Datenschutzrecht

Die neue EU-Datenschutz-Grundverordnung (DSGVO) – Was ist zu tun?

Seit dem 25. Mai 2018 gilt die neue Datenschutz-Grundverordnung der EU. Sie regelt den Umgang von Unternehmen mit personenbezogenen Daten. Das neue Recht ist global anwendbar und gilt für alle Unternehmen, die Waren und Dienstleistungen an Personen in der EU anbieten oder das Verhalten von Personen in der EU analysieren („Tracking" bzw. „Profiling"). Darunter fallen sowohl kostenpflichtige Produkte als auch Angebote, für die nicht bezahlt werden muss, wie z.B. das Versenden eines kostenlosen E-Books oder Newsletters. Das neue Recht gilt somit nicht nur für Unternehmen mit Niederlassung in der EU, sondern auch für Schweizer Unternehmen. Im Vergleich zum heutigen Schweizer Recht bringt die DSGVO unter anderem die folgenden wichtigen Neuerungen.

Information
Die betroffene Person ist zum Zeitpunkt der Erhebung personenbezogener Daten (z.B. Name, Geburtsdatum, Alter, Email-Adresse etc.) über die Datenbearbeitung zu informieren. Die Information hat in „präziser, transparenter, verständlicher und leicht zugänglicher Form, in einer klaren und einfachen Sprache" zu erfolgen. Dabei sollen sowohl der Zweck und die Rechtsgrundlage der Bearbeitung dargelegt werden als auch die berechtigten Interessen, auf welche sich der Verarbeiter stützt. Weiter sind die Empfänger der Daten, die Dauer der Speicherung sowie die Rechte der betroffenen Person anzugeben.

Einwilligung
Die Form der Einwilligung der betroffenen Person zur Datenbearbeitung untersteht den gleichen Anforderungen wie die erwähnte Information. Die blosse Untätigkeit, Stillschweigen oder bereits angekreuzte Kästchen stellen keine Einwilligung dar. Zudem ist die Einwilligung jederzeit widerrufbar.
Ab dem 16. Altersjahr dürfen Jugendliche die Einwilligung bei Online-Angeboten selbst erteilen. Die einzelnen Mitgliedstaaten der EU können das Mindestalter jedoch bis auf 13 Jahre reduzieren. Für Kinder unter dem Mindestalter ist die Erlaubnis der Eltern einzuholen, wobei dies technisch sicherzustellen ist.

Data Breach
Bei Verletzung des Schutzes personenbezogener Daten oder bei der Entdeckung von Sicherheitslücken sind diese Tatsachen der Aufsichtsbehörde zu melden. Könnte die Verletzung Risiken für die Rechte und Freiheiten von Personen zur Folge haben, muss der Verantwortliche bzw. das Unternehmen dies der Aufsichtsbehörde innerhalb von 72 Stunden melden. Unternehmen mit Niederlassung in der Schweiz, die von der DSGVO betroffen sind, müssen die Mitteilung an die zuständige Aufsichtsbehörde jedes einzelnen Mitgliedstaates machen, in dem Personen von der Verletzung betroffen sind.

Bei der Entdeckung einer möglichen Datenschutzverletzung, z.B. wenn Fremde in ein unternehmensinternes IT-System eingedrungen sind und Personendaten entwendet haben könnten, sind die möglicherweise betroffenen Personen zu informieren, wenn ein hohes Risiko für deren Rechte und Freiheiten besteht.

Datenverarbeitung durch Dritte
Fast alle Unternehmen nutzen die Unterstützung von Drittfirmen in ihrer Geschäftstätigkeit – von der Unterhaltsreinigung bis hin zum Outsourcing wesentlicher Unternehmensfunktionen wie z.B. bei einem Online-Shop die Konfektionierung und Auslieferung der Waren an Dritte wie Amazon & Co. Hier muss das Unternehmen sicherstellen, dass nicht nur das Unternehmen selber, sondern auch der Dritte personenbezogene Daten von Kunden nur in Übereinstimmung mit der DSGVO bearbeitet. Kurz gesagt, müssen von Auftragsbearbeitern sogenannte Konformitätsbescheinigungen eingeholt werden.

Datensicherheit
Datenschutz hat auch eine technische Seite in Sachen Sicherheit: Unternehmen müssen sicherstellen, dass Personendaten durch technische und organisatorische Möglichkeiten angemessen und ausreichend geschützt sind. Dies reicht von Zutrittsregelungen in Räume mit Personendaten über Passwort- und Zugriffsregelungen bis hin zum Backup.

Datenschutzbeauftragter
Die Ernennung eines Datenschutzbeauftragten ist für die meisten Unternehmen nicht zwingend. Eine Pflicht zur Ernennung eines Datenschutzbeauftragten gibt es nur für Unternehmen, deren Kerntätigkeit mit der systematischen Bearbeitung von Personendaten verbunden ist, wenn die Art, der Umfang oder der Zweck eine Anleitung und Überwachung der Mitarbeiter erfordern (z.B. Patientendaten eines Krankenhauses oder einer Arztpraxis). Bei Auftragsbearbeitern wie IT-Firmen, welche das Outsourcing von IT-Prozessen für Kunden anbieten, dürfte dies z.B. der Fall sein. Sodann besteht die Pflicht zur Benennung eines Datenschutzbeauftragten für Unternehmen, welche sensible Datenbearbeitungsvorgänge durchführen. Unternehmensgruppen können einen gemeinsamen Datenschutzbeauftragten wählen.

Benennung eines Vertreters
Unternehmen ohne Niederlassung in der EU, für welche die DSGVO gilt, müssen schriftlich einen Vertreter benennen. Der Vertreter muss in einem Mitgliedstaat ansässig sein, in dem die betroffenen Personen ihren Wohnsitz haben, deren personenbezogene Daten bearbeitet werden. Der Vertreter dient als Kontaktperson bzw. Anlaufstelle für die Aufsichtsbehörden und auch für die betroffenen Personen selbst. Die Verantwortung der Datenbearbeitung trägt jedoch weiterhin das Unternehmen.

Privacy by Design und Privacy by Default
Neu müssen die Grundsätze des Datenschutzes schon bei der technischen Ausgestaltung von Arbeitsabläufen und internen Prozessen berücksichtigt werden, z.B. durch Pseudonymisierung und Minimierung der bearbeiteten Daten (Privacy by Design). Zudem sind die Produkte und Dienstleistungen mit datenschutzfreundlichen Voreinstellungen anzubieten (Privacy by Default).

Datenschutz-Folgenabschätzung
Besteht ein hohes Risiko bei der Bearbeitung von Daten für Betroffene, muss neu eine Datenschutz-Folgenabschätzung (Privacy Impact Assessment, PIA) durchgeführt werden. Führt die Voranalyse zur Identifizierung spezifischer Risiken, so hat der Verantwortliche vor der Bearbeitung die Datenschutzbehörde bzw. den Datenschutzbeauftragten zu konsultieren.

Rechenschaftspflicht / „Accountability“
Der Bearbeiter von Personendaten ist für die Einhaltung der allgemeinen Grundsätze der Datenbearbeitung verantwortlich und muss auch nachweisen können, dass er diese einhält. Unternehmen werden somit gezwungen, ihre Verarbeitungsvorgänge zu dokumentieren. Dies erhöht für viele Unternehmen den Compliance-Aufwand beträchtlich.

Recht auf Vergessenwerden
Allen von einer Datenbearbeitung betroffenen Personen steht das Recht zu, die Löschung ihrer Daten zu verlangen. Datenverarbeitende Unternehmen müssen solche Daten in der Folge unverzüglich löschen, wenn nicht zwingende Gründe (Aufbewahrungsvorschriften bezüglich Geschäftsunterlagen, Buchhaltungsunterlagen, steuerliche Aufbewahrungspflichten, Dokumentationspflichten zur Rechtfertigung des eigenen Handelns oder zur Abwendung möglicher Haftpflichtansprüche etc.) entgegenstehen.

Unsere Empfehlungen
Überprüfen Sie, ob Sie von der DSGVO betroffen sind und, wenn ja, welche Massnahmen (rechtlich, organisatorisch und technisch) zur Umsetzung erforderlich sind.

Sollten Sie Fragen haben bzw. eine auf Ihre persönlichen Umstände bezogene Beratung wünschen, unterstützt Sie die BRUHIN KLASS AG gerne.

BRUHIN KLASS
Mit Recht

Baarerstrasse 12
Postfach
6302 Zug
Tel. +41 41 727 70 80

Dr. Stefan Klass
Rechtsanwalt und Notar
klass@bruhinklass.ch

Dr. Roland Bruhin
Rechtsanwalt und Notar
bruhin@bruhinklass.ch