

Rundschreiben Nr. 10S/2018

Bestimmt für: Geschäftsleitung, Personalverantwortliche

Arbeitgeberpolitik

Kareen Vaisbrot

Pfingstweidstrasse 102
Postfach
CH-8037 Zürich
Tel. +41 44 384 41 11

k.vaisbrot@swissmem.ch
www.swissmem.ch

Zürich, 5. Juni 2018

Information zur neuen EU-Datenschutzgrundverordnung (DSGVO)

Sehr geehrte Damen und Herren

Gerne informieren wir Sie zur Datenschutz-Grundverordnung (DSGVO) der EU, welche ab dem 25. Mai 2018 anzuwenden ist.

Dieses Rundschreiben vermittelt einen Überblick über die Änderungen, welche das neue Datenschutzrecht in der EU mit sich bringt, und fasst für die Unternehmen der MEM-Branche die wichtigsten Punkte nochmals zusammen:

Ist die DSGVO überhaupt für Schweizer Unternehmen relevant?

In erster Linie unterstehen Unternehmen mit Sitz in der EU dieser Verordnung. Unternehmen mit Sitz ausserhalb der EU fallen auch unter die DSGVO, wenn sie im Zusammenhang mit dem Anbieten von Waren und Dienstleistungen in der EU Daten von Kunden bearbeiten, die ihren Sitz im EU-Raum haben. Es ist daher davon auszugehen, dass die grosse Mehrheit der Unternehmen in der Schweiz in den Anwendungsbereich der DSGVO fällt.

Die Schweizer MEM-Unternehmen produzieren im und/oder exportieren in den EU-Raum. Produkte werden zunehmend auch über Online-Shops vertrieben. Wenn sich zum Beispiel die Liefer- und Zahlungskonditionen an Personen im EU-Raum richten oder wenn Sie regelmässig einen Newsletter an Personen mit Sitz in der EU versenden, dann fällt Ihr Unternehmen in den Geltungsbereich der neuen DSGVO.

Was müssen die Unternehmen also in Zukunft beachten?

Daten

Die DSGVO schützt personenbezogene Daten. Das sind Daten, welche sich auf eine natürliche Person beziehen. Daten von juristischen Personen fallen nicht darunter.

Weitergabe von Daten an Dritte

Grundsätzlich sind Sie darauf angewiesen, das explizite Einverständnis Ihres Kunden zu haben, dass seine Daten an Dritte (z.B. andere Konzerngesellschaft oder wenn Daten extern gehostet werden) weitergegeben werden können. Dies kann z.B. bei einer Anmeldung zum Newsletter oder beim Kauf eines Produkts durch die explizite Zustimmung des Kunden erfolgen. Hervorzuheben ist, dass auch eigene Konzerngesellschaften als Dritte gelten und folglich auch bei der konzerninternen Weitergabe von Daten die Regeln der DSGVO eingehalten werden müssen.

Eine Weitergabe der Personendaten ohne explizite Zustimmung und Wissen des Kunden an Dritte stellt einen Verstoß gegen die DSGVO dar und kann mit hohen Bussen sanktioniert werden. Bitte bedenken Sie, dass Mitarbeitende oftmals Daten weitergeben, ohne sich darüber bewusst zu sein, dass im Einzelfall eine solche Zustimmung des Kunden fehlt.

Voraussetzung für die Datenübermittlung ins Ausland

Ohne weiteres ist ein Transfer möglich, wenn im anderen Land ein angemessener Datenschutz besteht. Neben den EU-Staaten und der Schweiz haben aus der Sicht der EU nur wenige andere Ländern einen gleichwertigen Datenschutz.

Datensammlung in CRM

Die Sammlung, Verarbeitung und Nutzung von Kundendaten gehört zum Alltag eines Unternehmens. Die Speicherung dieser Daten im CRM-Tool muss transparent kommuniziert werden und die Daten dürfen nur so lange behalten werden, wie sie für den vorgesehenen Zweck notwendig sind. Daten, die Sie aktuell und künftig nicht mehr benötigen, sollten daher regelmässig gelöscht werden.

Innerhalb der IT-Infrastruktur ergeben sich unzählige Schnittstellen zwischen den CRM-Tools und anderen Tools. Diese können in den Bereichen Logistik, Kommunikation, Marketing, Produktentwicklung angesiedelt sein, welche ebenfalls Personendaten der Kunden verarbeiten und erfassen. Besonders bei der Weiterverwendung dieser Daten für Marketing und Kommunikationszwecke sollte man Vorsicht walten lassen. Im Hinblick auf die DSGVO sind die Datenflüsse klar zu analysieren, Schnittstellen wo möglich zu reduzieren und allenfalls mit einem Spezialisten zu klären.

Newsletter

Ein Newsletter gehört heute in beinahe allen Unternehmen zum Standard. Mit Inkrafttreten der DSGVO ändert sich auch hier einiges. So reicht das heute normalerweise verwendete Anmeldeverfahren via Onlineformular oder ähnlichem nicht mehr aus. Zur datenschutzkonformen Anmeldung wird nun ein sogenanntes «Double-Opt-in» verlangt. Nach der Anmeldung muss der neue Adressat dem Erhalt des Newsletters durch einen Bestätigungslink via Email zustimmen. Damit wird sichergestellt, dass die Identität und persönliche Zustimmung nochmals bestätigt wird.

Müssen bestehende Abonnenten nochmals zustimmen?

Die Bestimmungen der DSGVO kommen ebenfalls bei bereits bestehenden E-Mail Listen zur Anwendung. Deshalb sind die bereits bestehenden E-Mail Listen bezüglich ihrer Weiterverwendung zu überprüfen. Sofern Sie über eindeutige Aufzeichnungen der Zustimmung der Adressaten verfügen, können die E-Mail-Adressen weiter verwendet werden. Wenn nicht, dann sind Sie als Versender verpflichtet, eine neue und ausdrückliche Erlaubnis einholen, bevor Sie einen Newsletter oder andere Marketing-Kampagnen per Mail an Ihre bestehenden Kontakte senden dürfen.

Datenschutzbeauftragter, Vertreter in der EU, Datenschutz-Folgeabschätzung

Die DSGVO schreibt unter gewissen Umständen den Unternehmen vor, einen Datenschutzbeauftragten (DSB) zu benennen. Es gilt deshalb zu ermitteln, ob Sie von dieser Regelung betroffen sind. Trifft eines der nachfolgenden Kriterien zu, ist ein DSB notwendig und zu benennen:

- Die Verarbeitung personenbezogener Daten stellt eine Kerntätigkeit des Unternehmens dar und/oder erfordert eine umfangreiche regelmässige und systematische Überwachung der betroffenen Personen; oder
- Verarbeitung besonderer Kategorien personenbezogener Daten (z.B. Gesundheitsdaten, ethische Herkunft usw.) oder personenbezogene Daten über strafrechtlicher Verurteilungen und Straftaten stellt eine Kerntätigkeit der Organisation dar.

Bitte prüfen Sie, sofern Sie sensible Daten bearbeiten, ob Sie einen Datenschutzbeauftragten in ihrem Unternehmen benötigen.

Eine Datenschutz-Folgenabschätzung (DSFA) ist immer dann durchzuführen, wenn besonders sensible Daten verarbeitet werden oder die Datenverarbeitung dazu bestimmt war, die Persönlichkeit des Betroffenen, einschließlich seiner Fähigkeiten, Leistungen oder seines Verhaltens zu bewerten. In diesen Fällen prüft der Datenschutzbeauftragte die dem Verfahren innewohnenden besonderen Risiken für die Rechte und Freiheiten des Betroffenen. Am Ende dieser Prüfung gibt er eine Stellungnahme zur Rechtmässigkeit der Datenverarbeitung ab und bewertet die Risiken und deren mögliche Folgen für die persönlichen Rechte und Freiheiten der Betroffenen.

Vertreter in der EU

Unternehmen, die in Europa keine Niederlassung unterhalten, aber europäischen Bürgern Waren oder Dienstleistungen anbieten oder «Tracking» bzw. «Profiling» in Europa vornehmen, müssen gemäss Art. 27 Abs. 1 DSGVO einen EU-Vertreter bestellen. Art. 27 Abs. 2 lit. b DSGVO sieht Ausnahmen von der Verpflichtung zur Bestellung eines Vertreters vor, wenn die Datenverarbeitung:

- nur «gelegentlich» erfolgt und
- nicht in grösserem Umfang sensitive Daten gemäß Art. 9 Abs. 1 DSGVO und Art. 10 DSGVO umfasst und
- Risiken für die Rechte und Pflichten einzelner Bürger unter Berücksichtigung der Art, der Umstände, des Umfangs und des Zwecks der Datenverarbeitung unwahrscheinlich erscheinen.

Sammeln von Personendaten auf Ihrer Webseite

Personendaten werden oftmals für Marketingaktivitäten gesammelt, damit Produkte oder Dienstleistungen gezielter an die entsprechende Zielgruppe gerichtet werden können. Die Daten werden via Cookies über die Webseite gesammelt sowie im Google Analytics oder anderen Tools erfasst und später analysiert. Geo- und Retargeting sind hier die Stichworte. In diesem Zusammenhang gilt es zu beachten, dass Cookies auf der Webseite offen gegenüber den Besuchern kommuniziert werden müssen. Der Nutzer muss via Opt-in explizit zustimmen oder ablehnen. Es gilt auch hier der allgemeine Grundsatz, nur die Daten zu sammeln, die Sie für den Verwendungszweck wirklich benötigen.

Selfassessment

Seit einigen Wochen steht allen Interessierten ein Self-Assessment-Tools (DSAT) zur Verfügung. Es kann heruntergeladen werden und ist kostenlos. Dieses Tool hilft Unternehmen in der Schweiz (und anderswo), sich auf die DSGVO und das revidierte DSG (Basis: Entwurf des Bundesrats) vorzubereiten. Die Fragebögen und Tools werfen die relevanten Punkte zur Beurteilung der Rechtmässigkeit nicht nur auf, sondern geben mögliche Antworten vor und weisen auf mögliche Massnahmen hin.

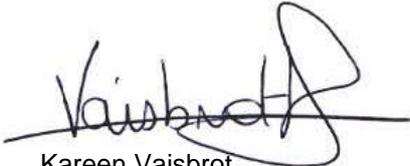
<http://www.dsat.ch>.

Weitere Informationen und Arbeitshilfen finden Sie unter:

economiesuisse «fitcheck» für Unternehmen: <http://www.economiesuisse.ch/de/datenschutz-online-check> oder: https://www.privacyofficers.at/Privacyofficers_Checkliste_Umsetzung_DSGVO_v2.0.pdf

Bei Fragen steht Ihnen Herr Claudio Haufgartner (044 384 42 26; c.haufgartner@swissmem.ch) gerne zur Verfügung.

Mit freundlichen Grüßen



Kareen Vaisbrot
Mitglied der Geschäftsleitung



Claudio Haufgartner
Ressortleiter Arbeitgeberpolitik