MMag. Birgit Harasser
Rechtsanwältin bei BRAND Rechtsanwälte GmbH

18 Monate DSGVO

Erste Bilanz. Sie war 2018 eines der meistdiskutierten Themen, seit rund eineinhalb Jahren ist sie nun anwendbar – die Europäische Datenschutz-Grundverordnung (DSGVO). Zeit, eine erste Bilanz zu ziehen.

Mehr Bewusstsein – mehr Beschwerden

Eines hat die DSGVO jedenfalls bewirkt, das Bewusstsein für Datenschutz ist massiv gestiegen. Nach einer Umfrage der Europäischen Kommission haben 73% der EU-Bürger schon von mindestens einem der Rechte für betroffene Personen (Information, Auskunft, Widerspruch, Löschung, Beschwerderecht etc) gehört. Dementsprechend gab es einen massiven Anstieg von Auskunfts- und Löschungsanfragen bei Unternehmen. Ebenso sind die Anfragen, Beschwerden und Verfahren bei den Datenschutzbehörden gestiegen. In den ersten zwölf Monaten gingen europaweit rund 150.000 Anfragen und Beschwerden bei den Aufsichtsbehörden ein.

Auswirkung in Unternehmen

Hat sich die DSGVO – wie im Vorfeld vielfach befürchtet – negativ auf die wirtschaftliche Entwicklung von Unternehmen ausgewirkt? Nach der Austrian-Business-Check-Umfrage des KSV ist dies klar nicht der Fall: Für 62% der Befragten hat die DSGVO keinen negativen Einfluss auf die Unternehmensfinanzen. Aber auch am Sicherheitsniveau hat sich wenig geändert, lediglich für 14% der Unternehmen hat die DSGVO zu einer gravierenden Sensibilisierung im Umgang mit Daten geführt. Rund die Hälfte der Unternehmen geben an, dass die DSGVO nichts am bestehenden Sicherheitsniveau verändert hat.

Dass Datensicherheit – und zwar nicht primär Cybersecurity – eines der Hauptthemen für Unternehmen – zeigt sich daran, dass im ersten Jahr DSGVO rund 90.000 „data breach notifications", also die verpflichtenden Meldungen von Unternehmen über eine Datenschutzverletzung bei den europäischen Datenschutzbehörden eingegangen sind. Die irische Behörde hat diese aufgeschlüsselt: 85% der Datenschutzverletzungen betrafen die unautorisierte Offenlegung von Daten; gefolgt von Verlust, Diebstahl oder unsachgemäßer Entsorgung von Papierdokumenten – erst danach kamen Hackerangriffe.

Klar ist inzwischen auch, dass es großen Aufholbedarf gibt. Spitzenreiter bei den in österreichischen Unternehmen umgesetzten Maßnahmen ist die Einführung oder Anpassung von Daten- und IT-Sicherheitsmaßnahmen – aber auch nur in 53% der Unternehmen. Nur rund die Hälfte hat die erforderlichen Zustimmungserklärungen eingeholt, das Verarbeitungsverzeichnis erstellt oder – wo nötig – einen Datenschutzbeauftragten bestellt. Weniger als die Hälfte der Unternehmen hat geprüft, wie man mit Auskunftsersuchen von Betroffenen umgeht, und lediglich 22% haben einen Prozess zum Umgang mit Datenmissbrauch oder Datenverlust festgelegt. Und in immerhin 10% der Unternehmen gab es noch überhaupt keine Umsetzung.

DSGVO-Umsetzung

Im Oktober hat die Berliner Datenschutzbeauftragte einen Bußgeldbescheid über 14,5 Mio Euro gegen die Deutsche Wohnen SE erlassen, weil personenbezogene Daten von Mietern in einem Archivsystem gespeichert wurden, bei dem nicht mehr erforderliche Daten nicht gelöscht werden konnten. Gehaltsabrechnungen, Auszüge aus Arbeits- und Ausbildungsverträgen, Steuer-, Sozial- und Krankenversicherungsdaten sowie Kontoauszüge wurden über Jahre gespeichert, ohne zu prüfen, ob dies rechtmäßig und noch erforderlich ist.

Gerade in der Immobilienwirtschaft werden besonders viele personenbezogene Daten verarbeitet – Namen und Adressdaten, Informationen zur Bonität, Kontodaten, Anzahl der im Haushalt lebenden Personen, Alter, Sozialversicherungsdaten, Beruf und Einkommen etc –, in Mietverträgen und Kaufverträgen, WEG-Protokollen, BK-Abrechnungen, für die Vermittlung und Verwaltung wie auch die Bewertung von Immobilien.

Diese Daten müssen auf Basis einer klaren Rechtsgrundlage und in einer für die betroffene Person transparenten Art verarbeitet werden, sie müssen auf das für den jeweiligen Zweck der Verarbeitung notwendige Maß beschränkt sein, dürfen nur so lange gespeichert werden, wie es erforderlich ist, und müssen so verarbeitet werden, dass eine angemessene Sicherheit gewährleistet ist.

Aus diesen Grundprinzipien und dem Erfordernis, dass jeder Verantwortliche deren Einhaltung nachweisen muss, folgen alle umzusetzenden Maßnahmen gemäß DSGVO: Verarbeitungsverzeichnis, technische und organisatorische Maßnahmen, Datenschutzerklärung, Einholung von Einwilligungen zu Werbung und Cookies, Umgang mit Betroffenenrechten wie Auskunftserteilung, Löschfristen, Verträge mit Auftragsverarbeitern, Konzept für den Umgang mit Datenmissbrauch oder Datenverlust.

DSGVO-Strafen – Schonfristende

Möglicherweise liegt die bislang mangelnde Umsetzung in Unternehmen auch daran, dass nach Inkrafttreten der DSGVO zunächst kaum Strafen verhängt wurden, sondern mehr verwarnt wurde. Im Vorfeld der DSGVO waren einer der medialen Aufmacher die zu erwartenden Millionenstrafen – bis zu 20 Mio Euro oder 4% des Jahresumsatzes. In den ersten Monaten nach Inkrafttreten der DSGVO hörte man wenig von Strafen, ein Jahr nach Inkrafttreten las man noch in vielen Medien, die Angst vor den Strafen der DSGVO sei völlig überzogen gewesen. Im Jänner 2019 kam aber bereits ein Paukenschlag, die französische Datenschutzbehörde CNIL verhängte wegen mangelnder Transparenz und Information eine Geldbuße von 50 Mio Euro gegen Google. Im Juli folgte die britischen ICO mit einer Strafe von 204 Mio gegen British Airways und 110 Mio gegen Marriott Hotels, in beiden Fällen wegen mangelnder Sicherheitsvorkehrungen. In Österreich hat die Datenschutzbehörde im Oktober eine Strafe von 18 Mio Euro gegen die Österreichische Post AG verhängt wegen der Verarbeitung von personenbezogenen Daten über die vermeintliche politische Affinität von Betroffenen.

In den meisten Fällen wurden natürlich keine Millionenstrafen verhängt und die Gesamtanzahl der verhängten Strafen ist bislang noch nicht sehr hoch, aber in den letzten Monaten ist ein deutlicher Anstieg zu verzeichnen. Es ist inzwischen klar ersichtlich, dass die europäischen Datenschutzbehörden es ernst meinen und ihre Gangart verschärfen. Daher ist es höchste Zeit, die erforderlichen Maßnahmen zur Einhaltung der DSGVO umzusetzen.

ZLB 2019/47