Braucht es zwingend einen Datenschutzberater?

Für kleinere und mittlere Unternehmen stellt sich im Rahmen der Umsetzungsarbeiten für das neue Datenschutzgesetz die Frage, ob sie die Rolle des Datenschutzberaters neu schaffen wollen. Auch wenn es im neuen Datenschutzgesetz freiwillig ist, so ist es in vielen Fällen sinnvoll, diese Rolle zumindest in Teilen einzuführen. Die Erfahrung mit dieser Rolle im Anwendungsbereich der Europäischen Datenschutz-Grundverordnung zeigt, dass die Compliance durch einen internen Datenschutzberater massgeblich verbessert wird.

Von Lukas Lezzi

Einleitung

Ab dem 1. September 2023 gilt in der Schweiz das revidierte Datenschutzgesetz (revDSG). Wie bereits im noch geltenden DSG wird es auch im revDSG die Rolle der internen, beratenden Datenschutzberater geben. Die Terminologie ist allerdings etwas anders: Neu sprechen wir von dem Datenschutzberater.

Im Anwendungsbereich der Europäischen Datenschutz-Grundverordnung (DSGVO) wird hingegen von dem Datenschutzbeauftragten gesprochen.

Definition und Anforderungen

Gemäss Art. 10 revDSG haben private Verantwortliche die Möglichkeit, einen Datenschutzberater zu ernennen. Der Datenschutzberater dient als Ansprechpartner sowohl für die betroffenen Personen als auch für die zuständigen Datenschutzbehörden in der Schweiz. Die Aufgabe dieser Rolle besteht darin, eine unabhängige und weisungsungebundene Beratungstätigkeit gegenüber dem Verantwortlichen auszuüben, um den Datenschutz zu stärken. Der Datenschutzberater trifft aber selbst keine Entscheidungen in Bezug auf die Datenbearbeitungen.

Die Ernennung ist immer freiwillig, selbst wenn besonders schützenswerte Personaldaten bearbeitet werden.

Verantwortliche, die einen Datenschutzberater beauftragen, können von

der Verpflichtung zur Konsultation des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) befreit werden, selbst wenn bei der Datenschutz-Folgenabschätzung Restrisiken festgestellt wurden (gemäss Art. 23 Abs. 4 revDSG). Eine Konsultation ist erforderlich, wenn sich aus einer Datenschutz-Folgenabschätzung ergibt, dass trotz der vom Verantwortlichen ergriffenen Massnahmen immer noch ein erhebliches Risiko für die Persönlichkeitsrechte oder die Grundrechte der betroffenen Person besteht.

Damit der Verantwortliche auf die Konsultationspflicht verzichten kann, muss der Datenschutzberater die folgenden Voraussetzungen erfüllen.

a. Der Datenschutzberater muss seine Funktion fachlich unabhängig und weisungsungebunden ausüben.

b. Der Datenschutzberater darf keine Tätigkeiten ausüben, die mit seinen Aufgaben als Datenschutzberater unvereinbar sind.
c. Der Datenschutzberater muss über die erforderlichen Fachkenntnisse verfügen, und
d. der Verantwortliche muss die Kontaktdaten der Datenschutzberater veröffentlichen und dem EDÖB mitteilen.

Art. 23 der Verordnung zum revDSG legt noch weitere organisatorische Anforderungen fest. So muss der Verantwortliche des Datenschutzberaters
a. die notwendigen Ressourcen zur Verfügung stellen;
b. Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten gewähren, die der Datenschutzberater zur Erfüllung seiner Aufgaben benötigt;
c. das Recht einräumen, in wichtigen Fällen das oberste Leitungs- oder Verwaltungsorgan zu informieren.

Pflichtenheft

Der Datenschutzberater nimmt üblicherweise die folgenden Aufgaben wahr:

- unternehmensinterne Beratung in Datenschutzfragen
- Überwachung der Einhaltung des Datenschutzes innerhalb des Unternehmens
- Kontaktperson für den EDÖB
- Bearbeitung und Beantwortung von Anfragen von betroffenen Personen
- Beratung in datenschutzrelevanten Prozessen, insbesondere zu Privacy by Design/Default, Meldepflichten bei Datenschutzverletzungen, Datenschutz-Folgenabschätzung und Supplier-Management
- Eskalationsbefugnisse an die Geschäftsleitung und den Verwaltungsrat
- regelmässige Rapportierung an den Verwaltungsrat
- Schulung der Mitarbeiter
- regelmässige Weiterbildung im Bereich des Datenschutzes

Organisatorische Einbettung im Unternehmen

Für KMU, welche nun eine solche Rolle einführen wollen, stellt sich nun die Frage, wie genau sie dies tun sollten, falls es im Unternehmen Funktionen gibt, welche nicht direkt Entscheidungsbefugnisse über die Datenbearbeitungen des Unternehmens haben. Hier ist insbesondere an Funktionen der 2nd Line of Defence zu denken, wie z. B. IT-Security, Compliance oder Risk. In vielen KMU wird es aber solche unabhängigen Funktionen, welche Bera-

tungs- und Kontrollaufgaben wahrnehmen, nicht geben. In diesem Fall ist es kaum möglich, die organisatorischen Anforderungen des revDSG zu erfüllen. Die Ausnahme von der Konsultationspflicht kann so nicht in Anspruch genommen werden. Allerdings hat diese für die überwiegende Anzahl von KMU keine praxisrelevante Bedeutung.

Nichtsdestotrotz ergibt es auch für kleine KMU ohne 2nd-Line-of-Defence-Funktionen Sinn, eine Person intern zu benennen, welche sich unternehmensintern um den Datenschutz kümmert. Diese Person ist dann zentrale Anlaufstelle für alle datenschutzrelevante Fragen, intern als auch extern. Wichtig ist, dass die Person über die entsprechenden Ressourcen, insbesondere Arbeitszeit und auch Budget für Weiterbildung oder für externe Beratung, verfügt, um diese Rolle auch wahrnehmen zu können.

Alternativ kann auch die Beauftragung eines externen Datenschutzberaters in Betracht gezogen werden. In den meisten Fällen ist zu empfehlen, eine unternehmensinterne Person zu benennen, weil diese die Abläufe und Gegebenheiten des Unternehmens besser kennt und dementsprechend diese Rolle effektiver wahrnehmen kann. Ein punktueller Beizug von externer Beratung, z. B. bei Datenschutzverletzungen, kann aber sinnvoll sein.

Strafrechtliche Risiken

Das revDSG bringt bei vorsätzlicher Verletzung gewisser Bestimmungen des Gesetzes strafrechtliche Konsequenzen mit sich. Das Delikt wird nur auf Antrag hin verfolgt. Es droht eine Strafe in Form einer Busse von bis zu CHF 250 000.–.

Für einen Datenschutzberater besteht grundsätzlich nur ein geringes Risiko, sich strafbar zu machen, wenn es zu Datenschutzverletzungen kommt, weil sie nur beratende Aufgaben hat. Es ist allerdings wichtig, dass sie von ihr festgestellte Missstände und die damit einhergehenden Meldungen an die Geschäftsleitung oder den Verwaltungsrat sauber dokumentiert.

Fazit

Für KMU ist die Ernennung eines internen Datenschutzberaters in den meisten Fällen sinnvoll, weil damit die Datenschutz-Compliance innerhalb des Unternehmens signifikant erhöht werden kann. Die Implementierung einer solchen Rolle innerhalb des Unternehmens ist auch sinnvoll, wenn auch die formellen Anforderungen des revDSG nicht erfüllt werden können.

- Die Ernennung eines internen Datenschutzberaters bleibt auch unter dem neuen Recht freiwillig.
- Die Schaffung einer solchen Rolle, welche die Anforderungen des revDSG erfüllt, führt zur Befreiung von der Konsultationspflicht des EDÖB bei der Datenschutz-Folgenabschätzung.
- Bei kleinen KMU, welche keinen revDSG-konformen Datenschutzberater einsetzen können, ergibt es trotzdem Sinn, eine Person intern zu benennen, welche als zentrale Anlaufstelle für den Datenschutz im Unternehmen dient. So kann die Datenschutz-Compliance entscheidend verbessert werden.
- Das strafrechtliche Risiko für den Datenschutzberater ist voraussichtlich tief, weil nur beratende Tätigkeiten wahrgenommen werden.

AUTOR

RA Dr.iur. Lukas Lezzi, ist selbstständiger Rechtsanwalt in Zürich (LezziLegal). Seine Tätigkeitsschwerpunkte liegen im Bereich Datenschutz- und Finanzmarktrecht.