Neue Datenschutzregelungen betreffen Schweizer Firmen

Nach einer zweijährigen Übergangsfrist tritt am 25. Mai 2018 die europäische Datenschutz-Grundverordnung (DSGVO) in Kraft. Dies kann auch auf Schweizer Unternehmen einschneidende Auswirkungen haben. Indessen hat der Schweizer Bundesrat am 15. September 2017 den überarbeiteten Entwurf des schweizerischen Datenschutzgesetzes veröffentlicht. Mit dem Inkrafttreten wird jedoch frühestens per 1. August 2018 gerechnet.

Was bedeuten diese Gesetzesänderungen für Schweizer Unternehmen und welche Risiken sind damit in Bezug auf die Handhabung, Speicherung und Verarbeitung von Daten verbunden?

Was bedeutet das Inkrafttreten der EU-Verordnung für Unternehmen mit Sitz in der Schweiz?

Durch die ausgedehnte geographische Anwendbarkeit sind nicht nur EU-Unternehmen von der Verordnung betroffen. Sofern Schweizer Unternehmen in der EU ansässigen natürlichen Personen Waren oder Dienstleistungen anbieten oder das Verhalten von natürlichen Personen in der EU nachverfolgen, findet die Verordnung de facto auf sie Anwendung.

Sie gilt zum Beispiel für die Verarbeitung und Speicherung von Daten, die europäischem Recht unterliegen (d.h. personenbezogene Daten von EU-Bürgern), und zwar unabhängig davon, ob die Daten für Marketingzwecke verwendet werden oder nur dazu, um eine bestehende Kundenbeziehung zu erfassen

Einige der EU Regelungen werden jedoch in der Schweiz nicht angewandt, wie zum Beispiel, dass Schweizer Unternehmen Verstösse nicht der zuständigen EU-Verwaltung melden müssen und Verwaltungsmassnahmen und Sanktionen gegen Schweizer Unternehmen nicht unmittelbar durchgesetzt werden können. Es bleibt abzuwarten welchen Einfluss die Regelung bei Verstössen in der Schweiz auf Tochterunternehmen Schweizer Konzerne in der EU haben wird.

Sanktionen beinhalten nicht nur Geldstrafen von bis zu 2% oder 4% des weltweiten Umsatzes, sondern auch die Möglichkeit des dauerhaften Verbots bestimmter Datenverarbeitungsaktivitäten, was in der Praxis bis hin zur Schliessung bestimmter Unternehmen führen könnte.

Aus der Sicht eines Risikomanagers bedeutet das, dass die Durchsetzbarkeit und die Schwere der Massnahmen durch die neue Verordnung in der EU deutlich erhöht werden. International operierende Unternehmen müssen die Einhaltung der Verordnung ab kommendem Mai sicherstellen und gewährleisten, dass die Bestimmungen für die Meldung bei den zuständigen Behörden eingehalten werden können (innerhalb von 72 Stunden). Durch die Identifizierung und die Bewertung der exponierten Vermögenswerte können Unternehmen eine risikobasierte Entscheidung darüber treffen, wie sie das verbleibende finanzielle Risiko kontrollieren und bewältigen.

Fokus auf EU-Datenschutz-Grundverordnung

Bis Mitte der 1990er Jahre waren die Datenschutzgesetze der EU-Mitgliedsstaaten überwiegend nicht harmonisiert. Das bedeutete, dass Unternehmen, die in der EU tätig waren, in Abhängigkeit von den nationalen gesetzlichen Anforderungen an unterschiedliche Compliance-Verpflichtungen gebunden waren.

Mit der 1995 eingeführten Richtlinie 95/46/EG schuf die EU eine weitgehend kohärente Grundlage für die Datenschutzgesetzgebung in den Mitgliedstaaten. Die Richtlinie (wie jede EU-Richtlinie) muss in nationales Recht der Mitgliedsstaaten umgesetzt werden. Obwohl die allgemeinen Grundsätze der Datenschutzgesetzgebung innerhalb der EU ähnlich sind, bestehen daher weiterhin Unterschiede zwischen den Gesetzen der einzelnen Mitgliedsstaaten und somit sind die Unternehmen weiterhin mit widersprüchlichen Anforderungen konfrontiert.

Zudem haben die verschiedenen EU-Mitgliedsstaaten unterschiedliche Ansätze verfolgt, um die Richtlinie umzusetzen und dadurch für viele Unternehmen Compliance-Probleme geschaffen.

Die zwischenzeitliche Weiterentwicklung der Informationstechnologie verursachte wesentliche Veränderungen hinsichtlich der Art und Weise, wie und wie häufig Menschen und Unternehmen kommunizieren und dabei Informationen austauschen. Die Daten selbst sind für viele Unternehmen zu einem immer wichtigeren Vermögenswert geworden. Die immense Datenmenge, die heute routinemässig erhoben und verwendet wird, übersteigt die Vorstellungskraft von 1995 bei Weitem.

Nicht nur das explosionsartige Wachstum von sozialen Netzwerken und die gängigeAnalyse von Big Data verdeutlichten die Tatsache, dass das damals bestehende Gesetz veraltet und dass ein neuer Ansatz für den Datenschutz erforderlich war. Dies führte dazu, dass die Europäische Kommission 2012 einen ersten Entwurf für eine Verordnung veröffentlichte.

Die wichtigsten Veränderungen

Herausforderungen für Unternehmen

- Stärkere Durchsetzungsbefugnisse Wer? Wofür?
- Neue Verpflichtungen für Datenverarbeiter / datenverarbeitende Unternehmen
- Erweiterter räumlicher Geltungsbereich
- Erhalt der Zustimmung von Betroffenenen für die Datenverarbeitung wird schwieriger. Erweiterte Informationspflichten
- Datenschutz durch Technik und datenschutzfreundliche Voreinstellung /
- Strenge Meldevorschriften für Datenschutzverstösse
- Das „Recht, vergessen zu werden“
- Das Recht, dem Profiling zu widersprechen
- Das Recht auf Datenportabilität

Chancen für Unternehmen

- Harmonisierung der Rechtsgrundlagen
- Risikobasierter Compliance-Ansatz
- „One-Stop-Shop“ (zentrale Behördenzuständigkeit)
- Pseudonymisierung

Der Zweck der neuen Verordnung

Der Zweck der Verordnung ist, die Datenschutzbestimmungen innerhalb der EU weiter zu harmonisieren und die Pflichten jener, die personenbezogene Daten nutzen und verarbeiten, auszuweiten und damit die Rechte der Bürger zu stärken. Gleichzeitig werden die neuen technologischen Entwicklungen berücksichtigt.

Die Verordnung wird innerhalb der EU direkt anwendbar sein, ohne dass eine nationale Umsetzung erforderlich ist. Es ist zu erwarten, dass Unternehmen kaum mit nationalen Unterschieden im Hinblick auf die Einhaltung von Datenschutzverpflichtungen konfrontiert sein werden. Es wird jedoch weiterhin Bereiche geben, wo zwischen den einzelnen Mitgliedsstaaten Unterschiede bestehen bzw. der Schutz in einem Mitgliedstaat weiter geht als jener, der durch die Verordnung gewährleistet wird.

Entwurf zur Revision des schweizerischen Datenschutzgesetzes

Während die Verordnung der Europäischen Union am 25. Mai 2018 in Kraft treten wird, hat der Bundesrat einen Entwurf zur Überarbeitung des schweizerischen Datenschutzgesetzes vorgelegt.

In Bezug auf potenzielle neue oder erhöhte Risiken umfasst die derzeitige Version des Entwurfs einige Bestimmungen, die einer sorgfältigen Planung / Vorsorge / Beachtung bedürfen. Der Gesetzesentwurf enthält einen risikobasierten Ansatz, der risikoreiche und risikoarme Aktivitäten unterscheidet. Zudem verpflichtet die Vorlage die verantwortlichen Personen, potenzielle Risiken bezüglich Datenschutzverstössen im Rahmen eines formalisierten Prozesses zu bewerten.

Was sind die nächsten Schritte?

Das EU-Parlament hat am 14. April 2016 der vorgeschlagenen Verordnung mit Mehrheit zugestimmt.. Seit der Veröffentlichung im EU-Amtsblatt besteht eine zweijährige Umsetzungsfrist. Am 25. Mai 2018 läuft dies ab und die Verordnung tritt in Kraft.

Der Datenschutz wird für Unternehmen genauso wie Kartellfragen mit einem erheblichen Compliance-Risiko verbunden sein und kann erhebliche aufsichtsrechtliche Sanktionen nach sich ziehen. Gemäss der Verordnung können es sich Unternehmen im Bereich Datenschutz nicht mehr leisten, sorglos Risiken einzugehen.

Die Verordnung wird in vielen Unternehmen weitgehende Veränderungen erforderlich machen. Es ist ratsam, jetzt damit zu beginnen, die Auswirkungen dieser Veränderungen zu prüfen und auf die Einhaltung der Verordnung hinzuarbeiten. Schon jetzt ist absehbar, dass es eine bestimmte Zeit dauern wird, bis die notwendigen Veränderungen im Unternehmen verankert sind, und es können erhebliche Veränderungen bestehender Prozesse erforderlich werden. In einem ersten Schritt müssen die Unternehmen, eine Bestandsaufnahme ihrer derzeitigen Datenbestände und ihres Compliance-Profils machen und danach systematisch bewerten, wie sich die Verordnung auf die bestehende Compliance auswirken wird.

Für die meisten Unternehmen wird dies ein umfangreiches Projekt sein. Unternehmen in Ländern wie Grossbritannien, die bislang von einer lockeren Datenschutzregelung profitiert haben, werden wohl das meiste tun müssen, um sich auf die neue harmonisierte Datenschutzregelung vorzubereiten.

Weitere Informationen

Bei Fragen wenden Sie sich bitte an Ihren Berater bei Willis Towers Watson oder an:

Samuel Trost
Head FINEX
+4144 804 45 57
samuel.trost@willistowerswatson.com