Auch Schwyzer KMU müssen Daten besser schützen

Am 1. September tritt das neue Datenschutzgesetz in Kraft, welches Personendaten stärker schützt. Höchste Zeit für die Schwyzer Unternehmen, sich mit den Anforderungen aus dem neuen Gesetz auseinanderzusetzen.

von Rahel Lüönd

Die Situation um das Datenschutzgesetz, das am 1. September in der ganzen Schweiz in Kraft tritt und sich stark ans EU-Recht anlehnt, lässt sich wohl am besten mit der Ruhe vor dem Sturm beschreiben. «Im Moment hört man noch wenig – wir erwarten aber mit der Gesetzesänderung, die ja ohne Übergangsfrist eintritt, eine gewisse Hektik», sagt Andreas Weber, Co-Geschäftsführer der Unternehmensplattform Schwyz Next. Er rät den Schwyzer KMU, in einem ersten Schritt die Relevanz fürs eigene Geschäft abzuschätzen und angemessen zu reagieren. «Für Unternehmen, die besonders schützenswerte Personendaten bearbeiten, ändert sich mit dem Gesetz mehr als für andere», fasst Weber zusammen. «Eine Auslegeordnung sollten jedoch alle vornehmen, damit sie auf dem neusten Stand sind.»

Datenschutzverantwortliche haften persönlich

Es gibt einige grundsätzliche Anpassungen, die alle Firmen im Auge behalten sollten: Der Datenschutz muss durch technische Massnahmen wie datenschutzfreundliche Voreinstellungen sichergestellt sein. Wer von einem Hackerangriff betroffen war und Daten verloren hat, muss dies künftig dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) melden. In der Schweiz ist – anders als in der EU – für die Bearbeitung von Personendaten weiterhin keine Einwilligung nötig – es sei denn, es handle sich um besonders schützenswerte Personendaten, etwa zur eigenen Gesundheit.

Den grössten administrativen Aufwand dürfte das Führen von Verzeichnissen darstellen. Überall dort, wo Daten bearbeitet werden, muss das nachvollziehbar festgehalten werden. Die Ernennung einer Datenschutzberaterin oder eines -beraters ist im Unterschied zur EU freiwillig, bringt aber gewisse Vorteile. Werden Daten bearbeitet, die ein hohes Risiko für die Betroffenen darstellen, kann die Beratungsperson anstelle des EDÖB gewisse Vorlagen prüfen.

Ein feiner aber entscheidender Unterschied zum EU-Recht gibt es auch bei den Sanktionen: Im Gegensatz zur EU, wo die Unternehmen in die Pflicht genommen werden, haften in der Schweiz natürliche Personen wie CEO, CIO oder andere. Die Sanktionen – möglich sind Bussen bis zu 250 000 Franken – könnten happig ausfallen. Weber sagt dazu: «Die Rechtsprechung wird mit den Jahren zeigen, wie hart die Bussen tatsächlich sein werden.»

Umgang mit Risiken lernen

Auch wenn die neuen Spielregeln zum Datenschutz nicht für alle gleich einfach umsetzbar seien, findet Andreas Weber die Hintergründe nachvollziehbar. «Mit dem technologischen Fortschritt ist es möglich geworden, grosse Mengen von Daten zu sammeln und damit zu arbeiten. Es ist im Interesse aller, dass wir Personendaten schützen und auch mit den Risiken umzugehen lernen.» ●

Die Unternehmensplattform Schwyz Next bietet Interessierten auf Anmeldung unter *schwyz-next.ch/events* ein Webinar und einen Workshop zum Thema an.

- Webinar «Revidiertes Datenschutzgesetz – eine Übersicht für KMU» am 13. Juni 2023 um 17 Uhr
- Ganztägiger Workshop zur Umsetzung im eigenen Unternehmen am 30. Juni in Goldau oder am 13. Juli in Pfäffikon.

Diese Fragen gilt es zu klären

Die folgenden Leitfragen helfen KMU, die wesentlichen Punkte im neuen Datenschutzgesetz umzusetzen. Für grössere Unternehmen mit 250 und mehr Beschäftigten sowie für Firmen mit besonders schützenswerten Daten gelten schärfere Richtlinien.

1. Welche personenbezogenen Daten haben wir im Unternehmen, und wie gehen wir mit ihnen um?
2. Sind die Daten genügend geschützt (z. B. durch Firewalls, Verschlüsselungen sowie durch die Sensibilisierung des Personals)?
3. Speichern wir sie in einer Cloud und falls ja, in welchen Ländern befinden sich deren Server?
4. Ist sichergestellt, dass die Daten nach der (gerechtfertigten) Nutzung gelöscht oder anonymisiert werden?
5. Stimmen unsere Datenschutzerklärung und die Verträge mit Subunternehmern noch?
6. Wie können wir Daten auf Anfrage Betroffener herausgeben oder systematisch löschen?
7. Wer meldet eine Verletzung des Datenschutzes (z. B. nach einem Hackerangriff), und wie ist der interne Ablauf?
8. Wer ist für den Datenschutz verantwortlich?