Georg Streit - Markus Dörfler
27.02.2018

Ist Ihr Unternehmen DSGVO-fit?

Nur noch drei Monate bis zum neuen Datenschutzrecht. Für Unternehmen, die sich damit noch nicht beschäftigt haben, wird es höchste Zeit. Herausgeber Mag. Georg Streit und Mag. Markus Dörfler zeigen auf, welche Punkte besonders kritisch sind.

Nach jahrelangem zähem Ringen auf höchster politischer Ebene konnte sich die Europäische Union im Mai 2016 auf ein neues Datenschutzrecht in Form der neue Datenschutz-Grundverordnung (DSGVO) einigen. Diese ist am 24.5. – weitestgehend unbemerkt – in Kraft getreten. Das „Unbemerktsein" war wohl auf Art 99 (2) zurückzuführen, der den Geltungsbeginn der DSGVO mit 25.5.2018 festlegt, weshalb die neuen Regeln erst ab diesem Zeitpunkt angewendet werden müssen. Auch der österreichische Gesetzgeber wartete über ein Jahr zu, bevor er darauf reagierte. Aber immerhin gibt es schon seit dem 31. Juli 2017 ein Bundesgesetz, mit dem das (bestehende) Datenschutzgesetz 2000 geändert wird (Datenschutz-Anpassungsgesetz 2018). Dieses Gesetz regelt – knapp zusammengefasst – die Umsetzung der DSGVO in Österreich durch Adaptierung des DSG 2000, das ab dem 25.5.2018 nun nur noch Datenschutzgesetz – DSG lauten wird. Aber auch – und insbesondere für Unternehmen ist dieser Stichtag relevant, denn dann müssen zahlreiche datenschutzrechtliche Prozesse bereits an die neue Rechtslage angepasst sein (widrigenfalls rigide Strafen drohen).

Wen betrifft die Datenschutzgrundverordnung?

Grundsätzlich muss die Datenschutzgrundverordnung von jeder natürlichen oder juristischen Person, Behörde, Einrichtung oder anderen Stelle, die personenbezogene Daten verarbeitet, eingehalten werden. Personenbezogene Daten liegen vor, wenn eine natürliche Person identifiziert oder identifizierbar ist. Identifizierbar ist eine natürliche Person dann, wenn sie aufgrund einer Kennung, Standortdaten, einer Online-Kennung oder anderen Merkmalen identifiziert werden kann. Zusammengefasst bedeutet das, dass **faktisch jedes Unternehmen** die Datenschutzgrundverordnung anwenden muss, da faktisch jedes Unternehmen Daten über natürliche Personen verarbeiten wird.

Datenverarbeitung neu

Schon bisher dürfen personenbezogene Daten nur verarbeitet (dazu gehört auch bereits das Erheben und Speichern der Daten) werden, wenn die Verarbeitung für einen konkreten legitimen Zweck erfolgt. Neben diesem konkreten Zweck der Datenverarbeitung müssen aber nun auch noch andere Qualitätsgrundsätze eingehalten werden. Bisher war es ausreichend, dass die Verarbeitung nach Treu und Glauben, für einen gewissen Zweck, in möglichst geringem Umfang, richtig, für einen begrenzten Zeitraum und sicher erfolgt. In Hinkunft muss die Verarbeitung auch transparent erfolgen. Das bedeutet, dass die jeweils betroffene Person über den Verarbeitungsvorgang vom jeweiligen Verantwortlichen (demjenigen, der entscheidet, dass und wie die Daten verarbeitet werden) **gegenüber dem Betroffenen offen legen muss, wie er die Daten verarbeitet,** die betroffene Person muss über den Verarbeitungsvorgang informiert werden. Bereits diese Änderung der rechtlichen Grundlagen führt dazu, dass Unternehmen ihre Prozesse an die neuen rechtlichen Gegebenheiten anpassen müssen.

Die Neuerungen gehen aber noch weiter: Schon bisher war es für eine wirksame Zustimmung zur Datenverarbeitung notwendig, dass der jeweilige Betroffene die Erklärung gültig, ohne Zwang und in Kenntnis der Sachlage erklärt, dass seine Daten verarbeitet werden dürfen. Dies wird durch die DSGVO weiter verschärft. Ab dem 25.5.2018 wird es **zwingend notwendig sein, dass der Verantwortliche den Nachweis erbringt, dass er tatsächlich eine wirksame Zustimmungserklärung eingeholt** hat – das gilt auch für bereits vor dem 25.5.2018 erteilte Zustimmungen. Alle Einwilligungen, die nicht den neuen Bestimmungen entsprechen, **werden ungültig**.

Darüber hinaus wird in Zukunft **auch die Verarbeitung von „besonderen Kategorien" von Daten** (bisher: sensible Daten) verschärft. Zu den besonderen Kategorien von Daten zählen Informationen, die besonders schutzwürdig sind, also solche über die rassische und ethnische Herkunft, politische Meinung, religiöse und weltanschauliche Überzeugung, eine allfällige Gewerkschaftszugehörigkeit, Gesundheitsdaten sowie Daten zur sexuellen Orientierung und zum Sexualleben. Aber auch genetische und biometrische Daten fallen nunmehr unter die „besonderen Kategorien" von Daten. Die **Verarbeitung dieser Daten ist unzulässig**, außer es gibt **konkrete, im Gesetz genannte Gründe**, welche die Verarbeitung erlauben.

Auskunftsrecht und Datenaktualisierung neu

Schon bisher gab es ein **Auskunftsrecht** des jeweiligen Betroffenen, mit dem er bei Verantwortlichen erfragen konnte, welche Daten über ihn verarbeitet werden. Wie schon bisher ist diese Auskunft einmal im Jahr kostenlos. In Hinkunft dauert die Frist statt acht Wochen nur mehr einen Monat, wird also de facto um die Hälfte verkürzt.

Eine weitere große Änderung ergibt sich für Unternehmen auch im Zusammenhang mit der **Aktualisierung von Daten**. Wenn ein Verantwortlicher Daten an einen Dritten weitergibt, ist er verpflichtet den Dritten auch über Änderungen der Daten zu informieren. So soll sichergestellt werden, dass die Datenbestände immer korrekt sind. Noch gravierender wiegt der Umstand, dass der Empfänger der Daten auch über den Umstand informiert werden muss, dass die Daten gelöscht wurden.

Technische Umsetzung

Änderungsbedarf bei Unternehmen herrscht auch im Rahmen der technischen Rahmenbedingungen. So sind die Unternehmer nunmehr verpflichtet, eine Datenübertragbarkeit zu gewährleisten. Der jeweilige Betroffene muss die Möglichkeit haben, die Daten von einem Verantwortlichen zu einem anderen Verantwortlichen mitzunehmen. Dazu muss der jeweilige Verantwortliche technische Schnittstellen implementieren, die die Übertragbarkeit ermöglichen. Datenschutzkonforme Grundeinstellungen runden das Bild ab. Die Datenerhebung muss den Prinzipien privacy by default und privacy by design folgen. Das bedeutet, dass die technische Verarbeitung sowie die Vorgabewerte (Defaultwerte) datenschutzfreundlich gestaltet sein müssen. Beispielsweise darf eine Datensammlung erst beginnen, wenn die betroffene Person eine aktive Handlung setzt. Dies kann etwa durch das Setzen eines Häkchens geschehen. Die Verarbeitung der Daten muss darüber hinaus datenschutzfreundlich sein. Personenbezüge müssen, sofern nicht unbedingt notwendig, gelöscht werden (Pseudonymisierung).

Technische Maßnahmen verpflichten den jeweiligen Verantwortlichen, nicht nur vor unrechtmäßigem Zugriff zu schützen, sondern sie müssen auch sicherstellen, dass die Daten immer verfügbar sind.

Organisatorische Anforderungen

Auf der organisatorischen Seite sind die Änderungen nicht weniger gravierend. Bisher hat der Verantwortliche die Datenverarbeitung bei der Datenschutzbehörde zu melden. Ab dem 25.5.2018 besteht eine Selbstverpflichtung. Der Verantwortliche muss dokumentieren, welche Verarbeitungsvorgänge im Rahmen seines Unternehmens erfolgen. Dazu muss er nicht nur konkret angeben, wo die Daten herkommen, was mit den Daten geschieht und wie lange die Daten gespeichert werden. Er muss auch zu den einzelnen

Datenverarbeitungsvorgängen klar darlegen, welche organisatorischen und technischen Maßnahmen er zum Schutz ergriffen hat.

Unter gewissen Voraussetzungen besteht auch die Verpflichtung, einen Datenschutzbeauftragten zu bestellen, zB dann, wenn die wesentliche Tätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, die eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen (z.B. Banken, Versicherungen, Kreditauskunfteien und Berufsdetektive) oder in der umfangreichen Verarbeitung sensibler Daten oder von Daten über strafrechtliche Verurteilungen oder Straftaten besteht (z.B. Krankenanstalten).

Folgen bei Fehlern

Unangenehm sind naturgemäß bei gesetzlichen Bestimmungen die Folgen, „wenn etwas schief geht". Die Datenschutzgrundverordnung definiert nicht nur sehr genau, wann eine Verletzung stattgefunden hat (bereits dann, wenn ein Dritter theoretisch Zugriff haben konnte), die Konsequenzen, die den jeweiligen Verantwortlichen treffen, sind drakonisch. Nicht nur, dass der jeweilige Verantwortliche **binnen 72 Stunden die Behörde über die Verletzung informieren muss**, der Verantwortliche muss auch einen Prozess implementiert haben, die jeweiligen Betroffenen über die Verletzung zu informieren. Sollte der Aufwand den einzelnen Betroffen zu informieren zu hoch sein, ist der Verantwortliche verpflichtet, die Verletzung zu veröffentlichen.

Wenn der Verantwortliche besonders viele Daten verarbeitet und ein großes Gefährdungspotenzial für die Betroffenen besteht, sollte also durch die Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten von betroffenen Personen bestehen, besteht die Verpflichtung, eine „Datenschutzfolgenabschätzung" zu erstellen. Unter welchen Umständen ein solches Risiko für die „Rechte und Freiheiten" besteht, ist derzeit aber noch offen.

Kontrolliert wird das bei den Verantwortlichen auf zweierlei Arten: Einerseits ist der Verantwortliche selbst verpflichtet – unter gewissen Voraussetzungen – einen Datenschutzbeauftragten zu bestellen, der intern die korrekte Verarbeitung von Daten prüft. Andererseits hat die **Aufsichtsbehörde** ein umfangreiches Recht, nicht nur die ordnungsgemäße Einhaltung zu prüfen, sondern auch jeden Verstoß zu strafen.

Die Strafdrohung ist dabei wahrlich gewaltig, sie beträgt bis zu EUR 20.000.000,00 oder 4 % des weltweiten Jahresumsatzes. Zwar ist für die Zukunft zu erwarten, dass die zuständigen Datenschutzbehörden einen Strafenkatalog erlassen, in dem die jeweiligen Strafen auf die jeweilige Unternehmensgröße angepasst werden, da das Gesetz jedoch vorsieht, dass die Strafen „abschreckend" sein sollen, liegt es wohl im Interesse der Unternehmen, die Datenschutzgrundverordnung ernst zu nehmen.

Fazit

All diese Änderungen führen dazu, dass zwar der datenschutzrechtliche Aufwand im Unternehmen größer wird, sie bieten jedoch auch eine Chance. Unternehmen haben mit den neuen Regeln die (einmalige) Gelegenheit (oder zumindest einen „gegebenen Anlass"), Arbeitsabläufe innerhalb des Unternehmens zu bereinigen und in einer nachvollziehbaren Art und Weise zu definieren. Nutzen Sie diese, wenn Sie nicht ohnedies schon längst DSGVO-fit sind.

Autoren

Mag. Georg Streit

Mag. Georg Streit ist seit 2000 Rechtsanwalt und seit 2001 Partner bei Höhne, In der Maur & Partner Rechtsanwälte. Seine Tätigkeitsschwerpunkte sind Immaterialgüterrecht, Wirtschafts- und Gesellschaftsrecht, Arbeitsrecht, Rundfunkrecht und Vergaberecht. Weiters ist er Lektor an den Universitäten Wien und Salzburg, Vortragender bei Seminaren und Lehrgängen.

Für WEKA ist er Herausgeber des Newsletters für Gesellschaftsrecht Online sowie für das Werk „Personengesellschaften in Fallbeispielen".

Mag. Markus Dörfler

Mag. Markus Dörfler ist Rechtsanwalt und Partner bei Höhne, In der Maur & Partner Rechtsanwälte und ua auf Datenschutzrecht und IT-Recht spezialisiert.

www.h-i-p.at