher als das bisherige deutsche Datenschutzrecht, dass nicht der Datenschutzbeauftragte sondern die Unternehmensleitung verantwortlich ist.

DERRA, MEYER & PARTNER
Rechtsanwälte PartGmbB

Was zulässig ist, bleibt nicht automatisch zulässig!

Die DS-GVO regelt auch die Frage, unter welchen Voraussetzungen eine Datenverarbeitung zulässig ist, grundlegend neu. Einwilligungen in die Datenverarbeitung sind nach dem 25.05.2018 nur noch gültig, wenn sie bereits den Anforderungen der DS-GVO entsprechen. Auch die gesetzlichen Zulässigkeitsregelungen ändern sich grundlegend, sodass eine Prüfung anhand der DS-GVO erforderlich ist. Das bedeutet zwar nicht, dass alles zwingend unzulässig wird, aber was zulässig bleibt, weiß man erst nach der Prüfung.

In der Gesamtschau

Alles neu macht der Mai 2018? Ja und nein – die bisherigen Prinzipien werden beibehalten, aber im Detail wird alles neu geregelt. Das zeigt sich zwar erst auf den zweiten Blick, ist aber nicht weniger wichtig oder weniger bußgeldbewehrt.

Gerade darin liegt aber ein Risiko, da der Ansatz „weiter so, bisher ist auch nichts passiert“ große Risiken birgt. Denn ob die nun geforderte Dokumentation und Organisation stattgefunden hat, lässt sich eben leicht prüfen und sanktionieren.

Einen Bestandsschutz, dass alte Datenverarbeitungen fortgesetzt werden dürfen, gibt es nicht! Der EU-Gesetzgeber sieht daher die Übergangsfrist von Inkrafttreten bis zur Geltung vor. Eine irgendwie geartete Karenzzeit nach dem 25.05.2018 wird es aber nicht geben. Dann ist die DS-GVO zu beachten.

Was jetzt getan werden muss!

Wie gehen Sie es an? In einem ersten Schritt müssen Sie sich die neuen Anforderungen für Ihr Unternehmen verdeutlichen. In einem zweiten Schritt erfassen Sie den Ist-Zustand und passen ihn an die Vorgaben der DS-GVO an.

Bei diesen Schritten unterstützen wir Sie gerne mit unserer Erfahrung!

Rechtsanwalt Dr. Jens Eckhardt, Derra, Meyer & Partner, Düsseldorf, Ulm, Berlin
Fachanwalt für IT-Recht, Datenschutz-Auditor (TÜV), Compliance-Officer (TÜV)
eckhardt@derra-d.de, Tel.: +49 211 17520660