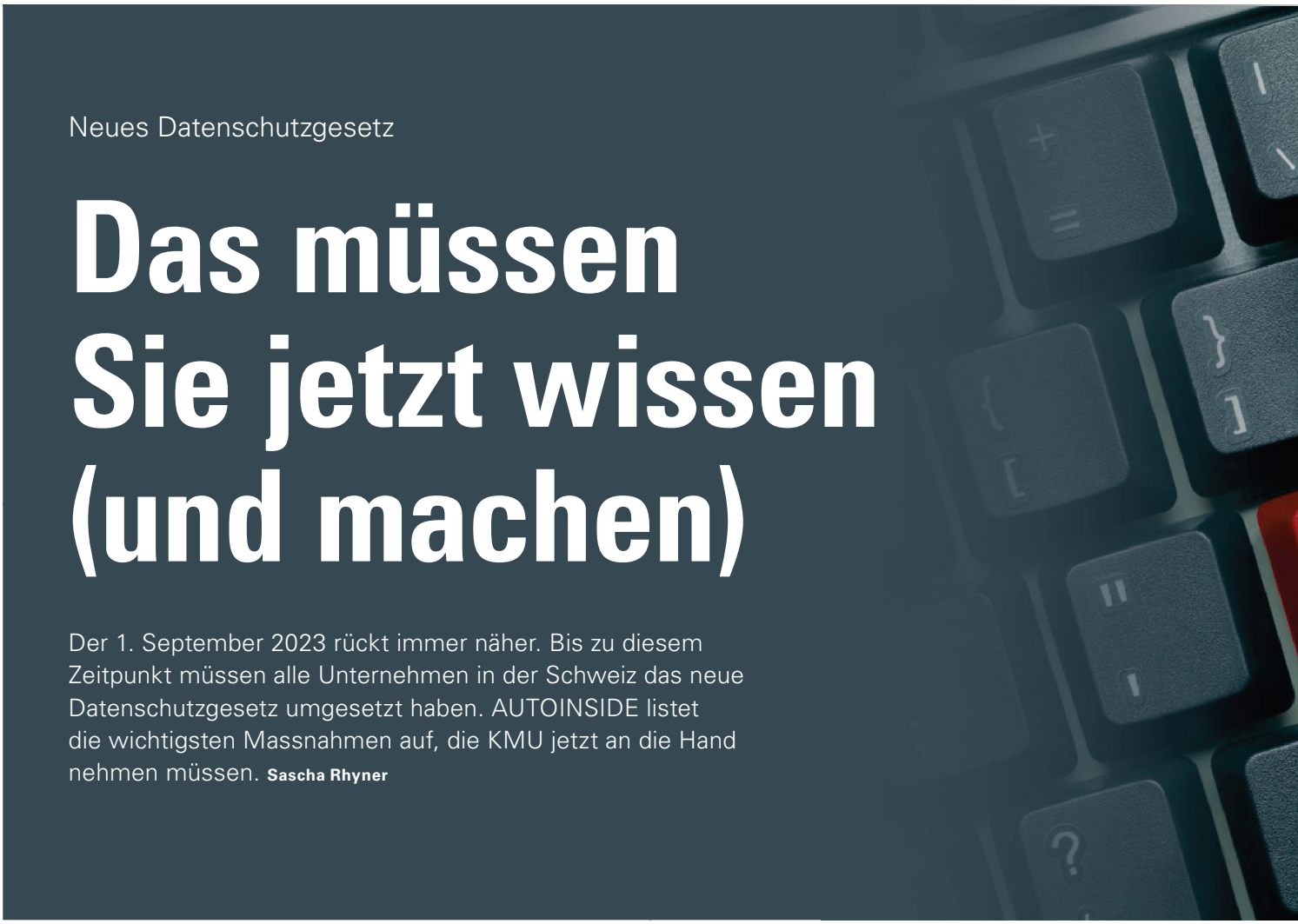

Neues Datenschutzgesetz

Das müssen Sie jetzt wissen (und machen)

Der 1. September 2023 rückt immer näher. Bis zu diesem Zeitpunkt müssen alle Unternehmen in der Schweiz das neue Datenschutzgesetz umgesetzt haben. AUTOINSIDE listet die wichtigsten Massnahmen auf, die KMU jetzt an die Hand nehmen müssen. **Sascha Rhyner**

Warum überhaupt ein neues Datenschutzgesetz (DSG), mag man sich fragen. Bei diesem Gedanken mag mitspielen, dass die EU im Mai 2018 eine neue Datenschutzgrundverordnung (DSGVO) erlassen hatte, was hierzulande ebenfalls gewisse Konsequenzen hatte. Das bisherige Datenschutzgesetz in der Schweiz hingegen datiert aus dem Jahr 1992. Das World Wide Web, entwickelt am Genfer Cern, ist nur gerade drei Jahre älter. Und 1992 wurden in den USA das erste GSM-fähige Mobiltelefon vorgestellt und in der Schweiz das Natel-D-Netz lanciert. Im Autobereich stellte Fiat den Cinquecento vor, um die Nachfolge des Topolino anzutreten, und es gab am 62. Auto-Salon erstmals eine Sonderschau zum Thema Elektro- und Solarmobile; VW präsentierte dort den Chico – damals noch als mögliches «Swatchmobil» gehandelt –, BMW den E1 und General Motors den Impact. Will heissen: Seither ist gerade in diesem Bereich technologisch ziemlich viel passiert.

Was aber sind die wichtigsten Neuerungen im Schweizer Datenschutzgesetz, Ausgabe 2023? AUTOINSIDE listet hier die wichtigsten Punkte für KMU auf.

«Besonders schützenswerte Personendaten» werden umfassender

Natürliche Personen werden künftig stärker geschützt. Bislang galten beispielsweise Angaben über die Herkunft einer Person, gesundheitsrelevante Aspekte oder Informationen über die Religionszugehörigkeit sowie politische Meinungen als besonders schützenswerte Personenangaben. Neu gelten auch genetische Daten wie ethnische Zugehörigkeiten sowie biometrische Daten (Fingerabdruck, Retinascan) als besonders schützenswert.

«Profiling» ist im DSG verankert

Unter «Profiling» versteht man Informationen wie Wohnort einer Person, wirtschaftliche Verhältnisse, Gesundheitszustand, Alter, Arbeitsleistung oder Hobbys und weitere Interessen. Durch diese Angaben lässt sich ein genaues Profil eines Menschen erstellen. Diese Daten dürfen zwar weiterhin erhoben werden, aber nurmehr mit allergrösser Sensibilität. Will heissen: Die Erhebung dieser Daten darf die Persönlichkeitsrechte nicht verletzen. Können aus den Angaben eindeutig Wesenszüge einer Person gelesen werden, spricht man von einem «Profiling mit hohem Risiko». Hier verlangt das neue DSG die ausdrückliche Einwilligung dieser Personen.

«Privacy by Default» und «Privacy by Design»

Diese beiden Begriffe sind im neuen DSG zentral. Deshalb ist es wichtig, ihre Bedeutung zu kennen. «Privacy by Default» heisst übersetzt: Datenschutz durch datenschutzfreundliche Voreinstellungen. Will heissen: Die Werkseinstellungen sind datenschutzfreundlich ausgestaltet. Dadurch sollen insbesondere Nutzer geschützt werden, die weniger technikaffin sind und beispielsweise auf den Webseiten die Datenschutzeinstellungen nur ungenügend wahrnehmen. Als mögliche Lösung für diese Herausforderung kann das Cookie-Banner so gestaltet werden, dass der User zwar aktiv verschiedene Cookies auswählen kann, aber in der Grundeinstellung (englisch default)

Foto: Shutterstock/AGVS-Medien

Tipps

KMU sollten unbedingt ihre Bestellformulare und andere relevante Datenerhebungstools genau anschauen und gegebenenfalls anpassen, damit diese im September 2023 rechtskonform sind. Es empfiehlt sich auf jeden Fall, sämtliche Daten genau zu analysieren und folgende Punkte zu klären:

- Welche Daten werden von wem erhoben (Kunden und Angestellte)?
- Welche dieser Daten stehen nicht in unmittelbarem Zusammenhang mit der erbrachten Leistung?
- Welche Daten gelten als besonders schützenswert?
- Wo sind diese Daten gespeichert?
- Ist der Schutz der Daten ausreichend?
- Wer hat intern oder extern Zugriff auf die Daten und ist dieser Zugriff wirklich notwendig?
- Wer ist intern für die Sicherheit der Daten zuständig? Ist diese Person ausreichend geschult?
- Welcher Prozess greift bei einem Datenleck und wer ist dafür verantwortlich?

Der AGVS kooperiert beim Thema Datenschutz mit dem spezialisierten Unternehmen Impunix, das die umfassende Umsetzung des Schweizer Datenschutzgesetzes, die Importeurs- bzw. Herstellerrichtlinien sowie die Empfehlungen des AGVS in Unternehmen überprüft und zertifiziert.

Weitere Infos unter:
impunix.ch

die notwendigen Kreuze bereits gesetzt sind. Es bezeichnet auch die Vorgabe, dass die erhobenen Personendaten mit dem Verwendungszweck übereinstimmen müssen. Werden mehr Daten als wirklich notwendig erhoben, müssen die Personen darüber informiert und muss ihre Zustimmung eingeholt werden.

«Privacy by Design» bedeutet: Datenschutz durch Technikgestaltung. Diesem Prinzip liegt zugrunde, dass sich der Datenschutz am besten einhalten lässt, wenn eine Software und Hardware von Grund auf so konzipiert und entwickelt wird, dass sie relevante Datenschutzmassnahmen von Anfang an berücksichtigt. Der Schutz personenbezogener Daten im Sinne des DSG erfolgt durch das frühzeitige Ergreifen technischer und organisatorischer Massnahmen (TOMs) im Entwicklungsstadium.

Benachrichtigungspflicht

Im Falle einer Verletzung des Schutzes von Personendaten hat der Verantwortliche unverzüglich, möglichst innert 72 Stunden nach Bekanntwerden, die Aufsichtsbehörde, die Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, über die Verletzung zu informieren (Fachbegriff «Data Breach Notification»). Zum anderen müssen auch die jeweiligen Personen informiert werden, deren Daten betroffen sind. Der Inhalt der Meldung an die Aufsichtsbehörden ist im Gesetz detailliert vorgeschrieben und umfasst neben Informationen zur Verletzung auch den Namen und die Kontaktdaten des Ansprechpartners beim Unternehmen. Hat die Verletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, sind die betroffenen Personen zu informieren.

Erweiterte Informationspflicht

Die Informationspflichten werden deutlich ausgebaut. Neu müssen die betroffenen Personen über jede Beschaffung von Personendaten informiert werden. Mit dem neuen Gesetz müssen ebenso Angaben zur Identität und Kontaktdaten des Verantwortlichen, zum Bearbeitungszweck und zu den Empfängerkreisen gemacht werden. Um es etwas übersichtlicher zu machen: Die nachstehenden Punkte sind Pflichtangaben:

- Identität und Kontaktdaten des/der Verantwortlichen
- Bearbeitungszwecke
- Bei Bekanntgabe von Daten: Empfänger oder die Kategorien der Empfänger
- Bei Datenweitergabe ins Ausland: der Staat oder das internationale Organ sowie die Garantie für einen geeigneten Datenschutz oder den Ausnahmetatbestand, falls keine solchen Garantien gegeben sind
- Bei indirekter Datenerhebung zusätzlich (Daten werden nicht bei der betroffenen Person selbst erhoben): die Kategorien der bearbeiteten Personendaten
- Durchführung automatisierter Einzelentscheidungen (jede Person hat das Recht auf Evaluierung des Entscheids durch einen Menschen)

Bei einer Weitergabe von Daten ins Ausland sollte die Einwilligung der betroffenen Person vorliegen beziehungsweise der Schritt vertragsrechtlich notwendig sein. Zusätzlich müssen Sie als KMU nachweisen können, dass auch im Zielland alle datenschutzrechtlich notwendigen Bestimmungen eingehalten werden.

Schutz betrifft ausschliesslich natürliche Personen

Die Revision des DSG bedeutet, dass Unternehmen und Organisationen, also juristische Personen, sich nicht mehr auf das Gesetz berufen können. Die Schutzinhalte gelten nur noch für natürliche Personen.

Risikoplanung

Wer in einem Schadensfall nicht nachweisen kann, dass er sich schon im Vorfeld vorbereitet hat, macht sich strafbar. Ziel ist, zusammenhängende Gefahren auf ein Minimum zu reduzieren – und das im Zweifel auch nachweisen zu können.

Und aufgepasst: Wer die Informationspflicht verletzt, eine unvollständige oder falsche Datenschutzauskunft gibt oder Personendaten unerlaubterweise ins Ausland übermittelt, dem droht eine Busse von bis zu 250 000 Franken. Wichtig ist dabei: Die Busse trifft nicht das Unternehmen selbst, sondern jene Person, die effektiv für die Verletzung des Datenschutzgesetzes verantwortlich ist. <