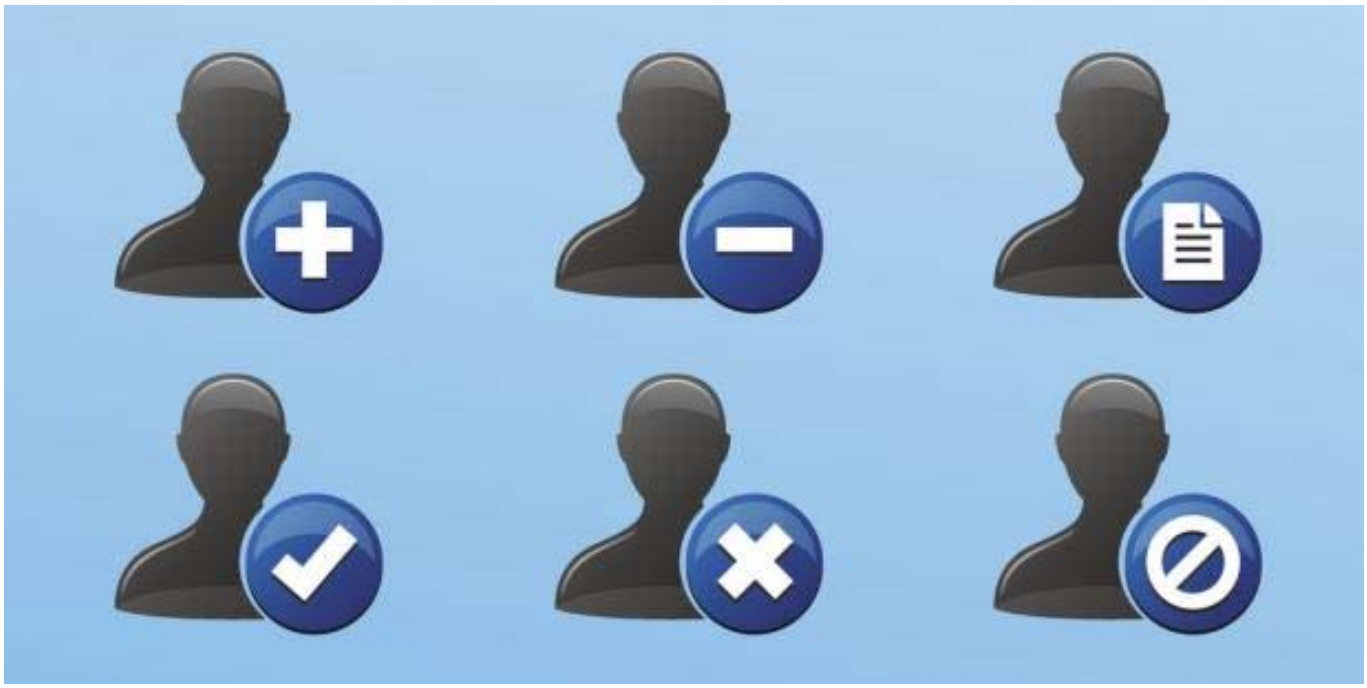
WIRTSCHAFT VOR 3 STUNDEN

Neue Datenschutz-Grundverordnung: Was KMU jetzt wissen müssen



© Bild: Getty Images/Istockphoto/iconeer/Istockphoto

Ab 25. Mai müssen alle Betriebe mit Personendaten sorgfältiger umgehen. Die 10 wichtigsten Punkten, endlich verständlich.

Ein einheitlicher Rechtsschutz für alle 500 Millionen EU-Bürger: Ab 25. Mai werden alle Datensammler und -verarbeiter stärker in die Pflicht genommen. An diesem Tag tritt ein EU-weit einheitliches, strenges Datenschutzgesetz in Kraft. Wer sich nicht daran hält, muss mit hohen Strafen rechnen. Betroffen sind nicht nur Datenkraken wie Facebook oder Google, sondern auch jeder kleine Handwerksbetrieb, der eine Kundendatei führt. Höchste Zeit also, sich um die Umsetzung zu kümmern, mahnen Experten, Panik sei jedoch nicht angebracht.

„Grundsätzlich sind viele der geltenden Regeln gar nicht so anders als bisher, jedoch hatten diese oft nicht die Bedeutung wie jetzt“, erläutert Markus Knasmüller, Prokurist beim BMD-Systemhaus und gerichtlich zertifizierter Sachverständiger für Datenschutz.

Vieles ist in Österreich ohnehin schon geregelt, der EU ging es um einheitliche Standards. Die zum Teil hohen Strafdrohungen würden vor allem dazu dienen, dass Firmen den Datenschutz ernster nehmen. Juristen warnen vor Rechtsrisiken aufgrund unklarer Gesetzesbestimmungen, die den Behörden viel Spielraum ließen. Das komplexe Regelwerk lässt nämlich viele Fragen offen. Der KURIER nahm die zehn wichtigsten Punkte aus Sicht von Klein- und Mittelbetrieben (KMU) unter die Lupe:

1. Transparenz

Ziel der Verordnung ist mehr Transparenz bei personenbezogenen Daten. Jeder sollte wissen, wann welche Daten wo über ihn wie lange gespeichert werden und wie sorgsam mit ihnen umgegangen wird. Für Firmen heißt das: Sie müssen klar und verständlich formulieren, wie personenbezogene Daten verarbeitet und verwendet werden.

2. Personenbezogene Daten

Zu unterscheiden sind sensible und nicht sensible Daten. Die häufigsten Personendaten in Firmendatenbanken sind allgemeine Kontaktdaten wie Name, Anschrift, eMail etc. Besonderen Schutz genießen sensible Daten. Sensibel sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen sowie religiöse oder weltanschauliche Überzeugungen hervorgehen sowie biometrische Daten wie Fingerabdruck oder Irisscan. Sensibel sind natürlich auch alle Gesundheitsdaten. Strengen Regeln unterliegt ferner die automatisierte Verarbeitung der Personendaten zur Profilbildung („Profiling“).

3. Einwilligung

Bitte vorher fragen. Firmen benötigen immer die Einwilligung der Person, dessen Daten sie speichern. Diese Einwilligung ist in vielen Fällen aber bereits vorhanden – etwa wenn eine Geschäftsbeziehung besteht – oder durch andere Rechtsgrundlagen abgedeckt. Liegt keine andere Rechtsgrundlage vor, ist eine Einwilligung einzuholen. Diese kann schriftlich, elektronisch oder auch mündlich (schwer zu beweisen!) erfolgen, etwa durch Anklicken eines Kästchens auf einer Internetseite. Achtung: Ist ein Kästchen bereits vorangeklickt, liegt keine gültige Einwilligung vor. Bei der Verarbeitung sensibler Daten muss jedenfalls eine ausdrückliche Einwilligungserklärung vorliegen.

4. Verzeichnispflicht

Es gelten verschärfte Dokumentationspflichten. Eine Neuerung ist das Führen eines Verarbeitungsverzeichnisses, das die bisherigen Meldungen an das Datenverarbeitungsregister (DVR) ersetzt. Von der Dokumentationspflicht ausgenommen sind Kleinbetriebe (unter 250 Mitarbeiter), die nur gelegentlich

personenbezogene Daten verarbeiten. Die genaue Abgrenzung hier ist aber schwierig. Das Verarbeitungsverzeichnis muss alle Programme enthalten, mit denen personenbezogene Daten verarbeitet werden. Diverse Softwareanbieter bieten dazu eigene Programme an. Diese dienen auch zur besseren Übersicht, wenn etwa jemand das Recht auf Auskunft oder Löschung – siehe Punkt 8 – begehrt. Zur Prävention von Datenmissbrauch oder Datendiebstahl muss im Register auch schon eine Folgenabschätzung enthalten sein. Diese gilt jedoch nur bei sensiblen Daten wie Gesundheitsdaten oder der systematischen Videoüberwachung von öffentlichen Orten.

5. Datenschutzbeauftragter

Zwingend vorgeschrieben ist ein Datenschutzbeauftragter für Behörden, öffentliche Stellen sowie Unternehmen, die regelmäßig und systematisch umfangreiche und sensible Datenmengen verarbeiten, z.B. Banken, Versicherungen oder Krankenanstalten. Auf Klein- und Mittelbetriebe trifft dies wohl nur in Ausnahmefällen zu, sie können aber freiwillig einen Beauftragen ernennen. Dieser muss entsprechend qualifiziert sein und genießt Kündigungsschutz. Seine Aufgabe ist es, die Einhaltung der DSGVO zu überwachen, Mitarbeiter zu schulen und mit Behörden zu kooperieren. Firmen können auch einen externen Datenschutzexperten beauftragen.

WIRTSCHAFT | VOR 3 STUNDEN

Datenschutz: Darf ich eigentlich noch ...?

Vom Gärtner bis zum Installateur: Anwalt Rainer Knyrim, Experte in Sachen Datenschutz, beantwortet Fragen aus der Praxis.

6. Auftragsverarbeiter

Werden Daten nicht nur im eigenen Unternehmen, sondern auch von externen Partnern gespeichert bzw. weiterverarbeitet, so gelten diese als Auftragsverarbeiter. Diese müssen vertraglich garantieren, dass sie die ihnen überlassenen Daten durch geeignete technisch-organisatorische Maßnahmen schützen. Ein solcher Auftragsverarbeiter kann ein IT-Provider sein, der den Web-Shop hostet, ein Steuerberater, ein Cloud-Dienstleister oder eine PR-Agentur. „Die Unternehmen sollten alle Verträge mit Kunden, Lieferanten oder diversen IT-Dienstleistern genau unter die Lupe nehmen und gegebenenfalls dokumentieren“, empfiehlt Martin Puaschitz, Obmann der Obmann der Fachgruppe Unternehmensberatung/IT (UBIT) in der Wirtschaftskammer Wien.

7. Unverlangte Werbung

Newsletter, also elektronische Nachrichten für Werbezwecke, dürfen schon jetzt nur bei einer aufrechten Geschäftsbeziehung oder nur nach Einwilligung des Empfängers – siehe Punkt 3 – versendet werden. Dasselbe gilt für Anrufe, SMS oder Nachrichten über Messengerdienste. Wenn sich jemand vom Newsletter abmeldet, darf er auch keine Zusendung mehr erhalten. Das Aushändigen einer Visitenkarte, um für Produkte oder Dienstleistungen in Kontakt zu bleiben, kann als Zustimmungserklärung gewertet werden – muss aber nicht.

8. Recht auf Löschung

Nichts ist ewig. Grundsätzlich dürfen Daten nur so lange gespeichert werden, wie es für den Speicherzweck erforderlich ist. Ein Unternehmen muss personenbezogene Daten löschen, wenn die betroffenen Personen darauf bestehen oder der Zweck, für den die Daten erhoben wurden, nicht mehr gegeben ist. Dabei muss auch sichergestellt werden, dass keine Spuren – etwa als Backup – bleiben („Recht auf Vergessen“). In der Praxis ist das endgültige Löschen nicht immer einfach, es werden daher diverse Lösch-Tools angeboten. Es gibt aber auch Ausnahmen von der Löschungspflicht, etwa wenn das Recht auf Meinungsäußerung höherwertig ist als das Datenschutzinteresse bzw. bei öffentlichem Interesse. Bei einer Löschung müssen auch alle Empfänger der ursprünglichen Daten darüber informiert werden. Weiters gibt es ein Recht auf Auskunft und ein Recht auf Korrektur falscher Daten. Die Umsetzungsfrist beträgt ein Monat.

9. Übertragbarkeit

Jede Person kann verlangen, dass ihre gespeicherten Daten an Dritte übertragen werden. Beispielsweise sollen Profildaten bei einem Online-Dienstleister mit wenigen Klicks zu einem anderen Anbieter „mitgenommen“ werden können. Die EU will damit Anbieterwechsel erleichtern und so den Wettbewerb fördern.

10. Strafen

Das bisherige Strafausmaß bei Datenschutz-Vergehen wurde deutlich ausgeweitet. Strafen von bis zu 20 Millionen Euro bzw. bis zu vier Prozent des Umsatzes drohen aber nur bei schwerwiegenden Verstößen. Die Verletzung der Dokumentationspflicht ist mit bis zu 10 Mio. Euro oder zwei Prozent des Umsatzes sanktioniert. Dabei hatte die EU vor allem Datenskandale von Großkonzernen im Visier. Bei kleineren Vergehen wird nicht gleich gestraft, sondern verwarnt. In Österreich sieht das Gesetz ausdrücklich das Prinzip „Beraten statt Strafen“ vor. Wenn Firmen ihre Hausaufgaben machen, würden keine hohen Strafen drohen, ist IT-Experte Puaschitz überzeugt. Zugleich warnt er vor Schlamperei oder Vogel-Strauß-Taktik. Gefinkelte Anwälte oder Wettbewerber könnten das ausnutzen. Beschwerden werden von der Datenschützbehörde behandelt, diese führt auch die weiteren Untersuchungen durch.

Im Falle von schweren Datenschutzverletzungen mit hohem Risiko für die Rechte der Betroffenen (z.B. Datenklau durch Hacker) müssen Betriebe dies umgehend der Datenschutzbehörde und den betroffenen Personen melden, sonst drohen ebenfalls Strafen. Die Meldefrist beträgt höchstens 72 Stunden nach Entdeckung. Betriebe, die das Thema bisher ignorierten, sollten also rasch mit der „Dateninventur“ beginnen. Diese Bestandsanalyse ist zwar aufwendig, aber nötig, um die neuen Auflagen zu erfüllen.

Weitere Hilfestellungen sowie Musterdokumente sind auf der Homepage der Wirtschaftskammer und Datenschutzbehörde zu finden.

ANITA
STAUDACHER

(kurier.at) Erstellt am 26.04.2018

DAS KÖNNTE SIE AUCH INTERESSIEREN

Neue Datenschutz-Grundverordnung der EU bleibt wirkungslos

Datenschutz-Grundverordnung: Medien bekommen Ausnahmeregelung

Datenschutz: Darf ich eigentlich noch ...?