Kellerhals Carrard

Kurz & Bündig

2/2017

Datenschutz-Grundverordnung der EU – Was Schweizer Unternehmen wissen müssen

Die Europäische Datenschutz-Grundverordnung (EU-DSGVO) wird in genau einem Jahr, am **25. Mai 2018**, direkt geltendes Recht in allen Mitgliedstaaten der EU.

Doch was bedeutet das für Schweizer Unternehmen? Ist die EU-DSGVO auch für Schweizer Unternehmen verbindlich? Und welche Pflichten werden den Unternehmen im Bereich des Datenschutzes auferlegt?

Anwendungsbereich der EU-DSGVO
Der Anwendungsbereich der EU-DSGVO ist sehr weit und reicht über die Grenzen der EU hinaus. In gewissen Konstellationen ist die EU-DSGVO deshalb auch für Unternehmen mit Sitz in der Schweiz anwendbar.

Das ist gemäss Art. 3 EU-DSGVO dann der Fall, wenn ein Schweizer Unternehmen 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. 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.

Pflichten für Unternehmen

A. 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.

Damit die Einwilligung der betroffenen Person gültig ist, müssen bestimmte Voraussetzungen gegeben sein:

- **Freie Entscheidung**
  Die Einwilligung ist nur gültig, wenn die betroffene Person sie freiwillig abgegeben hat. Die betroffene Person muss also eine echte Wahl haben, d.h. sie darf im Zuge der Einholung der Einwilligung nicht vor vollendete Tatsachen gestellt oder sonst in ihrer Entscheidung eingeschränkt werden. In diesem Zusammenhang ist insbesondere auch auf das sogenannte "Koppelungsverbot" hinzuweisen, wonach der Abschluss eines Vertrags nicht von der Verarbeitung weiterer Daten abhängig gemacht werden darf, die für die eigentliche Vertragsdurchführung gar nicht benötigt werden.

- **Ausführliche, erkennbare und bestimmte Information**
  Die betroffene Person muss vor Abgabe der Einwilligungserklärung über den Zweck der Beschaffung und Verarbeitung ihrer personenbezogenen Daten informiert werden. Dabei müssen alle für den konkreten Fall entscheidungsrelevanten Informationen enthalten sein und diese müssen genügend konkret sein. Eine Einwilligung ist also immer an einen bestimmten Zweck gebunden, welcher nicht zu allgemein gehalten werden darf. Die betroffene Person muss schliesslich in die Lage versetzt werden, die Informationen leicht zu erkennen und zu erkennen, dass ihr Handeln als Einwilligung qualifiziert wird.

- **Form und aktive Handlung**
  Gemäss EU-DSGVO genügt die Nachweisbarkeit der Einwilligung durch die verantwortliche Stelle. Die Einwilligung ist also nicht an eine bestimmte Form gebunden und kann auch elektronisch oder mündlich erfolgen. Allerdings soll die Einwilligung nur durch eine eindeutige Handlung zustande kommen. Damit ist regelmässig eine aktive Handlung der betroffenen Person notwendig, andere Varianten wie eine stillschweigende Zustimmung, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person würden daher keine Einwilligung darstellen. Erfolgt die Einwilligung schriftlich, so hat die Aufforderung dazu in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache sowie von anderen Sachverhalten getrennt zu erfolgen.

- **Widerruflichkeit**
  Die betroffene Person kann ihre Einwilligung jederzeit widerrufen. Es muss sichergestellt werden, dass dieser Widerruf genauso einfach erfolgen kann, wie die Einwilligung selbst.

B. "Privacy by Design" und "Privacy by Default"
Der Grundsatz "Privacy by Design" (Datenschutz durch Technik) bedeutet, dass der Verantwortliche bereits ab dem Zeitpunkt der Planung einer Datenverarbeitung (z.B. mittels eines neuen IT-Systems oder Prozesses) das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte betroffener Personen verringern und solchen Verletzungen vorbeugen muss. Beispiels-

weise sollen eine regelmässige Löschung von Daten oder deren standardmässige Anonymisierung vorgesehen werden. Als besonders bedeutsam für den technikgestützten Datenschutz wird jeweils die Datenminimierung hervorgehoben.

Der Grundsatz "Privacy by Default" (Datenschutz durch datenschutzfreundliche Voreinstellung) bedeutet, dass der Verantwortliche verpflichtet ist, mittels geeigneter Voreinstellungen sicherzustellen, dass standardmässig nur diejenigen Personendaten verarbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind. Beispielsweise muss eine Webseite grundsätzlich Einkäufe erlauben, ohne dass ein Benutzerprofil erstellt werden muss.

C. Ernennung eines Vertreters in der EU
Grundsätzlich müssen Schweizer Verantwortliche oder Auftragsdatenverarbeiter, die vom Anwendungsbereich der EU-DSGVO erfasst werden, einen Vertreter in der EU bezeichnen. Diese Pflicht entfällt insbesondere, 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.

D. Verzeichnis von Verarbeitungstätigkeiten
Der Verantwortliche hat ein Verzeichnis von Verarbeitungstätigkeiten im Unternehmen zu erstellen. Auftragsverarbeiter müssen ein analoges Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Verarbeitungstätigkeiten führen. Beim Verzeichnis handelt es sich um eine Dokumentation oder Übersicht über alle Prozesse und Verfahren im Unternehmen, bei welchen personenbezogene Daten verarbeitet werden. Dabei sind die wesentli-chen Angaben zur Datenverarbeitung anzugeben, wie z.B. die Datenkategorien, der Kreis der betroffenen Personen, der Zweck der Verarbeitung und allfällige Datenempfänger.

Ein Unternehmen muss dafür zunächst ermitteln, in welchen Fällen personenbezogene Daten von z.B. Kunden, Lieferanten oder Beschäftigten erhoben und verarbeitet werden. Hierzu bietet es sich an, zuerst alle innerhalb der Systemlandschaft des Unternehmens eingesetzten Anwendungen und Tools (z.B. Zeiterfassungssystem, CRM System, HR-Informationssystem) aufzulisten, in denen personenbezogene Daten gespeichert werden. Dies hilft gleichsam bei der Ermittlung der Datenflüsse im Unternehmen und kann auch als Grundlage für das Verzeichnis von Verarbeitungstätigkeiten dienen. Ausserdem werden Schweizer Unternehme ohnehin als Erstes eine Bestandesaufnahme vornehmen müssen, um eruieren zu können, ob sie vom Anwendungsbereich der EU-DSGVO erfasst werden.

E. 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.

F. 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.

G. 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.

Fazit und Hinweis

Revision des Datenschutzgesetzes in der Schweiz
Der Anwendungsbereich der EU-DSGVO ist sehr weit und auch Schweizer Unternehmen müssen prüfen, ob sie diese neuen Regeln zu beachten haben. Dies setzt zunächst voraus, dass Unternehmen jeglicher Grösse sich eine gewisse Datenschutzkompetenz aneignen und die Verantwortung dafür intern festlegen. 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. Betroffene Unternehmen werden insbesondere ihre internen Prozesse, Richtlinien, Verträge und Datenschutzerklärungen überarbeiten und allenfalls die Funktionsweise von IT-Systeme anpassen müssen.

Die Anstrengungen zur Einhaltung der neuen EU-DSGVO dürften sich gleich in zweifacher Hinsicht lohnen: Die Vernehmlassung zum Vorentwurf für ein neues Schweizer Datenschutzgesetz (VE-DSG) ist soeben abgeschlossen worden. Ein Gesetzesentwurf wird bereits diesen Herbst erwartet. Der Datenschutz soll auch in der Schweiz – in Anlehnung an die Regeln der EU-DSGVO und in Erfüllung der entsprechenden Konvention des Europarats (SEV 108) – gestärkt werden, insbesondere indem die Transparenz der Bearbeitung und die Kontrollmöglichkeiten der betroffenen Personen über ihre Daten verstärkt werden. Obwohl der bundesrätliche Vorentwurf in verschiedenen Punkten mit einem Swiss Finish übers Ziel hinausschiesst und die parlamentarische Beratung in dieser Form wohl nicht überleben wird, dürfte das Datenschutzthema deshalb auch bei Schweizer Unternehmen an Bedeutung gewinnen.

Wir werden Sie zur Revision des Schweizer Datenschutzgesetzes gern auf dem Laufenden halten.

Zürich, 25. Mai 2017

Dr. Daniel Alder
daniel.alder@kellerhals-carrard.ch

Dr. Nicolas Mosimann, LL.M.
nicolas.mosimann@kellerhals-carrard.ch

Virginie A. Rodieux, LL.M.
virginie.rodieux@kellerhals-carrard.ch

Dr. Cornelia Stengel
cornelia.stengel@kellerhals-carrard.ch