DSGVO: 10 Punkte-Checkliste für den Business-Alltag

veröffentlicht am 27. 9. 2018 von jake

© iStock / Getty Images

Die neue Datenschutz-Grundverordnung (DSGVO) ist seit 25. Mai 2018 in Kraft. Mehrere Hundert Beschwerden wurden in weniger als vier Monaten wegen verschiedener Verstöße bei der Datenschutz-Behörde eingereicht. Eine Checkliste mit 10 Punkten hilft Nutzern, vor allem KMU, vorhandene Mängel aufzudecken und entsprechende Maßnahmen zu setzen, um das Gesetz auch wirklich einhalten zu können.

Gut vier Monate nach Inkrafttreten der Datenschutz-Grundverordnung zieht das Linzer IT-Haus Fabasoft eine vorläufige Bilanz: Bei der österreichischen Datenschutzbehörde wurden mehr als 720 Beschwerden registriert. Demnach dürften noch immer nicht alle Unternehmen ihre Hausaufgaben und somit gesetzlichen Verpflichtungen nicht erfüllt haben. Manche Unternehmen haben die DSGVO unter anderem auch für ihre eigenen Belange allzu großzügig ausgelegt.

Fabasoft zitiert dabei den international anerkannten Datenschutzaktivisten Max Schrems: „Viele der Pop-Ups und E-Mails waren jedoch leider eine Ausgeburt an Fehlinterpretationen der DSGVO. Oft lassen lästige Nachrichten dem Nutzer keine echte Wahl und drängen zu Zwangszustimmungen."

Dies sei der Grund, warum die Datenschutzbehörde aktiv wurde.

Wer weiterhin auf Zwangszustimmung setzt, wird vor Gericht den Kürzeren ziehen. Beschwerden etwa gegen Facebook wurden via Irland beim Europäischen Datenschutzausschuss vorgelegt. Eine Beschwerde zum Auskunftsrecht bei Bankdaten wird nach einer Entscheidung gegen eine Bank beim Bundesverwaltungsgericht bearbeitet. Und im Fall einer unerlaubten Videoüberwachung sei bereits eine erste Strafe ausgesprochen worden. Ein steirisches Wettlokal sei laut Fabasoft-Aussendung zu einer Geldstrafe von 4800 Euro verdonnert worden, weil es illegal seine Kundschaft per Video überwacht hatte.

„Von Durchatmen darf noch keine Rede sein", warnt Andreas Dangl, Business Unit Executive Cloud Services bei Fabasoft. „So manche Organisation führt das ver-

pflichtende Verzeichnis von Verfahrenstätigkeiten in Excel im aufrichtigen Glauben, dass damit ihre DSGVO-Pflicht getan sei. Doch wer prüft die Einhaltung der Pflichten? Wer garantiert deren korrekte Wartung? Wer ist für die zukünftige DSGVO-Konformität verantwortlich?“ Sind diese Fragen nicht ausreichend zu beantworten, könnte der Datenschutz dem Unternehmen – trotz größter Bemühungen – zum Stolperstein werden.

DSGVO: Sicher in 10 Schritten

1. Arbeiten Sie mit einer strukturierten Datenbank
Zu viele Daten befinden sich nach wie vor in unstrukturierten elektronischen Informationen wie E-Mails, SMS, WhatsApp oder auch Fotos. Optimal ist der Einsatz einer strukturierten Datenbank, in der Unternehmen die exponentiell steigende Datenmenge auch zukünftig im Griff behalten.

2. Nutzen Sie DSGVO-konforme Einwilligungen für die Verwendung personenbezogener Daten
Eine Datenverarbeitung ist nur dann zulässig, wenn eine DSGVO-konforme Einwilligung vorliegt. Die Anforderungen an diese Einwilligungen wurden verschärft: unter anderem beträgt das Mindestalter 16 Jahre.

3. Beachten Sie Ausmaß und Notwendigkeit der Daten
Jedes „zu viel“ an personenbezogenen Daten stellt ein Risiko für Unternehmen dar. Es dürfen voreingestellt nur die Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck auch wirklich erforderlich sind.

4. Berücksichtigen Sie den Datenschutz schon bei der Konzipierung und Entwicklung von Software und Hardware
Alle Projekte, bei denen Unternehmen personenbezogene Daten verarbeiten, müssen nach dem Prinzip „Privacy by Design“ entwickelt werden. Unternehmen können bestehende Systeme entweder nachrüsten oder durch neue DSGVO-taugliche ersetzen.

5. Beziehen Sie alle Mitarbeiter in den Datenschutz mit ein
Generell gilt, dass Datenschutz nie nur Aufgabe einer einzelnen Person sein kann, sondern im Berufsalltag von jedem Mitarbeiter gelebt werden muss. Schulen Sie daher regelmäßig Ihre Mitarbeiterinnen und Mitarbeiter.

6. Verlassen Sie sich nicht auf die ISO/IEC 27001 Zertifizierung
Die ISO/IEC 27001 Zertifizierung reicht als Nachweis eines angemessenen Schutzes gegen unbefugte Zugriffe auf personenbezogene Daten alleine nicht aus. Unternehmen müssen stattdessen prüfen, ob diese Zertifizierung erweitert wurde, zum Beispiel durch Anpassung der Risikobeurteilungsmethode an die Rechte und Freiheiten nach DSGVO.

7. Bewerten Sie Risiken und Folgen für Betroffene immer im Voraus
Unternehmen müssen eine Datenschutz-Folgenabschätzung dann durchführen, wenn neue Technologien eingesetzt werden und die Verarbeitung dazu führt, dass für die Rechte und Freiheiten von Einzelpersonen ein hohes Risiko besteht.

8. Bei einer Datenschutzverletzung: Seien Sie schnell!
Die EU-DSGVO beinhaltet eine klare Vorgabe bei Datenschutzverletzungen: wird dem Unternehmen ein Vorfall bekannt, muss unverzüglich und in der Regel binnen 72 Stunden nach Bekanntwerden bei der zuständigen Aufsichtsbehörde eine Meldung gemacht werden.

9. Treffen Sie die Wahl des Verzeichnisses von Verarbeitungstätigkeiten gewissenhaft
Unternehmen benötigen ein flexibles und sicheres Verzeichnis, das sämtliche Verarbeitungsvorgänge im Umgang mit personenbezogenen Daten dokumentiert. Excel kann hier als kurzfristige Notlösung dienen, für den langfristigen Gebrauch empfehlen sich allerdings professionelle DSGVO-Managementsysteme, in denen datenschutzkonform gearbeitet werden kann.

10. Schaffen Sie ideale technische Voraussetzungen für das Management der Betroffenenrechte
Sollten Personen ihr „Recht auf Vergessenwerden“ in Anspruch nehmen, so reichen in der Regel die gängigen Löschfunktionen von Betriebssystemen und Datenbanken nicht aus, um die Anforderungen der EU-DSGVO zu erfüllen, da die Daten nicht tatsächlich physisch gelöscht werden. Datenschutz-Experten empfehlen hierfür eine eigene Software.

Quelle: https://www.trend.at/branchen/digital/dsgvo-punkte-checkliste-business-alltag-10374027