Stand der Revision des Schweizer Datenschutzgesetzes (DSG) – Inkrafttreten der Europäischen Datenschutzgrundverordnung (EU-DSGVO)

Im ersten Teil des vorliegenden Schreibens informieren wir Sie über den aktuellen Stand dieser Gesetzesrevision in der Schweiz. Gleichzeitig weisen wir Sie im zweiten Teil auf die Datenschutzgrundverordnung der EU hin, welche am 25. Mai 2018 in Kraft treten und teilweise auch für Schweizer Unternehmen relevant sein wird. Fazit und Empfehlungen dazu finden Sie auf Seite 3.

Stand der Revision des Schweizer Datenschutzgesetzes (DSG)

Wie die Staatspolitische Kommission des Nationalrats am 13. April 2018 mitteilte (Medienmitteilung abrufbar unter: https://www.parlament.ch/press-releases/Pages/mm-spk-n-2018-04-13.aspx), hat sie beschlossen, die Revision des Schweizer Datenschutzgesetzes in zwei Etappen aufzuteilen. In einer ersten Etappe sollen die notwendigen Anpassungen an die Schengen-Richtlinie vorgenommen werden, welche die Verarbeitung personenbezogener Daten im Bereich des Strafrechts betrifft. Erst die zweite Etappe wird die Totalrevision des Datenschutzgesetzes umfassen und auf alle Datenbearbeitungen durch private Datenbearbeiter und Bundesorgane Anwendung finden. Der Nationalrat wird sich in der Sommersession mit den vorgenommenen Anpassungen im Rahmen der 1. Etappe (Schengen-Richtlinie) befassen und gleichzeitig darüber entscheiden, ob er der Teilung der Revision des Datenschutzrechts zustimmt.

Der Nationalrat ist der erstbehandelnde Rat, was bedeutet, dass anschliessend auch der Ständerat noch über die Vorlage beraten wird.

Entsprechend wird ein Inkrafttreten der für unsere Mitglieder relevanten Bestimmungen des totalrevidierten Datenschutzgesetzes in der Schweiz derzeit nicht vor Mitte, eher Ende 2019 erwartet.

Inkrafttreten der Europäischen Datenschutzgrundverordnung (EU-DSGVO)

Die EU-DSGVO wird am **25. Mai 2018**, direkt geltendes Recht in allen Mitgliedstaaten der EU. Was das für Schweizer Unternehmen bedeutet bzw. ob und gegebenenfalls welche Pflichten ihnen auferlegt werden, soll nachfolgend im Sinne einer Übersicht kurz dargestellt werden.

A. Anwendungsbereich der EU-DSGVO

Der Anwendungsbereich der EU-DSGVO ist weit und reicht über die Grenzen der EU hinaus. Sie ist auf ein Schweizer Unternehmen gemäss Art. 3 EU-DSGVO dann anwendbar, wenn dieses personenbezogene Daten von natürlichen Personen verarbeitet, die sich in der EU befinden, falls das Schweizer Unternehmen

1. den betroffenen Personen in der EU Waren oder Dienstleistungen (entgeltlich oder unentgeltlich) anbietet oder
2. durch die Datenverarbeitung das Verhalten betroffener Personen in der EU beobachten will.

Für die Feststellung, ob **Waren und Dienstleistungen angeboten** werden, ist relevant, ob das (Schweizer) Unternehmen *offensichtlich beabsichtigt*, betroffenen Personen in der EU Waren oder Dienstleistungen anzubieten.

AGVS/UPSA
Wölflistrasse 5, Postfach 64, 3000 Bern 22
Telefon 031 307 15 15, Fax 031 307 15 16
info@agvs-upsa.ch, www.agvs-upsa.ch

Hinweise für eine solche Absicht ergeben sich gemäss den Erwägungen aus Faktoren wie der Verwendung einer Sprache oder Währung, die im jeweiligen EU-Mitgliedstaat, nicht aber in der Schweiz, gebräuchlich ist, in Verbindung mit der Möglichkeit, Waren oder Dienstleistungen in dieser anderen Sprache zu bestellen, oder die Erwähnung von anderen Kunden oder Nutzern, die sich in der EU befinden. Die blosse Zugänglichkeit der Webseite eines Schweizer Unternehmens in der EU ist hingegen noch kein Indiz für die Absicht dieses Unternehmens, dort auch Waren oder Dienstleistungen anbieten zu wollen.

Die Absicht, durch die Datenverarbeitung das **Verhalten betroffener Personen in der EU zu beobachten**, wird beispielsweise daran festgemacht, ob Internetaktivitäten dieser betroffenen Personen nachvollzogen (z.B. Google Analytics) und/oder Techniken zur Profilerstellung natürlicher Personen eingesetzt werden, welche beispielsweise die persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten der Personen analysiert oder vorhergesagt werden.

Damit ist klar, dass der Anwendungsbereich der EU-DSGVO sehr weit ist und auch Schweizer Unternehmen prüfen müssen, ob sie diese neuen Regeln zu beachten haben. Die nachfolgenden, ausgewählten Beispiele für Pflichten von Unternehmen aus der EU-DSGVO mögen einen ersten Eindruck vermitteln, sind aber keinesfalls als vollständige Checkliste zu verstehen.

B. Pflichten für Unternehmen

Information und Einwilligung der betroffenen Person

Im EU-Datenschutzrecht gilt – anders als in der Schweiz – das sog. „Verbot mit Erlaubnisvorbehalt“. Das heisst, die Datenverarbeitung ist generell verboten, so lange sie nicht durch ein Gesetz ausdrücklich erlaubt ist oder die betroffene Person in die Verarbeitung eingewilligt hat. Die betroffene Person kann ihre Einwilligung jederzeit widerrufen. Es muss sichergestellt werden, dass dieser Widerruf genauso einfach erfolgen kann, wie die Einwilligung selbst.

„Privacy by Design“ und „Privacy by Default“

Der Grundsatz „Privacy by Design“ (Datenschutz durch Technik) bedeutet, dass der Verantwortliche bereits im dem Zeitpunkt der Planung einer Datenverarbeitung das Risiko von Datenschutzverletzungen verringern und solchen vorbeugen muss. Beispielsweise soll eine regelmässige Löschung von Daten oder deren standardmässige Anonymisierung vorgesehen werden.

Der Grundsatz „Privacy by Default“ (Datenschutz durch datenschutzfreundliche Voreinstellung) bedeutet, dass standardmässig nur diejenigen Datenverarbeitungen erfolgen dürfen, die für den jeweiligen Verwendungszweck erforderlich sind. Beispielsweise muss eine Webseite grundsätzlich Einkäufe erlauben, ohne dass ein Benutzerprofil erstellt werden muss.

Ernennung eines Vertreters in der EU

Grundsätzlich müssen Schweizer Unternehmen, die vom Anwendungsbereich der EU-DSGVO erfasst werden, einen Vertreter in der EU bezeichnen. Diese Pflicht entfällt jedoch, wenn die Verarbeitung nur gelegentlich erfolgt, keine besonderen Datenkategorien verarbeitet werden und die Verarbeitung nicht zu einem Risiko für die Rechte und Freiheiten der natürlichen Person führt.

Verzeichnis von Verarbeitungstätigkeiten

Der Verantwortliche hat ein Verzeichnis von Verarbeitungstätigkeiten im Unternehmen zu erstellen. Dabei handelt es sich um eine Dokumentation oder Übersicht über alle Prozesse und Verfahren im Unternehmen, bei welchen personenbezogene Daten verarbeitet werden. Dabei sind die wesentlichen Angaben zur Datenverarbeitung anzugeben, wie z.B. die Datenkategorien, der Kreis der betroffenen Personen, der Zweck der Verarbeitung und allfällige Datenempfänger.

Meldepflicht: „Data Breach Notification"

Verletzungen des Schutzes personenbezogener Daten müssen der Aufsichtsbehörde möglichst innert 72 Stunden gemeldet werden. Es besteht nur dann keine Meldepflicht, wenn ein Risiko für Rechte und Freiheiten von Individuen unwahrscheinlich ist. Häufig müssen auch die betroffenen Personen benachrichtigt werden.

Datenschutz-Folgenabschätzung

Wenn eine Form der Verarbeitung wahrscheinlich ein hohes Risiko verursacht, insbesondere bei neuen Technologien oder aufgrund ihres Wesens, ihres Umfangs, ihres Kontexts oder ihrer Zwecke, muss eine Datenschutz-Folgenabschätzung durchgeführt werden. Wenn die Datenschutz-Folgenabschätzung ergibt, dass eine Datenverarbeitung ohne Massnahmen ein hohes Risiko bedeutet, muss die Aufsichtsbehörde konsultiert werden.

Folgen von Datenschutzverstössen

Die maximale Geldbusse beträgt bis zu 20 Millionen Euro oder bis zu 4% des gesamten, weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr; je nachdem, welcher Wert der höhere ist. Dabei gilt der Jahresumsatz des gesamten Konzerns, nicht der einer einzelnen juristischen Person. Ausserdem sieht die EU-DSGVO neu ein Verbandsklagerecht vor, womit zukünftig Verbraucherschutzverbände Rechte von Betroffenen geltend machen können.

C. Fazit und Empfehlungen

Der Anwendungsbereich der EU-DSGVO ist sehr weit und auch Schweizer Unternehmen müssen prüfen, ob sie diese neuen Regeln zu beachten haben. Die oben kurz dargestellten Beispiele für Pflichten von Unternehmen aus der EU-DSGVO mögen einen ersten Eindruck der Konsequenzen dieser EU-Gesetzgebung vermitteln. Angesichts der schwerwiegenden Sanktionen sind Schweizer Unternehmen gut beraten, die Einhaltung dieser neuen Vorschriften ernst zu nehmen.

Inzwischen gibt es bereits sehr nützliche und kostenlose Tools, welche bei der Beurteilung, ob die EU-DSGVO auf das eigene Unternehmen anwendbar ist, und bei den ggf. notwendigen Massnahmen weiterhelfen können:

- Im Sinne eines ersten kurzen Tests (ca. 6 Min.): Datenschutz "Online Check" der economiesuisse, abrufbar unter: www.economiesuisse.ch/de/datenschutz-online-check.
- Ausführlicher und präzise: Das Datenschutz Self Assessment Tool, abrufbar unter: www.dsat.ch. DSAT wurde von David Rosenthal der Kanzlei Homburger entwickelt, und wird von ihm zusammen mit David Vasella der Kanzlei Walder Wyss redaktionell betreut.