Neue EU Datenschutz-Grundverordnung und deren Auswirkungen auf Schweizer Unternehmen

Liebe Advantis Kunden

Am 27. April 2016 wurde die neue EU-DSGVO verabschiedet. Die zweijährige Übergangsfrist zur Umsetzung ist bald abgelaufen. Ab dem 25. Mai 2018 tritt die Datenschutz-Grundverordnung (DSGVO) in der gesamten EU in Kraft. Ab diesem Zeitpunkt gilt dieses einheitliche Datenschutzrecht für alle EU-Mitgliedstaaten.

Die EU-DSGVO ist aber nicht nur in den EU-Staaten anwendbar, sondern gilt für alle Unternehmen weltweit, die Waren oder Dienstleistungen an Personen in der EU anbieten oder das Verhalten von Personen in der EU analysieren. Daher können auch Sie als Schweizer Unternehmen davon betroffen sein!

In diesem Fachartikel fassen wir die wichtigsten Informationen zur neuen EU-DSGVO zusammen, zeigen Ihnen die möglichen Konsequenzen als Schweizer Unternehmen auf und präsentieren Ihnen gezielte Lösungsvorschläge.

Advantis Versicherungsberatung AG

Übersicht der wichtigsten Neuerungen durch die EU-DSGVO

Wer untersteht der neuen EU-DSGVO?

Die EU-DSGVO gilt für sämtliche personenbezogenen, identifizierbaren Daten von **Personen mit festem Wohnsitz in der EU**. Alle Unternehmen, die personenbezogene Daten kontrollieren oder verarbeiten (auch im Auftrag eines dritten Unternehmens), müssen die EU-DSGVO befolgen. Wie den verschiedenen Fachbeiträgen von Anwälten entnommen werden kann, betrifft dies auch viele Unternehmungen, welche ausserhalb der EU domiziliert sind. Dabei wird nicht zwischen dem Volumen der Datenbearbeitung oder der Art der bearbeiteten Personendaten unterschieden.

Von dieser Pflicht sind Unternehmen mit weniger als 250 Mitarbeiter und/oder die nur gelegentlich Personendaten bearbeiten grundsätzlich befreit, es sei denn, die Bearbeitung birgt erhebliche Risiken oder betrifft sensible Personendaten.

Nicht vom Schutz der EU-DSGVO erfasst werden die Daten von juristischen Personen. Zudem fällt die Datenbearbeitung im Rahmen von privaten oder familiären Tätigkeiten nicht in den Anwendungsbereich der EU-DSGVO.

Die nachfolgenden, ausgewählten Beispiele sollen einen guten Eindruck der Anforderungen der EU-DSGVO vermitteln, die Liste ist aber nicht abschliessend zu betrachten.

Informationspflicht und Einwilligung

Neu müssen die betroffenen Personen über die Datenbearbeitung informiert werden. Die Information muss «in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren Sprache» erfolgen. Das Unternehmen muss eine verantwortliche Person (Datenschutzbeauftragter) bestimmen. Diese muss den betroffenen Personen unter anderem seine Identität und Kontaktangaben mitteilen, aber auch den Zweck und die Rechtsgrundlage der Datennutzung, die Empfänger der Daten und die Dauer der Speicherung.

Die betroffene Person hat das Recht, vom Datenschutzbeauftragten des Unternehmens eine Bestätigung zu verlangen, dass ihre personenbezogenen Daten bearbeitet werden bzw. dass keine Daten bearbeitet werden. Im Fall einer Datenverwendung hat sie das Recht, Zugang zu diesen Daten zu erhalten.

Die betroffenen Personen müssen zukünftig Ihre Einwilligung freiwillig und unmissverständlich für jeden Einzelfall abgeben. Die Zustimmung hat «in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erfolgen». Eine stillschweigende Einwilligung (z.B. mittels bereits angekreuzte Kästchen) genügt nicht mehr. Die Zustimmung kann zudem jederzeit widerrufen werden.

Recht auf Löschung („Recht auf Vergessenwerden“)

Ähnlich wie im Schweizer Recht, haben die betroffenen Personen das Recht, eine schnellstmögliche Löschung ihrer Daten zu verlangen. Wurden die Daten an eine dritte Stelle übermittelt, so greift das „Recht auf Vergessenwerden“: Der Verantwortliche muss alle geeigneten Massnahmen treffen, um die involvierten Dritte davon in Kenntnis zu setzen, dass die Person die Löschung aller Verbindungen zu ihren persönlichen Daten bzw. die Löschung sämtlicher Kopien oder Reproduktionen dieser Daten verlangt hat.

Datenübertragbarkeit

Die betroffenen Personen haben das Recht, die Daten, die sie einem Unternehmen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten um diese einem anderen Verantwortlichen zu übermitteln, beispielsweise um den Dienstleistungsanbieter zu wechseln.

«Privacy by Design» und «Privacy by Default»

Des Weiteren gelten die nachfolgenden Grundsätze:

Der Grundsatz «Privacy by Design» beschreibt ausdrücklich, dass Datenverarbeitungssysteme von Beginn an das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte von Personen verringern und vorbeugen müssen (Datenschutz durch Technik), wie zum Beispiel eine regelmässige Löschung von Daten oder eine standardmässige Anonymisierung.

Der Grundsatz «Privacy by Default» bedeutet, dass das Unternehmen 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 dazu ein Benutzerprofil erstellt werden muss (Datenschutz durch datenschutzfreundliche Voreinstellungen).

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 diese Analyse ergibt, dass eine Datenverarbeitung ohne Massnahmen ein hohes Risiko darstellen, muss die Aufsichtsbehörde konsultiert werden.

Ernennung eines Vertreters in der EU

Untersteht eine Firma der EU-DSGVO und hat diese keine Niederlassung in der EU, besteht neu eine Pflicht zur Ernennung eines Vertreters mit Sitz in der EU. Von dieser Pflicht ausgeschlossen sind Unternehmen, die nur gelegentlich und keine umfangreiche Datenverarbeitung von EU ansässigen Personen vornehmen.

Meldung von Sicherheitslücken

Wird der Schutz von Personendaten verletzt, müssen Sie unverzüglich die zuständige Aufsichtsbehörde benachrichtigen. Unverzüglich bedeutet in diesem Kontext spätestens innert 72 Stunden nach Feststellung der Sicherheitslücke. Cyberangriffe müssen ohne Ausnahme den entsprechenden Behörden gemeldet werden.

Darauf kann einzig verzichtet werden, sofern kein Risiko für die Rechte und Freiheiten der betroffenen Personen besteht. Sollte die Datenschutzverletzung hingegen ein hohes Risiko darstellen, so müssen die Personen unverzüglich und in einfacher Sprache benachrichtigt werden.

Folgen durch Datenschutzverstössen

Bei einem Verstoss der EU-DSVGO können Bussen von bis zu 20 Millionen Euro, respektive 4% des weltweiten Umsatzes ausgesprochen werden, je nachdem, welcher Wert der höhere ist.

Die zivilrechtliche Haftung für Schadenersatz wird zudem zukünftig strenger ausgelegt, da die EU-DSGVO neu ausdrücklich eine Haftung auch für den immateriellen Schaden vorsieht.

Folgen für Schweizer Unternehmen

Die oben dargestellten Richtlinien über die Pflichten aus der EU-DSGVO für die Unternehmen 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. Im Wesentlichen kommen folgende Fragen auf Sie zu:

- Unabhängig von der Grösse Ihres Unternehmens, sind Sie von der EU-DSGVO betroffen?
- Wenn ja…
- Entsprechen Ihre Prozesse den Anforderungen der EU-DSGVO?
- Haben Sie ein Konzept erarbeitet, das die Löschung von personenbezogenen Daten über sämtliche IT-Systeme hinweg sowie ggf. auch auf Systemen bei Drittanbietern ermöglicht?
- Sind Sie in der Lage, Datenschutzverletzungen aufzudecken und binnen 72 Stunden mit den benötigten Informationen an die Aufsichtsbehörde zu übermitteln?
- Sind Sie in der Lage, auf Anfrage betroffener Personen bspw. deren Daten in einem strukturierten und maschinenlesbaren Format an Dritte weiterzugeben?
- Genügen Ihre Vorlagen zur Einholung von Einwilligungen betroffener Personen den Transparenzvorschriften?
- Sind Sie in der Lage, den verschärften Auskunftspflichten nachzukommen und Anfragen fristgerecht zu beantworten?

Was müssen Sie als Unternehmen konkret unternehmen?

Wir empfehlen folgende Vorgehensweise:

1

Bestandsaufnahme

- Ist Ihr Unternehmen von der EU-DSGVO betroffen
- Prozesse, in denen personenbezogene Daten verarbeitet werden
- Verträge mit datenschutzrelevanten Inhalten
- Datenschutzrelevante Dokumente der Organisation (AGBs, Einwilligungen, Datenschutzerklärungen)

2

Analyse

- Prüfung der Datenschutzorganisation auf Konformität zur EU-DSGVO und allfällige Lücken

3

Planung

- Evaluierung fehlender Anforderungen
- Priorisierung der ausstehenden Tätigkeiten anhand drohender Sanktionen
- Benennung eines Datenbeauftragten und/oder eines Vertreters in der EU
- Projekt aufsetzen um EU-DSGVO Konformität zu erreichen

4

Durchführung

- Implementierung und Dokumentation der Datenbearbeitungen
- Überprüfung und Definition von internen Prozessen zur Sicherstellung der Rechte der Betroffenen
- Überarbeitung datenschutzrelevanter Dokumente (AGBs, Einwilligungen, Verträge)
- Anpassung der technischen und organisatorischen Prozesse

5

Revision

- Überprüfung der Umsetzung von Massnahmen in internen Audits
- Überprüfung des Ablaufplans bei Verletzungen des Datenschutzes
- Überprüfung von Auftragsverarbeitern und Dienstleistern durch externe Audits
- Erstellung eines Abschlussberichts zur Dokumentation der Umsetzung und Überprüfung

Folgende Pflichten müssen Sie ab dem 25. Mai 2018 erfüllen:

1. Informationen bereitstellen und Einwilligung der Person einholen, deren Daten verarbeitet werden
2. «Privacy by Design» und «Privacy by Default» einhalten
3. Ein Verzeichnis der Verarbeitungstätigkeiten erstellen
4. Verletzungen des Datenschutzes unverzüglich an die Aufsichtsbehörde melden
5. Eine Datenschutz-Folgenabschätzung durchführen

Aufzählung nicht abschliessend.

Fazit:

Sollte Ihr Unternehmen unter den Anwendungsbereich fallen, müssen Sie die oben erwähnten Pflichten wahrnehmen, um EU-DSGVO konform zu sein. Wir empfehlen Ihnen, falls noch nicht geschehen, Ihre Datenbearbeitungsprozesse und Datenschutzmassnahmen einer genauen Überprüfung zu unterziehen und mit den notwendigen Vorbereitungsarbeiten unverzüglich zu beginnen.

Für die Unternehmen in der Schweiz, welche die EU-DSGVO nicht umsetzen müssen, bedeutet dies, dass solange die Adaption des Schweizer Datenschutzrechts nicht stattgefunden hat (siehe Box unten), diese Unternehmen vorläufig keinem verschärften Datenschutzrecht unterliegen.

Wenn Sie als Unternehmen die EU-DSGVO Anforderungen angehen, werden Sie Ihre Cybersicherheit automatisch erhöhen bzw. überprüfen müssen. In diesem Zusammenhang drängt sich die ergänzende Versicherung der Cyber Risiken auf. Mehr dazu auch hier:

Advantis Fachartikel Cyber Risiken

Bei Interesse beraten wir Sie diesbezüglich gerne.

Update zum Schweizer Datenschutzrecht

Am 15. September 2017 hat der Bundesrat die Botschaft zur Totalrevision des Bundesgesetztes über den Datenschutz (DSG) und den entsprechenden Gesetzesentwurf vorgelegt.

Die präsentierten Anpassungen haben zum Ziel das DSG zu modernisieren und an die EU-DSGVO anzugleichen. Die freie Datenübermittlung zwischen Schweizer Unternehmen und solchen in der EU soll weiterhin ungehindert möglich sein. Dies ist für die Schweizer Wirtschaft von zentraler Bedeutung. Damit dies gewährleistet bleibt, muss die Schweiz von der EU weiterhin als «Drittstaat mit angemessenem Datenschutzniveau» anerkannt werden.

Zurzeit berät sich das Parlament über den Gesetzesentwurf. Es wird erwartet, dass eine Annäherung an die EU-DSGVO stattfinden wird.

Mai 2018