Bild: Shutterstock/Rob Marmion

Neues EU-Datenschutzrecht und seine Bedeutung für Schweizer Unternehmen

Datenschutz: Was uns das EU-Recht angeht

Viele Schweizer Unternehmen wissen vermutlich noch gar nicht, dass sie von der kommenden EU-Datenschutzverordnung betroffen sind. **Von Ursula Widmer**

Die EU-Datenschutzgrundverordnung, die voraussichtlich im Mai 2018 in Kraft tritt, bedeutet eine grundlegende Neuordnung. Schweizer Unternehmen sind dadurch in zweifacher Hinsicht betroffen. Erstens werden sie in zahlreichen Fällen direkt dem Recht der Europäischen Union unterstellt sein, auch wenn die Bearbeitung der Daten in der Schweiz stattfindet. Zweitens wird das neue EU-Recht auch in der laufenden Revision des Schweizerischen Datenschutzrechts berücksichtigt werden müssen, damit die Gleichwertigkeit des schweizerischen Datenschutzes mit demjenigen in der EU auch weiterhin gewährleistet ist. Schweizerische Unternehmen sollten sich daher bereits jetzt mit dem neuen EU-Datenschutzrecht und den sich daraus für sie ergebenden möglichen Folgen befassen.

Einheitlich im ganzen EU-Raum

Aktuell haben die einzelnen EU-Mitgliedsstaaten auf der Grundlage der EU-Datenschutzrichtlinie von 1995 ihre eigenen Datenschutzgesetze. Die Richtlinie gewährt den Staaten erheblichen Spielraum. Dies führte zu deutlichen Unterschieden in den Datenschutzregelungen und im Datenschutzniveau zwischen den EU-Staaten. Für Betroffene ist es schwierig, ihre Rechte durchzusetzen, da es keine einheitlich zuständige Datenschutzbehörde gibt.

Die neue EU-Datenschutzgrundverordnung (EU-DSGVO) wird direkt in allen Mitgliedsstaaten gelten. Sie löst die bisherige EU-Datenschutzrichtlinie und die nationalen Datenschutzgesetze ab und ersetzt sie durch eine einheitliche EU-Regelung. Eine Umsetzung in nationales Recht ist nicht mehr erforderlich. Ausgenommen sind lediglich einzelne Punkte, bei denen die Verordnung den Mitgliedsstaaten einen Gestaltungsspielraum einräumt. Das gilt insbesondere für den wichtigen Bereich des Datenschutzes am Arbeitsplatz. Ferner können die Mitgliedsstaaten die Pflicht der Unternehmen zur Ernennung eines Datenschutzbeauftragten strenger regeln als die EU-DSGVO.

Mit der EU-DSGVO gelten in allen EU-Ländern gleich hohe Datenschutzstandards. Für Unternehmen bedeutet dies einerseits eine Vereinheitlichung und Vereinfachung der Rechtslage, andererseits aber auch strengere und teilweise neue Anforderungen sowie umfangreiche Anpassungsarbeiten, die bereits 2016 starten sollten.

Bedeutung fürs Schweizer Recht

Die neue EU-Regelung muss bei der Revision des Schweizer Datenschutzgesetzes berücksichtigt werden. Noch dieses Jahr wird der Bundesrat die Vernehmlassung zum revidierten Datenschutzgesetz durchführen. Es ist wichtig, dass das schweizerische Datenschutzrecht im Wesentlichen mit demjenigen der EU übereinstimmt. Nur dann anerkennt die EU den Datenschutz in der Schweiz als gleichwertig. Andernfalls würde der für schweizerische Unternehmen unerlässliche Datenaustausch mit Unternehmen in der EU unverhältnismässig erschwert.

Welcher Spielraum der Schweiz hier im Rahmen des autonomen Nachvollzugs des EU-Rechts verbleibt, wird sich noch zeigen. Dabei ist zu beachten, dass neue datenschutzrechtliche Vorgaben, insbesondere für die Behörden, auch aus der Fortentwicklung des Rechts zum Schengen-Raum entstehen. Ohnehin beachten Unternehmen in der Schweiz zunehmend auch ausländische Datenschutzvorgaben, die sie hier eigentlich (noch) nicht befolgen müssten. Ein Beispiel dafür ist die Information von betroffenen Personen im Fall sogenannter «Data Breaches» (Datenverlust, Datendiebstahl, Offenbarung von Daten an Unbefugte). Vor allem Tochterunternehmen von Gesellschaften aus Ländern, in denen solche Informationspflichten bereits gesetzlich vorgesehen sind, (zum Beispiel USA oder Deutschland), befolgen diese oft auch hierzulande.

Welche Firmen betroffen sind

Die EU-DSGVO gilt für alle Datenverarbeitungen im Zusammenhang mit den Geschäftsaktivitäten einer EU-Niederlassung eines Unternehmens oder mit den Tätigkeiten eines von einem Unternehmen mit der Datenbearbeitung beauftragten, in der EU domizilierten Dritten (sogenannter Auftragsdatenverarbeiter). Es spielt dabei keine Rolle, ob die eigentliche Datenbearbeitung in der EU erfolgt oder zum Beispiel in die Schweiz ausgelagert wurde. Wenn daher ein Unternehmen in der Schweiz über eine zentrale IT-Organisation verfügt, die auch Daten für Niederlassungen oder Tochtergesellschaften in der EU verarbeitet, so gilt für die Bearbeitung dieser Daten EU-Recht. Das Gleiche gilt, wenn ein schweizerisches Rechenzentrum für EU-Unternehmen oder als Subunternehmer eines Auftragsdatenverarbeiters in der EU tätig ist.

«Wenn ein Schweizer Unternehmen die Daten für seine EU-Niederlassungen hierzulande verarbeitet, gilt für die Bearbeitung dieser Daten trotzdem EU-Recht»

Ursula Widmer

Ebenso gilt die Verordnung für alle Unternehmen ausserhalb der EU, wenn sie Daten von in der EU ansässigen Personen bearbeiten, um diesen Waren oder Dienstleistungen in der EU anzubieten, oder wenn die Daten dazu dienen, das Verhalten der Personen zu beobachten, etwa durch Datenauswertung von Websitebesuchern oder von App-Nutzern aus der EU.

Das EU-Recht gilt somit für alle Schweizer Exporteure, Versandhändler, Betreiber von Plattformen für Onlinebestellungen jeder Art sowie für jeden Dienstleister, der seine Leistungen Kunden in der EU anbietet. Diese Unternehmen müssen einen Vertreter in der EU benennen, ausser die Bearbeitung der Daten von in der EU ansässigen Personen erfolgt nur gelegentlich und beinhaltet keine umfangreiche Bearbeitung von besonders schützenswerten Personendaten (zum Beispiel Gesundheitsdaten).

Nicht dem EU-Recht unterstehen dagegen Unternehmen, die ihre Leistungen zwar an in der EU ansässige Personen ▶

erbringen, diese jedoch nicht in der EU anbieten wie Restaurants, Hotels oder Bergbahnen. Betreiben solche Unternehmen jedoch eine Website und ermöglichen auf dieser Onlinebestellungen aus der EU, so sind sie dem EU-Datenschutzrecht unterstellt, denn ihre Leistungen werden in der EU angeboten.

Die wichtigsten Neuerungen

Datenschutzbeauftragter: Unternehmen, deren Kerngeschäft die regelmässige oder systematische Beobachtung von Betroffenen in grossem Umfang ist oder die in grossem Umfang sensitive Daten verarbeiten, sind verpflichtet, einen Datenschutzbeauftragten zu ernennen. Beim Beauftragten kann es sich um einen Mitarbeitenden des Unternehmens oder um einen externen Dienstleister handeln (zum Beispiel einen auf Datenschutzrecht spezialisierten Rechtsanwalt). Für eine Unternehmensgruppe kann ein gemeinsamer Datenschutzbeauftragter bestimmt werden.

Meldepflicht: Datenschutzverstösse, etwa bei Diebstahl, Verlust oder Offenbarung personenbezogener Daten an Unbe-

«Das EU-Recht gilt für alle Schweizer Exporteure, Versandhändler, Betreiber von Plattformen für Onlinebestellungen sowie für jeden Dienstleister, der seine Leistungen Kunden in der EU anbietet»

Ursula Widmer

fugte, sind innert 72 Stunden an die zuständige Datenschutzbehörde zu melden, ausser die Datenschutzverletzung führt voraussichtlich zu keinem Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen. Zusätzlich müssen die betroffenen Personen selbst benachrichtigt werden, wenn für sie ein hohes Risiko besteht.

Aufzeichnungspflicht: Unternehmen müssen Aufzeichnungen über ihre Datenverarbeitungsaktivitäten führen. Dies beinhaltet die Dokumentation von Kontaktdaten der für die Verarbeitung Verantwortlichen, die Zwecke der Datenbearbeitung, die Kategorien der verarbeiteten Daten, der allfälligen Empfänger, an die Daten weitergegeben werden, Datenübermittlungen in EU-Drittländer, die Fristen für die Löschung der verschiedenen Datenkategorien und eine Beschreibung der vorgesehenen technischen und organisatorischen Schutzmassnahmen. Auch Auftragsdatenverarbeiter müssen über die von ihnen im Auftrag ausgeführten Datenverarbeitungen über ähnliche Aufzeichnungen verfügen. Unternehmen mit weniger als 250 Mitarbeitenden sind von dieser Pflicht befreit, wenn die Datenverarbeitung kein Risiko für die betroffenen Personen darstellt und keine besonders schützenswerten Personendaten betrifft.

Privacy by design: Produkte und Services sind so zu erstellen, dass diese standardmässig nur diejenigen personenbezogenen Daten verarbeiten, die für den jeweiligen Zweck erforderlich sind.

Datenschutzfolgenabschätzung: Datenverarbeitungsprozesse, die hohe Risiken für die Rechte und Freiheiten der Betroffenen beinhalten, bedürfen einer vorgängigen unternehmensinternen Überprüfung, insbesondere bei der Verwendung neuer Technologien.

Recht auf Vergessenwerden: Die Durchsetzung des Rechts der Nutzer, Informationen wieder löschen zu lassen, wird erleichtert.

Portabilität: Die Nutzer müssen die Möglichkeit haben, Daten von einem Anbieter zum nächsten mitzunehmen.

Jugendschutz: Grundsätzlich dürfen Kinder unter 16 Jahren Onlinedienste wie Facebook, Video on Demand oder Chatrooms nur mit Zustimmung der Eltern nutzen. Den EU-Staaten steht es jedoch frei, tiefere Alterswerte festzulegen, wobei ein absolutes Mindestalter von 13 Jahren gilt.

One-Stop Shop: Betroffene sollen sich künftig in ihrer Sprache an die Datenschutzbehörde in ihrem Heimatstaat wenden können, auch wenn es um Datenschutzprobleme in einem anderen Mitgliedsstaat geht.

Strafmass: Unternehmen, die gegen die neuen Datenschutzregeln verstossen, droht eine Geldstrafe von bis zu maximal 20 Mio. Euro oder 4 Prozent des weltweiten Jahresumsatzes – je nachdem, welcher Betrag höher ist. Kleineren Unternehmen drohen keine derartigen Sanktionen, wenn es sich um erstmalige, versehentliche oder kleinere Verstösse handelt.

Zustimmung muss eindeutig sein

Neben diesen Neuerungen sieht die neue Verordnung zum Teil verschärfte Regelungen zu zentralen Punkten des Datenschutzrechts vor. Dies ist etwa der Fall bei der Information der Betroffenen über die Verarbeitung ihrer Daten sowie die Voraussetzungen für die Ausübung ihrer Rechte, den Inhalt der vertraglichen Regelung bei der Verarbeitung von Daten durch Dritte (Auftragsdatenverarbeitung) oder die Voraussetzungen zur Übermittlung von Personendaten in EU-Drittländer.

Insbesondere gelten in Zukunft auch verschärfte Anforderungen an die Einwilligung einer betroffenen Person zur Bearbeitung ihrer Daten. Voraussetzung ist eine unmissverständlich durch die betroffene Person abgegebene Willenskundgebung, z. B. durch eine ausdrückliche Erklärung oder eine eindeutige Handlung, wie z. B. das Betätigen eines «I agree»-Buttons auf einer Website. Eine bloss stillschweigende Einwilligung genügt nicht mehr (etwa, wenn auf einer Website ein durch den Anbieter bereits im Voraus angeklicktes Feld vom Betroffenen nicht deaktiviert wird). Wenn die Einwilligung in Form einer schriftlichen Erklärung erfolgt und diese auch noch weitere Sachverhalte betrifft, so muss die Regelung bezüglich der Datenbearbeitung in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache erfolgen, sodass sie von den anderen Sachverhalten klar unterschieden werden kann. Damit ist fraglich, ob Einwilligungen noch gültig sein werden, wenn der Kunde einen Vertrag unterzeichnet, der auf allgemeine Geschäftsbedingungen verweist, in denen die Regelung bezüglich der Datenbearbeitung enthalten ist.

Heutiger Handlungsbedarf

Für viele Schweizer Unternehmen ist die neue Verordnung direkt anwendbar, wenn sie im oder mit Bezug auf den EU-Raum operieren und in diesem Zusammenhang Daten von Kunden, Lieferanten oder in der EU eingesetzten Mitarbeitenden bearbeiten. Andere Unternehmen werden indirekt durch deren Einfluss auf die Revision des schweizerischen Datenschutzrechts von der neuen EU-Verordnung betroffen sein. Somit ist es für alle Schweizer Unternehmen wichtig, dass sie sich mit dem neuen EU-Datenschutzrecht und dessen Anforderungen vertraut machen und bereits jetzt mit der Vorbereitung für notwendige Anpassungen beginnen.

Standardkonditionen wie Musterverträge, allgemeine Geschäftsbedingungen, Datenschutz-Policys etc. sind zu überarbeiten, z. B. im Hinblick auf die Information über die Bearbeitung von Daten und bezüglich der neuen Gültigkeitsbedingungen für die Einwilligung der betroffenen Personen. Damit diese Zustimmung gültig eingeholt werden kann, müssen zudem die eingesetzten Applikationen angepasst werden. Auch die Verträge mit gewissen Geschäftspartnern müssen daraufhin geprüft werden, ob sie dem Datenschutz genügend Rechnung tragen und ggf. angepasst werden. Dies betrifft Partner, die im Rahmen ihrer Tätigkeit Zugang zu Personendaten haben oder diese im Auftrag eines Unternehmens bearbeiten, z. B. Dienstleister im Bereich Buchhaltung, Fakturierung, Inkasso, Mailings, Personalberater, Provider von Cloud Computing und Outsourcing Services oder IT-Wartungsfirmen.

Aufgrund des Privacy-by-Design-Ansatzes müssen Unternehmen ihre Produkte, Services und Datenverarbeitungsprozesse so anpassen, dass nur diejenigen Personendaten erhoben und bearbeitet werden, die effektiv benötigt werden. Ferner sollten die Verantwortlichen durch organisatorische Vorkehrungen sicherstellen, dass die datenschutzrechtlichen Anforderungen und insbesondere auch die neuen Pflichten effektiv umgesetzt werden. Schliesslich steht die Aktualisierung der bestehenden internen Weisungen, Reglemente und Policys zur Datenschutz-Compliance auf der To-do-Liste.

Dabei geht es nicht um eine einmalige Umstellung per 2018, sondern darum, den Datenschutz künftig permanent im laufenden Geschäftsbetrieb und bei Change-Prozessen sicherzustellen. Dies ist vor allem auch mit Rücksicht auf die Höhe der in der EU-Verordnung vorgesehenen Sanktionen wesentlich. Das bedingt, die Datenschutz-Compliance zur Chefsache zu erklären und das Management von Datenschutzrisiken unternehmensintern zu institutionalisieren. ■

Dr. Ursula Widmer ist Rechtsanwältin mit Spezialgebiet IT-, Datenschutz- und Telekommunikationsrecht und Mitglied der vom Bundesrat eingesetzten Expertengruppe «Zukunft der Datenbearbeitung und Datensicherheit»:
www.widmer.ch