RUOSS VOGELE

Risikobasierte Umsetzung der DSGVO durch Schweizer Unternehmen

Bulletin 3/2018

Zürich, Mai 2018

Management Summary

Zahlreiche Schweizer Unternehmen fallen unter den Anwendungsbereich der EU Datenschutz-Grundverordnung („DSGVO“). Diese Unternehmen sollten die neuen datenschutzrechtlichen Anforderungen risikobasiert umsetzen. Sie sollten das Risiko von Rechtsverletzungen durch geeignete Massnahmen möglichst reduzieren und dabei berücksichtigen, unter welchen Voraussetzungen und in welchem Verfahren im Verletzungsfall Geldbussen ausgefällt würden oder Schadenersatz zugesprochen würde und unter welchen Umständen im Verletzungsfall ein Reputationsschaden entstehen würde.

Dr. Alois Rimle
Rechtsanwalt, LL.M.

Inhalt

Neue Pflichten nach der DSGVO

DSGVO und Umsetzungserlasse

Die neue EU Datenschutz-Grundverordnung bzw. EU General Data Protection Regulation von 2016 („DSGVO") tritt im Mai 2018 in Kraft. Sie ist direkt anwendbar und ersetzt die EU-Datenschutzrichtlinie 95/46/EG. Die DSGVO wird durch Umsetzungserlasse der einzelnen EU/EWR-Mitgliedstaaten ergänzt, die sowohl präzisierende als auch ergänzende Normen enthalten. Dies gilt beispielsweise für das revidierte deutsche Bundesdatenschutzgesetz von 2017, („BDSG").

Weitergehende Pflichten nach der DSGVO

Die DSGVO kann auch auf Schweizer Unternehmen, die personenbezogene Daten aus dem EU/EWR-Raum verarbeiten, zur Anwendung kommen (siehe hinten). Die DSGVO enthält verschiedene neue Pflichten, die über die Anforderungen des gegenwärtigen Datenschutzgesetzes der Schweiz hinausgehen. Schweizer Unternehmen, soweit sie von der DSGVO betroffen sind, müssen insbesondere folgende neuen Pflichten beachten:

- *Pflichtinformationen:* Die Datenerhebung muss nicht mehr nur transparent erfolgen. Es sind neu verschiedene Pflichtinformationen mitzuteilen (Art. 13 und 14).
- *Einwilligung:* Einwilligungen müssen separat eingeholt werden und einen Hinweis auf die jederzeitige Widerrufbarkeit enthalten (Art. 7). Angaben in den AGB sind nicht ausreichend. Bei Kindern gelten besondere Vorschriften (Art. 8).
- *EU-Vertreter:* Ein Unternehmen ohne Niederlassung im EU/EWR-Raum muss einen Vertreter ernennen, es sei denn, die Verarbeitung erfolgt nur gelegentlich und birgt keine besonderen Risiken für die Rechte und Freiheiten natürlicher Personen (Art. 27).
- *Verzeichnis:* Ein Unternehmen und gegebenenfalls sein Vertreter müssen ein Verzeichnis aller Verarbeitungstätigkeiten erstellen, die ihrer Zuständigkeit unterliegen (Art. 30).
- *Data Breach:* Ein Unternehmen muss sicherstellen, dass auftretende Verletzungen des Schutzes personenbezogener Daten der Aufsichtsbehörde gemeldet (Art. 33) und betroffene Personen bei einem hohen Risiko von Auswirkungen benachrichtigt werden (Art. 34).
- *Folgeabschätzung:* Ein Unternehmen muss bei einem voraussichtlich hohen Risiko für die Rechte und Freiheiten natürlicher Personen Datenschutz-Folgeabschätzungen erstellen (*Privacy Impact Assessments*) und dabei allenfalls die Aufsichtsbehörde konsultieren (Art. 35 und 36);
- *Datenschutzbeauftragter:* Ein Unternehmer und ein Auftragsverarbeiter müssen unter Umständen einen betrieblichen Datenschutzbeauftragten ernennen (Art. 37-39).
- *Privacy by Design:* Ein Unternehmen muss datenschutzrechtliche Massnahmen der Technikgestaltung (z.B. Pseudonymisierung) ergreifen (Art. 25).
- *Privacy by Default:* Ein Unternehmen muss für datenschutzrechtliche Voreinstellungen sorgen (Art. 25).
- *Datentransfer-Verträge:* Es bestehen neue Vorgaben für Verträge mit Auftragsverarbeitern (z.B. Vetorecht von Kunden betreffend Subunternehmern; keine Datenexporte ohne Weisung oder Zustimmung des Kunden) (Art. 28). Gemeinsam für die Verarbeitung Verantwortliche müssen durch Vereinbarung festlegen, wer für was verantwortlich ist (Art. 26). Die vertraglichen Standardklauseln betreffend Datentransfer ins unsichere Ausland sollen angepasst werden.
- *Automatisierte Einzelentscheide:* Bei automatisierten Einzelentscheiden mit gewichtigen Folgen besteht ein Recht auf menschliches Gehör (Art. 22).
- *Datenportabilität:* Service-Nutzer können die über sie erhobenen Daten in einem gängigen Format zur eigenen Verwendung erhalten (Art. 20).
- *Begehren betroffener Personen:* Hinsichtlich der Begehren von betroffenen Personen (Auskunft, Berichtigung, Löschung, Widerspruch) bestehen Neuerungen für Dokumente und Prozesse (Art. 12 ff.).
- *Datenspeicherung:* Personenbezogene Daten müssen frühzeitig pseudonymisiert und dann auch gelöscht oder anonymisiert werden (vgl. Art. 5 und 32).
- *Besondere Datenkategorien:* Besondere Kategorien von personenbezogenen Daten dürfen (wie bisher im EU/EWR-Raum) nicht verarbeitet werden, es sei denn, eine Verarbeitung ist nach der DSGVO ausnahmsweise zulässig (Art. 9).

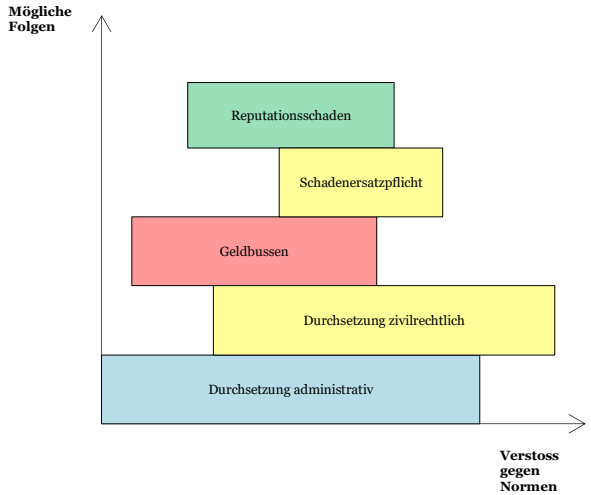
Verletzungsfolgen nach der DSGVO

Normen und Folgen von Normverstössen

Bei den Datenschutznormen der DSGVO handelt es sich um privatrechtliche, verwaltungsrechtliche und/oder strafrechtliche Normen. Es sind privatrechtliche Normen, soweit eine betroffene Person bei Normverstoss das Recht hat, Klage bei einem Zivilgericht einzureichen und eine Korrektur der Verarbeitung ihrer Daten und/oder Schadenersatz zu verlangen. Es sind verwaltungsrechtliche Normen, soweit eine Aufsichtsbehörde bei Normverstoss selbstständig oder auf Antrag eine Untersuchung einleiten und Handlungen oder Unterlassungen anordnen kann. Es sind schliesslich strafrechtliche Normen, soweit eine Aufsichtsbehörde oder ein Strafgericht bei Normverstoss eine Geldbusse oder eine Freiheits- oder Geldstrafe aussprechen kann.

Der Verstoss gegen eine Datenschutznorm der DSGVO kann nicht nur rechtliche Konsequenzen haben, sondern auch zu einem Reputationsschaden des Unternehmens führen, wenn ein Verfahren oder eine Sanktion öffentlich bekannt wird.

Der Verstoss gegen Normen der DSGVO und die mögliche Folgen können vereinfacht wie folgt dargestellt werden:



Geldbussen und Strafen

Im Rahmen der DSGVO können je nach Straftat folgende Geldbussen ausgesprochen werden: Geldbussen von bis zu 10‘000‘000 bzw. 20‘000‘000 Euro oder im Fall eines Unternehmens von bis zu 2% bzw. 4% seines gesamten weltweit erzielten Jahresumsatzes des vergangenen Geschäftsjahres, je nachdem, welcher der Beträge höher ist (Art. 83 Abs. 4 und 5 DSGVO). Neben den Geldbussen nach der DSGVO können die Mitgliedstaaten weitere strafrechtliche Sanktionen in ihren Umsetzungserlassen vorsehen. Beispielsweise sieht das deutsche BDSG Freiheits- und Geldstrafen für weitere strafrechtlich relevante Sachverhalte vor (§ 42 BDSG).

Das Verhängen von Geldbussen nach der DSGVO muss in jedem Einzelfall wirksam, verhältnismässig und abschreckend sein. Geldbussen können zusätzlich zu oder anstelle von verwaltungsrechtlichen Massnahmen verhängt werden. Bei der Entscheidung über die Verhängung einer Geldbusse und über den Bussbetrag müssen die verschiedenen Umstände des Einzelfalls berücksichtigt werden (Art. 83 Abs. 1 und 2 DSGVO).

Schadenersatzpflicht

Jede Person, die wegen eines Verstosses gegen die DSGVO einen materiellen oder immateriellen Schaden erleidet, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter und kann beim zuständigen Zivilgericht des betreffenden EU/EWR-Mitgliedstaats Klage einreichen (Art. 82 Abs. 1 und 6 DSGVO).

Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine verordnungswidrige Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seine speziell ihm auferlegten Pflichten verletzt oder Weisungen des Verantwortlichen missachtet hat (Art. 82 Abs. 2 DSGVO).

Administrative Durchsetzung

Jede Aufsichtsbehörde hat erforderliche Untersuchungsbefugnisse und Abhilfebefugnisse. Insbesondere kann sie einen Verantwortlichen oder einen Auftragsverarbeiter warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen die DSGVO verstossen. Sie kann einen Verantwortlichen oder einen Auftragsverarbeiter verwarnen, wenn dieser mit Verarbeitungsvorgängen gegen die DSGVO verstossen hat. Sie kann einen Verantwortlichen oder einen Auftragsverarbeiter unter Strafandrohung anweisen, seinen Pflichten nach der DSGVO zu entsprechen, personenbezogene Daten zu berichtigen oder zu löschen oder eine Datenverarbeitung zu beenden (Art. 58 Abs. 1 und 2 DSGVO). Jeder Mitgliedstaat kann durch Rechtsvorschriften zusätzliche

Befugnisse seiner Aufsichtsbehörde vorsehen (Art. 58 Abs. 6 DSGVO).

Zivilrechtliche Durchsetzung

Eine betroffene Person hat nach der DSGVO verschiedene Ansprüche gegenüber einem Unternehmen, das ihre Daten verarbeitet. Eine betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmässigkeit der aufgrund der Einwilligung bis zum Widerruf durchgeführten Verarbeitung nicht berührt (Art. 7 Abs. 3 DSGVO). Eine betroffene Person hat grundsätzlich das Recht, von dem Verantwortlichen Auskunft über die Verarbeitung sie betreffender Daten, die Berichtigung sie betreffender unrichtiger Daten, die Löschung sie betreffender Daten, die Einschränkung der Verarbeitung oder die Übertragung ihrer Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu verlangen (Art. 15 – 20 DSGVO).

Wenn das Unternehmen einem berechtigten Begehren nicht entspricht, kann die betroffene Person das zuständige Zivilgericht im betreffenden EU/EWR-Mitgliedstaat anrufen und den Anspruch zivilrechtlich durchsetzen.

Reputationsschaden

Wenn ein Verstoss gegen datenschutzrechtliche Vorschriften öffentlich bekannt wird, kann für das Unternehmen ein erheblicher Reputationsschaden resultieren. Das gilt auch im Fall der DSGVO. Unternehmen, die personenbezogene Daten verarbeiten, messen dem Reputationsschutz deshalb regelmässig erhebliche Bedeutung zu. Das UK Information Commissioner's Office (ico.) schreibt im Zusammemhang mit Big Data Folgendes: *„There is a trend amongst companies towards the development of what can be seen as an ethical approach to big data analytics, it is driven by commercial imperatives as much as regulatory requirements. It would harm a company's reputation if it were the subject of a media story about the misuse of personal data, while consumers can also publicise their views to the world instantly. This is an important consideration in a competitive world. There may well be a competitive advantage in being seen as a responsible and trustworthy custodian of customer data."* (ico., Big data and data protection, 2014, Version: 0.1, p. 46).

Verfahren nach der DSGVO

Verwaltungsrechtliches Verfahren

Zuständigkeit

Jeder EU/EWR-Mitgliedstaat sieht eine oder mehrere Aufsichtsbehörden vor, die für die Überwachung der Anwendung der DSGVO zuständig sind. Jede Aufsichtsbehörde ist für die Erfüllung der Aufgaben und die Ausübung der Befugnisse nach der DSGVO im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig (Art. 51 Abs. 1 und Art. 55 Abs. 1 DSGVO).

Die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen oder des Auftragsverarbeiters ist die federführende Aufsichtsbehörde für die von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführte grenzüberschreitende Verarbeitung. Dabei ist die federführende Aufsichtsbehörde der einzige Ansprechpartner der Verantwortlichen oder der Auftragsverarbeiter für Fragen der vom Verantwortlichen oder vom Auftragsverarbeiter durchgeführten grenzüberschreitenden Verarbeitung (Art. 56 Abs. 1 und 6 DSGVO).

Jede Aufsichtsbehörde muss in ihrem Hoheitsgebiet die Anwendung der DSGVO überwachen und durchsetzen (Art. 57 Abs. 1 lit. a DSGVO). Dabei hat sie erforderliche Untersuchungsbefugnisse und Abhilfebefugnisse.

Administrative Durchsetzung

Jede betroffene Person hat das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmasslichen Verstosses, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstösst. Die betroffene Person kann sich dabei durch einen Interessenverband ohne Gewinnorientierung vertreten lassen. Die Mitgliedstaaten können vorsehen, dass ein Interessenverband auch ohne Auftrag selbstständig Beschwerde einreichen kann (Art. 77 Abs. 1, Art. 80 DSGVO).

Die federführende Aufsichtsbehörde arbeitet mit den anderen betroffenen Aufsichtsbehörden zusammen und bemüht sich, einen Konsens zu erzielen. Die Aufsichtsbehörden übermitteln einander massgebliche Informationen und gewähren einander Amtshilfe, um die DSGVO einheitlich durchzuführen und anzuwenden, und treffen Vorkehrungen für eine

wirksame Zusammenarbeit. Die Aufsichtsbehörden führen gegebenenfalls gemeinsame Massnahmen durch. Um zur einheitlichen Anwendung der DSGVO im gesamten EU/EWR-Raum beizutragen, arbeiten die Aufsichtsbehörden im Rahmen eines Kohärenzverfahrens untereinander und gegebenenfalls mit der Kommission zusammen. Um die ordnungsgemässe und einheitliche Anwendung der DSGVO in Einzelfällen sicherzustellen, erlässt der Europäische Datenschutzausschuss in bestimmten Fällen einen verbindlichen Beschluss (Art. 56 Abs. 1, Art. 60 Abs. 1, Art. 61 Abs. 1, Art. 62 Abs. 1, Art. 63, Art. 65 Abs. 1 DSGVO).

Jede natürliche oder juristische Person hat das Recht auf einen wirksamen *gerichtlichen Rechtsbehelf* gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde. Für Verfahren gegen eine Aufsichtsbehörde sind die Gerichte des Mitgliedstaats zuständig, in dem die Aufsichtsbehörde ihren Sitz hat. Die betroffene Person kann sich dabei durch einen Interessenverband ohne Gewinnorientierung vertreten lassen. Die Mitgliedstaaten können vorsehen, dass ein Interessenverband auch ohne Auftrag selbstständig Klage einreichen kann (Art. 78 Abs. 1 und 3, Art. 80 DSGVO).

Grenzüberschreitende administrative Durchsetzung

Eine zuständige EU/EWR-Aufsichtsbehörde kann ein Verwaltungsverfahren auch gegen ein Unternehmen (als Verantwortlicher oder Auftragsverarbeiter) mit Sitz in der Schweiz eröffnen und durchführen. Wenn das Schweizer Unternehmen keine Niederlassung im EU/EWR-Raum hat, ist die Vollstreckung in der Schweiz allerdings fraglich. Der EDÖB kann bei einem solchen Verwaltungsverfahren im EU/EWR-Raum zwar grundsätzlich Amtshilfe leisten und erforderliche Informationen zur Verfügung stellen (Art. 49 E-DSG). Doch ist unklar, auf welcher gesetzlichen Grundlage administrative Verfügungen oder verwaltungsgerichtliche Entscheide in der Schweiz vollstreckt werden könnten.

Strafrechtliches Verfahren

Zuständigkeit

Die Aufsichtsbehörde in einem EU/EWR-Mitgliedstaat kann grundsätzlich auch Geldbussen nach Art. 83 DSGVO ausfällen (Art. 58 Abs. 1 lit. i DSGVO). Wenn die Rechtsordnung eines Mitgliedstaats keine Geldbussen vorsieht, kann Art. 83 DSGVO so angewandt werden, dass die Geldbusse von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird (Art. 83 Abs. 9 DSGVO). Beispielsweise sieht das revidierte deutsche BDSG vor, dass das Landgericht entscheidet, wenn die festgesetzte Geldbusse die Summe von 100‘000 Euro übersteigt (§ 41 Abs. 1 BDSG).

Verfahren

Wenn Geldbussen oder gar Freiheits- oder Geldstrafen ausgefällt werden, kommt grundsätzlich die Strafverfahrensordnung des jeweiligen EU/EWR-Mitgliedstaats zur Anwendung. Beispielsweise verweist das deutsche BDSG auf die Vorschriften des Gesetzes über Ordnungswidrigkeit und der allgemeinen Gesetze über das Strafverfahren, namentlich der Strafprozessordnung und des Gerichtsverfassungsgesetzes (§ 41 BDSG).

Grenzüberschreitendes Verfahren

Eine zuständige EU/EWR-Aufsichtsbehörde kann im Anwendungsbereich der DSGVO auch ein Strafverfahren gegen ein Schweizer Unternehmen eröffnen und durchführen. Wenn das Schweizer Unternehmen keine Niederlassung im EU/EWR-Raum hat, ist die Vollstreckung in der Schweiz allerdings nur beschränkt möglich. Insbesondere wäre eine entsprechende Strafbarkeit in der Schweiz erforderlich und bestünde eine Begrenzung im Höchstmass der entsprechenden Strafe in der Schweiz (Art. 94 Abs. 1 und 2 IRSG). Vorbehalten bleibt allenfalls eine Vollstreckung gegen den Vertreter des Schweizer Unternehmens im EU/EWR-Raum. Diesbezüglich besteht gegenwärtig noch Unklarheit.

Zivilrechtliches Verfahren

Zuständiges Zivilgericht

In jedem EU/EWR-Mitgliedstaat besteht ein zuständiges Zivilgericht, bei dem gegen einen Verantwortlichen oder einen Auftragsverarbeiter im Fall eines Verstosses gegen die DSGVO geklagt werden kann. Im Einzelfall sind die Gerichte des EU/EWR-Mitgliedstaats zuständig, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Klagen können wahlweise auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren Aufenthaltsort hat (Art. 79 Abs. 2 DSGVO).

Zivilrechtliches Verfahren

Jede betroffene Person hat das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen Verantwortlichen oder einen Auftragsverarbeiter, wenn

sie der Ansicht ist, dass die ihr aufgrund der DSGVO zustehenden Rechte infolge einer nicht im Einklang mit der DSGVO stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden. Die betroffene Person kann sich dabei durch einen Interessenverband ohne Gewinnorientierung vertreten lassen. Die Mitgliedstaaten können vorsehen, dass ein Interessenverband auch ohne Auftrag selbstständig Klage einreichen kann (Art. 79 Abs. 1, Art. 80 DSGVO).

Grenzüberschreitendes zivilrechtliches Verfahren

Es kann auch ein Schweizer Unternehmen vor einem Zivilgericht im EU/EWR-Raum wegen einer verordnungswidrigen Verarbeitung personenbezogener Daten verklagt werden. Im Verhältnis zwischen der Schweiz und dem EU/EWR-Raum bestimmt sich die zivilrechtliche Zuständigkeit für Schadenersatzansprüche und andere zivilrechtliche Ansprüche nach dem LugÜ (Titel II des LugÜ). Dasselbe gilt für die Anerkennung und Vollstreckung von zivilrechtlichen Entscheidungen von EU/EWR-Gerichten in der Schweiz (Titel III des LugÜ).

Anwendungsbereich der DSGVO

Niederlassung im EU/EWR-Raum

Schweizer Unternehmen unterstehen räumlich der DSGVO, soweit sie im EU/EWR-Raum eine Niederlassung haben. Art. 3 Abs. 1 DSGVO enthält folgende Regelung zum räumlichen Anwendungsbereich: „*Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.*“

Es ergibt sich, dass jede Verarbeitung personenbezogener Daten durch ein Schweizer Unternehmen im Rahmen der Tätigkeiten einer Niederlassung im EU/EWR-Raum der DSGVO untersteht, gleichgültig, ob die Verarbeitung in oder ausserhalb des EU/EWR-Raums stattfindet. Es kommt allein darauf an, ob im Rahmen der Geschäftstätigkeit der EU/EWR-Niederlassung personenbezogene Daten verarbeitet werden.

Dabei setzt eine Niederlassung die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Auf die Rechtsform kommt es dabei nicht an. Es kann sich um eine Zweigniederlassung oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handeln (Einleitungsziffer 22 DSGVO).

Keine Niederlassung im EU/EWR-Raum

Schweizer Unternehmen können räumlich der DSGVO selbst dann unterstehen, wenn sie keine Niederlassung im EU/EWR-Raum haben. Art. 3 Abs. 2 DSGVO enthält folgende Regelung zum räumlichen Anwendungsbereich („*Marktortprinzip*“): „*Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht (a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist; (b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.*“

Es ergibt sich, dass für die Anwendung der DSGVO keine Niederlassung im EU/EWR-Raum erforderlich ist, wenn die Datenverarbeitung dazu dient, betroffenen natürlichen Personen, die sich im EU/EWR-Raum befinden, Waren oder Dienstleistungen anzubieten. Dabei kommt es darauf an, ob offensichtlich beabsichtigt ist, betroffenen Personen in einem oder mehreren EU/EWR-Mitgliedstaaten Waren oder Dienstleistungen anzubieten. Unternehmen mit Sitz ausserhalb des EU/EWR-Raums haben dieselben Regeln anzuwenden wie Unternehmen mit Sitz im EU/EWR-Raum. Auf diese Weise wird der Schutz der Rechte von Bürgern im EU/EWR-Raum sichergestellt und es werden gleiche Wettbewerbsbedingungen für Unternehmen im EU/EWR-Raum und Unternehmen ausserhalb des EU/EWR-Raums geschaffen (Zerdick, Art. 3 Rz 2).

Es ergibt sich weiter, dass die DSGVO auch ohne Niederlassung im EU/EWR-Raum zur Anwendung kommt, wenn die Verarbeitung der Daten von betroffenen natürlichen Personen, die sich im EU/EWR-Raum befinden, dazu dient, das Verhalten dieser betroffenen Personen zu beobachten, soweit ihr Verhalten im EU/EWR-Raum erfolgt. Ob eine relevante Verhaltensbeobachtung vorliegt, sollte daran festgemacht werden, ob ihre Internetaktivitäten nachvollzogen werden, inklusive der möglichen nachfolgenden Verwendung von Techniken zur Ver-

arbeitung personenbezogener Daten, durch die von einer natürlichen Person ein Profil erstellt wird, das insbesondere die Grundlage für sie betreffende Entscheidungen bildet oder anhand dessen ihre persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder prognostiziert werden sollen (Einleitungsziffer 24 DSGVO). Es fallen insbesondere jegliche Formen des Trackings (Beobachten, Sammeln, Auswerten des Surfverhaltens betroffener Personen im Internet) und das Profiling (Erstellen von Profilen von Kunden, Mitarbeitenden oder anderen, um bestimmte persönliche Aspekte wie Leistung, Gesundheit, Aufenthaltsorte etc. zu bewerten oder Vorhersagen zu treffen) im Internet durch Analyse-Tools, die wie beispielsweise Cookies die individuelle Rückverfolgbarkeit der Nutzer ermöglichen oder zum Zweck der individuellen Werbung (targeted advertising) erfolgen, unter die Bestimmung (Kurzpapier 7 der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz –DSK), Marktortprinzip: Regelungen für aussereuropäische Unternehmen, Stand: 26. Juli 2017; vgl. zu „Profiling“ auch Rosenthal, S. 9 ff.).

Grenzüberschreitende Auftragsverarbeitung

Wenn ein Schweizer Unternehmen als Verantwortlicher seine Daten von einem Auftragsverarbeiter im EU/EWR-Raum verarbeiten lässt (z.B. Could), ist die DSGVO direkt auf den Auftragsverarbeiter anwendbar. Es ist hingegen nicht klar, wie es sich mit dem verantwortlichen Schweizer Unternehmen verhält. Wenn es nicht der DSGVO unterliegt, muss es vertraglich in die Pflicht genommen werden. Die Rechtslage ist unklar.

Wenn ein Schweizer Unternehmen als Auftragsverarbeiter für ein Unternehmen im EU/EWR-Raum Dienstleistungen erbringt, ist die DSGVO direkt auf das verantwortliche Unternehmen anwendbar. Es ist aber nicht klar, wie es sich mit dem Schweizer Dienstleister verhält. Wenn er nicht der DSGVO unterstellt ist, muss er vertraglich verpflichtet werden. Die Rechtslage bedarf einer weiteren Klärung.

Anwendung auf Schweizer Unternehmen

Anwendung bestimmen

Ein Schweizer Unternehmen sollte zuerst bestimmen, ob die DSGVO überhaupt auf die eigene Datenverarbeitung zur Anwendung kommt. Ein Teil der Datenverarbeitung kann aufgrund einer Niederlassung im EU/EWR-Raum oder deshalb unter den Anwendungsbereich der DSGVO fallen, weil sich von der Datenverarbeitung betroffene Personen im EU/EWR-Raum aufhalten.

Gegebenenfalls gibt es für ein Schweizer Unternehmen unterschiedliche Möglichkeiten, wie die DSGVO umgesetzt werden kann. Es kann die DSGVO als universellen Standard im gesamten Konzern umsetzen. Dieser Ansatz erscheint angemessen, wenn in einem erheblichen Umfang Daten von natürlichen Personen verarbeitet werden, die sich im EU/EWR-Raum aufhalten (z.B. viele EU/EWR-Privatkunden). Es kann die DSGVO auch nur dort umsetzen, wo sie tatsächlich gilt. Dieser Ansatz dürfte verfolgt werden, wenn die DSGVO nur in marginalen Bereichen zur Anwendung kommt (z.B. lokale HR-Daten, Tracking von Benutzern auf eigener Webseite, Verarbeitung von Daten weniger EU/EWR-Privatkunden).

Ein Schweizer Unternehmen, das nicht unter den Anwendungsbereich der DSGVO fällt, kann sich entschliessen, die DSGVO freiwillig umzusetzen. Eine freiwillige Umsetzung wird vor allem dann zum Tragen kommen, wenn ein Schweizer Unternehmen zu einer international tätigen Gruppe gehört, welche den europäischen Datenschutzstandard gruppenweit implementieren will. Eine freiwillige Umsetzung kann aber auch dann sinnvoll sein, wenn in Zukunft eine Geschäftstätigkeit im EU/EWR-Raum geplant ist. Dabei kann berücksichtigt werden, dass in der Schweiz voraussichtlich 2019 ohnehin ein revidiertes Datenschutzgesetz mit vergleichbaren Pflichten in Kraft treten wird (wohl mit zweijähriger Übergangsfrist).

Anwendung spezifizieren

Die DSGVO enthält nicht alle datenschutzrechtlichen Normen, die auf eine Verarbeitung von Daten von natürlichen Personen im EU/EWR-Raum („EU/EWR-Daten“) durch ein Schweizer Unternehmen zur Anwendung kommen. Jeder EU/EWR-Mitgliedstaat erlässt zusätzlich einen Umsetzungser-

lass, der präzisierende und ergänzende Normen enthält. Ein betroffenes Schweizer Unternehmen, das geschäftlich im EU/EWR-Raum tätig ist, muss sowohl die Bestimmungen der DSGVO als auch jene des anwendbaren nationalen Umsetzungserlasses befolgen. Zudem muss es die Praxis der zuständigen Aufsichtsbehörde und der zuständigen Gerichte beachten.

Es ergibt sich, dass ein Schweizer Unternehmen anhand der Niederlassungen und der Aufenthaltsorte der von der eigenen Datenverarbeitung betroffenen Personen bestimmen muss, in welchen EU/EWR-Mitgliedstaaten die Umsetzungserlasse und die Praxis von Aufsichtsbehörden und Gerichten zu beachten sind. Erst dann ist es in der Lage, die DSGVO vollständig und angemessen über die Zeit umzusetzen. Wenn ein Schweizer Unternehmen zu einer international tätigen Gruppe gehört, die in der Schweiz und verschiedenen EU/EWR-Mitgliedstaaten geschäftlich tätig ist, kann es aus Effizienzgründen sinnvoll sein, europaweit einheitlich den höchsten Standard der Datenverarbeitung anzuwenden. Die Gruppe kann sich beispielsweise nach dem deutschen Umsetzungserlass und der deutschen Praxis richten und auf diese Weise grundsätzlich auch den zusätzlichen Anforderungen in den anderen EU/EWR-Mitgliedstaaten und der Schweiz entsprechen.

Anwendung zuordnen

Jede Verarbeitung von personenbezogenen Daten wird nach der DSGVO grundsätzlich einem Unternehmen rechtlich zugeordnet. Eine Gesellschaft oder eine Niederlassung wird im Rahmen der DSGVO als Verantwortliche oder Mitverantwortliche oder als Auftragsverarbeiterin einer Datenverarbeitung identifiziert. Auf diese Weise wird bestimmt, welche Gesellschaft oder Niederlassung für eine Datenverarbeitung verantwortlich ist und wer welche Pflichten erfüllen muss und wer im Verletzungsfall im Rahmen eines Zivil-, Verwaltungs- oder Strafverfahrens zur Rechenschaft gezogen werden kann.

Wenn ein Schweizer Unternehmen zu einer international tätigen Gruppe gehört, die auch im EU/EWR-Raum geschäftlich tätig ist, sollte gruppenintern klar sein, welche Datenverarbeitung zu welcher Geschäftstätigkeit und Gruppengesellschaft gehört und in welchem Umfang ein Auftragsverarbeiter in die Pflicht genommen wird. Andernfalls besteht die Möglichkeit, dass die Schweizer Gruppengesellschaft von einer Aufsichtsbehörde oder einem Gericht im EU/EWR-Raum für die gruppenweite Datenverarbeitung mitverantwortlich gemacht wird (vgl. Urteil des Europäischen Gerichtshofs vom 13. Mai 2014 in Sachen Google Spain SL und Google Inc.). Im Ergebnis sollte bei unklaren Verhältnissen in Kundenverträgen spezifiziert und teilweise nach aussen kommuniziert werden (z.B. auf der Webseite), welche Gruppengesellschaft bzw. Niederlassung für die Datenverarbeitung in welchem Mitgliedstaat verantwortlich ist. Zudem sollten die Pflichten von Auftragsverarbeitern vertraglich ausreichend spezifiziert werden. Auf diese Weise kann grundsätzlich gesteuert werden, gegen welche Gruppengesellschaft bzw. Niederlassung oder gegen welchen Dienstleister ein künftiges Zivil-, Verwaltungs- oder Strafverfahren gerichtet sein müsste und wer dafür die Verantwortung zu tragen hätte und haften würde.

Anwendung vermeiden

Schweizer Unternehmen können die Anwendung der DSGVO allgemein dadurch vermeiden, dass sie keine personenbezogenen Daten im EU/EWR-Raum (grenzüberschreitend oder über eine Niederlassung) zum Zweck der eigenen Geschäftstätigkeit erheben und verarbeiten.

Schweizer Unternehmen, die die Anwendung der DSGVO vermeiden wollen, sollten insbesondere sicherstellen, dass sich aus dem eigenen Internetauftritt keine Absicht erkennen lässt, betroffenen Personen in einem oder mehreren EU/EWR-Mitgliedstaaten Waren oder Dienstleistungen anzubieten. Die blosse Zugänglichkeit der Website des Verantwortlichen, des Auftragsverarbeiters oder eines Vermittlers im EU/EWR-Raum, einer E-Mail-Adresse oder anderer Kontaktdaten oder die Verwendung einer Sprache, die in dem Drittland, in dem der Verantwortliche niedergelassen ist, sind allgemein gebräuchlich und hierfür kein ausreichender Anhaltspunkt. Hingegen können andere Faktoren darauf hindeuten, dass der Verantwortliche beabsichtigt, den Personen im EU/EWR-Raum Waren oder Dienstleistungen anzubieten, wie etwa die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Waren und Dienstleistungen in dieser anderen Sprache zu bestellen, oder die Erwähnung von Kunden oder Nutzern, die sich im EU/EWR-Raum befinden (Einleitungsziffer 23 DSGVO).

Der rein zu Präsentationszwecken erfolgte Webauftritt eines Schweizer Unternehmens stellt keine rele-

vante Dienstleistung in diesem Sinne dar. Es ist auch nicht ausreichend, mittels einer Webseite die Dienste lediglich zugänglich zu machen (Pilz, Art. 3 Rz 28). Hingegen ist gegenwärtig noch unklar, ab wann die Beobachtung des Verhaltens von europäischen Besuchern der Webseite ein Tracking oder Profiling darstellt. Deshalb wird Schweizer Unternehmen, die eine Anwendung der DSGVO vermeiden wollen, zurzeit teilweise empfohlen, europäische Besucher im Sinne eines „dis-targetings" vom Tracking oder Profiling auszunehmen (vgl. Peter, S. 1 ff; Klar, Art. 3 Rz 101).

Reduktion des Verletzungsrisikos

Verletzungsrisiko

Wenn ein Schweizer Unternehmen gegen eine Norm der DSGVO verstösst, besteht das Risiko, dass es in Zukunft infolge des Normverstosses rechtliche Konsequenzen und allenfalls einen Reputationsschaden tragen muss. Es besteht für das Unternehmen ein Rechtsverletzungsrisiko und ein mit diesem zusammenhängendes Reputationsrisiko. Realisiert sich das Risiko, so entstehen dem Unternehmen oder seinen Organen und Angestellten auf die eine oder andere Weise Zusatzkosten. Insofern können sowohl das Rechtsverletzungsrisiko als auch das Reputationsrisiko ökonomisch als Risiko von Zusatzkosten verstanden werden. Einem Unternehmen entstehen beispielsweise Zusatzkosten, wenn ein Verfahren eröffnet wird, Geldbussen verhängt werden, Schadenersatz zugesprochen wird, eine Datenverarbeitung untersagt wird oder der Umsatz aufgrund eines öffentlich bekannt gewordenen Datenlecks zurückgeht.

Reduktion des Verletzungsrisikos

Ein betroffenes Schweizer Unternehmen sollte bei der Umsetzung der DSGVO versuchen, das Rechtsverletzungsrisiko und das Reputationsrisiko, d.h. das Risiko von Zusatzkosten als Folge eines Normverstosses möglichst zu reduzieren. Ein Unternehmen sollte die Normen der DSGVO im Hinblick darauf umsetzen, dass bei einem Normverstoss in Zukunft Geldbussen ausgefällt werden können, Schadenersatz zugesprochen werden kann und/oder ein Reputationsschaden entstehen kann. Bei einer risikobasierten Umsetzung der DSGVO muss berücksichtigt werden, nach welchen Kriterien und in welchem Verfahren und von welcher zuständigen Aufsichtsbehörde Geldbussen verhängt würden, von welchem zuständigen Gericht Schadenersatz zugesprochen würde und unter welchen Umständen ein Reputationsschaden eintreten würde, um auf diese Weise das entsprechende Risiko effektiv zu reduzieren und Zusatzkosten möglichst zu vermeiden (siehe RV Bulletin 6/2017 zu Reduktion von Rechts- und Reputationsrisiken durch antizipative Normumsetzung im Unternehmen, S. 10 und 13).

Bewusste Tragung des Verletzungsrisikos?

Ein betroffenes Schweizer Unternehmen kann sich entschliessen, die DSGVO (teilweise) nicht umzusetzen und das entsprechende Risiko von Zusatzkosten bewusst zu tragen. Ein solcher Ansatz macht bei einer langfristigen Betrachtung im Interesse des Unternehmens ökonomisch nur dann Sinn, wenn die anfallenden Kosten der Normumsetzung höher eingeschätzt werden als die möglichen künftigen Kosten aus einem Normverstoss während eines langen Zeithorizonts (Kosten als Produkt von Eintrittswahrscheinlichkeit und möglicher Kostenhöhe).

Das Kostenrisiko einer Nichtbeachtung der DSGVO ist m.E. selbst bei einem Schweizer Unternehmen, das über keine Niederlassung im EU/EWR-Raum verfügt, relativ hoch. Eine bewusste Risikotragung kann deshalb für gewöhnlich nicht in Betracht gezogen werden. Künftige Kosten einer Rechtsverletzung können erheblich sein (z.B. hohe Geldbussen). Zudem können Normverstösse von verschiedenen Anspruchsgruppen (d.h. Kunden, Interessenverbände, Behörden) noch während einer langen Zeit rückwirkend angezeigt bzw. verfolgt werden.

Nur ausnahmsweise mag eine bewusste Nichtumsetzung der DSGVO durch ein Schweizer Unternehmen, das über keine Niederlassung im EU/EWR-Raum verfügt, aus einer Risikoperspektive als vertretbar erscheinen. Dies kann m.E. dann der Fall sein, wenn das Unternehmen nur gelegentlich und unwesentlich EU/EWR-Daten verarbeitet und deshalb nach der DSGVO auch keine Pflicht besteht, einen Vertreter im EU/EWR-Raum zu ernennen (Art. 27 Abs. 2 lit. a DSGVO). In solchen Fällen erscheint es unwahrscheinlich, dass in Zukunft eine Aufsichtsbehörde im EU/EWR-Raum ein Verfahren gegen das Schweizer Unternehmen eröffnet oder dass eine betroffene Person bei einem Gericht im EU/EWR-Raum gegen das Schweizer Unternehmen eine Klage einreicht. Eine Beschränkung auf die Einhaltung der Pflichten nach dem Datenschutzgesetz in der

Schweiz (das in absehbarer Zeit revidiert wird) erscheint vertretbar.

Vermeidung von Geldbussen

Risiko von Geldbussen

Es besteht das Risiko, dass Geldbussen oder gar Freiheitsstrafen ausgesprochen werden, wenn Schweizer Unternehmen bzw. deren Organe oder Mitarbeitende mit Entscheidungsbefugnis gegen Normen der DSGVO oder eines Umsetzungserlasses verstossen. Allerdings kann eine Geldbusse nicht wegen jeder rechtswidrigen Datenverarbeitung, sondern nur dann verhängt werden, wenn folgende qualifizierende Voraussetzungen erfüllt sind:

- Es liegt ein klarer Verstoss gegen eine ausreichend bestimmte Datenschutznorm vor (Legalitätsprinzip).
- Der Verstoss gegen die Datenschutznorm ist systematisch, erfolgt wiederholt oder hat gravierende Auswirkungen. Er beruht auf fehlenden oder ungenügenden datenschutzrechtlichen Massnahmen (vgl. Art. 83 Abs. 2 lit. a, c, d, e, f, g, h, i und j DSGVO).

Eine rechtswidrige Datenverarbeitung kann grundsätzlich nur dann zu einer Geldbusse führen, wenn sie auf fehlenden oder offensichtlich unzureichenden Datenschutzmassnahmen seitens des Unternehmens beruht. Ein Unternehmen kann das Risiko von Geldbussen deshalb durch geeignete Massnahmen effektiv reduzieren. Geeignete Massnahmen zur Risikoreduktion können insbesondere darin bestehen, die Datenmenge zu reduzieren, eine risikoreiche Datenverarbeitung zusätzlich einzuschränken, die formellen Anforderungen zu erfüllen, getroffene Massnahmen bei Bedarf anzupassen und mit der zuständigen Aufsichtsbehörde zusammenzuarbeiten.

Datenmenge reduzieren

Je weniger personenbezogene Daten aus dem EU/EWR-Raum verarbeitet werden, desto kleiner ist die Wahrscheinlichkeit einer Geldbusse wegen eines Verstosses gegen die DSGVO. Schweizer Unternehmen sollten die Erhebung von personenbezogenen Daten im EU/EWR-Raum und deren Speicherung deshalb auf einen notwendigen Umfang reduzieren (Art. 5 Abs. 1 lit. c und e DSGVO).

Ein Schweizer Unternehmen kann die Datenmenge insbesondere durch folgende neu vorgeschriebene Massnahmen reduzieren:

- Privacy by Default: Datenerhebung einschränken;
- Privacy by Design: Systeme anpassen und Anonymisierung und Löschung von Daten.

Risikoreiche Datenverarbeitung anpassen

Datenverarbeitung ist nicht gleich Datenverarbeitung. Es gibt Datenverarbeitungen, die kaum zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen, und es gibt Datenverarbeitungen, die zu einem erheblichen Risiko für die Rechte und Freiheiten natürlicher Personen führen. Letztes ist beispielsweise der Fall, wenn besondere Datenkategorien (z.B. Gesundheitsdaten) verarbeitet werden, eine Profiling stattfindet, die Datenverarbeitung umfangreich ist oder eine grosse Zahl von Personen betroffen ist (vgl. Art. 83 Abs. a und g DSGVO). Bei solchen Datenverarbeitungen besteht das Risiko, dass infolge eines Normverstosses hohe Geldbussen ausgefällt werden.

Es erscheint deshalb für ein Schweizer Unternehmen sinnvoll, sich bei der Umsetzung materieller Anforderungen der DSGVO auf risikoreiche Verarbeitungen von EU/EWR-Daten zu konzentrieren. Dabei muss sich eine Datenverarbeitung (wie bisher) an den Verarbeitungsgrundsätzen orientieren und gerechtfertigt sein. Prozesse müssen dokumentiert und die Dokumentation muss aufbewahrt werden, um die Einhaltung der datenschutzrechtlichen Pflichten nachträglich nachweisen zu können. Insbesondere die Einhaltung der Verarbeitungsgrundsätze muss nachgewiesen werden können (Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO).

Formelle Anforderungen erfüllen

Aufsichtsbehörden und Gerichte können Geldbussen grundsätzlich nur dann aussprechen, wenn nachweislich ein Normverstoss vorliegt (Legalitätsprinzip). Ein Normverstoss lässt sich vor allem bei formellen Vorschriften, die klare Anforderungen enthalten, nachträglich leicht nachweisen. Daraus ergibt sich ein Risiko von Geldbussen, wenn gegen formelle Anforderungen der DSGVO verstossen wird.

Vor diesem Hintergrund ist es für ein betroffenes Schweizer Unternehmen empfehlenswert, die formellen Anforderungen der DSGVO im Wesentlichen

umzusetzen. Es sollte die erforderlichen Standard-Dokumente (z.B. Datentransferverträge, Einwilligungserklärung) erstellen. Es sollte die notwendigen Prozesse (z.B. Prozess zur Erstellung von Folgeabschätzungen) implementieren. Es sollte Verantwortliche bestimmen und Mitarbeitende ausbilden, damit die Standard-Dokumente auch tatsächlich verwendet und die Prozesse auch tatsächlich befolgt werden.

Ein betroffenes Schweizer Unternehmen kann das Risiko von Geldbussen insbesondere durch die Umsetzung folgender formeller Anforderungen der DSGVO reduzieren:

- Vertreter ernennen, wenn keine Niederlassung im EU/EWR-Raum besteht;
- Informationsdokumente und Einwilligungserklärungen überprüfen und anpassen;
- Datentransfer-Verträge überprüfen und anpassen;
- Verzeichnis der Verarbeitungstätigkeiten erstellen;
- Verantwortlichkeiten bestimmen; interne Datenschutzbeauftragte allenfalls auch ohne entsprechende Pflicht ernennen;
- Prozesse zu Betroffenenrechte, Meldung von Sicherheitsverstössen und Folgeabschätzungen erstellen;
- Schulungen und Audits durchführen;
- allenfalls notwendige Datenportabilität sicherstellen.

Massnahmen reaktiv anpassen

Es liegt in der Natur des Datenschutzrechts, dass eine Datenverarbeitung nur dann rechtskonform sein kann, wenn sie über die Zeit an neue Gegebenheiten angepasst wird. Datenschutzrecht handelt von der Verarbeitung von Daten anderer Personen. Diese anderen Personen haben ein grundsätzliches Recht, weitgehend über ihre eigenen Daten zu bestimmen (*Grundrecht auf informationelle Selbstbestimmung*). Sie können beispielsweise ihre Einwilligung widerrufen oder unter Umständen die Berichtigung oder Löschung ihrer Daten verlangen, sodass ein Unternehmen verpflichtet ist, die Datenverarbeitung fallbezogen nachträglich anzupassen. Des Weiteren kann nachträglich eine umfassende Anpassung der Datenverarbeitung erforderlich sein, wenn Aufsichtsbehörden ihre Praxis ändern oder Berufsverbände Datenschutznormen in einem Geschäftsbereich spezifizieren.

Ein betroffenes Schweizer Unternehmen sollte vor diesem Hintergrund die eigene Datenverarbeitung gewissermassen „änderungsoffen“ ausgestalten und dabei voraussehen, welche Anpassungen später möglicherweise erforderlich sein werden. Es sollte organisatorische und technische Massnahmen ergreifen, um die Datenverarbeitung in Zukunft mit geringem Aufwand anpassen zu können, und bei Bedarf auch effektiv anpassen. Auf diese Weise kann es nicht nur einer administrativen oder gerichtlichen Durchsetzung zuvorkommen. Es kann auch Geldbussen vermeiden oder wenigstens reduzieren.

Zusammenarbeit mit Datenschutzbehörden

Ein betroffenes Schweizer Unternehmen sollte im Fall eines (meldepflichtigen) Zwischenfalls oder einer (drohenden) Untersuchung proaktiv und frühzeitig mit der zuständigen Aufsichtsbehörde zusammenarbeiten. Ein solches Verhalten hilft für gewöhnlich, wenn es darum geht, Geldbussen abzuwenden oder mindestens zu reduzieren. Im Übrigen gilt, dass für den Fall einer Nichtbefolgung von behördlichen Anweisungen zusätzliche Geldbussen drohen (Art. 83 Abs. 5 lit. e und Abs. 6 DSGVO).

Vermeidung von Schadenersatz

Schadenersatzrisiko

Es besteht das Risiko, dass ein Schweizer Unternehmen vor einem Zivilgericht in einem EU/EWR-Mitgliedstaat auf Schadenersatz verklagt wird, wenn es EU/EWR-Daten rechtswidrig verarbeitet und betroffene Personen dadurch einen nachweisbaren Schaden erleiden.

Schadenansprüche können im Bereich der Verarbeitung von personenbezogenen Daten vor allem dann entstehen, wenn unberechtigte Dritte widerrechtlichen Zugriff auf personenbezogene Daten erhalten. Beispielsweise wurde in San Franzisco kürzlich eine Sammelklage gegen Facebook eingereicht, weil Cambridge Analytica unrechtmässig Zugriff auf personenbezogene Daten von ca. 85 Mio. Nutzern erhielt.

Des Weiteren gibt es Arten von Datenverarbeitungen, die naturgemäss eine hohe Schadenneigung

aufweisen. Das gilt etwa für die Verarbeitung von Daten zur Kreditwürdigkeit, die Verarbeitung von Gesundheitsdaten oder genetischen Daten oder die automatisierte Entscheidungsfindung im Einzelfall.

Datensicherheit, spezifische Einwilligung

Ein Schweizer Unternehmen, das unter den Anwendungsbereich der DSGVO fällt, kann das Schadenersatzrisiko zunächst dadurch reduzieren, dass es für eine angemessene Datensicherheit sorgt. Dadurch kann verhindert werden, dass unberechtigte Personen etwa Zugriff auf Kundendaten des Unternehmens erhalten und den Kunden dadurch ein Schaden entsteht.

Des Weiteren kann ein betroffenes Schweizer Unternehmen für die Durchführung einer schadengeneigten Datenverarbeitung unter Umständen spezifische Einwilligungserklärungen mit Hinweis auf mögliche Schadenfolgen einholen. Auf diese Weise kann es das Risiko, dass die Datenverarbeitung als rechtswidrig beurteilt wird, reduzieren. Schadenersatz kann nur bei einer rechtswidrigen Datenverarbeitung zugesprochen werden.

Vermeidung von Reputationsschaden

Reputationsrisiko

Es besteht grundsätzlich ein Reputationsrisiko, wenn ein Schweizer Unternehmen personenbezogene Daten verarbeitet und dabei gegen die DSGVO verstösst. Datenschutzverstösse, wenn sie öffentlich bekannt werden, können zu einem Umsatzrückgang und/oder höheren Kosten seitens des Unternehmens führen (vgl. RV Bulletin 6/2017 zu Reduktion von Rechts- und Reputationsrisiken durch antizipative Normumsetzung im Unternehmen, S. 21 ff.).

Ob ein Reputationsschaden entsteht, hängt davon ab, wie private Anspruchsgruppen auf bekannt gewordene Datenschutzverstösse des Unternehmen reagieren. Beispielsweise können sich Kunden von einem Unternehmen abwenden, wenn öffentlich bekannt wird, dass ihre Daten zweckwidrig verwendet wurden, eine Untersuchung eröffnet oder eine Klage eingereicht wurde (vgl. Art. 34 DSGVO).

Transparenz, Public Relations

Ein Schweizer Unternehmen sollte die Beziehungen zu privaten Anspruchsgruppen pflegen und sicherstellen, dass deren Erwartungen an die Datenverarbeitung nicht enttäuscht werden. Es sollte informieren, auf welche Weise es personenbezogene Daten verarbeitet und möglicherweise in Zukunft verarbeiten wird.

Des Weiteren sollte ein Schweizer Unternehmen proaktiv über die eigenen Datenschutzmassnahmen informieren. Es kann beispielsweise auf der eigenen Webseite die Datenschutz- und Datensicherheitsmassnahmen beschreiben, die es zum Schutz seiner Kunden und Mitarbeitenden ergriffen hat. Zusätzlich sollte es auf den Fall eines „Skandals“ (z.B. Datenverlust oder unerwartetes Untersuchungsverfahren) vorbereitet sein. Es sollte gegebenenfalls rasch geeignete Customer Relations- und Public Relations-Massnahmen ergreifen können (z.B. Korrektur der Datenverarbeitung und deren Kommunikation nach aussen).

Literaturverzeichnis

Klar Manuel, in: Jürgen Kühling und Benedikt Buchner (Hrsg.), Datenschutz-Grundverordnung, Kommentar C.H. Beck, 2017

Peter Christian, DSGOV und E-DSG fordern Schweizer Spitäler, Heime und Spitex, in Jusletter 26. Februar 2018

Pilz Carlo, in: Peter Gola (Hrsg.), Datenschutz-Grundverordnung, C.H. Beck 2017

Rosenthal David, Der Entwurf für ein neues Datenschutzgesetz, in: Jusletter 27. November 2017

Unabhängige Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz –DSK), Kurzpapier 7, Marktortprinzip: Regelungen für aussereuropäische Unternehmen, Stand: 26. Juli 2017

Zerdick Thomas, in: Eugen Ehmann und Martin Selmayr (Hrsg.), DS-GVO, Datenschutz-Grundverordnung, Kommentar, 2017

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
BDSG	Deutsches Bundesdatenschutzgesetz, revidiert im Jahr 2017
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DS-Grundverordnung)

E-DSG	Entwurf des revidierten Datenschutzgesetzes der Schweiz
EDÖB	Eidg. Datenschutz- und Öffentlichkeitsbeauftragter
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
IRSG	Bundesgesetz über internationale Rechtshilfe in Strafsachen von 1981
LugÜ	Lugano-Übereinkommen von 2007

Weitere Publikationen im Datenschutzrecht

- Regelung des Datenschutzes im multinationalen Konzern (eine Übersicht), 2014 (d/e)
- Entwicklungen im Unternehmens-Datenschutzrecht der Schweiz und der EU, 2012 (d)
- Entwicklungen im Unternehmens-Datenschutzrecht der Schweiz und der EU, 2010
- Entwicklungen im Datenschutzrecht für Unternehmen in der Schweiz und der EU, 2009-2 (d)
- Entwicklungen im Datenschutzrecht für Unternehmen in der Schweiz und der EU, 2009-1 (d/e)
- Revidiertes Datenschutzrecht für Unternehmen in der Schweiz, 2007 (d)
- Dokumenten- und Datenaufbewahrung im schweizerischen Unternehmen, 2006 (d)