bratschi

Markus Näf
Master of Law, Rechtsanwalt
Partner
Lehrbeauftragter für Informatikrecht und
Projektmanagement an der Fachhochschule St. Gallen
Telefon +41 58 258 10 00
markus.naef@bratschi.ch

Umsetzung der Europäischen Datenschutz-Grundverordnung in Schweizer Unternehmen

Am 25. Mai 2018 wird die Europäische Datenschutz-Grundverordnung (EU DSGVO) nach einer zweijährigen Übergangsfrist in allen Ländern der Europäischen Union (EU) vollziehbar. Diese Bestimmungen gelten nicht nur für Unternehmen in der EU, sondern auch für Unternehmen, die Waren und Dienstleistungen in der EU anbieten oder das Verhalten von Personen in der EU bearbeiten. Schweizer Unternehmen müssen daher abklären, ob die Verordnung auf Sie anwendbar ist und die neuen Vorschriften einhalten, um mögliche Sanktionen zu vermeiden.

1. Anwendbarkeit auf Schweizer Unternehmen

Die DSGVO findet auf alle Unternehmen Anwendung, die in der EU ansässig sind und Personendaten verarbeiten, unabhängig ob die Verarbeitung in der EU stattfindet. Weiter findet die Verordnung in folgenden Fällen auch Anwendung auf Unternehmen mit Sitz ausserhalb der EU:

- bei Verarbeitung von Personendaten im Zusammenhang mit dem Angebot von Waren und Dienstleitungen an Personen in der der EU
- bei Beobachtung des Verhaltens von Personen in der EU

Schweizer Unternehmen müssen prüfen, ob Sie der DSGVO unterliegen.

2. Welche Unternehmen unterliegen der DSGVO nicht?

Die Regulierung betrifft Daten von natürlichen Personen und bezieht sich nur auf Personendaten. Als personenbezogene Daten zählen alle Informationen die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, aber auch zu Standortdaten, einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Die DSGVO gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person. Sobald aber weitergehende Personendaten zum Beispiel in einem Customer Relationship Management System (CRM) erfasst und bearbeitet werden unterliegt diese Erfassung der Regulierung.

Unternehmen die im Business-to-Business Bereich tätig sind und keine Waren- oder Dienstleistungen in der EU anbieten und allenfalls nur einzelne Einkaufsverträge mit Unternehmen in der EU abwickeln, unterliegen der DSGVO nicht. Die Internetseite darf in diesem Fall nicht auf EU-Kunden ausgerichtet sein.

3. Was sind die notwendigen Umsetzungsschritte

Der Grundsatz der EU DSGVO ist ein «**Verbot der Verarbeitung von Personendaten, mit Erlaubnisvorbehalt».**

3.1 Rechtsmässigkeit der Datenbearbeitung

Das Unternehmen muss daher bei jeder Bearbeitung von Personendaten prüfen, welcher Rechtfertigungsgrund dafür besteht. Es kommen vorwiegend folgende drei Gründe in Frage:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Massnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

Das Unternehmen trägt die Beweislast für den Rechtfertigungsgrund und insbesondere die Einwilligung kann nur spezifisch nach vorgängiger Aufklärung erfolgen.

Entsprechend sind im Unternehmen die Vertragsbestimmungen und allgemeinen Geschäftsbedingungen (AGB) an die neuen Vorschriften anzupassen.

3.2 Datenbearbeitung durch Dritte

Bei der Datenweitergabe an einen Dritten sind zwei Fälle zu unterscheiden:

(i) **Die Datenweitergabe im Sinne eines Outsourcings**, indem ein Dritter als Auftragsverarbeiter (Processor) die Daten für den Auftraggeber (Controller) bearbeitet und sie nicht für eigene Zwecke nutzt. Diese ist zulässig wenn sich der Auftraggeber an die gleichen Datenschutzbestimmungen hält, die Daten nicht für eigene Zwecke nutzt und eine Ver-

einbarung zwischen den beiden besteht. In den meisten Fällen müssen durch den Verantwortlichen und den Auftragsverarbeiter sogenannte Verarbeitungsverzeichnisse geführt werden.

(ii) **Die Datenweitergabe an einen Dritten für seine eigenen Zwecke**: Hier ist ein Rechtfertigungsgrund für die Datenweitergabe erforderlich. Bei einem Verkauf der Daten muss normalerweise eine Einwilligung vorliegen.

Jede rechtliche Einheit gilt als Dritter, entsprechend gelten diese Regeln auch unter Konzerngesellschaften.

3.3 Datenübermittlung ins Ausland

Die Datenübermittlung ins Ausland ist ohne weitere Formalitäten zulässig, wenn das entsprechende Land einen gleichwertigen Datenschutz hat. Leider haben dies neben der Schweiz und der EU nur sehr wenige Länder.

Datenübermittlung in Drittstaaten ist neu grundsätzlich zulässig:

- in Länder mit einem angemessenen Schutzniveau (keine besondere Einwilligung notwendig), dies sind neben allen EU Ländern und der Schweiz nur sehr wenige Länder[1].
- wenn zwischen den Unternehmen ein Datentransfer-Vertrag aufgrund von Standardvertragsklauseln der EU abgeschlossen wurde.
- wenn der Datentransfer im Konzern auf der Basis von Binding Corporate Rules, welche jedoch behördlich genehmigt werden müssen, stattfindet.
- wenn nach Information und Aufklärung über die spezifischen Risiken eine Einwilligung der Betroffenenen vorliegt.
- wenn eine Einzelgenehmigung durch eine Datenschutzaufsichtsbehörde erteilt wurde.

Die Einwilligung dürfte hier der wichtigste Rechtfertigungsgrund sein. Es können aber auch gerechtfertigte Interessen geltend gemacht werden, zum Beispiel bei der Auftragsabwicklung mit einem Kunden im entsprechenden Land.

Unternehmen müssen prüfen, in welchen Ländern ihre Daten bearbeitet, gespeichert und wohin sie übermittelt werden. Es sind die entsprechenden Voraussetzungen für eine Datenübermittlung zu schaffen.

4. Formelle Anforderungen

Die DSGVO schreibt neue Verhaltensregeln für Unternehmen vor:

[1] Aus der Sicht der EU haben neben allen EU-Ländern die folgenden Länder einen gleichwertigen Datenschutz: Schweiz, Kanada, Argentinien, Guernsey, Jersey, Isle of Man, Israel, Neuseeland, Andorra, Färöer Inseln, Australien, Urugay. Bei den USA gelten aufgrund des Privacy Shields Abkommens nur Unternehmen als gleichwertig, die diesem beigetreten sind.

4.1 Datenschutzbeauftragter

Unternehmen müssen einen betrieblichen Datenschutzbeauftragten ernennen, wenn die Kerntätigkeit des Unternehmens in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche, regelmässige und systematische Überwachung von betroffenen Personen erforderlich machen oder in umfangreicher Verarbeitung besonderer Kategorien von Daten[2] besteht.

Die nationalen Gesetzgeber in der EU können in diesem Fall diese Bestimmungen verschärfen, so besteht in Deutschland für die meisten Unternehmen die Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten, wenn mehr als neun Personen automatisiert oder mehr als zwanzig Personen nicht-automatisiert personenbezogene Daten verarbeiten.

4.2 Vertreter in der EU

Schweizer Unternehmen müssen, wenn sie keine Niederlassung in der EU haben, zwingend schriftlich einen Vertreter in der EU benennen, sofern ihre Datenverarbeitung folgendes umfasst:

(i) betroffenen Personen in der EU Waren oder Dienstleistungen entgeltlich oder unentgeltlich anzubieten, oder

(ii) das Verhalten betroffener Personen zu beobachten («Tracking» bzw. «Profiling»), soweit ihr Verhalten in der EU erfolgt.

Der Vertreter muss schriftlich bestellt werden und er vertritt das ausländische Unternehmen in der EU gegenüber den Datenschutzbehörden.

Bei Bedarf können wir Ihnen einen Vertreter in Deutschland bereitstellen.

4.3 Datenschutz-Folgeabschätzung

Unternehmen müssen eine Datenschutz-Folgeabschätzung (DSFA) durchführen, wenn die Verarbeitung personenbezogener Daten ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen haben könnte, wie zum Beispiel Verarbeitungsvorgänge mit

[2] Besondere Kategorien von Daten umfassen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit sowie genetischeund biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten und weiter Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

grossen Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene, die eine grosse Zahl von Personen betreffen könnten und;

- neue Technologien eingesetzt werden;
- Profiling und automatisierte Entscheidungen eingesetzt werden;
- grossflächige Videoüberwachung betrieben wird;
- biometrische Daten verarbeitet werden.

Mit der DSFA müssen die Risiken und die Folgen für die betroffenen Personen abgeschätzt werden und Massnahmen zur Risikominimierung ergriffen werden. Wenn ein hohes Risiko für die Persönlichkeitsrechte der betroffenen Personen besteht muss die DSFA zwecks Bewilligung der Datenbearbeitung der Aufsichtsbehörde vorgelegt werden.

Die pflichtwidrige Nichtdurchführung der DSFA oder die fehlende Information der Aufsichtsbehörde bei hohen Risiken wird mit einer Busse sanktioniert.

Wir empfehlen im Zweifelsfall immer eine DSFA durchzuführen und die Beurteilung zwecks Beweis zu dokumentieren.

5. Ausblick

Gleichzeitig mit der DSGVO hätte auch die sogenannte Cookies-Richtlinie (E-Privacy-Richtlinie) In Kraft gesetzt werden sollen. Diese regelt wie der Nutzer auf Internetseiten oder in Onlineapplikationen über eingesetzte Cookies, Tracker, Web-Beacons, Social Media Plugins etc. informiert werden muss. Diese Tools übermitteln Daten an einen Dritten und erfordern daher eine Zustimmung des Nutzers. Dies ist heute noch unterschiedlich geregelt: Informationsbanner zum Anklicken der Zustimmung, nur Informationsbanner oder nur Information in den allgemeinen Geschäftsbedingungen.

Die Datenschutz- und Nutzungsbedingungen der Internetseiten sind auf die korrekte Information und Einwilligungsform vor dem 25. Mai 2018 zu prüfen.

Die Revision des Schweizerischen Datenschutzgesetzes ist erst in der parlamentarischen Behandlung und wird voraussichtlich frühestens auf den 1. Juli 2019 in Kraft treten. Die Revision beinhaltet praktisch die gleichen Vorgaben wie die DSGVO. Es ist aber zu beachten, dass bis zu diesem Zeitpunkt in der Schweiz teilweise noch abweichende Bestimmungen gelten.

Wir empfehlen den Unternehmen jedoch die Vorgaben der DSGVO bereits heute umzusetzen, damit werden voraussichtlich auch die Bestimmungen des neuen schweizerischen Datenschutzgesetzes eingehalten.

Basel
Lange Gasse 15
Postfach
CH-4052 Basel
Telefon +41 58 258 19 00
Fax +41 58 258 19 99
basel@bratschi.ch

Bern
Bollwerk 15
Postfach
CH-3001 Bern
Telefon +41 58 258 16 00
Fax +41 58 258 16 99
bern@bratschi.ch

Lausanne
Avenue Mon-Repos 14
Postfach 5507
CH-1002 Lausanne
Téléfone +41 58 258 17 00
Téléfax +41 58 258 17 99
lausanne@bratschi.ch

St. Gallen
Vadianstrasse 44
Postfach 262
CH-9001 St. Gallen
Telefon +41 58 258 14 00
Fax +41 58 258 14 99
stgallen@bratschi.ch

Zug
Industriestrasse 24
CH-6300 Zug
Telefon +41 58 258 18 00
Fax +41 58 258 18 99
zug@bratschi.ch

Zürich
Bahnhofstrasse 70
Postfach
CH-8021 Zürich
Telefon +41 58 258 10 00
Fax +41 58 258 10 99
zuerich@bratschi.ch