Datenschutz

EU-DSGVO: Die Zeit läuft

Mit der EU-Datenschutz-Grundverordnung (DSGVO) wird der Datenschutz zu einem festen Bestandteil des Risikomanagements. Verfahren und Prozesse müssen bis zum 25. Mai 2018 überprüft und angepasst werden. Nachfolgend Hinweise zur Umsetzung.

Die EU-DSGVO tritt am 25. Mai 2018 in Kraft. Im Gegensatz zur Richtlinie 95/46/EG, die von den EU-Mitgliedstaaten erst in nationales Recht umgesetzt werden musste, gilt die DSGVO ab diesem Zeitpunkt unmittelbar in allen EU-Mitgliedstaaten.

Eine aus der Verordnung heraus mögliche Nutzung von Öffnungsklauseln wurde in einem Datenschutz-Anpassungsgesetz beschlossen und am 31. Juli 2017 im Bundesgesetzblatt veröffentlicht.

Unternehmen sollten nunmehr, bis zum Inkrafttreten der DSGVO, ihre Verfahren und Prozesse überprüfen und an die neuen Vorgaben anpassen. Der Datenschutz wird damit auch zu einem festen Bestandteil des eigenen Risikomanagementsystems.

Wichtige Umsetzungsschritte

Im Hinblick auf die bereits bestehende Richtlinie 95/46/EG und das daraus auf nationaler Ebene bestehende BDSG ist davon auszugehen, dass Datenschutz in den meisten Häusern bereits gelebt wird und damit – im Vergleich zu anderen europäischen Mitgliedstaaten – in der Unternehmenskultur angekommen ist. Somit dürften bereits grundsätzliche Maßnahmen zum Schutz der personenbezogenen Daten etabliert sein.

Die Herausforderung besteht nun darin, den derzeitigen Ist-Stand im Datenschutz an die neue Verordnung anzupassen. Hierzu ergeben sich zwangsläufig verschiedene praktische Aufgabenstellungen. Diesen müssen sich die Unternehmen widmen, um den Anforderungen der DSGVO gerecht werden zu können. Im Folgenden werden einige wesentliche Aspekte der DSGVO aufgegriffen sowie wichtige Umsetzungsschritte dargestellt:

1. **Haben Sie einen Datenschutzbeauftragten benannt?**
   Art. 37 der DSGVO nennt die Kriterien, wann ein Datenschutzbeauftragter nach neuem Recht „benannt“ werden muss. Der § 38 des neuen Nachfolgegesetzes des alten BDSG, des Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU (DSAnpUG-EU), konkretisiert dies in bewährter Form: ab mindestens zehn Personen, die mit einer ständigen automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

   Aber Achtung: Auch wer keinen Datenschutzbeauftragten nach neuem Recht benennen muss, ist gut beraten, sich mit dem Datenschutz in seinem Unternehmen zu beschäftigen.
2. **Haben Sie ein Verzeichnis von Verarbeitungstätigkeiten erstellt?**
   Bislang musste der Verantwortliche in Ihrem Unternehmen nach dem BDSG ein internes und ein öffentliches Verfahrensverzeichnis führen. Das öffentliche Verzeichnis entfällt künftig. Gemäß DSGVO sind das Unternehmen (Verantwortlicher) und nunmehr auch Auftragsverarbeiter verpflichtet, ein Verzeichnis von Verarbeitungstätigkeiten zu erstellen und zu führen. Als datenverarbeitendes Unternehmen sollten Sie prüfen, welche inhaltlichen Anforderungen Art. 30 DSGVO an das neue Verzeichnis stellt, diese mit Ihrem alten Verzeichnis abgleichen und ggf. ergänzende Veränderungen vornehmen.

   Sinnvollerweise sollten Sie den Prozess der Risiko- und Datenschutz-Folgenabschätzung nach Art. 35 DSGVO für die Betroffenen mit in die Dokumentation einbinden. Sie kommen so gleichzeitig der notwendigen Nachweispflicht nach.
3. **Haben Sie eine Übersicht Ihrer Auftragsverarbeiter?**
   Auftragsverarbeiter kann eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle sein, die personenbezogene Daten im Auftrag des Verantwortlichen (Ihr Unternehmen) verarbeitet. Die bisherigen vertraglichen Regelungen basierten auf dem § 11 BDSG und gestalten sich nunmehr weitgehend über den Art. 28, der

DSGVO und nach § 62 DSAnpUG-EU. Die Analyse Ihrer Vertragsdatenbank (Vertragsspiegel) nach vorhandenen Verträgen mit Auftragsverarbeitern sowie die Anpassung der Verträge entsprechend den neuen gesetzlichen Vorgaben ist dringend anzuraten.

4. **Haben Sie Ihre technischen und organisatorischen Maßnahmen (TOMs) neu dokumentiert?**
   Der Art. 32 DSGVO gibt vor, dass geeignete technische und organisatorische Maßnahmen vorzuhalten sind, um den Risiken für die Rechte und Freiheiten natürlicher Personen mit einem angemessenen Schutzniveau begegnen zu können. Diese sollten sich nicht nur in der bereits erwähnten Verarbeitungsübersicht wiederfinden, sondern auch separat dokumentiert werden: Dies empfiehlt sich mit Blick auf eine verbundene Risikobetrachtung und Maßnahmenbeschreibung unter Berücksichtigung des Technikstands und der Implementierungskosten. Ein Verfahren zur Überprüfung der Wirksamkeit der TOMs sollte gemäß Art. 32 Abs. 1 lit. d DSGVO implementiert werden. Dies kann auch über ein bestehendes Informationssicherheitsmanagementsystem und den dort bereits integrierten PDCA-Kreislauf (Plan – Do – Check – Act) mit abgebildet werden.
5. **Weitere Schritte, die umgesetzt und beachtet werden sollten**

- Interner Prozess zur Gestaltung der Meldepflichten bei Datenpannen gemäß Art. 33 und 34 DSGVO
- Interner Prozess zur Umsetzung des „Rechts auf Löschung“ und des „Rechts auf Vergessenwerden“ gemäß Art. 17 DSGVO und § 58 DSAnpUG-EU
- Interner Prozess zur Umsetzung des „Auskunftsrechts“ gemäß Art. 15 DSGVO und § 57 DSAnpUG-EU
- Umsetzungsprozess zur Erfüllung der Informationspflichten bei der Erhebung von personenbezogenen Daten (hier auch Ihren Internetauftritt beachten) gemäß Art. 12, 13, 14 DSGVO und § 55 DSAnpUG-EU
- Prüfung eingesetzter Einwilligungen nach Art. 7 DSGVO und § 51 DSAnpUG-EU

Und nicht zuletzt ist auch daran zu denken, die Mitarbeiter/-innen entsprechend den neuen gesetzlichen Normen zu sensibilisieren und zu schulen.

… und wenn wir versuchen, es auszusitzen?

Verstöße gegen die Europäische Datenschutz-Grundverordnung können in Zukunft hohe Strafen nach sich ziehen. Es drohen Bußgelder von bis zu 20 Millionen Euro oder bis zu 4 % des globalen Unternehmensumsatzes (Art. 83 DSGVO). Der Bußgeldrahmen soll wirksam und abschreckend sein. Vielleicht sind kleinere Unternehmen in der Höhe nicht vollständig betroffen, aber auch kleinere Bußgelder können schmerzlich sein und ggf. die eigene Reputation schwächen.

Sollten Sie sich die Frage stellen, ob Sie in Ihrem Unternehmen die DSGVO beachten müssen, so sei hier angemerkt, dass die Gültigkeit der Verordnung alle in der EU ansässigen Unternehmen betrifft. Verarbeiten Sie personenbezogene Daten im Sinne von Art. 2 und 3 der DSGVO, so müssen Sie in Ihrer betrieblichen Praxis die Regelungen der Verordnung entsprechend beachten.

AUTOR UND ANSPRECHPARTNER

Thomas Grebe
Leiter IT-Sicherheit und Datenschutz,
E-Mail: thomas.grebe@geno-tec.de

Fazit

Wenn man sich die grundlegenden Maßnahmen, wie vor beschrieben, vergegenwärtigt hat und umsetzt, so sind die wichtigsten Meilensteine für den Start der neuen DSGVO gelegt.

Der ab dem 25. Mai 2018 beginnende öffentliche Diskussionsprozess um die richtige Auslegung strittiger Datenschutzfragen im Inland und in der EU wird die Basis in verschiedenen Punkten verändern, so dass an den bisher gesetzten Eckpunkten nachjustiert werden muss.

Wem die Umsetzung der datenschutzrechtlichen Aufgaben im Moment lästig erscheint, sollte der wirtschaftliche Mehrwert als Anreiz dienen. Er ergibt sich durch die Prozessprüfung, in dessen Folge die Datenqualität verbessert bzw. die Datenquantität entsprechend reduziert werden kann. Nicht zu vergessen sei darüber hinaus die Rechenschaftspflicht („Accountability“, Art. 5 Abs. 2 DSGVO), verbunden mit zahlreichen Dokumentations- und Nachweispflichten zur Einhaltung der Datenschutzvorgaben gegenüber den zuständigen Aufsichtsbehörden. Hier gilt, mit Aristoteles gesprochen: „Wer schreibt, der bleibt“! ▬