Dr. Walter Burger & Partner
Steuerberatungsgesellschaft mbB

Neue Datenschutzgrundverordnung – Selbstverteidigung für Unternehmen

Von Rechtsanwalt Jan N. Machunsky - Datenschutzbeauftragter

Am 25. Mai 2018 tritt die Datenschutzgrundverordnung (DSGVO) in Kraft. Eigentlich ändert sich im Verhältnis zum Bundesdatenschutz nicht viel – eigentlich. Denn ab dem 25. Mai ist der Dornröschenschlaf des Datenschutzes beendet: es wird auch ohne konkreten Anlass systematisch kontrolliert und hart durchgegriffen werden. Nach dem aktuellen Diskussionsstand ist mit einer Schonfrist für Datensünder nicht zu rechnen.

Womit müssen Sie ab dem 25. Mai rechnen?

- ✓ Auskunftsersuchen durch die Behörden
- ✓ Aufforderung, etwa das Verfahrensverzeichnis innerhalb weniger Tage vorzulegen
- ✓ Drastische Geldbußen, von bis zu 4 % des weltweiten Jahresumsatzes
- ✓ Abmahnwelle durch darauf spezialisierte Anwaltskanzleien

Was ist zu tun?

So bürokratisch und umsatzfern die Aufgaben auch sind, es muss gehandelt werden, um drastischen Konsequenzen vorzubeugen. Zu den Aufgaben gehören:

- ✓ Erstellung eines Verfahrensverzeichnisses
- ✓ Bestellung eines Datenschutzbeauftragten
- ✓ Datenschutzerklärung (Website)
- ✓ Hinweise zur Datenverarbeitung sowie Einwilligungen
- ✓ Technische und organisatorische Maßnahmen zur Datensicherheit

Die 1. Verteidigungslinie – Außenverteidigung

Die Experten sind sich darüber einig, dass die vollständige Einhaltung aller Regeln ebenso illusorisch ist, wie deren komplette Umsetzung bis zum 25. Mai. Es sind also Prioritäten zu setzen. Angesichts der drohenden Abmahnwelle sind zunächst Mängel abzustellen, die von außen ohne Weiteres erkennbar sind.

Punkt 1 – der betriebliche Datenschutzbeauftragte

Es ist leicht zu prüfen, ob ein Unternehmen einen Datenschutzbeauftragten hat, da dieser in allen Datenschutzinformationen genannt werden muss (Art. 37 Abs. 7 DSGVO). Fehlen diese Informationen, haben Abmahnanwälte ein leichtes Spiel und Fehler sind nachträglich kaum zu verteidigen.

Mehr zum betrieblichen Datenschutzbeauftragten weiter unten.

Punkt 2 – der Außenauftritt

Ein weiterer unmittelbarer Angriffspunkt sind die nach Art. 13 und 14 DSGVO erforderlichen Datenschutzinformationen, die wesentlich umfangreicher sein müssen, als bisher. Entsprechende Angaben auf Websites müssen also dringend angepasst werden.

Die 2. Verteidigungslinie – Innenverteidigung

Die materielle Umsetzung des Datenschutzes findet innerhalb der Firma statt. Diese Umsetzung müssen Sie allerdings gegenüber der Datenschutzbehörde nachweisen können – Sie müssen auch in der Lage sein, auf Anfragen von Betroffenen kurzfristig Auskunft zu erteilen.

Punkt 3 – Dreh- und Angelpunkt: das Verarbeitungsverzeichnis

In Art. 30 der DSGVO wird die Führung eines Verzeichnisses aller Verarbeitungstätigkeiten vorgeschrieben. Hauptzweck dieses Verzeichnisses ist der Nachweis DSGVO-konformer Datenverarbeitung. Gleichzeitig dient das Verzeichnis für die interne Überprüfung der Datensicherheit und die sogenannte „Gab Analysis“. Zu beiden Punkten später mehr.

Punkt 4 – Datensicherheit in der IT: TOMs oder „Technische und organisatorische Maßnahmen“

Hier geht es um die eigentlichen Fragen der Datensicherheit, für die die IT-Spezialisten gefragt sind. Wie sind die Zugriffsrechte der Mitarbeiter geregelt, welche Maßnahmen gibt es zur Abwehr von Cyberattacken und zum Virenschutz. Welche Sicherheitsmaßnahmen sind bei der Nutzung sozialer Medien, Handys oder privaten E-Mail-Accounts getroffen.

In technischer und organisatorischer Hinsicht ist insbesondere auf folgende Punkte zu achten:

- ✓ Es sind Schutzmechanismen gegen einen unbefugten Zugriff zu ergreifen
- ✓ Personenbezogene Daten müssen vor unberechtigter Veränderung geschützt werden.
- ✓ Die Daten müssen dauerhaft verfügbar sein. Es muss Vorkehrungen für einen Ausfall der IT geben.
- ✓ Mitarbeiter dürfen nur auf die Daten zugreifen, die Sie zur Verrichtung Ihrer Tätigkeit benötigen.
- ✓ Die elektronische Unternehmenskommunikation hat verschlüsselt stattzufinden, um einen unberechtigten Zugriff auf die Daten zu vermeiden.
- ✓ Der Zugang zu Büro- und Lagerräumen in denen sich personenbezogene Daten befinden ist zu erschweren.
- ✓ Unterlagen sowie Notebooks und Smartphones müssen geschützt werden (Passwort) und ebenso auch vor unberechtigter Einsichtnahme geschützt werden (Sichtschutz).
- ✓ Laufende Anforderungen
- ✓ Nachdem die Datenschutzsysteme installiert wurden, sind neue Verarbeitungs-prozesse einzuschätzen und zu erfassen.
- ✓ Die Mitarbeiter sind regelmäßig im Datenschutz zu schulen

Die 3. Verteidigungslinie – Spezialaufgaben

Punkt 5 – Gap Analysis

Gap heißt Lücke und „Gap Analysis“ schlicht Lückensuche oder Fehlersuche.

Basis dieser Suche ist das Verarbeitungs- und Verfahrensverzeichnis. Es sind zum Beispiel folgende Punkte zu klären:

- ✓ Ist die Datenverarbeitung rechtlich zulässig. Gibt es Einwilligungen der Betroffenen, ist sie zur Erfüllung eines Vertrages notwendig, dient sie berechtigten Interessen (Rechtmäßigkeit)
- ✓ Werden die Daten tatsächlich benötigt (Datensparsamkeit)
- ✓ Ist der Zugriff von Mitarbeitern auf die Daten beschränkt, die Sie für Ihre Arbeit benötigen (Zugriffsrechte)
- ✓ Sind die Rechner hinreichend gegen den räumlichen Zugang durch Unbefugte geschützt (Zugangskontrolle)
- ✓ Sind Firewall und Virenscanner ausreichend und aktuell (Cyber Security)
- ✓ Werden Daten gelöscht, wenn sie nicht mehr erforderlich sind, gibt es Löschroutinen? (Löschkontrolle)
- ✓ Sind die Daten auf dem neuesten Stand und fehlerfrei (Datenrichtigkeit)

Was noch zu bedenken ist:

Es gibt weitere Regelungen in der DSGVO, die es zu beachten gilt und auf die man vorbereitet sein sollte:

Punkt 6 Betroffenenrechte

Nach Art. 15 der DSGVO – einer recht langen Vorschrift – haben die „Betroffenen" umfangreiche Auskunftsrechte darüber, welche Daten von Ihnen wo und wie gespeichert sind und wo sie sich gegebenenfalls beschweren können. Daneben gibt es Ansprüche auf Datenübertragung oder Datenlöschung.

Punkt 7 Meldepflichten

Jeder Datenschutzverstoß und jede Datenpanne muss innerhalb von maximal 72 Stunden bei der Datenschutzbehörde gemeldet werden. Neben Cyberattacken kann schon ein verlorenes Diensthandy meldepflichtig sein.

Punkt 8 Datenschutzrichtlinien

Interne Datenschutzrichtlinien geben den Mitarbeitern Orientierung und Verhaltensanweisungen und dokumentieren gegenüber den Behörden, dass der Datenschutz ernst genommen wird.

Zur Vertiefung:

Nachfolgend noch eine etwas ausführlichere Darstellung von Verarbeitungsverzeichnis und Datenschutzbeauftragter.

Das Verzeichnis von Verarbeitungstätigkeiten

Es muss ein Überblick über alle Tätigkeiten im Unternehmen verschafft werden, die personenbezogene Daten automatisieren sowie teilweise automatisiert verarbeitet werden. (Verfahrensverzeichnis). Ebenfalls sind nicht automatisierte Vorgänge zu erfassen, die in einem Dateisystem gespeichert werden oder werden sollen.

Betroffen sind unter anderem:

- ✓ Kundendaten, Kundenbestellungen
- ✓ Buchführung
- ✓ Terminverwaltung, Mailprogramme
- ✓ Firmenwebsites, Soziale Medien
- ✓ Personalakten, Firmenintranet, Urlaubslisten

Hier ist jeweils unter anderem festzuhalten, zu welchem Zweck die Verarbeitung erfolgt, wer dafür zuständig ist, wer darauf Zugriff hat und an wen die Daten übermittelt werden.

Der Datenschutzbeauftragte

Der Datenschutzbeauftragte soll den Verantwortlichen, das heißt etwa der Unternehmensleitung bzw. dem Vereinsvorstand als kompetenter Ansprechpartner in Datenschutzfragen zur Seite stehen. Die Verantwortung für die Einhaltung des Datenschutzes verbleibt jedoch bei den Verantwortlichen.

Ab wann brauche ich einen Datenschutzbeauftragten?

Wann ein Datenschutzbeauftragter zu bestellen ist, hängt einerseits von der Anzahl der im Unternehmen beschäftigen Personen, andererseits von der Art der verarbeiteten Daten ab.

1. Beschäftigen Sie mindestens zehn Personen in Ihrem Unternehmen bzw. Verein, welche automatisiert personenbezogene Daten verarbeiten?
   ➔ Sie benötigen einen Datenschutzbeauftragten.

   Hier spielt es keine Rolle, in welchem Beschäftigungsverhältnis diese Personen zu Ihnen stehen und ob diese ehrenamtlich arbeiten. Selbst die Arbeitszeit spielt keine Rolle.
2. Verarbeiten Sie in Ihrem Unternehmen oder Verein Daten folgender Art:
   - ✓ Gesundheitsdaten?
   - ✓ Daten zur rassischen oder ethnischen Herkunft?
   - ✓ Daten zur sexuellen Orientierung bzw. zum Sexualleben?
   - ✓ Daten, aus denen die religiöse oder weltanschauliche Überzeugung hervorgeht?
   - ✓ Daten über die politische Meinung?
   - ✓ Daten zur Gewerkschaftszugehörigkeit?
   - ✓ Daten über strafrechtliche Verurteilungen und Straftaten
   - ✓ Genetische Daten?
   - ✓ Biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person?

   Sofern die Verarbeitung dieser Daten eine Kerntätigkeit Ihres Unternehmens darstellt, benötigen Sie einen Datenschutzbeauftragten.

3. Bildet die regelmäßige und systematische Überwachung von Personen die Kerntätigkeit Ihres Unternehmens?
   ➔ Sie benötigen einen Datenschutzbeauftragten.

Sofern Sie einen Datenschutzbeauftragten benötigen, bieten sich Ihnen zwei Varianten an:

Interner Datenschutzbeauftragter:

Ein interner Datenschutzbeauftragter kennt das Unternehmen bereits gut. Er fällt jedoch für die Zeiten der Aus- und Fortbildung sowie während der Arbeit als Datenschutzbeauftragter aus. Darüber hinaus entstehen Kosten für die Aus- und Fortbildung sowie Literatur.

Externer Datenschutzbeauftragter:

Ein externer Datenschutzbeauftragter hat den Vorteil, dass er keinerlei Einarbeitungszeit benötigt, keinerlei Aus- und Fortbildungs-, sowie Literaturkosten entstehen. Darüber hinaus übernimmt einen Teil der Haftung ein externer Datenschutzbeauftragter. Zudem werden Sie in allen Fragestellungen rund um den Datenschutz objektiv beraten.

Sollten Sie Beratungsbedarf haben oder einen externen Datenschutzbeauftragten benötigen, freuen wir uns über Ihre Kontaktaufnahme.

Dr. Machunsky & Partner Rechtsanwälte

Rupertistr. 21a

22609 Hamburg

Tel.: 040 95060

Mail.: kanzlei@dr-machunsky.de

Web.: www.dr-machunsky.de