Wertvoller Rat in Datenschutzfragen

Marktübersicht Die Anforderungen, die mit dem neuen Datenschutzgesetz auf hiesige KMU zukommen, sind mannigfaltig und nicht für alle gleich. Eine Beratung ist empfehlenswert.

Von Matthias Wintsch

Mit dem neuen Schweizer Datenschutzgesetz kommen auch neue Pflichten auf Schweizer KMU zu. «Das Thema nimmt auf KMU-Leitungsebene noch nicht den Stellenwert ein, welcher den Unternehmensrisiken angemessen wäre», weiss aber Markus Bekk, Partner bei Forfa Consulting. Und auch David Vasella, Partner bei der Anwaltskanzlei Walder Wyss, schätzt den Wissensstand bei den hiesigen KMU als «sehr niedrig» ein. Einzig KMU, die in regulierten Bereichen oder für regulierte Kunden tätig sind, sind seiner Erfahrung nach auf dem aktuellsten Stand. Michèle Balthasar, Geschäftsführerin von Balthasar Legal, spricht derweil die schon geleistete Vorarbeit an: «Viele KMU haben sich wohl bereits bei der Einführung des europäischen Datenschutzrechts, der DSGVO, im Jahre 2018 mit gewissen Datenschutzthemen befasst.» Sie ergänzt aber, dass sich auch diese Unternehmen dem Thema seither vermutlich nur wenig gewidmet haben. Handlungsbedarf sieht Reto Zbinden, Gründer und Inhaber von Swiss Infosec, dort, «wo eine hohe Aussenwirkung oder ein hohes Schadenspotential (inklusive Reputation) auf die neuen Bussenrisiken trifft.»

Das dürfte auf viele Unternehmen zutreffen. Doch welche Änderungen sind für die KMU am wichtigsten? «Ausbau der Informationspflichten – das heisst einer Datenschutzerklärung –, Erstellung von Bearbeitungsverzeichnissen, Durchführung von Datenschutz-Folgeabschätzungen und die Pflicht zur Meldung von Verletzungen der Datensicherheit», listet etwa Marius Vischer von Epartners Rechtsanwälte auf. Reto Fanger, Rechtsanwalt bei der Advokatur Fanger, legt weiter das Augenmerk auf die strafrechtlichen Folgen, wenn man bei der Umsetzung des Datenschutzes Fehler begeht – das sind immerhin Bussen von bis zu 250'000 Franken bei vorsätzlichen oder eventualvorsätzlichen Verletzungen der gesetzlichen Vorgaben. Auch hier können Unternehmen, die sich im Rahmen der DSGVO bereits mit modernem Datenschutz auseinandergesetzt haben, von der Vorarbeit profitieren, wie Markus Bekk von Forfa Consulting er-

NEUN SCHWEIZER BERATER IN DATENSCHUTZFRAGEN

UNTERNEHMEN	ADVOKATUR FANGER	BALTHASAR LEGAL	EPARTNERS RECHTSANWÄLTE	FORFA CONSULTING
Gründungsjahr	2011	2021	2007	2017
Anzahl Mitarbeiter	4	3	13 (11 Anwälte)	10
Standorte	Luzern	Zürich	Zürich	Zug
Branche/Ausrichtung	Anwaltskanzlei	Beartung, Rechtsdienstleistung, Informationssicherheit	Anwaltskanzlei	Beratungs- und Prüfungsunternehmen
Kernkompetenzen und Schwerpunkte	Datenschutz (Beratung, Umsetzung, DPO), ICT-Recht	Beratung Datenschutz und Datensicherheit, Datenschutzbeauftragte, digitales Energierecht	IT, Daten & Technologie, Industrie & Anlagebau, Bau & Immobilien	Informations- und Cybersicherheit, Notfall- und Krisenmanagement, Governance/Risk/Compliance, Datenschutz, regulatorische Fragen
Kundensegmente	KMU, Verbände, öffentliche Verwaltungen	kleinere, mittlere und grosse Unternehmen (Industrie, Kommunikation, Gastgewerbe, Gesundheitswesen)	KMU, Grossunternehmen, öffentliche Hand	alle Unternehmensgrössen; Finanzsektor, Industrie, öffentlicher Sektor
Top-Referenzen/ Kunden	k.A.	Aare Energie, Knecon, Bio-Familia	k.A. (aufgrund Anwaltsgeheimnis)	auf Anfrage
URL	www.advokatur-fanger.ch	www.michele-balthasar.ch	www.epartners.ch	www.forfa.ch

■ = ja, ❑ = nein; k.A = keine Angaben; 1) Fusion der drei Vorgängerkanzleien im Jahr 2000

gänzt: «Wer heute die DSGVO bereits umsetzt hat, hat bereits eine sehr gute Grundlage. Für alle anderen steht eine zeitkritische Aufgabe ins Haus, die es nicht zu unterschätzen gilt.»

Checkliste der Massnahmen

Als zwingend notwendige Massnahmen für ein KMU im Rahmen dieser Aufgabe wiederholt Alexander Schmid, Rechtsanwalt bei Epartners Rechtsanwälte, die Publikation einer Datenschutzerklärung, die Erstellung von Bearbeitungsverzeichnissen (sofern notwendig, wobei in jedem Fall empfohlen) und die Durchführung von Datenschutz-Folgeabschätzungen. Seine Checkliste für weiterführende Massnahmen besteht aus der Dokumentation der Massnahmen für die Gewährleistung der Datensicherheit, der vertraglichen Absicherung der Auftragsbearbeitungen, der Definition der Prozesse zur Bearbeitung von Auskunfts-, Berichtigungs- und Löschungsbegehren von Betroffenen, die Definition der Prozesse zur Meldung von Verletzungen der Datensicherheit, die Information und Schulung der Mitarbeitenden sowie den Erlass von internen Richtlinien. Ausserdem könne eine organisatorische Verantwortlichkeit für den Datenschutz bestimmt werden.

Letzteres – die Bestimmung eines Verantwortlichen für den Datenschutz – ist zwar gesetzlich nicht verankert, aber gegebenenfalls sinnvoll, so Reto Fanger von der Advokatur Fanger: «Das Gesetz schreibt dies nicht vor. Wenn aber die Bearbeitung von Personendaten für das KMU ein zentrales Geschäftsfeld darstellt, wenn das KMU in Bereichen mit besonders schützenswerten Personendaten tätig ist oder wenn das KMU eine gewisse Grösse und Komplexität aufweist, ist ein DPO (Data Protection Officer, Datenschutzberater nach revDSG) zu empfehlen.» Wolfgang Sidler, CEO und Inhaber von Sidler Information Security, ist ebenfalls der Meinung, dass ein interner DPO je nach Unternehmensgrösse Sinn machen kann, ergänzt aber, dass es auch möglich ist, diesen extern in einem Mandat zu engagieren.

In aller Regel sollte man sich von einem Spezialisten beraten lassen, so David Vasella von Walder Wyss. «Es sind zwar viele Informationen verfügbar, aber die Anwendung und besonders auch die Einschätzung der Risiken und damit verbunden die Priorisierung ist ohne fachliche Unterstützung zumindest sehr anspruchsvoll», wie er anfügt. David Rosenthal, Partner und Leiter Data & Privacy bei Vischer, empfiehlt ebenfalls einen Workshop mit einem Coach oder Berater, in dem man anschauen kann, was man schon gemacht hat und was es noch zu tun gibt. Sein Rat ist aber, auch selbst das Heft in die Hand zu nehmen: «Versuchen Sie möglichst viel selbst zu machen, damit Sie das Know-how intern aufbauen.»

Dominic Staiger, CEO von Priverion, pflichtet der Empfehlung zu einer Beratung bei – besonderes Augenmerk richtet er dabei auf die Risiken im Rahmen der Auslandsübertragung und Vertragsgestaltung. Als weiteres Hilfsmittel nennt er unterstützende Softwarelösungen: «Ein Grossteil der Datenschutzthemen lassen sich mit entsprechenden Datenschutztools bearbeiten.»

Pragmatismus statt Angst

Bei der Anbieterwahl sind Erfahrung und Pragmatismus die beiden wichtigsten Auswahlkriterien, so ein Grossteil der Experten. Reto Zbinden von Swiss Infosec: «Bei der Auswahl eines Beraters sollten die juristische Ausbildung, Fachkompetenz und praktische Erfahrung aus vergleichbaren Mandaten im Zentrum stehen.» Wolfgang Sidler von Sidler Information Security sieht das ähnlich und ergänzt: «Etwas Pragmatik sollte auch dabei sein – so nach dem Motto: Nur das Nötigste umsetzen.» Und David Rosenthal von Vischer warnt vor Angstmacherei und leeren Versprechen: «Wählen Sie nicht jemanden, der Ihnen Angst zu machen versucht mit den Strafdrohungen im neuen Gesetz oder Ihnen verspricht, Sie vollständig datenschutzkonform zu machen. Das ist nämlich nicht möglich.» ■

PRIVERION	SIDLER INFORMATION SECURITY	SWISS INFOSEC	VISCHER	WALDER WYSS
2017	2009	1989	1857[1)]	1972
25	1	43	265	500
Zürich, München, New York	Hünenberg, Zug	Sursee, Zürich, Bern	Basel, Zürich, Genf	Zürich, Bern, Basel, Lugano, Lausanne, Genf
Software & Beratung	Datenschutz- und Informationssicherheits-Experte	Beratungs- und Ausbildungsunternehmen, Personalverleih, externe Datenschutzbeauftragte/Data Protection Officer, IT Security	Recht	Anwaltskanzlei
Privacy & InfoSec Spezialist, weltweites Beratungsnetzwerk	Datenschutz, GDPR, Informationssicherheit, ISO 27001, Risiko-Management, CISO und DPO as a Service	Datenschutzrecht, IT-Recht, Informationssicherheit, IT Sicherheit, Integrale Sicherheit	Wirtschaftsrecht, einschliesslich IT-Recht, Datenschutzrecht, Medienrecht, Arbeitsrecht, Aufsichtsrecht	Datenschutz, Datenrecht allgemein, Compliance allgemein
mittlere und grosse Unternehmen, inbesondere im internationalen Kontext	KMU, Pharma und Industrie	Industrie, öffentliche Verwaltungen, Gesundheitswesen, Banken, Versicherungen, KMU	Startup bis Grosskonzerne aus der Schweiz und dem Ausland, besonders stark in Gesundheitswesen, Biotech, Finanzindustrie	kotierte Unternehmen bis zu KMU und Privatpersonen
Glencore, Pilatus Aircraft, UNIA	Geistlich Pharma, Synlab Suisse, Lipoid Kosmetik	Visana, Stadt Kloten, Hornbach (Schweiz)	k.A.	Migros, Zurich, Zur Rose
www.priverion.com	www.sidler-security.ch	www.infosec.ch	www.vischer.com	www.walderwyss.com

Quelle: «Swiss IT Magazine»