Hilfe, die Behörde kommt! – Was tun?

Sicher haben Sie sich, während Sie sich mit der Umsetzung datenschutzrechtlicher Themen beschäftigt haben, schon das ein oder andere Mal gefragt, ob die Datenschutzbehörde einfach irgendwann vor der Tür Ihres Unternehmens stehen und Einlass verlangen kann. Darf die Behörde dies überhaupt? Muss sie sich ankündigen?

Dieser Newsletter beschäftigt sich mit diesen Fragen und geht zunächst auf die Befugnisse und Aufgaben der Datenschutz-Aufsichtsbehörden ein und beschäftigt sich in einem zweiten Teil damit, wie Sie als kontrolliertes Unternehmen mit einer etwaigen Überprüfung (Vor-Ort oder schriftlich) umgehen können.

1. Aufgaben und Befugnisse der Aufsichtsbehörde

Um verstehen zu können, auf welcher Grundlage die Aufsichtsbehörde eine Kontrolle des Unternehmens durchführen darf, sind zunächst ihre Aufgaben und Befugnisse zu beleuchten.

Jedes Bundesland hat gem. § 40 BDSG eine/n Landesbeauftragte/n für den Datenschutz. Es gibt somit insgesamt 16 Landesbeauftragte in Deutschland. Zusätzlich existiert noch der Bundesbeauftragte für Datenschutz und Informationsfreiheit. Dessen Stellung ist in § 18 BDSG geregelt, wohingegen sich die Stellung der 16 Landesdatenschutzbeauftragten aus Art. 52 DSGVO ergibt. Letztere handeln dabei weisungsfrei und unabhängig, um eine einheitliche Anwendung der DSGVO herbeizuführen und deren Umsetzung zu überwachen.

Zu den Hauptaufgaben der nationalen Aufsichtsbehörden gehören ausweislich des Art. 57 DSGVO im Wesentlichen:

- → Die Überwachung und Durchsetzung der DSGVO
- → Die Bearbeitung von Anfragen und Beschwerden von Betroffenen (Art. 57 Abs. 1 lit. e, f DSGVO)
- → Die Durchführung der notwendigen Untersuchungen über die Anwendung der DSGVO
- → Die Sensibilisierung von Verantwortlichen für die Verpflichtungen der DSGVO
- → Die Erstellung von Black- und Whitelisten für die Datenschutz-Folgenabschätzung
- → Die Festlegung von sog. Standard-Vertragsklauseln, die die Rechtsgrundlage für die Datenübermittlung in Drittländer darstellen

Um die vorgenannten Aufgaben erfüllen zu können und vor allem um sicherzustellen, dass innerhalb der EU ein gleichwertiger Datenschutzstandard vorherrscht, werden die Aufsichtsbehörden mit bestimmten Befugnissen ausgestattet. Diese lassen sich in drei wesentliche Kategorien einteilen:

- → Untersuchungsbefugnisse gem. Art. 58 Abs. 1 DSGVO
- → Abhilfebefugnisse gem. Art. 58 Abs. 2 DSGVO
- → Genehmigungsbefugnisse und beratende Befugnisse gem. Art. 58 Abs. 3 DSGVO

Im Rahmen dieses Newsletters möchten wir nur näher auf die Untersuchungsbefugnisse eingehen. Die DSGVO räumt den Aufsichtsbehörden nämlich weitreichende Kompetenzen ein, damit diese ihrem Auftrag, der Schaffung eines einheitlichen Datenschutzniveaus, nachkommen können. Hierzu kann sie:

- → Den Verantwortlichen anweisen, alle Informationen bereitzustellen, die für die Erfüllung der Aufgaben der Aufsichtsbehörde erforderlich sind
- → Datenschutzüberprüfungen vor Ort vornehmen, ohne dass hierzu ein konkreter Anlass vorliegen muss
- → Den Verantwortlichen auf entsprechende Verstöße hinweisen und deren Beseitigung anordnen
- → Den Verantwortlichen anweisen, ihr Zugang zu allen personenbezogenen Daten und Informationen zu verschaffen, die sie im Rahmen ihres Prüfauftrages benötigt
- → Vom Verantwortlichen den Zugang zu den Geschäftsräumen, einschließlich der Datenverarbeitungsanlagen verlangen. Hier gilt allerdings, dass diese Untersuchungsbefugnisse im Einklang mit dem geltenden Verfahrensrecht ausgeübt werden sollen.[1] Es bedarf also hierfür eines richterlichen Beschlusses. Liegt ein solcher vor und ist dieser formell ordnungsgemäß, existieren keine Möglichkeiten, die Kontrolle der Behörden zurückzuweisen. Auch eine der Kontrolle voraus gehende Ankündigung ist nicht zwingend.

Die Behörde kann allerdings auch – als Alternative zu den Vor-Ort-Kontrollen – Fragebögen versenden oder automatisierte Online-Audits durchführen. Diese dienen der Behörde natürlich in erster Linie dazu, sich ein Bild vom aktuellen Ist-Zustand zu machen und dann aber auch in einem zweiten Schritt die Abweichungen vom Soll-Zustand zu bewerten und entsprechende Maßnahmen zu treffen. Hier kann die Behörde den Verantwortlichen dazu auffordern, rechtswidrige Datenverarbeitungsvorgänge abzustellen, aber auch Hinweise dazu erteilen, wie bei bestimmten Vorgängen Datenschutzkonformität erreicht werden kann. Ein Prüfbesuch der Behörde ist, wie sich aus dem vorstehend Gesagten ergibt, somit möglich, aber wohl eher als ultima ratio oder für den Fall anzunehmen, in dem permanente oder schwerwiegende Verstöße vorliegen.

Ob die Behörde zudem ein Bußgeld verhängt, richtet sich nach der Schwere des festgestellten Verstoßes und danach, ob der Verantwortliche aktive Maßnahmen ergreift, um etwaige Rechtsverletzungen abzustellen. *Aber Achtung: Diese Bußgelder haben es in sich und können bis zu 20.000.000 EUR oder im Fall eines Unternehmens bis zu 4% des gesamten Vorjahresumsatzes betragen.*[2]

2. Konkretes Verhalten im Unternehmen

Sollte also eines Tages unverhofft die Datenschutzbehörde vor der Tür stehen, sollten Sie die folgenden Verhaltensregeln beachten:

[1] ErwGr 129.

[2] Eine Auflistung von bisher (In Europa oder speziell in Deutschland) verhängten Bußgelder können Sie bei Interesse hier einsehen: https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php

- → Ruhe bewahren!
- → Informieren Sie die Geschäftsführung und den Datenschutzbeauftragten.
- → Arbeiten Sie mit der Behörde zusammen und verweigern Sie keine Kontrollmaßnahmen.
- → Setzen Sie die Damen und Herren in einen Besprechungsraum und übergeben Sie die Ordner mit den Verfahrensverzeichnissen, Datenvorfällen, Laufzetteln etc.

Sollten Sie einen Prüf-Fragebogen bekommen, kontaktieren Sie den Datenschutzbeauftragten. Dieser unterstützt Sie gern bei der Beantwortung der Fragen und bei der Zurverfügungstellung der entsprechenden Dokumente. Die Behörde wird Ihnen in dem Anschreiben eine Frist setzen, innerhalb derer sie die Beantwortung der Fragen erwartet. Auch hier gilt: Scheuen Sie sich nicht, die Behörde um eine Verlängerung der Frist zu bitten. Das Zusammentragen der Informationen kann seine Zeit in Anspruch nehmen. Sprechen Sie aber auch ein solches Vorgehen mit Ihrem Datenschutzbeauftragten ab.

3. Zusatz: Wie kann so ein Prüf-Fragebogen der Behörde aussehen?

Die folgenden Angaben dazu, wie so ein Datenschutz-Prüfbogen aussehen kann, sind natürlich nicht abschließend und erheben auch keinen Anspruch auf Vollständigkeit. Sie dienen lediglich als Beispiel, damit Sie sehen, auf welche Fragen Sie sich im Falle einer Überprüfung einstellen müssen:

1. Wie stellen Sie sicher, dass jede (neue) Verarbeitung von personenbezogenen Daten in das Verzeichnis für Verarbeitungstätigkeiten[3] aufgenommen wird?
2. Auf welcher Rechtsgrundlage verarbeiten Sie personenbezogene Daten?
3. Wie stellen Sie sicher, dass die Rechte von Betroffenen innerhalb der entsprechenden Fristen gewahrt werden?
4. Gewährleisten Sie durch technische und organisatorische Maßnahmen ein angemessenes Datenschutz-Niveau?
5. Wie prüfen Sie im Unternehmen Verarbeitungstätigkeiten mit einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen? Führen Sie eine Datenschutz-Folgenabschätzung durch? Identifizieren Sie bereits risikobehaftete Verarbeitungen?
6. Sind für sämtliche Auftragsverarbeiter entsprechende Verträge vorhanden und sind diese an die DSGVO angepasst?
7. Haben Sie einen Datenschutzbeauftragten in Ihrem Unternehmen?
8. Wie gehen Sie mit Datenschutzvorfällen um?
9. Können Sie die Punkte 1.-8. nachweisen?

Bei der Beantwortung dieser Fragen ist es wichtig, dass Sie wahrheitsgemäß antworten. Skizzieren Sie bei der Beantwortung die unternehmensinternen Prozesse und versenden Sie Musterdokumente für die entsprechenden Vorgänge. Die in der DSGVO verankerte Rechenschaftspflicht verpflichtet Sie zur Dokumentation der o.g. Prozesse.

Sollten Sie zu diesem Themenkreis Fragen haben, stehen wir Ihnen jederzeit gerne zur Verfügung.

Ihr Team der RKM Data GmbH

[3] Zur Erstellung des Verarbeitungsverzeichnisses siehe Newsletter 08/2020.