Wer hat Angst vor dem neuen EU-Datenschutzrecht?

Von Mgr. Bc. Tomáš Mudra

Unternehmen wie Führungskräften drohen hohe Geldbußen

Möglicherweise haben Sie noch nie davon gehört, aber am 4. April 2016 hat das EU-Parlament nach langer Diskussion die Europäische Datenschutz-Grundverordnung (DS-GVO) verabschiedet. Ziel der Verordnung ist es, die Verarbeitung personenbezogener Daten EU-weit einheitlich zu regeln. Ab dem Datum ihrer Veröffentlichung im Amtsblatt, die am 4. Mai 2016 erfolgt ist, läuft damit die Frist von 20 Tagen bis zum Inkrafttreten der DS-GVO in allen EU-Staaten, mithin am 25. Mai 2016. Nach Ablauf einer Übergangsfrist von weiteren zwei Jahren ist die DS-GVO dann ab dem 25. Mai 2018 EU-weit verbindlich. Da der europäische Gesetzgeber die Form der Verordnung und nicht der Richtlinie gewählt hat, wird die DS-GVO unmittelbar und ohne Umsetzung durch nationale Gesetze ab Ende Mai 2018 europaweit, also auch in Tschechien, anwendbar.

Neue Anforderungen an Unternehmen

Das erklärte Ziel der DS-GVO ist es, den Schutz persönlicher Daten von Menschen auf der einen Seite gegenüber deren Verwendung und Bearbeitung durch Unternehmen auf deren anderen Seite auf europaweit möglichst hohem Niveau zu gewährleisten. Das Regelwerk der Verordnung richtet sich daher grundsätzlich an Unternehmen aller Größen, die daher für ihren Geschäftsbetrieb das geforderte Datenschutzniveau bis spätestens zum 25. Mai 2018 herstellen und danach beibehalten müssen. Dies hat der Gesetzgeber nicht leicht gemacht – die DS-GVO hat in ihrer deutschen Fassung über 260 Seiten, über 100 davon entfallen alleine auf die amtliche Begründung. Der Gesetzgeber hat augenscheinlich zwar an die Schwierigkeiten kleiner und mittlerer Unternehmen gedacht, sieht jedoch in der Verordnung selbst nur wenige Erleichterungen von deren strengen Regeln vor.

Was sollte man daher für sein Überleben in der Welt des neuen Datenschutzrechts beachten?

Anwendungsbereich der Verordnung

Zuerst ist festzuhalten, dass alle Marktteilnehmer in Europa an dieses Recht gebunden werden. Hierunter fallen alle in der EU tätigen Unternehmen, die Personendaten von Unionsbürgern verarbeiten, andererseits aber auch datenverarbeitende Unternehmen, die keine Niederlassung in der EU haben, aber Dienstleistungen auf dem europäischen Markt anbieten, zum Beispiel auch Online-Dienstleistungen wie Facebook oder Twitter.

Das Ziel ist ganz klar – alle Geschäftstätigkeiten auf dem europäischen Markt, die eine Verarbeitung von Kunden- und Mitarbeiterdaten enthalten, müssen datenschutzrechtskonform geplant und durchgeführt werden.

Aus sachlicher Sicht werden alle ganz oder teilweise automatisierten Verarbeitungen ebenso wie nichtautomatisierte Verarbeitungen personenbezogener Daten, die in einer Datei gespeichert sind, durch die Verordnung abgedeckt. Dabei ist die Definition dessen, was „personenbezogene Daten" sind, sehr weit. Hierunter fallen alle Informationen bestimmt, die sich auf eine identifizierte oder beispielsweise anhand von Angaben über ihren Standort, ihre IP-Adresse oder auch über Cookies identifizierbare natürliche Person beziehen.

Stärkung der Verbraucherrechte und neue Informationspflichten für Unternehmen

Weil die Verarbeitung personenbezogener Daten, so die Begründung der Verordnung, „im Dienst der Menschheit stehen" soll, werden die Rechte von Verbrauchern in der Verordnung stark betont. Datenverarbeitende Unternehmen müssen natürliche Personen über die Verarbeitung in umfassender, lesbarer und verständlicher Weise informieren. Diese Informationen müssen zum Zeitpunkt der Erhebung der Personendaten bereitgestellt werden. Wurden die Daten aus anderen Quellen als direkt vom Betroffenen erhoben, muss die Information innerhalb eines Monats nach Erlangung der Daten, spätestens jedoch zum Zeitpunkt, wenn die Daten zur Kommunikation verwendet werden sollen, oder im Zeitpunkt ihrer ersten Offenlegung einem anderen Empfänger, erfolgen.

Dem Betroffenen mitgeteilt werden müssen unter anderem auch der Verwendungszweck der personenbezogenen Daten, die Rechtsgrundlage für die Verarbeitung, die Empfänger der personenbezogenen Daten, die Dauer der Speicherung oder die Quelle, aus der die Daten stammen. Hingewiesen werden muss auch auf mögliche Folgen der Datenverarbeitung, falls diese beispielsweise in automatisierten Entscheidungsprozessen, einschließlich Profiling, eingesetzt werden, oder auf mögliche nachteilige Folgen der Nichtbereitstellung der Daten, wenn die Bereitstellung gesetzlich oder vertraglich vorgeschrieben ist.

Die natürliche Person muss auch über ihre Rechte belehrt werden. Die Belehrung wird recht umfangreich ausfallen, da die neuen DS-GVO sehr viele Verbraucherrechte gibt. Ein Beschwerderecht bei einer Aufsichtsbehörde überrascht niemanden, aber wissen Sie, was zum Beispiel durch das Recht auf Berichtigung, das Recht auf Vergessenwerden oder das Recht auf Datenübertragbarkeit abgedeckt ist? Letzteres bedeutet zum Beispiel, dass der Unternehmer meine von ihm verarbeiteten Daten mir in einem maschinenlesbaren, gängigen und anderswo weiterverarbeitenden Format übergeben muss. Der Gesetzgeber hatte hierbei wahrscheinlich Portale wie Facebook in Sinn, die Regelung gilt jedoch allgemein, nicht nur für Social Media.

Drastische Geldbußen und Umkehr der Beweislast

Künftig können bei Datenschutzverstößen sehr hohe Geldbußen anfallen. Diese können bei schweren Verstößen bis zu 20 Millionen Euro oder bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs eines Unternehmens betragen, je nachdem, welcher der Beträge höher ist. Im Falle von Siemens wären dies beispielsweise rund 3 Milliarden Euro. Damit nicht genug, denn auch Führungskräften, Datenschutzbeauftragten oder anderen für den Umgang mit Informationen verantwortlichen Entscheidungsträgern drohen im schlimmsten Falle Geldbußen von bis zu 20 Millionen Euro. Abgesehen davon kann jede Person, die wegen einer Datenschutzverletzung Schaden erlitten hat, Schadenersatz vom verantwortlichen Unternehmen verlangen, der auch immaterielle Schäden umfasst.

Bei alledem erfolgt eine Umkehr der Beweislast. Nicht die zuständige Behörde muss den Nachweis für den Verstoß gegen das Datenschutzrecht erbringen, vielmehr muss das Unternehmen belegen, dass es sämtliche Regeln der DS-GVO einhält. Dieser Beweis wird vor Gericht nur dann überzeugend zu führen sein, wenn das Unternehmen über ein ausgefeiltes Datenschutzmanagementsystem verfügt, das die getroffenen Maßnahmen zur Umsetzung der rechtlichen Vorgaben umfassend dokumentiert.

Keine Altfallregelung

Die zweijährige Übergangsfrist sollte durch die Unternehmen intensiv genutzt werden, um alle betroffenen unternehmensinternen Prozesse, Geschäftsmodelle und Verträge ebenso wie Form und Inhalt der Kommunikation mit dem Verbraucher zu durchleuchten und an die neue Rechtslage anzupassen. Dies ist besonders wichtig, weil die DS-GVO keine Altfallregelung enthält, d.h. man kann sich ab dem Stichtag im Mai 2018 im Falle einer Beanstandung nicht darauf berufen, die nicht verordnungskonformen Tatsachen seien bereits vor Wirksamwerden der neuen Verordnung entstanden.

Wie hoch im Einzelfall der Umstellungsaufwand sein wird, hängt vom jeweiligen Unternehmen ab. Anpassungsbedarf wird es ganz sicher in jedem Unternehmen geben.

Der Autor ist Jurist bei UEPA advokáti s.r.o.

UEPA advokáti s.r.o.
Voctářova 2449/5, 180 00 Praha 8
Tel.: +420 234 707 444, Fax: +420 234 7017 404
E-Mail: office@uepa.cz
www.uepa.cz