CORNELIA MATTIG
SIMON ZUBER

DATENSCHUTZ IM UNTERNEHMEN
Einmaliger Kraftakt oder Dauerthema?*

Die Unmengen an täglich verarbeiteten Daten machen Datenschutz zu einem Thema für jedes Unternehmen. Das Recht des Einzelnen, vor Missbräuchen geschützt zu werden, ergibt sich aus dem Grundrecht auf Schutz der Privatsphäre. Ständige Datenflüsse erfordern einen ständigen Schutz, daher ist die Einhaltung des Datenschutzes im Unternehmen kein einmaliger Kraftakt.

1. AUSGANGSLAGE

Ständige Datenflüsse sind aus dem heutigen Alltag wegen der Digitalisierung und der Globalisierung nicht mehr wegzudenken. Begriffe wie Cloud-Computing, Big Data, Blockchain oder Internet of Things gehören zum Alltag und werfen immer wieder neue Fragen auf. *Die Europäische Union (EU)* hat im Rahmen dieser Entwicklungen eine Strategie für einen digitalen Binnenmarkt entwickelt, welche sicherstellen soll, dass das Potenzial des digitalen Zeitalters optimal genutzt werden kann. Teil dieser Strategie ist die Modernisierung des Datenschutzes, die *Datenschutz-Grundverordnung (DSGVO)* der EU, die am 25. Mai 2018 in Kraft getreten ist [1].

Die DSGVO wirkt unmittelbar und direkt [2]. Im Gegensatz zu einer Richtlinie erfordert die Verordnung keine Umsetzung in das nationale Recht der Mitgliedstaaten. Die DSGVO setzt sich zum Ziel, den Schutz personenbezogener Daten von natürlichen Personen sicherzustellen, ohne dabei den freien Verkehr von personenbezogenen Daten in der EU zu stark einzuschränken (Art. 1 DSGVO). Die DSGVO führt, neben sehr hohen inhaltlichen Anforderungen an verschiedene Bereiche in einem Unternehmen, auch Schadenersatzklagen sowie Bussgelder ein [3]. Die DSGVO erlangt Gültigkeit über die Grenzen der EU hinaus mittels der Einführung eines extraterritorialen Anwendungsbereichs [4]. Die DSGVO ändert die gesamte Datenschutzrechtslandschaft von Grund auf.

Teil der Strategie zum digitalen Binnenmarkt [5] ist auch die E-Privacy-Verordnung, die am 26. Oktober 2017 vom EU-Parlament als Ergänzung zur DSGVO angenommen wurde [6]. Diese ist in der medialen Berichterstattung neben der DSGVO etwas untergegangen. Doch sie wird für die digitale Wirtschaft von besonderer Bedeutung sein. Sie wird den Schutz der Privatsphäre bei elektronischer Kommunikation im Allgemeinen betreffen und als Spezialregelung Vorrang gegenüber der DSGVO haben. Der Begriff der elektronischen Kommunikation wird in der neuen E-Privacy-Verordnung sehr weit ausgelegt und unter anderem auch die Kommunikation zwischen Maschinen erfassen [7]. Gerade für Werbezwecke wird die Nutzung von Kommunikationsdaten erheblich eingeschränkt werden, da zum Beispiel der Einsatz von Tracking-Cookies nur noch mit aktiver und informierter Einwilligung zulässig sein wird [8]. Die E-Privacy-Verordnung wird ebenfalls einen sehr weiten geografischen Anwendungsbereich sowie ähnliche Sanktionsmechanismen wie die DSGVO enthalten [9]. Aufgrund des weiten räumlichen Anwendungsbereichs wird die E-Privacy-Verordnung auch für Schweizer Unternehmen relevant.

In der Schweiz ist das Datenschutzrecht zurzeit in Revision. Das Ziel dieser Revision ist es, das Recht an die neue technologische Realität und die Anforderungen der europäischen Gesetzgebung anzupassen. Am 15. September 2017 hat der Bundesrat die Botschaft zur Totalrevision des *Datenschutzgesetzes (DSG)* verabschiedet [10]. Das Inkrafttreten des revidierten DSG muss noch abgewartet werden, da sich die Diskussion um die Ausgestaltung der Revision etwas hinzieht [11].

2. ALLGEMEINES ZUR DSGVO – UMSETZUNG IN DER TREUHANDBRANCHE

2.1 Anwendungsbereich. Die DSGVO findet Anwendung auf Verantwortliche und Auftragsverarbeiter, welche personenbezogene Daten verarbeiten (Art. 2 DSGVO). Der räum-

CORNELIA MATTIG, LL.M., RECHTSANWÄLTIN, FRORIEP LEGAL AG, ZÜRICH

SIMON ZUBER, BSC WIRTSCHAFTSINFORMATIK, TREUHAND- UND REVISIONSGESELLSCHAFT MATTIG-SUTER UND PARTNER, SCHWYZ

liche Anwendungsbereich der DSGVO richtet sich nach zwei Anknüpfungspunkten; der Niederlassung in der Union und dem Marktort (Art. 3 DSGVO). Das Niederlassungsprinzip bringt keine Erweiterung des Anwendungsbereichs, anders das Marktortprinzip, welches den extraterritorialen Ansatz verstärkt. Das Marktortprinzip umfasst das Angebot von Waren und Dienstleistungen und die Verhaltensüberwachung in der EU durch Personen in einem Drittstaat (Art. 3 (2) DSGVO). Beim Angebot von Waren oder Dienstleistungen muss ein solches Angebot «offensichtlich beabsichtigt» sein (Erwägungsgrund 23 DSGVO). Entsprechende Indikatoren sind daher die Zugänglichkeit der Website, die Kontaktdaten, die Verwendung der Sprache oder die Verwendung der Währung. Schliesslich sind die tatsächlichen Umstände für die Anwendbarkeit entscheidend [12]. Die Verhaltensüberwachung geht weiter als die Beobachtung von Internetaktivitäten. Die *Artikel-29-Datenschutzgruppe (WP29)* geht davon aus, dass es eine Handlung durch den Verantwortlichen braucht (z. B. Absicht, Personendaten zu verarbeiten) [13]. Die offene Umschreibung des Anbietens von Dienstleistungen sowie des Verarbeitens von Daten gibt den Datenschutzbehörden und Gerichten einen grossen Ermessensspielraum. Aufgrund des extraterritorialen Charakters der DSGVO ist als Kontaktstelle entsprechend auch ein Vertreter in der EU zu benennen (Art. 27 DSGVO). Der Vertreter dient den Aufsichtsbehörden als Anlaufstelle für in Drittstaaten niedergelassene Verantwortliche oder Auftragsverarbeiter. Nach Art. 4 (17) DSGVO wird der Vertreter nicht nur als Kontakt beschrieben, sondern als echter Vertreter mit Pflichten. Eine Busse im Sinne von Art. 83 Abs. 4 lit. a DSGVO richtet sich dennoch gegen den Verantwortlichen sowie den Auftragsverarbeiter und nicht gegen den Vertreter.

Treuhänder haben in jedem Fall mit personenbezogenen Daten im Sinne der DSGVO zu tun, da sie mit Informationen arbeiten, welche es ermöglichen eine Person zu identifizieren (vgl. Art. 2 DSGVO). Verarbeitung im Sinne der DSGVO bedeutet, die Bearbeitung von solchen Daten in einem automatischen oder auch manuell erstellten Ablagesystem. Es ist hierbei wohl von einer sehr breiten Definition auszugehen [14]. In sachlicher Hinsicht besteht in Bezug auf die Anwendbarkeit der DSGVO auf Treuhänder wohl kein Fragezeichen. Für Schweizer Treuhänder stellt sich einzig die Frage, ob sie territorial unter die DSGVO fallen. Dies ist im Einzelfall abzuklären.

2.2 Grundsätze, Pflichten und Rechte. Art. 5 DSGVO regelt die Grundsätze der Verordnung und damit die wesentlichen Vorgaben, welche bei unklaren Begriffen auch zur Auslegung herangezogen werden können [15]. Diese Grundsätze

> *«Treuhänder haben in jedem Fall mit personenbezogenen Daten im Sinne der DSGVO zu tun.»*

sind Rechtmässigkeit, Treu und Glauben (Verhältnismässigkeit), Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Rechenschaftspflicht. Die in der DSGVO vorgesehenen Bussen und Sanktionen drohen, wenn die Grundprinzipien nicht oder mangelhaft umgesetzt sind (vgl. Art. 77 ff. DSGVO).

Die DSGVO schreibt vor, dass eine Datenverarbeitung nur rechtmässig ist, wenn eine Rechtsvorschrift dies vorsieht. Die in der DSGVO beschriebenen Erlaubnistatbestände sind sehr breit formuliert, damit der freie Datenverkehr sichergestellt ist (Art. 6 DSGVO). Darin widerspiegelt sich gerade der Grundsatz der Rechtmässigkeit. In Art. 9 DSGVO sind weitere Erlaubnistatbestände für die Verarbeitung von besonderen Datenkategorien geregelt. Für diese ist die Verarbeitung weiter eingeschränkt.

Die Verarbeitung von personenbezogenen Daten darf nur für festgelegte, eindeutige und rechtmässige Zwecke erfolgen. Der Zweck entscheidet über die Rechtmässigkeit unter Beachtung der Zweck-Mittel-Relation. Daneben müssen Daten dem Zweck angemessen, sachlich relevant, richtig und auf dem neusten Stand sein. Die Bearbeitung ist zudem auf

die Verarbeitung der erforderlichen Daten beschränkt. Die Daten sind im Weiteren vom Verantwortlichen oder Auftragsverarbeiter durch geeignete technische und organisatorische Massnahmen zu schützen [16].

Da der Verantwortliche für die Einhaltung der Grundsätze zuständig ist und deren Einhaltung nachweisen muss, führt dies für ihn zu einer erheblichen Dokumentations- und Nachweispflicht. Das heisst, bei der Planung und Einführung von Prozessen oder Strukturen muss die dazugehörende Dokumentation mitgeplant werden [17]. Der Verantwortliche kann hierbei nach einem risikobasierten Ansatz vorgehen. Die Einhaltung von Rechtsvorschriften ist integraler Bestandteil eines *internen Kontrollsystems (IKS)*. Dies macht eine Anpassung des Risikomanagements und des IKS notwendig. Dabei sollte systematisch vorgegangen werden. Für Schweizer Unternehmen stellt sich zunächst die zentrale Frage, in welchem Umfang das Unternehmen Anpassungen zur Umsetzung der DSGVO vornehmen will [18]. Dabei ist auch zu berücksichtigen, ob und in welchem Umfang personenbezogene Daten von in der EU ansässigen Personen verarbeitet werden [19]. Nachdem die Frage nach der Anwendbarkeit geklärt ist, sollten die zentralen Geschäftsprozesse identifiziert und auf ihre Konformität mit der DSGVO überprüft werden [20]. In diesem Rahmen kann ein Unternehmen auch weitere Pflichten, wie eine Datenschutz-Folgenabschätzung, treffen [21]. Eine Risikoabschätzung zu diesem Zeitpunkt erscheint auch dann angebracht, wenn eine solche nicht zwingend vorgesehen ist. Die im zweiten Schritt identifizierten Geschäftsprozesse müssen im Rahmen einer Risikobewertung analysiert werden, und das IKS ist dementsprechend anzupassen [22]. Die DSGVO auferlegt den Verantwortlichen weitgehende Informationspflichten in Bezug auf die Datenerhebung sowohl bei Betroffenen als auch bei Dritten [23]. Im Rahmen der Integration von Urteilen des *Europäischen Gerichtshofs (EuGH)* gelten zudem striktere Löschpflichten und das Recht auf Vergessenwerden [24]. Seit dem 25. Mai 2018 gelten auch erhebliche Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen, die Pflicht, technische datenschutzrechtliche Voreinstellungen und Massnahmen zu integrieren, ein Verarbeitungsverzeichnis zu erstellen, sowie Pflichten in Bezug auf die Datensicherheit [25].

«Seit dem 25. Mai 2018 gelten erhebliche Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen.»

Die DSGVO gibt betroffenen Personen weitgehende Rechte (Art. 15 ff. DSGVO). Der Grundsatz ist dabei, dass jede betroffene Person das Recht hat, zu wissen, ob und welche Daten über sie verarbeitet werden. Daneben bestehen noch weitere spezifische Rechte. Im Prinzip soll der Betroffene die Kontrolle über seine Daten behalten [26].

2.3 Übermittlung personenbezogener Daten und unabhängige Aufsichtsbehörden. Die DSGVO schränkt zudem die Übermittlung von personenbezogenen Daten von der EU in ein Drittland ein, sofern nicht geeignete Garantien ein angemessenes Datenschutzniveau sicherstellen (Art. 46 ff. DSGVO). Die Europäische Kommission kann feststellen, dass ein Drittstaat über ein angemessenes Datenschutzniveau verfügt. Die Schweiz geniesst eine solche Anerkennung seit 2000, daher können Daten zurzeit noch mühelos aus der EU in die Schweiz übermittelt werden [27]. Allerdings kann eine solche Anerkennung durch die Kommission widerrufen oder geändert werden, daher ist eine Anpassung an das EU-Recht für die Schweiz sehr wichtig [28].

Die unabhängige Aufsicht ist ein weiterer zentraler Aspekt der DSGVO. In der heutigen Zeit, wo die Verarbeitung von personenbezogenen Daten allgegenwärtig ist, stellen diese Aufsichtsbehörden die Wächter des Digitalzeitalters dar [29]. Der EuGH hat dies noch unterstrichen, indem er gesagt hat, dass Aufsichtsbehörden objektiv und unparteiisch sein müssen. Um dies zu erreichen, dürfen diese keinen externen direkten oder indirekten Einflüssen unterliegen [30]. Dieser Begriff der völligen Unabhängigkeit wurde in der DSGVO nun noch präzisiert (vgl. Art. 52 DSGVO). Auch wurden die Kompetenzen der Aufsichtsbehörden durch die DSGVO verstärkt (Art. 58 DSGVO). Schweizer Unternehmen, die auf dem EU-Markt tätig sind, sollten die erweiterten Kompetenzen und die Stärkung der Aufsichtsbehörden im Hinterkopf behalten. Die Unternehmen unterstehen den Aufsichtsbehörden am Ort ihrer Niederlassung und werden auch dort für Verletzungen haftbar gemacht [31]. Für den Fall, dass ein Schweizer Unternehmen keine Niederlassung in der EU hat, ist die Aufsichtsbehörde am Sitz des EU-Vertreters zuständig [32]. Die DSGVO sieht eine enge Kooperation zwischen den Aufsichtsbehörden vor und zielt auf eine One-Stop-Shop-Lösung ab. Dabei wird die Aufsichtsbehörde am Ort der Hauptniederlassung zur federführenden Aufsichtsbehörde und koordiniert die verschiedenen Aufsichtsbehörden [33].

Abbildung: **ZENTRALE PFLICHTEN FÜR UNTERNEHMEN**

- → Erweiterte Dokumentations- und Nachweispflichten
- → Risikobasierter Datenschutz (Integration im IKS)
- → Informationspflichten bei der Datenerhebung
- → Datenschutz-Folgenabschätzung, sofern eine solche vorgeschrieben ist
- → Striktere Löschpflichten und Recht auf Vergessenwerden
- → Erhebliche Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen
- → Datenschutz durch Technik und datenschutzrechtliche Voreinstellungen
- → Verzeichnis von Verarbeitungstätigkeiten
- → Datensicherheit
- → Zusätzliche Verantwortung für Datenschutzbeauftragte
- → Bezeichnung eines Vertreters

2.4 Schweizer Unternehmen. Aufgrund des erweiterten räumlichen Anwendungsbereichs kann die DSGVO global Anwendung finden. Unternehmen sollten daher die Anwendbarkeit der DSGVO überprüfen, insbesondere unter Berücksichtigung der erweiterten Haftungsgrundlagen sowie der hohen Bussen für Verantwortliche und Auftragsverarbeiter (Art. 82 ff. DSGVO). Die DSGVO setzt in diesem Zusammenhang auch Kriterien für die Bemessung der Bussgelder fest. Betroffene Unternehmen können mit der Umsetzung von Massnahmen anhand dieses Katalogs ihr Bussenrisiko vermindern (Art. 83 DSGVO). Kriterien sind u. a. Umstände, Verarbeitungsart, Verschulden, wirtschaftliche Folgen, technische Massnahmen, Schadensminderung, Befolgung früherer Anordnungen der Aufsichtsbehörde oder Befolgung von Verfahrensregeln und Zertifizierungsverfahren. Unternehmen können gerade auf die letztgenannten Kriterien einen grossen Einfluss ausüben.

Bei der Umsetzung der DSGVO sollten Unternehmen die elf Punkte gemäss *Abbildung* beachten. Wo noch Lücken bestehen, empfiehlt es sich, diese rasch zu schliessen. Je nach Tätigkeit des Unternehmens sind die einzelnen Pflichten von unterschiedlichem Gewicht.

Eine Mehrheit der Schweizer Unternehmen schenken dem Datenschutz bereits heute grosse Beachtung. Allerdings sind sie vielerorts mit der Dokumentation noch nicht auf dem erforderlichen Stand.

3. DATENSCHUTZREVISION IN DER SCHWEIZ

Die Totalrevision des Schweizer Datenschutzgesetzes verfolgt verschiedene Ziele. Die Hauptaspekte betreffen die Verbesserung der Transparenz von Datenbearbeitungen, Stärkung der Selbstbestimmung der betroffenen Personen über ihre Daten sowie die Anpassung an neue Technologien und an die geänderten gesellschaftlichen Verhältnisse [34].

Zudem soll im Rahmen der Revision eine Anpassung an die DSGVO erfolgen, um sicherzustellen, dass das Schweizer Datenschutzrecht über ein angemessenes Schutzniveau im Vergleich mit der EU verfügt. Dadurch soll gewährleistet werden, dass die Angemessenheitsentscheidung der EU-Kommission stehen bleibt und Daten mühelos aus der EU in die Schweiz übertragen werden können [35]. Daneben musste die Schweiz die EU-Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts als Schengen acquis übernehmen, wozu sie aufgrund des Schengen-Abkommens verpflichtet ist. Spannend ist im Besonderen die Totalrevision des DSG (E-DSG) als Teil der Vorlage, welche zurzeit im Parlament noch diskutiert wird [36].

Die Vorlage wird, wie bereits erwähnt, in mehreren Etappen behandelt. Die Übernahme der Richtlinie ist bereits im Parlament verabschiedet worden, während bezüglich der Revision des DSG noch kein Ende der Diskussion in Sicht ist [37]. Das E-DSG lehnt sich stark an die DSGVO an. Es wird aber dennoch einige Unterschiede aufweisen, insbesondere verwendet das Schweizer Gesetz oftmals andere Bezeichnungen als die DSGVO (z. B. Datenschutzberater in der Schweiz und Datenschutzbeauftragter in der EU). Das E-DSG ist in verschiedene Teile gegliedert. Es beginnt mit den Grundsätzen und regelt danach den Datenschutz durch Technik, datenschutzfreundliche Voreinstellungen sowie die Datensicherheit. Gleich wie die DSGVO sieht auch das E-DSG spezielle Regeln in Bezug auf die Bearbeitung durch Auftragsarbeiter sowie die Ernennung eines Datenschutzberaters vor. In eine ähnliche Richtung geht der Entwurf auch in Bezug auf Kodizes, Zertifizierungsmöglichkeiten und die Bekanntgabe von Personendaten ans Ausland. Anders als die DSGVO sieht das E-DSG noch zusätzlich eine Regelung zu Daten von verstorbenen Personen vor. Kontrovers diskutiert wird vor allem der Unterschied bei den Sanktionen. Während das EU-Recht verwaltungsrechtliche Sanktionen vorsieht (vgl. Art. 77 ff. DSGVO), hat das E-DSG Strafbestimmungen aufgestellt (Art. 54–60 E-DSG). Damit ist das Schweizer Sanktionssystem schärfer, obschon die vorgesehenen Bussen tiefer scheinen.

«Schweizer Unternehmen sind mit der Dokumentation noch etwas im Rückstand.»

4. DATENVERLETZUNG – WIE GEHE ICH VOR?

4.1 DSGVO. Compliance mit der DSGVO ist das eine, das andere ist, was ein Unternehmen bei einer Datenverletzung tun muss.

Grundsätzlich sieht die DSGVO vor, dass eine Verletzung des Schutzes von personenbezogenen Daten innert 72 Stunden nach Bekanntwerden der Aufsichtsbehörde zu melden ist (Art. 33 DSGVO). Der Artikel besagt zudem, dass nicht jede Verletzung gemeldet werden muss. Allerdings ist die Abwägung eher schwierig [38]. Bei einer grenzüberschreitenden Verletzung ist die federführende Aufsichtsbehörde zu benachrichtigen [39]. Eine Datenverletzung liegt u. a. vor, wenn personenbezogene Daten gelöscht, verloren, verändert oder unbefugt einem Dritten zugänglich gemacht wurden (Art. 4 (12) DSGVO). Das heisst, eine solche Verletzung kann beispielsweise gegeben sein, wenn jemand seinen Arbeitscom-

puter im Zug vergisst, eine E-Mail mit vertraulichen Informationen einem falschen Empfänger zustellt oder wenn der Server gehackt wird. Im Zeitpunkt, wo der Verantwortliche vernünftigerweise von einer solchen Verletzung ausgehen kann, beginnen die 72 Stunden zu laufen [40]. Die Information an die Aufsichtsbehörde muss gewisse Mindestinformationen enthalten, weshalb es sinnvoll ist, den Ablauf bei einer Verletzung im Vorhinein zu definieren [41].

«Eine Implementierung des Datenschutzes im IKS ist ein guter Weg, die regelmässigen Kontrollen zu institutionalisieren.»

Bei einem Unternehmen in einem Drittstaat, welches keine Niederlassung in der EU hat, empfiehlt die WP29, dass eine Meldung an jene Aufsichtsbehörde erfolgen soll, in deren Gebiet der Vertreter des Verantwortlichen seinen Sitz hat [42]. Neben der Meldung an die Aufsichtsbehörde darf die Kommunikation mit dem oder den Betroffenen nicht vergessen werden (Art. 34 DSGVO).

4.2 E-DSG. Aus Art. 22 E-DSG ergibt sich keine bestimmte Frist, innert welcher eine Verletzung der Datensicherheit dem Eidg. Datenschutz- und Öffentlichkeitsbeauftragten gemeldet werden muss. Das Gesetz beschränkt sich auf die Formulierung «unverzüglich». Es ist davon auszugehen, dass man sich bei dieser Wortwahl an der EU-Frist von 72 Stunden orientieren kann. Die Erstellung einer Mustermeldung sowie eines Ablaufprotokolls ist ebenfalls empfehlenswert, um die Meldung unverzüglich zu erstatten. Abgesehen von der unterschiedlichen Frist, kann für eine Meldung einer Datensicherheitsverletzung auf eine Meldung nach DSGVO verwiesen werden.

5. FAZIT UND EMPFEHLUNG AN TREUHÄNDER

Zur erfolgreichen und raschen Umsetzung der DSGVO und mit hoher Wahrscheinlichkeit auch des revidierten DSG sind die unter 2.4 beschriebenen Punkte zu beachten. Dies ist, wie im Titel erwähnt, zu Beginn ein Kraftakt für jedes Unternehmen, bis die erforderlichen Dokumente und Prozesse erst einmal schriftlich festgehalten sind. Allerdings ist der Datenschutz eine andauernde Geschichte, und Überprüfungen bzw. Lückenanalysen müssen regelmässig vorgenommen werden [43].

Es ist festzuhalten, dass der Datenschutz in der EU sowie für Schweizer Unternehmen ein Dauerthema bleiben wird. Gerade die noch anstehenden Revisionen in der Schweiz und auch in der EU werden uns noch lange beschäftigen. Zudem ist es beim Datenschutz mit einer einmaligen Umsetzung nicht getan. Der Datenschutz muss im täglichen Betrieb aufrechterhalten werden [44]. Dabei ist zu beachten, dass die Unterstützung des Managements für den Datenschutz ungebrochen ist. Aus der DSGVO geht klar hervor, dass regelmässige Audits und die Implementierung der dadurch entdeckten Compliance-Defizite Teil der unternehmerischen Pflichten sind [45]. Eine Implementierung des Datenschutzes im IKS ist ein guter Weg, die regelmässigen Kontrollen zu institutionalisieren [46]. Es sind zudem regelmässige Schulungen im Unternehmen vorzunehmen, damit auf Zwischenfälle und Anfragen von Betroffenen entsprechend reagiert werden kann. Neue Verarbeitungstätigkeiten sind zudem laufend zu erfassen [47]. In diesem Sinn ist auch aus Fehlern nach Datenverletzungen zu lernen.

Auch wenn die DSGVO am 25. Mai 2018 in Kraft getreten ist, bleibt das Datenschutzrecht ein aktuelles Thema, denn mit der einmaligen Implementierung ist es nicht getan. Es heisst, am Ball zu bleiben. ■

Anmerkungen: *Die Autoren danken Claudia Mattig sowie Monika Camenzind (Mattig-Suter und Partner) herzlich für deren Unterstützung bei der Erstellung dieses Beitrags. **1)** European Commission, Why we need a Digital Single Market, 6.5.2015. **2)** Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) im Amtsblatt der Europäischen Union, Abl. L 119/1. **3)** Vgl. Wybitul Tim, EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 28. **4)** Vgl. Art. 3 (2) und (3) DSGVO; Erwägungsgrund 23 f. DSGVO; WP 29, WP 234 rev.01.; Opinion 2/2017 on data processing at work WP 249.21. **5)** European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final. **6)** European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final. **7)** Art. 2 E-Privacy Regulation. **8)** Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247. **9)** Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247; Bergamelli Manuel, Die Auswirkung der neuen DSGVO auf die Schweiz, in: Jusletter 30. April 2018, Rz. 18. **10)** Vgl. Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017. **11)** Vgl. Husi-Stämpfli Sandra, Die DSG-Revision oder: Ein Beziehungsdrama in drei Akten, in Jusletter 7. Mai 2018. **12)** Vgl. Wybitul, S. 27. **13)** WP 29, WP 243rev.01, S. 8. **14)** Vgl. Handbook on European data protection law (2014), S. 70 f; CJEU, C-101/01, Bodil Lindqvist, 06.11.2003. **15)** Wybitul, S. 13. **16)** Handbook on European data protection law (2014), S. 81 ff. **17)** Wybitul, S. 49 ff. **18)** Vgl. Weka IKS <https://www.weka.ch/themen/finanzen-controlling/iks-und-risikomanagement/internes-kontrollsystem/article/eu-dsgvo-einheitliche-regelung-von-compliance-und-iks-beischweizer-unternehmen/> besucht 28.06.2018. **19)** Art. 3 (2) und (3) DSGVO. **20)** Weka. **21)** Wybitul, S. 39. **22)** Weka. **23)** Wybitul, S. 33 ff. **24)** Wybitul S. 43; CJEU, C-131/12, Google Spain, 13.05.2014. **25)** Wybitul S. 45 ff. **26)** Handbook on European Data Protection (2018), S. 206 ff. **27)** Bergamelli, Rz. 24. **28)** Botschaft Totalrevision Datenschutzgesetz, S. 6944 ff. **29)** Handbook (2018), S. 189. **30)** CJEU European Commission v. Federal Republic of Germany (GC), 09.03.2010, para 27 ff. **31)** Bergamelli, Rz. 27. **32)** WP 29, Guidelines on Personal data breach notification under Regulation 2016/679, WP 250rev.01, S. 32. **33)** Handbook (2018), S. 198 f. **34)** Botschaft Totalrevision Datenschutzgesetz, S. 6944 ff. **35)** Bergamelli, Rz. 24. **36)** Botschaft Totalrevision Datenschutzgesetz, S. 6944 ff. **37)** Vgl. Husi-Stämpfli. **38)** Vgl. WP 29, Guidelines on Personal data breach notification under Regulation 2016/679; WP 29, WP 250rev.01, S. 18, 22 ff. **39)** WP 29, Guidelines on Personal data breach notification under Regulation 2016/679, WP 250rev.01, S. 5. **40)** WP 29, Guidelines on Personal data breach notification under Regulation 2016/679, WP 250rev.01, S. 11. **41)** Art. 33 (3) DSGVO. **42)** WP 29, Guidelines on Personal data breach notification under Regulation 2016/679, WP 250rev.01, S. 18. **43)** Vgl. Feiler Lukas und Horn Bernhard, Umsetzung der DSGVO in der Praxis (2018), S. 24. **44)** Vgl. Feiler und Horn, S. 24. **45)** Vgl. Feiler und Horn, S. 24. **46)** Vgl. Weka. **47)** Vgl. Feiler und Horn, S. 24.