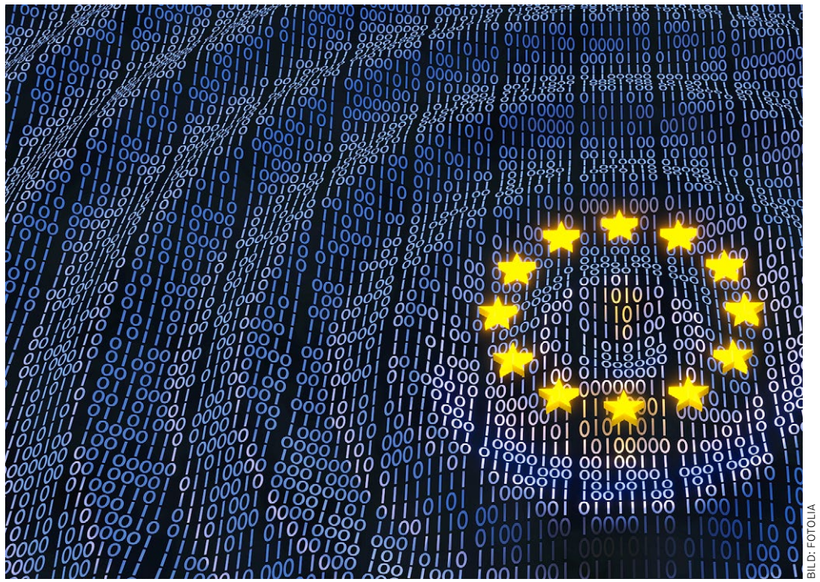

BILD: FOTOLIA

# Europa macht Ernst mit Datenschutz

Eine geplante Totalrevision soll das hiesige Datenschutzgesetz an die europäische Datenschutzgrundverordnung annähern. Vieles ist aber noch offen. Worum es geht und warum es auch für Schweizer Banken relevant ist.

*Von Monika Pfaffinger und Nadine Balkanyi-Nordmann*

Datenschutz ist in der globalisierten und digitalisierten Gesellschaft von einem Rand- zu einem Kernthema geworden. Es ist nicht übertrieben, von einer neuen Ära zu sprechen. Sie zeigt sich in rechtlichen Revisionswellen, in der konsequenteren behördlichen Durchsetzung, in unzähligen politischen Vorstössen sowie in der prominenten Thematisierung in den Medien. Den Individuen, das ist belegt, ist Datenschutz auch heute wichtig. Reputations- und Vertrauensverlust als Folge von Datenschutzverstössen schlagen sich nicht zuletzt wirtschaftlich nieder. Folglich ist Datenschutz heute in vielerlei Hinsicht von hoher Relevanz.

**Akuter Handlungsbedarf**

Für Schweizer Unternehmen und ihre Datenverarbeitungen kann nunmehr, nebst dem eidgenössischen Datenschutzgesetz (DSG), auch die europäische Datenschutz-Grundverordnung (EU-DSGVO) mit ihren weitreichenden Vorgaben einschlägig sein. Eine geplante Totalrevision des DSG will dieses zwar an die EU-DSGVO annähern, allerdings hat die staatspolitische Kommission des Nationalrates im Januar 2018 die Etappierung des Projekts beschlossen. Vieles ist damit offen; etwas steht allerdings schon heute fest: Selbst nach der Revision wird das Schutzniveau des DSG tiefer bleiben als das der EU-DSGVO.

Mit seinem aktuellen Inhalt ist die Differenz zwischen schweizerischem und europäischem Datenschutzniveau markant. Hinzu kommt, dass Anforderungenk, die bisher gegolten haben, weitgehend ignoriert worden sind. Dieses sogenannte Vollzugsdefizit macht den Handlungsbedarf bei Schweizer Unternehmen umso grösser und dringlicher.

**Anwendungsbereich der EU-Datenschutzgrundverordnung**

Schweizer Finanzdienstleister sind somit gut beraten, wenn sie die Einschlägigkeit der Erlasse für sich prüfen, denn: Das europäische Recht ist gemäss Art. 3, Abs. 2 EU-DSGVO, ebenso durch Unternehmen zu beachten, die keine Niederlassung im EU-Raum haben, die dort aber marktaktiv werden, indem sie Waren/Dienstleistungen in der EU anbieten (lit. a) oder die das Verhalten von Betroffenen in der EU beobachten (lit. b). Wird man von beiden Erlassen erfasst, stellen sich grundlegende strategische sowie organisatorische Fragen. Der Anwendungsbereich der EU-DSGVO lässt sich anhand eines zeitlichen, sachlichen, persönlichen und räumlichen Elementes bestimmen. Es ist mit einer extensiven Auslegung auch insofern durch die europäischen Behörden zu rechnen.

- Zeitlich ist eine Umsetzung bis zum 25. Mai 2018 vorgeschrieben.
- Sachlich und persönlich erfasst die EU-DSGVO die «Verarbeitung personenbezogener Daten von natürlichen Personen». Personenbezogen sind Angaben, die sich auf eine identifizierte/identifizierbare natürliche Person beziehen wie Bankkunden-, Mitarbeiter- und Investorendaten. Auch die Produktwebsite eines Schweizer Asset Managers mit Online-Angebot von Finanzprodukten für Personen in der EU generiert personenbezogene Angaben: Gemäss europäischem Gerichtshof (EuGH) können dynamische IP-Adressen für Provider wie Website-Betreiber Personendaten sein (vgl. EuGH, 18. Oktober 2016, C-528/14 Rz. 49). Geschützt sind nur natürliche Personen, nicht anwendbar ist die EU-DSGVO auf die Verarbeitung von Angaben juristischer Personen. Die Abgrenzung ist allerdings keineswegs trivial, wie das Beispiel von CRM-Systemen illustriert, in denen Kundenbeziehungen elektronisch mit Notizen erfasst werden: Interessiert sich die Repräsentantin einer juristischen Person für Bankprodukte und wird die Kundenbeziehung persönlich und individualisiert gepflegt, sodass sie auf das die juristische Person vertretende Individuum «durchschlagen», ist die EU-DSGVO wohl anwendbar. Der Verarbeitungsbegriff ist weit und meint nahezu jeden Umgang mit Personendaten.
- Räumlich gilt die EU-DSGVO zunächst für Verantwortliche, die im Rahmen der Tätigkeit in einer EU-Niederlassung Personendaten bearbeiten, selbst, wenn die Verarbeitung ausserhalb der EU stattfindet (Niederlassungsprinzip, Art. 3, Abs. 1 EU-DSGVO). Ein Beispiel ist die zentrale Führung der Personaldossiers von Mitarbeitenden eines Schweizer Finanzdienstleisters mit EU-«Branches/Subsidiaries». Zudem ist die europäische Verordnung anwendbar, wenn Waren oder Dienstleistungen betroffenen natürlichen Personen in der EU angeboten werden (Angebotstatbestand/Marktortprinzip, Art. 3, Abs. 2, lit. a EU-DSGVO). Sodann fällt man in den Scope der EU-DSGVO bei der Verhaltensbeobachtung von Personen in der EU (Trackingtatbestand, Art. 3, Abs. 2 lit. b EU-DSGVO).

**Die neue europäische Datenschutzgrundverordnung wird auch hiesige Unternehmen betreffen, die keine Niederlassung im EU-Raum haben.**

Betreibt eine Schweizer Bank eine Homepage und eine Person klickt an, um diese als privater Investor in einem EU-Land zu besuchen, und wird das Surfverhalten getrackt, wird insofern auch für eine Schweizer Bank als Homepage-Betreiberin und Tracker in die europäische Datenschutzverordnung relevant. Nicht zu vergessen ist deren Anwendbarkeit im Zuge von Auftragsdatenverarbeitungen gemäss Art. 28 EU-DSGVO für Schweizer Banken, zum Beispiel aufgrund eines Background-Screenings von einem in Deutschland lebenden Bewerber, der bei einer Schweizer Bank arbeiten will oder infolge des Outsourcings von «Payroll-Services» respektive eines «New Joiner-Screenings», das in das EU-Ausland gesendet wird. Ist die EU-DSGVO auf Datenverarbeitungen von in der Schweiz agierenden Unternehmen anwendbar, werden insofern die umfassenden und weitreichenden Pflichten der EU-DSGVO einschlägig.

**Kerninhalte, Kerndifferenzen**

Rechtlich am Anfang eines mit der EU-DSGVO konformen Handelns steht die Sicherstellung, dass ein Erlaubnistatbestand gemäss Art. 6, Abs. 1, EU-DSGVO, vorliegt. Die EU geht – anders als das Schweizer DSG – vom Grundsatz des Verarbeitungsverbotes mit Erlaubnisvorbehalten aus. Die Einwilligung ist dann einzuholen, wenn kein anderer Erlaubnistatbestand greift, wobei die Anforderungen an ihre Gültigkeit hoch angesetzt werden. Hingegen bedingt eine zulässige Verarbeitung nach DSG keinen Erlaubnistatbestand, womit auch die Einwilligung keine grundsätzliche Voraussetzung für rechtmässige Datenbearbeitungen ist.

An diesem System will man im Zuge der Totalrevision festhalten. Für Unternehmen mit doppeltem Scope wird sich in der Praxis folglich – kann ein anderer Erlaubnistatbestand nicht angerufen werden – das Prinzip der Einwilligung durchsetzen. Eine weitere Kerndifferenz zwischen EU-DSGVO und DSG wird sodann im Sanktionssystem zu finden sein: Bei den Geldbussen nach EU-DSGVO handelt es sich um (drakonische) Verwaltungssanktionen und um eine unmittelbare Unternehmenshaftung. Sie können mit bis zu maximal 20 Millionen Euro oder mit bis zu 4 Prozent des weltweiten Umsatzes pro Jahr – je nachdem, was höher ist – eine kartellähnliche Höhe erreichen. Fahrlässigkeit genügt (vgl. Art. 83 f. EU-DSGVO). Hingegen schlägt man in der Schweiz eine persönliche Strafbarkeit für den vorsätzlich handelnden Verantwortlichen vor – ein umstrittener Punkt, der dem DSG eine eigene Schärfe verleihen würde.

**Facettenreiche Risiken fordern Umsicht**

Die Relevanz, Unternehmen datenschutzkonform aufzustellen, geht indes weit über das Sanktions- und Bussenrisiko hinaus. Hinzutreten können Schadenersatz- und Haftungsrisiken durch Ansprüche der Datensubjekte oder innerhalb der Konzernstruktur, Untersuchungs- und Verfahrenskosten, Reputationsschäden und Vertrauensverluste mit finanziellen Auswirkungen oder die Verweigerung von Aufträgen gemäss Art. 28 EU-DSGVO. Zudem steht den EU-Behörden ein umfassendes Arsenal an Untersuchungs- und Massnahmenbefugnissen zur Verfügung, was einschneidende Konsequenzen für betroffene Unternehmen haben kann (vgl. Art. 58 EU-DSGVO). Es ist unübersehbar: Mit dem Datenschutz und seiner Einhaltung meint man es ernst. Entsprechend riskant ist es, die Implementierung einer Datenschutz-Compliance auf die leichte Schulter zu nehmen oder allzu pragmatisch anzugehen.

Für Schweizer Unternehmen und ihre Datenverarbeitungen kann nunmehr, nebst dem eidgenössischen Datenschutzgesetz, auch die europäische Datenschutzgrundverordnung mit ihren weitreichenden Vorgaben einschlägig sein.

**Auf dem Weg zur Datenschutz-Compliance**

Um die komplexe Aufgabe der Datenschutz-Compliance zu bewerkstelligen, ist eine für das jeweilige Unternehmen passende Methodologie erforderlich. Ihre Entwicklung erfolgt anhand einer umfassenden Kartografierung, die eine Analyse von Produkten, inneren Risiken (insbesondere Art, Tiefe und Breite der verarbeiteten Personenangaben), Verarbeitungsprozessen sowie der rechtlichen Anforderungen umfasst. Gehirn und Herz der Datenschutz-Compliance ist das Verarbeitungsverzeichnis. Die Inventarisierung der Verarbeitungsvorgänge muss einen Detailgrad aufweisen, anhand dessen die Risiken sowie die Einhaltung der rechtlichen Vorgaben evaluiert werden können. Ergibt das Datenschutz-Assessment Abweichungen, folgt eine risikobasierte Definierung und Priorisierung der Massnahmen (Stichwort: Data-Governance).

Ein Datenschutz-Compliance-Programm erfasst als Kernelemente namentlich die internen Prozesse, Systeme und die Organisation (und damit die technischen und organisatorischen Massnahmen, sog. TOM), die Betroffenenrechte und die Pflichten im Umgang mit Verstössen. Stets zu beachten sind umfassende Dokumentationspflichten, denn die EU-DSGVO verlangt, dass jederzeit Rechenschaft über ihre Einhaltung abgelegt werden kann (Stichwort: Accountability). Der Bedeutungswandel muss im gesamten Unternehmen adressiert werden. Denn: Datenschutz gehört in die DNA des Unternehmens integriert. •

**DR. IUR. MONIKA PFAFFINGER** ist Head of Data Protection and Privacy Praxis, Lexperience AG, Legal & Compliance Services;
**LIC. IUR. NADINE BALKANYI-NORDMANN** ist CEO der Lexperience AG, Legal & Compliance Services, Rechtsanwältin, LL.M., FCIArb.