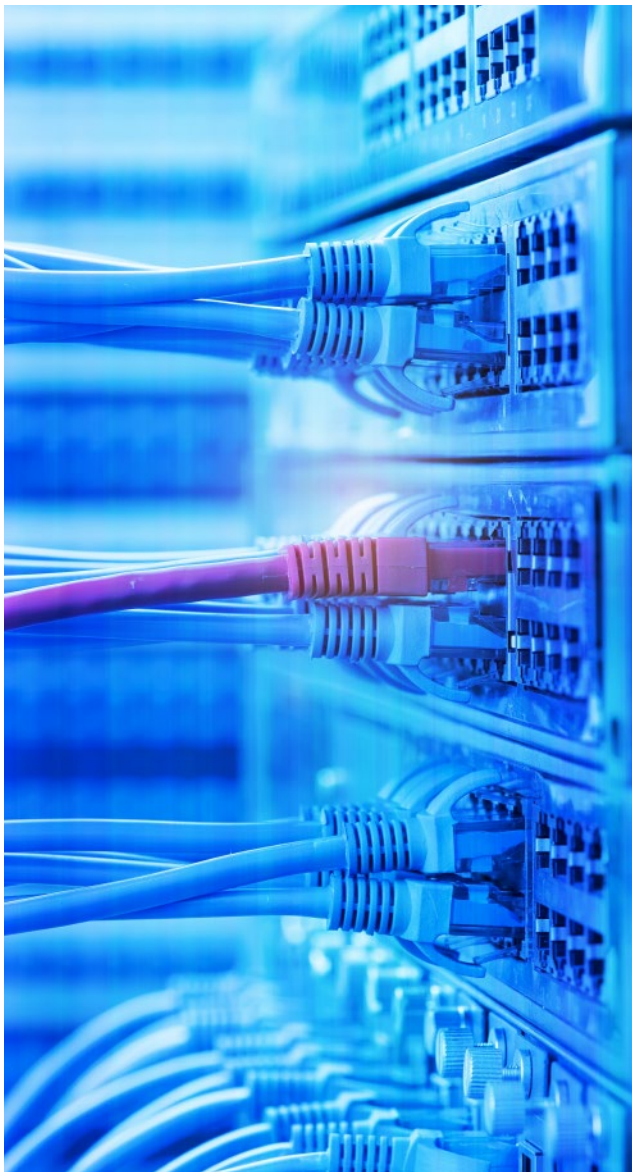
WIRTSCHAFTSRECHT I März 2018

EU-Datenschutz-Grundverordnung vom 27. April 2016

1. Ausgangslage



Im Zuge des digitalen Zeitalters kommt dem Schutz der Personendaten eine wichtige Bedeutung zu. Daten sind für die moderne Informations- und Kommunikationsgesellschaft von überragender Bedeutung. Das Sammeln und Nutzen von Daten bildet zwar seit jeher Bestandteil eines funktionierenden Staatswesens und einer modernen Wirtschaft, ist jedoch auch mit Gefahren, insbesondere für die einzelnen Bürger, verbunden. Gerade die sich in rasanter Geschwindigkeit entwickelnde IT hat diese Gefahren verschärft. Dem Staat kommt die Aufgabe zu, die Gesellschaft vor solchen Missbräuchen in der Datenbearbeitung zu schützen.[1] In den letzten Jahren haben zahlreiche Staaten ihre Datenschutzgesetzgebung angepasst und versucht, den Entwicklungen und Herausforderungen des modernen IT-Zeitalters zu begegnen.

In der Europäischen Union tritt am 25. Mai dieses Jahres die neue Datenschutz-Grundverordnung (DSGVO) in Kraft, und in der Schweiz liegt auf Bundesebene der Entwurf eines neuen Datenschutzgesetzes vor. Mit diesen Erlassen sollen die Rechte des Einzelnen verbessert werden. Für Gesellschaften mit Sitz in der Schweiz findet grundsätzlich das schweizerische Datenschutzrecht Anwendung. Allerdings gilt es auch die EU-Datenschutz-Grundverordnung zu beachten, da diese auch auf Unternehmen *ausserhalb* der EU anwendbar ist, wenn diese Personen mit Wohnsitz in der EU Waren oder Dienstleistungen anbieten oder eine Verhaltensüberwachung durchführen und in diesem Zusammenhang Daten von Personen mit Wohnsitz in der EU bearbeiten. Zahlreiche Schweizer Unternehmen sind somit von der Verordnung betroffen und müssen die verschiedenen Anforderungen rechtlicher, organisatorischer und technischer Natur bis zu ihrem Inkrafttreten im kommenden Mai unternehmensintern umsetzen.

[1] BELSER/EPINEY/WALDMANN, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, S. 1 ff.

Im Vergleich zum geltenden Schweizer Datenschutzgesetz (DSG) werden mit der europäischen DSGVO verschiedene wichtige und teilweise strenge Neuerungen eingeführt. Die nachfolgenden Ausführungen sollen dazu einen Überblick geben; zudem wird kurz auf den aktuellen Entwurf des Schweizer Datenschutzgesetzes eingegangen.

2. Kerngehalt der Regelungen der DSGVO

2.1 Anwendungsbereich

Die Verordnung entfaltet eine extraterritoriale Wirkung, d.h. der Anwendungsbereich der Verordnung wird auf Unternehmen mit Sitz ausserhalb der Europäischen Union ausgeweitet: Gemäss Art. 3 Abs. 2 DSGVO ist die Verordnung auf Datenverarbeitungen anwendbar, wenn das betreffende Unternehmen zwar über keine Niederlassung in der EU verfügt, seine Waren und Dienstleistungen aber in der EU bzw. Personen mit Wohnsitz in der EU anbietet oder alternativ das Verhalten von Personen in der EU beobachtet.

Was unter «Anbieten von Waren und Dienstleistungen» zu verstehen ist, wird in der DSGVO nicht näher definiert. Massgeblich ist stets der tatsächliche Inhalt eines Angebots im Einzelfall. Wesentlich ist die Ausrichtung auf den (Endkunden-) Markt in der EU. Erforderlich ist somit ein grenzüberschreitendes Element.[2] Bietet ein Schweizer Unternehmen etwa Personen in der EU die Möglichkeit, Waren oder Dienstleistungen über seine Website oder App zu bestellen, so dürfte der Anwendungsbereich der DSGVO erfüllt sein. **Das blosse Betreiben einer Website, die auch von Personen in der EU abgerufen werden kann, reicht hingegen grundsätzlich nicht.**[3] Im Übrigen ist es unerheblich, ob die konkreten Waren oder Dienstleistungen entgeltlich angeboten werden. Auch das kostenlose Angebot ist ausdrücklich von der Bestimmung erfasst. Ob ein Unternehmen unter den Anwendungsbereich fällt, ist letztlich aufgrund der konkreten Geschäftstätigkeit unter Berücksichtigung der spezifischen Umstände zu beurteilen. Aufgrund der zum Teil weitreichenden Folgen der Unterstellung unter die Verordnung, insbesondere in organisatorischer Hinsicht, ist es empfehlenswert, eine genaue Prüfung vorzunehmen.

Die zweite Variante der sog. «Verhaltensbeobachtung» zielt auf Unternehmen ausserhalb der EU, die zwar keine Waren oder Dienstleistungen anbieten, jedoch personenbezogene Daten erheben, um über die Aktivität von Personen in der EU namentlich zu Marketingzwecken im Internet Profile betreffend persönliche Vorlieben oder Verhaltensweise zu erstellen. Damit sollen insbesondere Betreiber von sozialen Netzwerken im Internet erfasst werden.[4]

Schliesslich findet die Verordnung gegebenenfalls auch Anwendung auf Schweizer Unternehmungen, die personenbezogene Daten von Personen in der EU bearbeiten, sei dies im Auftrag eines Unternehmens mit Sitz in der EU oder wenn sie Daten von Auftragsverarbeitern in der EU bearbeiten lassen, beispielsweise durch einen EU-Cloud-Anbieter.[5]

2.2 Einwilligung

Nach den allgemeinen Grundsätzen des Datenschutzrechts dürfen Personendaten nur rechtmässig bearbeitet werden. Eine unrechtmässige Bearbeitung stellt ohne Weiteres eine widerrechtliche Verletzung der Persönlichkeit dar.[6] Rechtmässig ist eine Datenbearbeitung insbesondere, wenn die betroffene Person in die Bearbeitung ihrer Daten eingewilligt hat (Art. 6 Abs. 1 lit. a DSGVO). Die DSGVO setzt in Art. 7 neu teilweise strenge formelle und inhaltliche Anforderungen an eine wirksame Einwilligung.

Eine gültige Einwilligung unterliegt gem. Art. 7 DSGVO (Art. 4 Ziff. 11 und Erw. 40 ff.) folgenden Voraussetzungen.[7]

- Die Einwilligung muss *freiwillig,* das heisst in Abwesenheit von Zwang erteilt werden. Es gilt zudem das *Kopplungsverbot.* Die Einwilligung darf namentlich nicht von der Erfüllung eines Vertrags abhängig gemacht werden.
- Die Einwilligung muss durch eine *ausdrückliche,* aktive Handlung erfolgen. Der Nachweis, dass die betroffene Person in die Verarbeitung eingewilligt hat, obliegt dabei dem Verarbeiter bzw. Unternehmen. In der Praxis führt dies zu einer umfassenden Dokumentationsobliegenheit.
- Die Einwilligungserklärung muss gut sicht- und lesbar *getrennt* von den anderen Themen dargestellt werden.
- Die Einwilligung muss inhaltlich genügend *bestimmt* sein. Es muss insbesondere klar erkennbar sein, zu welchen Zwecken die Datenverarbeitung erlaubt wird.
- Sie ist in einer einfachen und klaren Sprache zu formulieren und an *keine Bedingungen* zu knüpfen.
- Die Einwilligung hat *zeitlich vor der Datenbearbeitung* zu erfolgen. Eine nachträgliche Erklärung ist nicht zulässig.
- Hinsichtlich der Form macht die DSGVO keine Vorgaben. Da der Nachweis des Vorliegens einer gültigen Einwilligung dem Verarbeiter obliegt, empfiehlt es sich, die Einwilligung durch Textform nachweisbar zu gestalten.

---

[2] ENNÖCKL, Handkommentar Europäische Datenschutzgrundverordnung, Baden-Baden 2017, N 13 zu Art. 3.

[3] Erw. 23 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016, ABl. L 119/1 vom 4. Mai 2016.

[4] Erw. 24 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016, ABl. L 119/1 vom 4. Mai 2016; ENNÖCKL, Handkommentar Europäische Datenschutzgrundverordnung, Baden-Baden 2017, N 15 zu Art. 3.

[5] Diese Frage ist indes umstritten und zurzeit Gegenstand von Diskussionen in der Schweiz, vgl. dazu VASELLA, Zum Anwendungsbereich der DSGVO, digma 2017, S. 220–222 m.w.H.

[6] BELSER/EPINEY/WALDMANN, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, S. 518 f.

[7] Vgl. dazu eingehend INGOLD, Handkommentar Europäische Datenschutzgrundverordnung, Baden-Baden 2017, N 14 ff. zu Art. 7.

Gemäss Art. 7 Abs. 3 DSGVO hat die betroffene Person sodann die Möglichkeit, ihre Einwilligung jederzeit zu widerrufen. Ein bestimmter Widerrufsgrund ist nicht erforderlich. Die Widerrufsmöglichkeit muss so einfach wie die Erteilung der Einwilligung sein. Erfüllt eine Einwilligung im Einzelfall nicht die Anforderungen gemäss DSGVO, ist der verordnungswidrige Erklärungsinhalt unverbindlich und die darauf gestützte Datenverarbeitung nicht legal (Art. 7 Abs. 2 Satz 2 DSGVO).

2.3 Informationspflicht

Art. 13 DSGVO sieht eine detaillierte und umfassende Informationspflicht des Datenverarbeiters gegenüber der betroffenen Person vor, soweit dieser personenbezogene Daten erhebt oder weiterverarbeitet. Der datenschutzrechtlichen Informationspflicht liegt der Grundsatz der Transparenz und Fairness zugrunde. Den betroffenen Personen soll ermöglicht werden, zu beurteilen, ob ihre Daten gesetzeskonform behandelt werden.[8]

Art. 13 DSGVO macht im Rahmen einer umfassenden Aufzählung *Vorgaben zum Informationsumfang*. Dieser betrifft im Wesentlichen Informationen zum Grundverhältnis, zur konkreten Datenverarbeitung und Informationen über die Rechte der betroffenen Personen. So hat der Datenverarbeiter seine Kontaktdaten, allenfalls die Kontaktdaten des Datenschutzbeauftragten bekanntzugeben. Weiter bedarf es insbesondere der Angabe des Zwecks, für die die personenbezogenen Daten verarbeitet werden sollen und die Dauer der Datenaufbewahrung (zumindest jedoch Kriterien für deren Festlegung). Ferner erstreckt sich der Umfang der Informationspflicht auf Informationen zu Übertragungsverhältnissen, beispielsweise die Angabe, ob die Daten in ein Drittland oder an eine internationale Organisation übermittelt werden. Sodann umfasst die Informationspflicht bestimmte Vorgaben zu Hinweisen auf die Rechte der betroffenen Personen. So ist gem. Art. 13 Abs. 2 lit. b DSGVO namentlich auf das Auskunftsrecht (Art. 15 DSGVO), Rechte zur Berichtigung und Löschung (Art. 16 und 17 DSGVO), zur Einschränkung der Verarbeitung (Art. 18 DSGVO), das Widerspruchsrecht und das Recht auf Datenportabilität (Art. 20 DSGVO) hinzuweisen.

Die Informationspflicht ist an keine Formvorschrift gebunden. In zeitlicher Hinsicht ist dem Wortlaut der Bestimmung zu entnehmen, dass die entsprechenden Informationen «zum Zeitpunkt der Erhebung» mitgeteilt werden müssen. Dieser Zeitpunkt fällt in der Regel mit der Einwilligungserklärung der betroffenen Person zusammen, da eine gültige Einwilligung eine genügende Informiertheit der betroffenen Person voraussetzt.[9]

2.4 Recht auf Löschung («Recht auf Vergessenwerden»)

Artikel 17 Abs. 1 DSGVO statuiert das sogenannte Recht auf Vergessenwerden, das heisst das Recht der betroffenen Person zur Löschung der sie betreffenden personenbezogenen Daten. Der Anspruch auf Löschung besteht, wenn die verarbeiteten personenbezogenen Daten für die Zweckerreichung nicht mehr notwendig sind, die betroffene Person ihre Einwilligung zur Datenverarbeitung widerrufen hat, sie Widerspruch gegen die Verarbeitung einlegt und keine vorrangig berechtigten Gründe für die Verarbeitung vorliegen, eine Rechtspflicht zur Löschung besteht oder die Datenverarbeitung unrechtmässig erfolgt ist.

Der Datenverarbeiter ist verpflichtet, die betreffenden personenbezogenen Daten zu löschen. Die DSGVO regelt die Modalitäten für die Ausübung des Löschungsrechts nicht ausdrücklich. Das Löschungsrecht ist auf Antrag der betroffenen Person geltend zu machen, wobei neben der Schriftform auch die elektronische oder mündliche Form zulässig sind. Gemäss Art. 12 Abs. 2 und 3 DSGVO hat der Datenverarbeiter der betroffenen Person die Ausübung ihres Löschungsrechts zu erleichtern und sie spätestens innert einem Monat ab Antragseingang über die auf ihren Löschungsantrag hin unternommenen Massnahmen zu informieren.[10]

Das Recht auf Löschung ist kein absolutes Recht. Es besteht nur bei einer unrechtmässigen Datenverarbeitung. Art. 17 Abs. 3 DSGVO sieht eigene Ausnahmetatbestände vor, die einem Löschungsbegehren der betroffenen Person im Einzelfall entgegenstehen. Eine Löschung ist insbesondere ausgeschlossen, wenn die Datenverarbeitung zur Ausübung des Rechts auf freie Meinungsäusserung und Information erforderlich und deshalb rechtmässig ist, eine Rechtspflicht zur Datenverarbeitung besteht, die Verarbeitung in Wahrnehmung einer Aufgabe im öffentlichen Interesse oder im Bereich öffentliche Gesundheit erfolgt oder wenn die betreffenden personenbezogenen Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen durch den Datenverarbeiter oder Betroffenen erforderlich sind.[11]

2.5 Recht auf Datenübertragbarkeit

Art. 20 DSGVO gewährt der betroffenen Person einen Anspruch darauf, die sie betreffenden personenbezogenen Daten, welche sie zuvor einem Datenverarbeiter bereitgestellt hat, in einem strukturieren, gängigen und maschinenlesbaren Format zu erhalten und ohne Behinderung an Dritte zu übermitteln. Dieses Recht umfasst auch den Anspruch, dass die

[8] Vgl. Erw. 60 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016, ABl. L 119/1 vom 4. Mai 2016.
[9] INGOLD, Handkommentar Europäische Datenschutzgrundverordnung, Baden-Baden 2017, N 12 ff. zu Art. 13.
[10] PEUKER, Handkommentar Europäische Datenschutzgrundverordnung, Baden-Baden 2017, N 10 ff. zu Art. 17.
[11] Vgl. dazu eingehend PEUKER, Handkommentar Europäische Datenschutzgrundverordnung, Baden-Baden 2017, N 57 ff. zu Art. 17.

Daten direkt von einem Datenverarbeiter an einen anderen Datenverarbeiter übermittelt werden. Die Norm soll namentlich Anbieterwechsel beispielsweise bei sozialen Netzwerken oder Kreditkarten erleichtern und betont ganz grundsätzlich, dass Personendaten der betreffenden Person und nicht dem Datenverarbeiter gehören.[12]

3. Organisatorisches und Technisches

3.1 Vertreter in der EU

Art. 27 Abs. 1 DSGVO sieht vor, dass Datenverarbeiter, die gemäss Art. 3 Abs. 2 DSGVO vom Anwendungsbereich der Verordnung erfasst werden, das heisst insbesondere über keine Niederlassung in der EU verfügen, im Unionsgebiet obligatorisch einen Vertreter zu benennen haben. Dazu gibt es zwei Ausnahmen: *Erstens* sind Behörden oder öffentliche Stellen ausländischer Staaten oder internationale Organisationen nicht von der Pflicht zur Bestellung eines Vertreters erfasst. *Zweitens* entfällt die Pflicht zur Vertreterbestellung, wenn die Verarbeitung nur gelegentlich erfolgt, nicht in grösserem Umfang besonders schützenswerte Daten betroffen sind und durch die Datenverarbeitung voraussichtlich kein Risiko für die Rechte und Freiheiten natürlicher Personen birgt.

Persönliche Anforderungen im Sinne einer Qualifikation der Vertreter werden nicht gestellt. In räumlicher Hinsicht muss der Vertreter zwingend in einem Mitgliedstaat mindestens einer betroffenen Person seine Niederlassung haben. Die Bestellung erfolgt einseitig und vorzugsweise durch eine schriftliche Erklärung.[13] Gemäss Art. 27 Abs. 4 DSGVO kommt dem Vertreter die Funktion einer Anlaufstelle für Aufsichtsbehörden und betroffenen Personen bei sämtlichen Fragen im Zusammenhang mit der Datenverarbeitung zu. Im Aussenverhältnis bleibt die Verantwortlichkeit des Datenverarbeiters durch die Vertreterbestellung unberührt. Für die Einhaltung der DSGVO bleibt somit stets der Datenverarbeiter in der Schweiz verantwortlich.[14]

3.2 Datenschutzbeauftragter

Art. 37 Abs. 1 DSGVO sieht für gewisse (abschliessende) Fallgruppen von Datenverarbeitungen die Pflicht zur Benennung eines Datenschutzbeauftragten vor. Von dieser Pflicht ist zunächst *der gesamte öffentliche Sektor* mit Ausnahme der Gerichte erfasst.

Daneben stellt die Verordnung auf *spezifische Arten der Verarbeitung* personenbezogener Daten ab. Ein Datenschutzbeauftragter ist zu benennen, wenn die Kerntätigkeit des Datenverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs sowie ihrer Zwecke eine umfangreiche regelmässige und systematische Überwachung von betroffenen Personen erforderlich machen. Weiter sind Datenverarbeiter von der Pflicht zur Benennung erfasst, wenn deren Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäss Art. 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäss Art. 10 besteht.

Der Datenschutzbeauftragte ist aufgrund seiner beruflichen Qualifikationen und seines Fachwissens benannt. Er kann ein Beschäftigter des Datenverarbeiters oder ein Auftragsverarbeiter sein. Art. 39 Abs. 1 DSGVO verankert den wesentlichen Aufgabenbereich des Datenschutzbeauftragten. Dieser umfasst insbesondere die Unterrichtung und Beratung des Unternehmens im Zusammenhang mit Fragen des Datenschutzrechts, die Überwachung der Einhaltung der Verordnung und anderer Datenschutzvorschriften. Er hat zudem mit den zuständigen Aufsichtsbehörden zusammenzuarbeiten und dient diesen als Anlaufstelle für sämtliche mit der Verarbeitung zusammenhängenden Fragen. Der Datenverarbeiter hat die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen und der Aufsichtsbehörde mitzuteilen.[15]

3.3 Verzeichnis von Verarbeitungstätigkeiten

Art. 30 DSGVO sieht als wesentliches Element zur Kontrolle von Datenverarbeitungen eine Dokumentationspflicht zur Führung von Verarbeitungsverzeichnissen vor. Diese Pflicht trifft sowohl die Datenverarbeiter als auch allfällige Auftragsverarbeiter. Gemäss Abs. 5 sind von dieser Dokumentationspflicht jedoch jene Unternehmen ausgenommen, welche *weniger als 250 Mitarbeiter* beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nur gelegentlich erfolgt und wenn die Verarbeitung nicht besondere Datenkategorien gemäss Art. 9 DSGVO betrifft bzw. nicht personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 DSGVO einschliesst.

Hinsichtlich der Dokumentationsweise schreibt Abs. 3 vor, dass die jeweiligen Verzeichnisse schriftlich oder elektronisch zu führen sind. Die Vorgaben zum Umfang bzw. Inhalt der Dokumentation unterscheidet sich danach, ob es sich um ein Verzeichnis des Datenverarbeiters oder des Auftragsverarbeiters handelt. Die einzelnen im Verzeichnis aufzuführenden Angaben sind abschliessend in Abs. 1 und 2 aufgelistet und

[12] Die Bestimmung kann aber bspw. auch im Banken- und Versicherungsbereich und ganz allgemein bei Verbraucherverträgen von Bedeutung sein, vgl. SYDOW, Handkommentar Europäische Datenschutzgrundverordnung, Baden-Baden 2017, N 13 u. 21 zu Art. 20.

[13] INGOLD, Handkommentar Europäische Datenschutzgrundverordnung, Baden-Baden 2017, N 7 f. zu Art. 27.

[14] INGOLD, Handkommentar Europäische Datenschutzgrundverordnung, Baden-Baden 2017, N 12 zu Art. 27; vgl. auch Art. 27 Abs. 5 DSGVO.

[15] Zum Ganzen vgl. HELFRICH, Handkommentar Europäische Datenschutzgrundverordnung, Baden-Baden 2017, N 111 ff. zu Art. 37.

umfassen unter anderem Namen und Kontaktdaten des Datenverarbeiters, die Zwecke der Verarbeitung, die Beschreibung der Kategorien betroffener Personen und personenbezogenen Daten und gegebenenfalls Übermittlungen von Daten an ein Drittland. Das Verzeichnis ist gem. Abs. 4 auf Anfrage den zuständigen Aufsichtsbehörden zur Verfügung zu stellen.

3.4 Datenschutz-Folgenabschätzung

Für gewisse Formen von Datenverarbeitungen schreibt Art. 35 DSGVO vor, dass der Datenverarbeiter eine sogenannte Datenschutz-Folgenabschätzung durchzuführen hat. Diese dient dazu, im Fall eines voraussichtlich hohen Risikos für die Rechte und Freiheiten natürlicher Personen das datenschutzrechtliche Risiko zu erkennen und eingehender zu bewerten sowie vorbeugende Massnahmen zu treffen. Die Verpflichtung zur Vornahme einer Folgenabschätzung besteht gemäss Art. 35 Abs. 1 DSGVO, wenn die Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung ein hohes Risiko für die Rechte und Freiheit natürlicher Personen zur Folge hat. Diese Pflicht kann beispielsweise bei der Einführung neuer Technologien entstehen.

Die Verordnung umschreibt drei Regelfälle, bei deren Vorliegen von einem hohen Risiko für die Datenschutzrechte von Personen auszugehen ist und deshalb eine Datenschutz-Folgenabschätzung zwingend erforderlich machen (vgl. Art. 35 Abs. 1 DSGVO): *Erstens* im Fall einer systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen, die auf automatisierte Verarbeitung einschliesslich Profiling gründet. Als typischer Beispielsfall wird etwa die Ablehnung eines Kreditvertrags aufgrund eines vorangehenden Scorings genannt.[16] *Zweitens* ist eine Folgeabschätzung auch erforderlich, wenn eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäss Art. 9 Abs. 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäss Art. 10 erfolgt. *Drittens* ist eine Folgenabschätzung zwingend erforderlich im Fall einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche. Aus dem Merkmal «systematisch umfangreich» ergibt sich, dass einzelne oder temporäre Überwachungsmassnahmen keine Pflicht zur Folgeabschätzung auslösen. Erforderlich ist vielmehr ein eigentliches Überwachungssystem wie etwa bei einer weiträumigen Überwachung öffentlicher Bereiche.[17]

Hinsichtlich der Ausgestaltung bzw. des Inhalts der Folgeabschätzung schreibt Art. 35 Abs. 7 DSGVO einen Mindestinhalt vor. Danach muss die Folgeabschätzung zumindest was folgt beinhalten: (i) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung; (ii) eine Bewertung der Notwendigkeit und Verhältnismässigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck und (iii) die zur Bewältigung der Risiken geplanten Abhilfemassnahmen wie beispielsweise Sicherheitsvorkehrungen.[18]

3.5 Meldung von Datenschutzpannen

Gemäss Art. 33 Abs. 1 DSGVO sind Datenverarbeiter im Fall einer Verletzung des Schutzes personenbezogener Daten verpflichtet, dies unverzüglich und möglichst binnen 72 Stunden nach Kenntnis der Verletzung der zuständigen Aufsichtsbehörde zu melden. Birgt die Verletzung voraussichtlich ein hohes Risiko, ist auch die betroffene Person selber unverzüglich zu benachrichtigen. Als Verletzung des Schutzes personenbezogener Daten gilt gemäss Art. 4 Ziff. 12 DSGVO eine Verletzung der Sicherheit, die – unbeabsichtigt oder unrechtmässig – zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung bzw. unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Eine Ausnahme der Meldepflicht besteht einzig für den Fall, dass die Verletzung voraussichtlich kein Risiko für die Rechte und Freiheiten natürlicher Personen darstellt. Auch diesbezüglich gibt es in der Verordnung Vorschriften über den Mindestinhalt der Meldung (vgl. Art. 33 Abs. 3 DSGVO).

4. Sanktionen

Die Verordnung gewährt den Aufsichtsbehörden eine grosse Bandbreite an Sanktionsinstrumenten. Bei Verstössen gegen die Verordnung kann gegen das betreffende Unternehmen unter Umständen eine Busse in der Höhe von EUR 20 Millionen oder vier Prozent des gesamten weltweit erzielten Jahresumsatzes verhängt werden (Art. 83 DSGVO). Hinzu kommen gegebenenfalls Schadenersatzansprüche von Personen, welchen durch den Verstoss gegen die Verordnung ein Schaden erwachsen ist.[19] Fraglich ist jedoch, ob solche Sanktionen gegen Unternehmen in der Schweiz direkt durchgesetzt werden können.

5. Novellierung des Schweizer Datenschutzgesetzes

Auch in der Schweiz sind gesetzgeberische Bestrebungen zur Revision der Datenschutzgesetzgebung im Gang. Am 15. September 2017 hat der Bundesrat den Entwurf für ein totalrevidiertes Datenschutzgesetz (DSG) veröffentlicht. Die

[16] SASSENBERG/SCHWENDEMANN, Handkommentar Europäische Datenschutzgrundverordnung, Baden-Baden 2017, N 12 zu Art. 35.
[17] SASSENBERG/SCHWENDEMANN, Handkommentar Europäische Datenschutzgrundverordnung, Baden-Baden 2017, N 15 zu Art. 35.
[18] Vgl. WIDMER, Datenschutz-Folgenabschätzung, digma 2017 224–231, 223.
[19] Vgl. zum Ganzen POPP, Handkommentar Europäische Datenschutzgrundverordnung, Baden-Baden 2017, N 1 zu Art. 83; vgl. ferner OBERLIN/BOSSARDT, Datenschutz-Compliance: Die Anforderungen der EU-DSGVO und des VE-DSG der Schweiz, CB 2017 245–249, 247.

Stossrichtung ist zwar dieselbe wie jene der DSGVO. Zahlreiche Regelungskomplexe sollen in das Schweizer Recht übernommen werden. In gewissen Bereichen geht das revidierte DSG jedoch weniger weit, insbesondere in Bezug auf die vorgesehenen Sanktionen. Wann das neue Datenschutzgesetz in Kraft treten wird, ist nicht mit Bestimmtheit zu sagen. Als frühester Zeitpunkt wird Herbst 2018 genannt. Die Staatspolitische Kommission des Nationalrats kündigte am 12. Januar 2018 an, dass sie die Revision des DSG in zwei Teilen behandeln will. In einem ersten Schritt soll aufgrund der zeitlichen Dringlichkeit die aufgrund der Schengen-Verträge notwendige Umsetzung von EU-Recht vorab beraten werden. Anschliessend solle die Totalrevision des DSG ohne Zeitdruck angegangen werden.[20] Es bleibt offen, welche Verzögerungen sich daraus ergeben und welchen Inhalt das total revidierte DSG dereinst aufweisen wird. Klar ist aber, dass das Schweizer DSG auf alle Schweizer Unternehmen anwendbar ist und zwar unabhängig, ob deren Geschäftstätigkeit einen Bezug zu Personen in der EU aufweisen wird oder nicht.

6. Fazit

Die EU-Datenschutz-Grundverordnung wird am 25. Mai 2018 in Kraft treten. Aufgrund ihrer extraterritorialen Wirkung sollten Schweizer Unternehmen eingehend prüfen, ob und inwiefern sie in den Anwendungsbereich der Verordnung fallen. Findet die Verordnung auf sie Anwendung, sind die erforderlichen Massnahmen rechtlicher, organisatorischer und technischer Natur im Unternehmen umzusetzen. Soweit dies bisher noch nicht geschehen ist, empfiehlt es sich, die entsprechenden Arbeiten nun rasch an die Hand zu nehmen.

VOSER RECHTSANWÄLTE

MLaw Matthias Neumann

[20] Medienmitteilung des Staatspolitischen Kommission des Nationalrates vom 12. Januar 2018 betreffend die Revision des Datenschutzrechtes.