Ein Jahr DSGVO und die Schweiz

Know-how Ein ganzes Jahr schon ist die Datenschutz-Grundverordnung der EU (EU-DSGVO) anwendbar. Was bisher geschah.

Von Martin Steiger

Mit der Datenschutz-Grundverordnung (DSGVO) – englisch General Data Protection Regulation (GDPR) – vereinheitlichte und verschärfte die Europäische Union (EU) per 25. Mai 2018 ihr Datenschutzrecht. Seit dem 20. Juli 2018 gilt die DSGVO im gesamten Europäischen Wirtschaftsraum (EWR), das heisst auch im Fürstentum Liechtenstein, in Island und in Norwegen.

99 Artikel, 173 Erwägungsgründe und 69 Öffnungsklauseln

Die DSGVO umfasst 99 Artikel und 173 erläuternde Erwägungsgründe. Die Verordnung soll nicht nur den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten gewährleisten, sondern auch den freien Datenverkehr sicherstellen und ersetzte 2018 die Datenschutz-Richtlinie der EU. Als Verordnung ist die DSGVO direkt anwendbar und musste durch die Mitgliedstaaten nicht erst in nationales Recht umgesetzt werden. Allerdings gibt es 69 Öffnungsklauseln, Ausnahmen und Optionen im nationalen Recht, zum Beispiel bei der Altersgrenze für die Einwilligung durch Kinder, beim Auskunftsrecht und bei der Pflicht zur Ernennung von Datenschutzbeauftragten.

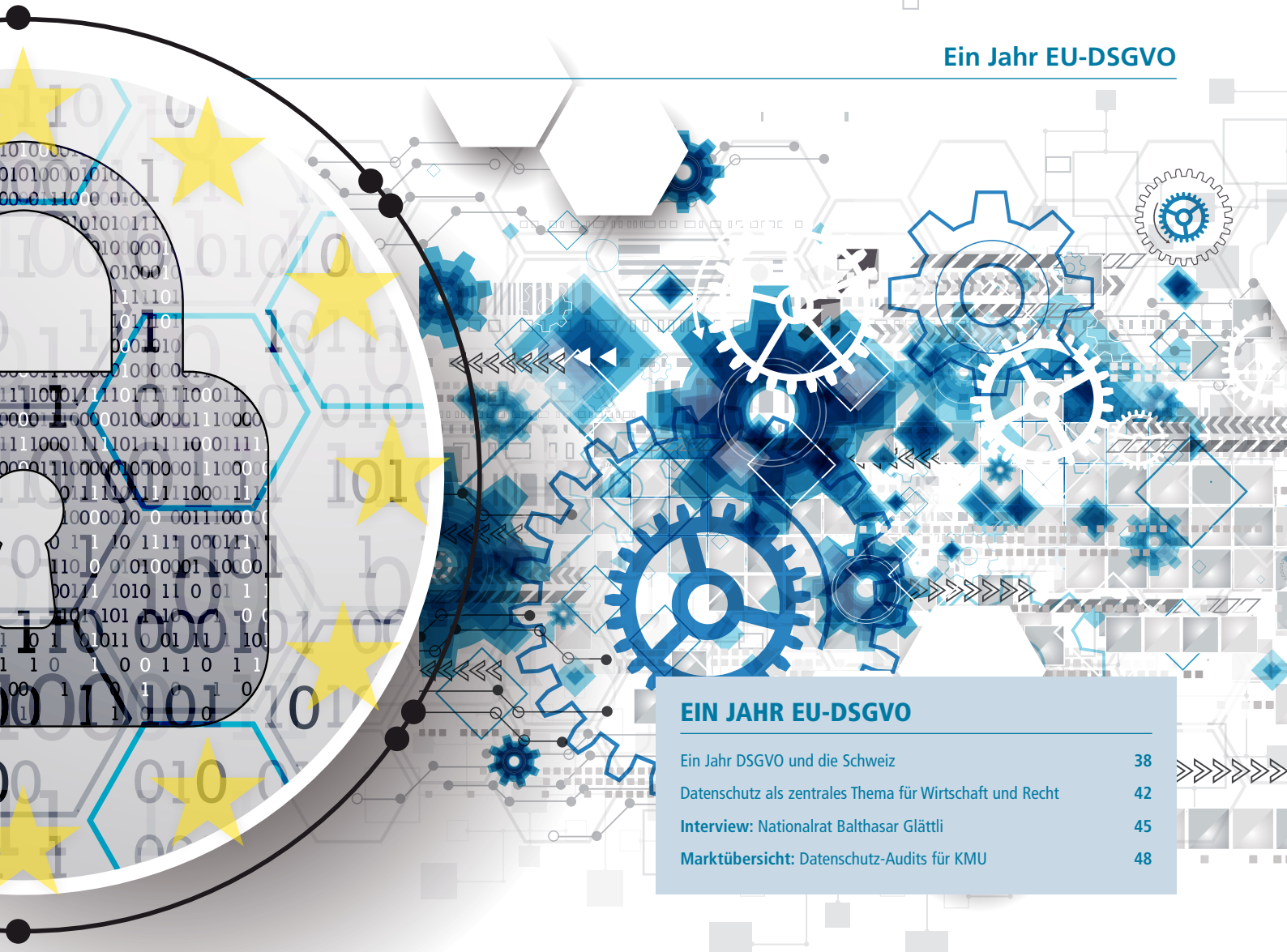
Auf den ersten Blick nennt die DSGVO zwar ausdrücklich und erstmals in Europa ein eigentliches Recht auf Datenschutz, hält im Übrigen aber an den bestehenden Grundsätzen im Datenschutzrecht fest. Ein solcher Grundsatz und eine Selbstverständlichkeit ist die Rechtmässigkeit der Verarbeitung personenbezogener Daten. Weitere Grundsätze sind Datenminimierung (Datensparsamkeit), Datensicherheit, Erforderlichkeit, Richtigkeit, Transparenz und Zweckbindung. Im Vorfeld der Geltung der DSGVO hiess es deshalb häufig, es ändere sich doch gar nicht so viel.

Auf den zweiten Blick zeigt sich, dass es für die Umsetzung der DSGVO nicht genügt, das bestehende Recht einzuhalten (oder umzusetzen). Die Erklärung dafür ist einfach: Mit der DSGVO wurde das Datenschutzrecht in Europa nicht nur vereinheitlicht, sondern mit besten Absichten und politisch gewollt auch erheblich verschärft.

Rechtmässigkeit der Verarbeitung personenbezogener Daten

Die DSGVO gilt für jede Verarbeitung personenbezogener Daten. Die Begriffe «personenbezogene Daten» und «Verarbeitung» sind umfassend zu verstehen. Gemäss DSGVO gilt – wie schon im früheren europäischen Datenschutzrecht – ein Verbot mit Erlaubnisvorbehalt. Die Verarbeitung personenbezogener Daten ist verboten, sofern sie nicht ausnahmsweise erlaubt ist. Im heutigen Informationszeitalter, wo die Verarbeitung von Informationen alltäglich ist, führt dieser Ansatz dazu, dass Daten geschützt und Informationen minimiert werden. Eigentlich sollte der freie Fluss von Informationen wünschenswert sein, dabei sollten aber die betroffenen Personen geschützt werden.

Gleichzeitig gilt die DSGVO für alle Verantwortlichen, die personenbezogene Daten verarbeiten: Ob Google, ein KMU oder ein Verein solche Daten verarbeitet, spielt für die Pflichten gemäss DSGVO mehrheitlich keine Rolle. In allen Fällen gilt,



EIN JAHR EU-DSGVO

dass personenbezogene Daten nur für eindeutige, festgelegte und legitime Zwecke erhoben werden dürfen. Daten dürfen in einer Form, welche die Identifizierung von betroffenen Personen ermöglicht, nur so lange gespeichert werden, wie es für die jeweiligen Zwecke erforderlich ist. Ausserdem ist bei der Verarbeitung immer eine angemessene Sicherheit der personenbezogenen Daten zu gewährleisten und es muss detailliert Rechenschaft über die Einhaltung der DSGVO abgelegt werden können.

Einwilligung und andere Rechtfertigungsgründe

Bei den Ausnahmen, die eine Verarbeitung personenbezogener Daten gemäss DSGVO rechtfertigen, steht in der öffentlichen Wahrnehmung die Einwilligung der betroffenen Personen im Vordergrund. Im Alltag wird man entsprechend ständig darum gebeten, in die eine oder andere Verarbeitung der eigenen Daten einzuwilligen. Dabei geht vergessen, dass die meisten Einwilligungen nicht rechtswirksam sind, weil sie nicht freiwillig, informiert und unmissverständlich erfolgten. So darf die Einwilligung nicht in Allgemeinen Geschäftsbedingungen (AGB) versteckt werden und vorangekreuzte Kästchen für die Einwilligung sind unzulässig. Weiter müssen erteilte Einwilligungen beweisbar sein, können umgekehrt von den betroffenen Personen aber jederzeit widerrufen werden.

Cookie-Banner, die behaupten, man erteile durch die weitere Nutzung einer Website seine Einwilligung, verhelfen auch nicht zur Rechtswirksamkeit. Niemand käme auf die Idee, auf diesem Weg die Einwilligung in die kostenpflichtige Nutzung einer Website rechtswirksam einholen zu können, doch ist der Glaube weit verbreitet, eine solche Einwilligung in Verhaltensüberwachung sei möglich.

In der Folge ist es häufig sinnvoll, auf mindestens einen anderen Rechtfertigungsgrund zu setzen. Für Unternehmen sind insbesondere die folgenden beiden Bedingungen relevant:

- Die Verarbeitung ist für die Vertragserfüllung oder für vorvertragliche Massnahmen erforderlich, zum Beispiel für die Beantwortung von Anfragen über ein Kontaktformular oder per Telefon, aber auch um eine Leistung erbringen oder eine Ware verkaufen zu können. Bei einem Kontaktformular ist es deshalb normalerweise nicht erforderlich, eine Einwilligung einzuholen.
- Die Verarbeitung ist zur Wahrung der überwiegenden eigenen Interessen erforderlich. Dabei muss eine Abwägung gegenüber den Interessen sowie Grundfreiheiten und Grundrechten der betroffenen Personen stattfinden. Als berechtigte Interessen gelten gemäss DSGVO unter anderem die Betrugsbekämpfung, Direktwerbung (!) und Informationssicherheit. Es muss aber immer auf die vernünftigen Erwartungen der betroffenen Personen abgestellt werden.

Drei weitere mögliche Bedingungen sind die Erforderlichkeit zur Erfüllung einer rechtlichen Verpflichtung, für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, und die lebenswichtigen Interessen einer betroffenen Person. Eine rechtliche Verpflichtung kann beispielsweise in der Aufbewahrung von Daten für Buchhaltung und Steuern liegen.

Zusätzliche Hürden gelten für die Verarbeitung besonderer Kategorien personenbezogener Daten. Dazu zählen Daten be-

treffend ethnischer Herkunft, Gewerkschaftszugehörigkeit, politische und weltanschauliche Meinungen, aber auch biometrische und genetische Daten sowie Daten zum Sexualleben.

Bei Minderjährigen ist die eigene Einwilligung grundsätzlich erst ab 16 Jahren wirksam. In Deutschland und Frankreich gilt diese allgemeine Altersgrenze, während sie in Österreich und Italien im Rahmen einer Öffnungsklausel auf 14 Jahre heruntergesetzt wurde. Bei jüngeren Minderjährigen müssen die Träger der elterlichen Verantwortung die Einwilligung erteilen.

Pflichten für Unternehmen und andere Verantwortliche

Die DSGVO bringt eine Reihe von Pflichten und Vorgaben mit sich, die Neuland für die meisten betroffenen Unternehmen sind und zu einem umfassenden Datenschutzmanagement zwingen. Nachfolgend eine Übersicht von Pflichten, die betroffene Unternehmen im Rahmen der DSGVO einhalten müssen.

Informationspflichten

Unabhängig vom Rechtfertigungsgrund verlangt die DSGVO, dass die betroffenen Personen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache über die Verarbeitung ihrer Daten sowie über ihre Rechte informiert werden. Die Information muss grundsätzlich bei der Erhebung der Daten erfolgen. Gängige Möglichkeiten für die Information sind Datenschutzerklärungen in Apps und auf Websites sowie Merkblätter, die beim ersten persönlichen Kontakt abgegeben werden.

Die Informationspflicht umfasst über ein Dutzend Punkte. Dazu zählen unter anderem Namen und Kontaktdaten des Verantwortlichen, die Zwecke der Datenverarbeitung einschliesslich Nennung der Rechtsgrundlagen, die allfällige Absicht zur Datenübermittlung in Drittländer und deren Absicherung sowie die Dauer oder zumindest die Kriterien für die Dauer der Speicherung personenbezogener Daten. Ausserdem muss über die zahlreichen Rechte der betroffenen Personen ausdrücklich informiert werden, unter anderem über das umfassende Auskunftsrecht, das Recht auf Berichtigung, das Recht auf Löschung (Recht auf Vergessenwerden), das Recht auf Einschränkung der Verarbeitung, das Recht auf Datenübertragbarkeit, das Widerspruchsrecht und das Recht auf Beschwerde bei einer Datenschutzaufsichtsbehörde. Die Information darf nicht bloss einmalig erfolgen, sondern muss bei jeder Verarbeitung stattfinden. Die Informationspflicht besteht auch, wenn die betroffenen Personen bereits Kenntnis von der Verarbeitung ihrer Daten haben. Die Informationspflicht ist kleinteilig und umfangreich, was den administrativen Aufwand erhöht und bei betroffenen Personen zu einer Informationsüberflutung führt. Wann haben Sie zuletzt eine Datenschutzerklärung gelesen?

Bei Datenschutzverletzungen bestehen eine Meldepflicht gegenüber der zuständigen Aufsichtsbehörde und eine Benachrichtigungspflicht gegenüber den betroffenen Personen. Der Spielraum, sich auf Ausnahmen zu berufen, wurde gegenüber dem früheren europäischen Datenschutzrecht eingeschränkt.

Dokumentations- und Rechenschaftspflichten

Verantwortliche, die personenbezogene Daten verarbeiten, sind umfassend dokumentations- und rechenschaftspflichtig. Dazu gehört, dass ein Verzeichnis aller Verarbeitungstätigkeiten geführt werden muss. Das Verzeichnis muss für jede einschlägige Verarbeitung im Wesentlichen aufführen, welche personenbezogenen Daten für welche Zwecke mit welchen Mitteln und unter welcher Verantwortung – zum Beispiel selbst oder bei Dritten sowie im Ausland – verarbeitet werden. Ausserdem muss dokumentiert werden, wie die Sicherheit der Verarbeitung (Datensicherheit) mit angemessenen technischen und organisatorischen Massnahmen (TOMs) gewährleistet wird. Das Verarbeitungsverzeichnis soll als Ausgangslage für das Datenschutzmanagement dienen. Allerdings können nur Aufsichtsbehörden Einsicht verlangen, so dass viele Verantwortliche das Risiko eingehen, das Verarbeitungsverzeichnis nur einmalig oder sogar erst bei Bedarf zu erstellen.

Pflichten bei der Auftragsverarbeitung

Die DSGVO erlaubt die Auslagerung der Datenverarbeitung an Dritte (Outsourcing). Allerdings muss die Auftragsverarbeitung vertraglich abgesichert werden, wofür die DSGVO zahlreiche Vorgaben nennt. In der Praxis kommen standardisierte Auftragsverarbeitungsverträge zum Einsatz, wie sie inzwischen viele Auftragsverarbeiter ihren Kunden per Mausklick standardmässig anbieten. Häufig werden solche Verträge abgeschlossen, obwohl gar keine Auftragsverarbeitung vorliegt. So ist beispielsweise eine Anwaltskanzlei normalerweise keine Auftragsverarbeiterin und es gibt viele Fälle einer gemeinsamen Verantwortlichkeit, unter anderem bei Facebook-Seiten.

Geldbussen und andere Folgen von Verstössen gegen die DSGVO

Die Durchsetzbarkeit und Glaubwürdigkeit der DSGVO soll insbesondere mit Sanktionen gestärkt werden. Die DSGVO sieht Geldbussen von bis zu 20 Millionen Euro oder von bis zu vier Prozent des weltweiten Jahresumsatzes – relevant ist der jeweils höhere Betrag – vor. Auch eine persönliche Haftung von einzelnen verantwortlichen Personen in Unternehmen ist möglich.

Verhängte Geldbussen gemäss DSGVO müssen abschreckend, verhältnismässig und wirksam sein. Der Rahmen für Geldbussen zielt offensichtlich auf weltweit tätige Internet-Unternehmen wie Facebook, Google oder Samsung. Bei anderen Unternehmen können schon wesentlich tiefere Geldbussen wirksam sein. Dazu kommt, dass die Aufsichtsbehörden zahlreiche weitere Befugnisse wie beispielsweise Anweisungen und Untersuchungen einsetzen können, die auch ohne Sanktionen einen erheblichen Aufwand verursachen können.

Für Schlagzeilen sorgte eine 50 Millionen Euro-Busse gegen Google in Frankreich. Die französische Datenschutzaufsichtsbehörde warf Google vor, die Informationspflichten verletzt und keine rechtswirksame Einwilligung für die Verarbeitung personenbezogener Daten für Werbezwecke eingeholt zu haben. Vor Geltung der DSGVO hätte in Frankreich ein Bussgeld von maximal 150’000 Euro verhängt werden können.

In Deutschland wurden inzwischen rund 100 Fälle von verhängten Geldbussen bekannt. Ein kleines Hamburger Unternehmen wurde vorerst mit 5000 Euro für einen fehlenden Auftragsverarbeitungsvertrag gebüsst, der Onlinedienst Knuddel mit 20’000 Euro wegen der fehlenden Verschlüsselung von Passwörtern bei einem Datendiebstahl. In einem Fall, wo Gesundheitsdaten öffentlich abrufbar waren, betrug die Busse 80’000

Euro. In Portugal trafen Sanktionen ein Spital im Zusammenhang mit dem Zugriff auf Patientendaten (400'000 Euro), in Dänemark ein Taxiunternehmen mit über neun Millionen nicht mehr benötigten Datensätzen (1'200'000 dänische Kronen, rund 160'000 Euro) und in Polen ein Unternehmen für das Abgreifen von Kontaktinformationen im Internet für Werbezwecke (220'000 Euro).

Verschiedene Aufsichtsbehörden kündigten in letzter Zeit an, die Schonfrist sei abgelaufen und Fehler würden jetzt teurer. Die bisherige Zurückhaltung lag auch daran, dass die Aufsichtsbehörden erst einmal selbst damit beginnen mussten, die DSGVO umzusetzen. Dazu kommt, dass sie tausende von Meldungen von betroffenen Personen erhalten und diese erst abarbeiten müssen. Aus diesem Grund sind viele Verfahren hängig oder werden erst noch eröffnet.

Die teilweise befürchtete Abmahnwelle wegen Datenschutzverletzungen ist bislang ausgeblieben. Während deutsche Abmahnungen wegen Urheberechtsverletzungen alltäglich sind, konnten sich Datenschutz-Abmahnungen bislang nicht etablieren. Das liegt an fehlenden finanziellen Anreizen für die Abmahner, aber auch daran, dass kaum jemand selbst in der Lage ist, die DSGVO in jeder Hinsicht einzuhalten.

Auswirkungen auf die Schweiz

Die DSGVO ist grundsätzlich nur im EWR einschliesslich EU anwendbar. Unternehmen und andere Verantwortliche mit Sitz in einem EWR-Mitgliedstaat, die personenbezogene Daten bearbeiten, unterliegen vollumfänglich der DSGVO. Das gilt auch für Filialen, Tochtergesellschaften, Zweigniederlassungen und sonstige Ableger von Schweizer Unternehmen im EWR.

Anwendbarkeit der DSGVO in der Schweiz

Ausnahmsweise gilt die DSGVO unter zwei alternativen Bedingungen gemäss dem sogenannten Marktortprinzip auch für die Verarbeitung personenbezogener Daten in – aus Sicht des EWR – Drittländern wie der Schweiz:

- Die DSGVO ist für Verantwortliche in der Schweiz einerseits anwendbar, wenn die Datenverarbeitung im Zusammenhang mit dem offensichtlich beabsichtigten Angebot von Dienstleistungen oder Waren – auch kostenlos – an Personen im EWR steht. Viele Unternehmen in der Schweiz bieten ihre Dienstleistungen gegenüber Personen im EWR an oder verkaufen Waren an Personen im Fürstentum Liechtenstein. Auch ein E-Mail-Newsletter, der sich unter anderem an Personen im EWR richtet, kann ein kostenloses Angebot im Sinn der DSGVO darstellen.
- Andererseits ist die DSGVO für Verantwortliche in der Schweiz anwendbar, wenn sie das Verhalten von Personen im EWR beobachten. Gemeint ist in erster Linie die Aufzeichnung von Aktivitäten im Internet, insbesondere mit der Möglichkeit, ein Profil der betroffenen Personen zu erstellen. Solches Tracking erfolgt beispielsweise mit dauerhaft oder zumindest langfristig gespeicherten Cookies sowie sonstigem Fingerprinting oder mit der Aufzeichnung der Nutzung von Apps und Websites (Session Replay).

Nicht relevant für die Anwendbarkeit der DSGVO in der Schweiz ist die Staatsbürgerschaft der betroffenen Personen. Die DSGVO gilt gemäss dem Marktortprinzip aus schweizerischer Sicht nur für Personen im EWR und zwar unabhängig von der Staatsbürgerschaft. Für einen deutschen Staatsbürger beispielsweise, der seine Ferien in der Schweiz verbringt oder in der Schweiz lebt, gilt die DSGVO hingegen nicht. Die DSGVO gilt auch nicht für Unternehmen in der Schweiz, die Aufträge von Kunden im EWR ausführen oder Grenzgänger beschäftigen.

Allerdings verpflichten sich viele Unternehmen – häufig ohne Not – vertraglich gegenüber ausländischen Kunden und Lieferanten zur Einhaltung der DSGVO oder unterstellen sich in ihrer Datenschutzerklärung freiwillig der DSGVO. In dieser Situation liegt das grösste Risiko nicht in Geldbussen von Aufsichtsbehörden, sondern in rechtlichen Auseinandersetzungen mit Vertragspartnern, wenn sich zeigt, dass man die DSGVO nicht einhält. Auch können vertragliche Verpflichtungen wie Audits oder Zertifizierungen zu hohen Kosten führen.

EU-Datenschutz-Vertreter und sonstige Umsetzung in der Schweiz

In jedem Fall ist die DSGVO für viele Unternehmen in der Schweiz teilweise anwendbar und sie müssen die zahlreichen Pflichten der Verordnung in Bezug auf Personen im EWR – und nur in Bezug auf solche Personen – einhalten. Dazu zählt insbesondere, dass grundsätzlich ein EU-Datenschutz-Vertreter als zusätzliche Anlaufstelle für Aufsichtsbehörden und betroffene Behörden benannt werden muss. Viele Unternehmen in der Schweiz berücksichtigen die DSGVO richtigerweise in ihrer Datenschutzerklärung, vergessen aber, einen EU-Datenschutz-Vertreter zu benennen und zu erwähnen. Allenfalls wird auch ein Datenschutzbeauftragter benötigt, der aber nicht mit dem EU-Datenschutz-Vertreter identisch sein darf. Sofern ein Datenschutzbeauftragter benötigt wird, ist es normalerweise sinnvoll, sich für eine interne Lösung zu entscheiden.

Wer in der Schweiz die DSGVO ganz oder teilweise umsetzt, hat immerhin den Vorteil, gelassen auf das revidierte Datenschutzgesetz (DSG) warten zu können. Das DSG wird die DSGVO zwar nicht übernehmen, sich aber in vielen Punkten an der DSGVO orientieren. Dazu zählen zusätzliche Informations- sowie Dokumentations- und Rechenschaftspflichten, aber auch neue Kompetenzen für den Eidgenössischen Datenschutz -und Öffentlichkeitsbeauftragten (EDÖB) sowie verschärfte Sanktionsmöglichkeiten. Mit dem revidierten DSG soll insbesondere sichergestellt werden, dass die Europäische Kommission den Datenschutz in der Schweiz weiterhin als angemessen beurteilt. Ohne diesen Anerkennungsbeschluss könnte sich die Schweiz nicht mehr am freien Datenverkehr in Europa beteiligen, was einen erheblichen wirtschaftlichen Schaden bedeuten würde. ■

DER AUTOR

Martin Steiger ist Anwalt und Unternehmer für Recht im digitalen Raum. Ein Schwerpunkt seiner Tätigkeit bei seiner Anwaltskanzlei Steiger Legal und beim Legaltech-Startup Papiertiger liegt im Datenschutzrecht. Martin Steiger ist unter anderem Mitglied im Advisory Board des Centre for Digital Responsibility (CDR) und im Expertenausschuss der Swiss Data Alliance. Er unterrichtet am Schweizerischen Institut für Betriebsökonomie (SIB) und engagiert sich bei der Digitalen Gesellschaft in der Schweiz.