

Informationsbrief: Datenschutz - Privacy

Sehr geehrte Klienten!

Am 25. Mai 2018 tritt die neue EU-Datenschutzverordnung 2016/679 (GDPR – General Data Protection Regulation) in Kraft: bis dahin müssen alle Unternehmen die neuen Bestimmungen umgesetzt haben. Mit diesen wird das Datenschutzrecht innerhalb Europas vereinheitlicht, um dem Einzelnen mehr Kontrolle über die eigenen Daten zu gewähren. Die Richtlinien ersetzen nicht die bestehenden nationalen Normen, sondern ergänzen diese.

Nachstehend eine Übersicht der wichtigsten Neuerungen:

Der Begriff „personenbezogene Daten“ wird erweitert: dazu zählen nun auch all jene Daten, welche die Identifizierung einer Person oder eine Profilbildung ermöglichen. Es empfiehlt sich daher zunächst zu erheben, welche personenbezogenen Daten im Betrieb erhoben und verarbeitet werden.

Es gilt der Grundsatz der Zweckbindung: die Daten dürfen ausschließlich für den im Vorfeld festgelegten, eindeutigen und legitimen Zweck erhoben werden

Die Verarbeitung der Daten kann weiterhin nur dann stattfinden, wenn der Betroffene seine Einwilligung dazu gibt oder wenn Verträge zu erfüllen sind. Den Betroffenen ist verständlich darzulegen, welche Daten bei welcher Gelegenheit erhoben und verarbeitet werden, wer der Empfänger ist, warum die Daten erhoben werden und vieles mehr. Erstmalig ist in der Einwilligung auch die Dauer anzugeben, für die die personenbezogenen Daten gespeichert werden. Die Einwilligung und alle weiteren Rechtstexte wie Vertragsklauseln, AGBs usw. sind dementsprechend anzupassen.

Den Betroffenen wird nun auch das „Recht auf Vergessen“, d.h. auf Löschung ihrer Daten eingeräumt. Auch dieses Recht ist im Informationsschreiben explizit anzuführen. Dasselbe gilt für das „Recht auf Datenübertragbarkeit“: mit der Datenübertragbarkeit hat der betroffene Bürger das Recht, die ihn selbst betreffenden Daten in einem maschinenlesbaren Format zu erhalten.

Mit welchen technischen und organisatorischen Maßnahmen der Schutz der personenbezogenen Daten gewährleistet wird, ist nicht mehr im Detail vorgegeben. Vielmehr wird es dem Unternehmen selbst überlassen die geeigneten Maßnahmen auszuwählen und umzusetzen. Vorgegeben ist lediglich, dass die Maßnahmen dem Schutzbedürfnis der Daten, dem Stand der Technik und dem bestehenden Risiko angemessen sein müssen.

Der Verantwortliche muss alle geeigneten Schutzmaßnahmen ergreifen und darüber auch Rechenschaft ablegen (Dokumentationspflicht).

Etwaige Haftungsansprüche, auch für moralische Schäden, können vom Betroffenen leichter geltend gemacht werden und die Einhaltung der neuen Regelungen muss daher nachgewiesen werden.

Falls auch ein Datenaustausch mit Partnerunternehmen stattfindet muss sichergestellt werden, dass die Daten über die ganze Verarbeitungskette hinweg den notwendigen Schutz erfahren: im Schadensfall haften nämlich alle Beteiligten.

Eine Datenpanne („Data Breach“), d.h. eine unrechtmäßige oder unbeabsichtigte Verletzung des Schutzes der personenbezogenen Daten wie z.B. ein telematischer Einbruch, eine unbeabsichtigte Verbreitung oder ein Verlust von Daten ist innerhalb von 72 Stunden an die zentralen Aufsichtsbehörden zu melden.

Nach wie vor ist für die Einhaltung der Datenschutzbestimmungen die Ernennung eines „Datenschutzbeauftragten“ (DPO - „Data Protection Officer“) vorgesehen, aber nur mehr für Unternehmen, welche in ihrer Kern-tätigkeit personenbezogene Daten systematisch verarbeiten. Für alle anderen ist die Ernennung des Datenschutzbeauftragten freiwillig.

Empfehlenswert sind für alle Unternehmen nun folgende Schritte:

1. Feststellung und Auswertung aller Prozesse mit personenbezogenen Daten
2. Risikoanalyse der jeweiligen Daten und Fest- und Umsetzung von entsprechenden Sicherheitsmaßnahmen
3. Anpassung der Rechtstexte

Von Seiten einiger Software-Hersteller wird derzeit der Irrglauben verbreitet, dass vor allem die Technik angepasst werden muss. Für die kleineren bis mittleren Betriebe ist es allerdings ausreichend vor allem Dokumente anzulegen bzw. abzuändern. Dies kann auch durch die Firmenleitung passieren.

Außerdem lassen die Aufsichtsbehörden verbreiten, dass die Datenschutzverordnung zwar definitiv mit 25. Mai 2018 in Kraft tritt und es hier keinen Aufschub geben wird, gleichzeitig aber weisen sie darauf hin, dass der Fokus der Kontrollen bei den großen Strukturen liegen wird.

Meran, den 16.05.2018

Mit freundlichen Grüßen

Kanzlei König:Skocir:Kiem