

Wenn die Datenschutzbehörde klingelt ...

28.5.2020 – Mehrere tausend Verfahren hat es in Österreich im Zusammenhang mit der DSGVO bereits gegeben, in den meisten Fällen waren Beschwerden von Betroffenen Anlass. Birgit von Maurnböck, Spezialistin für Datenschutz in der Afpa, zeigte auf, wie die Datenschutzbehörde vorgeht, was sie darf und wie man sich auf den „Ernstfall“ vorbereiten kann.

Auch wenn die Coronakrise momentan aufmerksamkeitsmäßig alles überdeckt, bleiben profane Dinge trotzdem „am Tisch“. Für die Versicherungs- und Finanzberaterbranche etwa die Frage: „Die Datenschutzbehörde klopft an. Worauf muss ich vorbereitet sein?“

Diese Herausforderung abseits des täglichen Geschäfts war Thema eines Webinars der [Verbands der österreichischen Finanz- und Versicherungsprofessionisten](#) (Afpa): Ja, es gibt einiges zu beachten wenn sich die Datenschutzbehörde meldet – aber man kann den Ernstfall proben.

Die „Lotsin für Datenschutzrecht und praktische DSGVO-Umsetzung“ in der Afpa, Birgit von Maurnböck, ist eine auf Datenschutzrecht spezialisierte Juristin und als Unternehmensberaterin für die Themen Datenschutz, Compliance und IT tätig.

So hat sie schon etliche Verfahren vor der Datenschutzbehörde (in weiterer Folge: DSB) auf Unternehmensseite begleitet. Bei dem Webinar ging sie daher auf praktische Fragen ein.

Was bisher geschah

Oft führen Beschwerden von Betroffenen oder auch Mitbewerbern zu einer Prüfung – zum Beispiel aus dem Grund, weil der Betroffene meint, seine Betroffenenrechte seien nicht rechtskonform erfüllt worden.

Bisher waren und sind mehrere tausend Verfahren in Österreich anhängig. Auch wenn die bisherigen Strafen meist nicht sehr hoch gewesen seien (mit Ausnahme der Österreichischen Post), gilt: „Unwissenheit schützt vor Strafe nicht“, warnt Maurnböck.

Natürlich leitet die Datenschutzbehörde auch amtswegig Verfahren ein, wenn sie beispielsweise aufgrund der Meldung einer Datenpanne den Verdacht hegt, dass in einem Unternehmen DSGVO und Datenschutzgesetz nicht eingehalten werden.

Es beginnt mit Briefen

Grundsätzlich meldet sich die DSB schriftlich (an): mit einer „Aufforderung zur Stellungnahme“ zu einer ihr zugegangenen Beschwerde.

Nun gilt es, die dort formulierten Vorhaltungen genau zu prüfen, sicherheitshalber die Datenverarbeitung des betreffenden Beschwerdeführers einzuschränken und innerhalb der Antwortfrist schriftlich Stellung zu nehmen.

Wenn man vielleicht wirklich Verabsäumtes auch gleich ausbessert, könne die DSB von einer Strafe absehen. Ebenso kann man der DSB natürlich Argumente vorbringen, warum man meint, rechtskonform gehandelt zu haben. Vor allem dann, wenn es um Graubereiche aufgrund der noch sehr jungen DSGVO-Auslegung gibt.

Einschauen

Die DSB kann Einschau in das Verarbeitungsverzeichnis verlangen und erfragen, wie viele und welche Verantwortliche, Verarbeitungen, Auftragsverarbeiter (Vertragsvollständigkeit!) es gibt und ob Datenschutzfolgeabschätzungen durchgeführt wurden. Sie kann sich auch einzelne Verarbeitungen vorführen lassen und die Schulung der Mitarbeiter überprüfen.

Eine Datenschutzfolgenabschätzung muss man verpflichtend machen, wenn mindestens zwei der folgenden Kriterien zutreffen:

- Umfangreiche Verarbeitung besonderer Datenkategorien (Gesundheitsdaten, Religion, etc.),
- Umfangreiche Verarbeitung strafrechtsbezogener Daten,
- Erfassung von Standortdaten,
- Verarbeitung von Daten schutzwürdiger Personen (Personen unter 14 Jahren, Arbeitnehmer, Patienten),
- Zusammenführung bzw. Abgleich von Daten aus mehreren Verarbeitungen zu unterschiedlichen Zwecken, wenn die betroffenen Personen diese Verarbeitung üblicherweise nicht erwarten können und wenn die Daten nicht direkt bei der betroffenen Person erhoben wurden.

Vor-Ort-Schwächen

Weiters kann die DSB bei einem höchstpersönlichen Besuch im Unternehmen selbst EDV-Systeme, die Zutritts/Zugangsmöglichkeiten, die Papierablage (wer hat worauf Zugriff?) oder auch die Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen (TOMs) kontrollieren.

Einen praktischen Tipp zur Vorbereitung auf einen DSB-Besuch hat Maurnböck noch: „Den Ernstfall proben!“

Also etwa eine unangekündigte Prüfung durch qualifizierte Dritte (Auditoren) durchspielen lassen, regelmäßig interne Überprüfungen und Mitarbeiterschulungen machen und dokumentieren – aus Fehlern lernen und Fehlendes umgehend vervollständigen.

[Manfred Kainz](#)