

Ein herausforderndes Betätigungsfeld

Am 2. Datenschutz-Fortbildungsseminar der UFL standen die Stolpersteine für Unternehmen bei der Anwendung der DSGVO im Fokus.

Oliver Beck

Die Datenschutzgrundverordnung (DSGVO) hat das Thema Datenschutz ins Zentrum des gesellschaftlichen Bewusstseins gerückt und stellt hinsichtlich ihrer Anwendung nicht zuletzt die Unternehmen vor kleinere und grössere Herausforderungen. Das zweite Datenschutz-Fortbildungsseminar der Privaten Universität im Fürstentum Liechtenstein (UFL) hat sich einigen dieser Stolpersteine gewidmet. Dabei begnügten sich die internationalen Referenten an der vom Datenschutzverein, der Datenschutzstelle, der LIHK und der BEWB Rechtsanwälte AG mitorganisierten Veranstaltung nicht mit der blossen Problembeschreibung. Die Teilnehmer durften sich auch über viele wertvolle Ratschläge freuen.

Trotz DSGVO existieren weiterhin nationale Unterschiede

Gerade für international tätige Unternehmen ist ein gesetzeskonformer Datenschutz bisweilen eine enorme Aufgabe, wie Christine Wohlwend, Datenschutzbeauftragte bei der Hoval, in ihren Ausführungen deutlich machte. Die DSGVO, merkte sie an, strebe nach länderübergreifender Vereinheitlichung und Vereinfachung des Datenschutzes. Und das sei im Sinne nun bestehender «ähnlicherer Anforderungen» sicher auch teilweise gelungen. «Zugleich gibt es aufgrund von Öffnungsklauseln aber Spielräume, die national unterschiedlich genutzt werden.» Für die Datenschutz-Verantwortlichen einer international agierenden Firma wie der Hoval bringt dies nicht zuletzt die Aufgabe mit sich, dass sie sich detaillierte Kenntnisse zu diesen Öffnungsklauseln aneignen müssen. Eine weitere Herausforderung besteht laut Wohlwend darin, nationale Datenschutzgesetze zu berücksichtigen, die zusätzlich zur DSGVO bestehen. Etwa in der Schweiz oder Singapur, wo die Hoval jeweils eine Niederlassung unterhält und die DSGVO bekanntlich nicht unmittelbar anwendbar ist.

Allein schon diese beiden Umstände lassen in den Augen der Datenschutzbeauftragten des Liechtensteiner Traditionsbetriebs nur einen Schluss zu: «Datenschutz ist ein Team-sport.» Eine einzelne Person, betont sie, könne diese umfassende Aufgabe gar nicht bewältigen. Vielmehr brauche es den Einbezug und die Zusammenarbeit verschiedener Akteure sowie einen regelmässigen Austausch. Wichtig ist dabei weniger das Erreichen von Perfektion, sondern eine kontinuierliche Verbesserung, wie Wohlwend gelernt hat. «Letztlich geht es darum, das Risiko für eine Verletzung des Datenschutzes zu minimieren.» Im Zuge dessen, auch das hat sie erfahren, ist insbesondere der Dialog mit den nationalen Aufsichtsorganen wertvoll. Wenn keine Lösungen in Sicht sind, sei es auf alle Fälle ratsam,



Die Anwendung der DSGVO stellt viele Unternehmen auch zweieinhalb Jahre nach ihrem Inkrafttreten vor viele Herausforderungen. Bild: iStock

den Kontakt proaktiv zu suchen. «Das ist definitiv besser, als sich zu verrennen. In der Regel sind die Aufsichtsbehörden gern bereit, Hilfe zu leisten.»

Wie dem Auskunftsrecht am besten Rechnung getragen wird

Jutta Sonja Oberlin von der International Association of Privacy Professionals rückte in ihrem Referat die Frage in den Fokus, wie Unternehmen dem Auskunftsrecht, das die DSGVO einer Person einräumt, am besten gerecht werden. Gerade der Auskunftsanspruch, erklärte sie, sei von herausragender Relevanz. «Er steht praktisch am Anfang aller Rechte des Datenschutzsubjekts.» Grund genug also, um den Unternehmen einen kleinen Guide an die Hand zu geben. Zunächst, so Oberlin, gehe es darum, eine funktionale Basis für ein gesetzeskonformes Vorgehen zu generieren. Die hierfür wichtigsten Schritte: Durchführung einer Lückenanalyse, Anfertigen einer zeitlich gerne etwas ambitionierteren Roadmap, Schaffen eines Überblicks über die personenbezogenen Daten im Unternehmen, Ver-

antwortungen zuweisen, den ersten Kontakt für Anfragen definieren und die Mitarbeiter schulen.

Der Prozess der Bearbeitung selbst umfasst dann im wesentlichen die Bestätigung des Empfangs einer Anfrage, den allfälligen Einbezug der relevanten Abteilungen in die Bearbeitung, die Einhaltung der vorgegebenen Fristen (respektive die frühzeitige Information, dass eine Einhaltung nicht möglich ist) sowie die Auskunft. Auch für Letzteres gibt es wiederum eine Reihe von Kriterien, die es zu beachten gilt. Eine Auskunft muss etwa transparent und verständlich formuliert sein, leicht zugänglich und kann mündlich, elektronisch wie schriftlich erfolgen. Allerdings, so Oberlin, rate sie von einer mündlichen Auskunft ab. «Denn am Ende ist das Unternehmen in der Beweis-pflicht, dass es eine solche tatsächlich erteilt hat.»

Ein EuGH-Urteil mit weitreichenden Folgen

Vorsicht walten lassen müssen Unternehmen mit Sitz in einem EU-/EWR-Land auch beim Transfer von perso-

nenbezogenen Daten an Unternehmen in Drittstaaten, wie Marie-Louise Gächter, Leiterin der liechtensteinschen Datenschutzstelle, in ihrem Referat ausführte. Bei der Frage nach der Legitimität eines solchen Datentransfers ist entscheidend, dass die Daten an ihrem Bestimmungsort auf ein Schutzniveau treffen, das jenem der Länder entspricht, in denen die DSGVO unmittelbar angewendet werden kann. «Um dies sicherzustellen», so Gächter, «kennt die DSGVO insgesamt sechs Möglichkeiten.» Sogenannte Angemessenheitsbeschlüsse, mit denen die EU einem Drittstaat ein angemessenes Niveau attestiert, bilden dabei die populärste Methode. Ebenfalls ein beliebtes Mittel ist die Nutzung von Standardvertragsklauseln bei Vertragsabschlüssen zwischen dem datenimportierenden und dem datenexportierenden Unternehmen.

Allerdings sind die Voraussetzungen hier seit gut einem halben Jahr nicht mehr die gleichen. Im Juli 2020 erklärte der Europäische Gerichtshof (EuGH) den Angemessenheitsbe-

schluss für die USA – einen der wichtigsten Datenimportstaaten – aufgrund der dortigen Datenzugriffsbefugnisse von Überwachungsbehörden für ungültig. Doch damit nicht genug: Das Gericht erschwerte zugleich auch den Weg über die Standardklauseln – und zwar nicht für Datentransfers in die USA allein, sondern ganz grundsätzlich in alle Länder ohne Angemessenheitsbeschluss. «Standardklauseln», erklärt Gächter, «sind zwar weiterhin gültig. Aber neu existiert eine grosse Hürde: Das Unternehmen muss über eine auf den Einzelfall bezogene Prüfung feststellen, ob im Drittstaat ein angemessener Datenschutz gewährleistet werden kann.»

Im Wissen um die Herausforderung, welche die Prüfungspflicht für die Unternehmen bedeutet, hat der Europäische Datenschutzausschuss eine Anleitung erarbeitet, die sich derzeit noch in der Konsultation befindet. Einen kleinen Ausblick wagte Gächter trotzdem schon. Unternehmen müssten im Zuge einer Prüfung künftig genau abklären, ob eine Überwachungsbehörde auf personenbezogene Daten zugreifen könne, meint die Expertin. Ausserdem kämen sie nicht umhin, Gesetzeslage und Rechtspraxis im Drittstaat zu analysieren. «Im Fall der USA mag dies aufgrund der verfügbaren Informationen gut bewältigbar sein. Für andere Länder dürfte das aber durchaus herausfordernd werden.» Wird bei der Prüfung festgestellt, dass das Schutzniveau ungenügend ist, sind gegebenenfalls zusätzliche Massnahmen wie eine Verschlüsselung oder eine Pseudonymisierung zu ergreifen. «Oder man verzichtet auf den Datentransfer.»

Auch Schweiz attestiert USA kein adäquates Schutzniveau mehr

Für die Schweiz als Nicht-EU/EWR-Mitglied hat das EuGH-Urteil von diesem Sommer grundsätzlich keine direkten Auswirkungen. Allerdings beurteilte in dessen Lichte auch der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) Adrian Lobsiger das US-Schutzniveau für Daten aus der Schweiz neu, wie dieser gegenüber den Teilnehmern des Seminars erläuterte. Im September habe er schliesslich entschieden, die indikative Länderliste des EDÖB abzuändern. Seither attestiert die Schweiz den USA kein adäquates Schutzniveau mehr.

Bezüglich eines Datentransfers in die USA stehen Schweizer Unternehmen neu folglich vor den gleichen Herausforderungen wie beim Transfer in einen anderen Staat, der gemäss EDÖB-Liste kein angemessenes Schutzniveau aufweist. Doch es gebe Lösungsansätze, so Lobsiger. Lösungsansätze, die in etwa die gleichen sind, wie sie Gächter aufzeigte: die Bedingungen im Importstaat analysieren, die Wahrscheinlichkeit eines staatlichen Eingriffs eruieren und Daten anonymisieren und verschlüsseln.

gassnerbau
Ihr Spezialist in Baufragen

+423 388 01 00

gassnerbau.li

FIRMENSÜCHE.LI
Grösste digitale Wirtschaftsdatenbank
Firmen | Personen | FL | Schweiz