Datenschutz-Audits für KMU

Marktübersicht Ob interne Standortbestimmung oder externe Prüfung – Datenschutz-Audits haben Hochkonjunktur und sind ein wichtiges Werkzeug auf dem Weg zur Compliance. Wir zeigen neun Anbieter von Datenschutz-Audits in der Schweiz.

Von Matthias Wintsch

Nationalrat Balthasar Glättli erklärt ab Seite 45 dieser Ausgabe, dass die Einführung der DSGVO einen erzieherischen, ja gar aufrüttelnden Charakter für Schweizer Unternehmen gehabt habe. Somit sollte spätestens mit dem Inkrafttreten der Europäischen Datenschutz-Grundverordnung allen Schweizer Unternehmen die Notwendigkeit zum bewussten Umgang mit Datenschutz klar geworden sein. Wirklich allen? Nein, ein beachtlicher Anteil von Unternehmen bewegt sich offensichtlich noch immer mit erschreckender Unwissenheit durch den Datendschungel und lebt mit Zweifeln, ob die Sicherheitsmassnahmen in ihren Datenverarbeitungs- und Datenschutz-Prozessen der Prüfung einer Aufsichtsbehörde genügen würden. So lautet die Antwort von Johannes Troppmann, Managing Director von IS4IT Schweiz, auf die Frage, wie es um die Datenschutzstandards in Schweizer KMU stehe: «Um es positiv zu formulieren: Nicht so gut.» Es gebe mittlerweile, so Troppmann weiter, gar eine Reihe von Untersuchungen und Analysen, welche dies untermauern würden, die Ursachen dafür seien aber mannigfaltig. Auch Aldo Rodenhäuser, Head of Security bei Adnovum, bezeichnet die Datenschutzlage in Schweizer KMU als «eher schlecht» und gibt zu bedenken, dass viele der Betroffenen vor einem «unüberwindbaren Berg von Anforderungen» stehen würden. In der Folge würden Datenschutz- und Informationssicherheitsthemen nicht genügend finanzielle Mittel zukommen. Rodenhäuser: «Einige KMU vertrauen dabei auf Software- und Hardware-Hersteller und eine Standard-Konfiguration, ohne diese

NEUN SCHWEIZER ANBIETER VON DATENSCHUTZ-AUDITS

NAME	ADNOVUM	BBI SOFTWARE	FORFA CONSULTING	INFOGUARD
Am Markt seit	1988	1994	2017	2001
Anzahl Mitarbeiter	600	10	7	120
Anzahl Kunden	k.A.	k.A.	10	300
Datenschutz-Audits	■	■	■	■
Externer Datenschutz-beauftragter	■	■	■	■
Vorlagen, Dokumente, Merkblätter	❑	■	■	■
Schulungen	■	■	■	■
Hotline	❑	❑	❑	❑
Prüfung von eingesetzten Dritt-Services	■	■	■	■
Weitere Dienstleistungen	IT-, Technology-, Security- und IAM-Consulting; Unterstützung für schnelle und sichere Digitalisierung von Geschäftsprozessen; Konzeption und Umsetzung innovativer Business- und Security-Lösungen; User Experience Design; Application Management	Lizenzmanagement; Softwarebeschaffung; Software-Audit	Informationssicherheitsberatung	Beratung; Aufbau eines Datenschutz-Managementsystems; Datenschutz-Managementplattform; E-Privacy-Datenschutz-Gütesiegel; IT-Sicherheitslösungen
Website	www.adnovuvm.ch	www.bbi.ch	www.forfa.ch	www.infoguard.ch

■ = ja, ❑ = nein; k.A = keine Angaben

gross zu hinterfragen. Andere wiederum sind sich nicht bewusst, was es heissen könnte, wenn man eine Glühbirne an das interne Netzwerk des Unternehmens anschliessen würde. Hier muss noch etwas mehr Awareness geschaffen werden.»

Kaum Ressourcen für Datenschutz

Untätigkeit birgt aber gewisse Risiken, wie die Experten feststellen. Marco Kurmann, Geschäftsführer von BBI Software, erklärt: «Viele Unternehmen haben noch nichts in diesem Bereich unternommen. Sie warten ab und schauen, ob es wirklich zu den angedrohten Bussen kommt.» Wie den Aussagen der Spezialisten zu entnehmen ist, geht es dabei nicht zwingend um mangelnden Informationsstand, sondern um die Bereitschaft zu Investitionen, wie die Geschäftsführerin von Integratio, Henriette Baumann, erklärt: «Im September 2018 veröffentlichte die ZHAW eine Studie zum Datenschutz in Schweizer Unternehmen, die sich mit unseren Erfahrungen weitgehend deckt: Der Grossteil der Unternehmen misst dem Datenschutz zwar eine hohe Bedeutung zu, stellt aber kaum Ressourcen zur Verfügung. Ein Viertel der Unternehmen geht davon aus, dass sie von der DSGVO betroffen sind – die Einschätzungen von Datenschutzexperten liegen weit höher.»

Die Anbieter gehen aber auch wiederholt auf die grossen Unterschiede ein, die in Schweizer KMU vorzufinden sind. So scheinen die Unternehmen, die offensichtlich kritische Personendaten (beispielsweise Gesundheitsdaten oder religiöse Hintergründe) verarbeiten, über die nötige Sensibilität zu verfügen und Massnahmen getroffen zu haben. «Beim Datenschutz gibt es das durchschnittliche KMU nicht. Hier sehen wir die gesamte Bandbreite an Reifegraden», kommentiert Dominic Staiger, Geschäftsführer von SIDD, und fügt an: «Viele KMU, welche Daten aus der speziellen Kategorie verarbeiten, sind hier bereits sensibilisiert und holen sich häufig externe Unterstützung ins Unternehmen.» Und auch Wolfgang Sidler, CEO von Sidler Informatik, bestätigt dieses Bild: «Aus unseren Erfahrungen wird das Thema Datenschutz sehr unterschiedlich wahrgenommen. Branchen im Bereich Pharma oder Medizin erkennen, dass ihnen ein guter Datenschutz einen Mehrwert gibt.»

Eine einleuchtende Begründung für die verspätete oder zaghafte Umsetzung der Massnahmen in den Firmen liefert derweil Markus Bekk, Partner bei Forfa Consulting: «Die verzögerte Anpassung des Schweizer DSG hat bei den Unternehmen für Unsicherheit bezüglich des Zielzustands gesorgt und die Umsetzung von Datenschutz-Projekten verzögert.» Es bleibt also vorerst zu hoffen, dass die auf 2020 geplante abgeschlossene Revision des hiesigen Datenschutzgesetzes etwas mehr Klarheit und Willen zum Handeln für Schweizer KMU mit sich bringt.

Ein Audit ist so oder so sinnvoll

Besteht in einem Unternehmen diese Klarheit noch nicht, kann ein Datenschutz-Audit oder -Assessment Licht ins Dunkel bringen. An dieser Stelle muss festgehalten werden, dass die Semantik bei den beiden Begriffen nicht ganz klar ist: Unter einem Audit (Prüfung) verstehen einige Anbieter einen strengeren Prozess als unter einem Assessment (Beurteilung, Bewertung), bei anderen scheinen die Begriffe für dasselbe verwendet zu werden. Im Kern geht es jedoch so oder so um eine Bewertung der Datenschutzstandards und -prozesse in einem Unternehmen, also um eine Standortbestimmung mit oder ohne weitere Elemente wie Mitarbeiter-Interviews oder einem resultierenden Massnahmenkatalog.

Sinnvoll sei ein Audit in jedem Fall, so Reto Zbinden, CEO von Swiss Infosec: «Grundsätzlich macht es für jedes Un-

INTEGRATIO	IS4IT SCHWEIZ	SIDD INSTITUT FÜR DATENSCHUTZ UND DATENSICHERHEIT	SIDLER INFORMATION SECURITY	SWISS INFOSEC
1995	2009	2017	2009	1989
10	k.A.	8	1	37
89	k.A.	k.A.	5	800
■	■	■	■	■
■	■	■	■	■
■	❑	■	■	■
■	❑	■	■	■
■	❑	❑	■	■
■	■	■	■	■
Externer Datenschutzbeauftrager nach DSGVO (EU) und DSG (CH); Unterstützung bei der Umsetzung der Anforderungen der DSG/ DSGVO; Rechtliche Beratung im Bereich Datenschutz; Schulung und Sensibilisierung; IT-Security	Vorbereitung & Audits ISMS; Aufbau Risk Management; Risk Assessments; Aufbau Governance; Security Awareness	EU-Vertreter (Art. 27 DSGVO); Eigene DSGVO Software & Software-Entwicklung	ISMS Aufbau bis zur ISO 27001 Zertifizierung; Erstellen eines DSGVO-Weisungs-Framework; Security Officer auf Zeit; Datenschutzbeauftragter (DPO) auf Zeit; Informationssicherheit für Entscheidungsträger; Spezielle Funklösungen (HB9RYZ)	Implementierung Datenschutz (DSGVO/DSG); Umsetzung/Überprüfung technisch-organisatorische Massnahmen (IT Security); Rechtsberatung Digitalisierung (Cloud Compliance & Security); Aufbau/ Betrieb SMS (ISO 27001); Mandate externe CISO und EU-Vertreter
www.integratio.com	www.is4it.ch	sidd.swiss	www.sidler-security.ch	www.infosec.ch

Quelle: «Swiss IT Magazine»

ternehmen Sinn, ein Datenschutz-Audit durchführen zu lassen, und sei es alleine bezüglich des rechtskonformen Umgangs mit Personendaten in der Personalabteilung.» Weiter betont Zbinden, dass die regelmässige Wiederholung eines Audits ebenfalls zu empfehlen sei, «um die Datenschutzkonformität laufend zu gewährleisten und zu verbessern». Johannes Troppmann von IS4IT pflichtet Zbinden bei – es stelle sich nicht die Frage, ob ein Audit sinnvoll sei, sondern in welchem Rahmen, gerade auch im Hinblick auf die Revision des Schweizer Datenschutzgesetzes (DSG).

Die meisten Anbieter sind sich einig, wann ein Audit mit Sicherheit durchgeführt werden sollte. So erklärt etwa Christian Matt, Principal Cyber Security Consultant bei Infoguard: «Als Schweizer KMU ist es sinnvoll, ein Datenschutz-Audit durchzuführen, wenn personenbezogene Daten, insbesondere sensible Daten, gesammelt oder verarbeitet werden. Das Audit kann als Nachweis zur Einhaltung der geltenden Bestimmungen und der eigenen Sorgfaltspflichten eingesetzt werden. Ein Prüfbericht oder gar ein E-Privacy Datenschutz-Gütesiegel können sowohl intern zur Sensibilisierung der Mitarbeitenden als auch gegenüber externen Stellen, beispielsweise Kunden, zur Positionierung als vertrauenswürdiger Partner eingesetzt werden.» Aus Matts Aussage stechen besonders zwei Punkte hervor: Zum einen misst er dem Datenschutz einen starken geschäftlichen Mehrwert zu, nämlich mehr Vertrauen gegenüber den Kunden sowie die Sensibilisierung von Mitarbeitern und Kundschaft. Zum zweiten nennt er die Verarbeitung von Personendaten von EU-Bürgern nicht als Bedingung (was im DSGVO-Kontext in fast jedem Ratgeber zu lesen war), sondern hält die Aussage allgemein. Dies ist besonders relevant, weil sich die Datenschutz-Standards von DSGVO und dem revidierten Schweizer DSG stark ähneln sollen und damit letztlich die meisten Schweizer Unternehmen von strengeren Datenschutzrichtlinien betroffen sein dürften.

Soll − Ist = Gap-Analyse

Wenn es um den Ablauf eines Audits geht, gleichen sich die Vorgehensweisen der meisten Anbieter mehrheitlich. Es scheinen sich für diese Audits also Best Practices etabliert zu haben. So definiert der Kunde gemeinsam mit dem Anbieter zuerst, in welchem Umfang und in welchen Bereichen eine Prüfung stattfinden soll. Dominic Staiger von SIDD etwa spricht dabei von einer anfänglichen Kontextanalyse: «In der Kontextanalyse werden zuerst das Unternehmen und generell die dort verarbeiteten Daten betrachtet. Hieraus ergeben sich die Mindestanforderungen sowie auch die Ziele des Kunden.» Der Prüfungsprozess umfasst je nach Situation verschiedene Elemente wie die Prüfung von Dokumenten, technische Abklärungen und Tests, Workshops und nicht zuletzt Interviews. Wie Aldo Rodenhäuser von Adnovum ergänzt, können besonders letztere dazu dienen, undokumentierte Punkte aufzudecken, die etwa während der Dokumentenprüfung nicht ersichtlich wurden. Auf Basis der Ergebnisse wird eine Ist-Analyse erstellt, ein Abbild der derzeitigen Datenschutz-Situation im Unternehmen. Henriette Baumann von Integratio spezifiziert: «Die Ist-Analyse erfolgt unter Einbezug der Mitarbeitenden und der verantwortlichen Stellen im Unternehmen. Es werden Interviews geführt und bestehende Dokumentationen, Datensammlungen, Verarbeitungen, IT-Systeme und Vertragswerke gesichtet. Nach der Gewichtung und Kategorisierung der Datensammlungen und Verarbeitungen ist klar, für welche Verarbeitungen die DSGVO greift und es kann eine Identifikation der Unternehmensrisiken erfolgen.» Ebenfalls üblich ist die Erstellung einer Gap-Analyse, welche auf Basis der Ist-Situation die Lücken zum Soll-Zustand aufzeigt. Das Endprodukt ist in den meisten Fällen ein Prüfbericht und auf Wunsch Massnahmenkataloge und Empfehlungen zu möglichen Handlungsfeldern.

Datenschutz leben

«Ein Audit ist nur eine Bestandsaufnahme – in den meisten Fällen ergibt sich aus den ermittelten Erkenntnissen ein Handlungsbedarf für das Unternehmen. Zur Verbesserung des Schutzniveaus und zur Einhaltung der gesetzlichen Anforderungen müssen die im Prüfbericht enthaltenen Empfehlungen in einer nächsten Phase umgesetzt werden», erklärt Christian Matt von Infoguard das Nachspiel eines Datenschutz-Audits. Die aufgeführten Dienstleister bieten in der Regel neben dem Audit selbst weiterführende Services an und helfen auf Wunsch bei der Umsetzung der Massnahmen im Betrieb, auf deren langfristige Umsetzung besonderes Augenmerk gelegt wird. Marco Kurmann von BBI Software etwa erklärt: «Datenschutz ist nicht einfach nur ein Projekt, es muss in der Firma auch weiterhin gelebt werden.» So sind sich viele Experten einig, dass Datenschutz auf längere Sicht eine Aufgabe für die Exec-Etage ist und kein Weg an einer nachhaltigen Auseinandersetzung mit dem Thema Datenschutz vorbeiführt. ■

DER SELBSTTEST

Neben der Option eines Datenschutz-Audits gibt es die Möglichkeit einer selbständigen Evaluierung. Solche Werkzeuge sind für eine Standortbestimmung und die Sensibilisierung auf unterschiedliche Datenschutz-Themenbereiche gedacht und können eine professionelle, auf die Firma zugeschnittene Beratung nur teilweise ersetzen. Ein verbreitetes Tool in der Schweiz, das Datenschutz Self Assessment Tool (DSAT), steht kostenlos zum Download zur Verfügung und wird von den beiden auf Datenschutz spezialisierten Schweizer Anwälten David Rosenthal von Homburger und David Vasella von Walter Wyss herausgegeben. Das Tool geht von einer 80:20-Regel aus, die meisten Datenbearbeitungen und Prozesse sollten damit abgebildet werden können, es erhebt aber bewusst keinen Anspruch auf eine vollständige Abdeckung aller Fälle, allfällige Risiken trägt dabei der Anwender. Bei komplizierten Datenbearbeitungen oder tiefschürfenden Fragen empfehlen die Herausgeber das Hinzuziehen von Experten. Inhaltlich besteht das Tool aus PDF-Fragebögen, die eine Standortbestimmung ermöglichen, parallel dazu die Datenschutzkonformität dokumentieren und letztlich Empfehlungen für Massnahmen liefern. Weiter können der gesamte Prozess und die eingegebenen Informationen archiviert werden, sodass ein Unternehmen in der Folge seiner Rechenschaftspflicht nachkommen kann. Das Tool kann unter www.dsat.ch heruntergeladen werden, eine ausführliche Dokumentation steht ebenfalls bereit. Weitere vergleichbare, aber meist weniger umfangreiche Fragebögen werden etwa von Economiesuisse und dem Büro des Eidgenössischen Datenschutzbeauftragten herausgegeben.