AHK Deutsch-Tschechische Industrie- und Handelskammer
Česko-německá obchodní a průmyslová komora

bpv BRAUN PARTNERS

GDPR (Obecné nařízení o ochraně osobních údajů) – co je potřeba doopravdy udělat?

Arthur Braun, M.A

bpv Braun Partners s.r.o.

(+420) 224 490 000
arthur.braun@bpv-bp.com

25. květen 2018 bude prvním dnem účinnosti obecného nařízení o ochraně osobních údajů č. 2016/679 (GDPR) — dnem, který dělá mnohým společnostem vrásky na čele. Důvody pro jejich obavy jsou dva: za prvé jsou to nově zavedené, velmi vysoké pokuty, které mohou být uloženy až v částce 20 milionů euro, nebo ve výši 4 % celkového obratu dané společnosti, za druhé je to ale také skutečnost, že v minulosti byla ochrana osobních údajů ze strany českých společností považována za irelevantní, pročež této oblasti bylo věnováno minimální množství pozornosti. Německé společnosti naproti tomu mají například již dlouho zaveden institut pověřence pro ochranu osobních údajů a k ochraně osobních údajů přistupují s náležitou odpovědností.

Častá porušení zákona č. 101/2000 Sb. o ochraně osobních údajů nebyla v České republice doposud téměř postihována a když, tak pokuty byly poměrně nízké. Za pár měsíců tomu však již bude jinak a je potřeba zdůraznit, že nařízení GDPR je přímo aplikovatelné ve všech zemích EU a nemůže být zmírněné ani příliš mírnou aplikací v praxi. Na druhou stranu se mi však zdá, že ze strany všech poradců a rádců je rozséváno zbytečně moc paniky.

Co tedy musím jako podnikatel opravdu udělat?

1. V první řadě si musím uvědomit, která data ve spojitosti s osobními údaji zpracovávám, zejména pak, zdali se jedná např. o velmi citlivé údaje jako např. zdravotní záznamy, pro které platí velice přísná pravidla, nebo zda se jedná o běžné záznamy týkající se např. zaměstnanců podnikatele. Ale pozor, např. i informace zaznamenaná v CRM souboru, že určitý zákazník nemá být pozván do steakhousu, protože jako hinduista nejí hovězí, představuje zrovna ve smyslu výše uvedeného velmi citlivý údaj. Stejně tak se třeba nedoporučuje založit si Whats-app skupinovou konverzaci za účelem diskutování nových nastavení týkající se zpracování osobních údajů... Zpracováním osobních údajů může být potom například i videozáznam průmyslové haly! Následující rady a tipy pak může využít širší spektrum čtenářů než jen zpracovatelé velmi citlivých osobních údajů.

2. Pokud zpracovávám zákaznická data, budu muset zkontrolovat účel zpracování, resp. být schopen dostatečně odůvodnit, proč tato data zpracovávám. To platí o to více, pokud tato data předávám dále – zpracovatelům či subzpracovatelům. Předávání / ukládání / zpracovávání dat mimo Evropskou Unii je nezávisle na nařízení GDPR problematické a mělo by být vždy konzultováno s odborníky na zpracovávání osobních údajů.

3. Je možné, že se mě bude týkat povinnost jmenovat pověřence pro ochranu osobních údajů. Tato situace však určitě nenastane v případě, že jsem výrobní společnost a zpracovávám pouze kmenové údaje týkající se zaměstnanců, a naopak určitě nastane, pokud jsem pojišťovna nebo například společnost podnikající v oblasti energetiky (prodejce). I pokud již v rámci společnosti působí někdo jako pověřenec pro ochranu osobních údajů, je možné, že pro něj budu muset s příchodem nařízení GDPR připravit novou pracovní smlouvu.

4. Musím také prověřit, kdo z mých zaměstnanců a poskytovatelů služeb má přístup k osobním údajům a zda dochází ke zpracování těchto údajů jen v zákonných, resp. smluvně sjednaných mezích. Samozřejmostí je také, že musím smazat osobní údaje, které již nepotřebuji. Každý správce či zpracovatel osobních údajů musí zvolit vhodná technická a organizační opatření, na základě kterých budou rizika narušení bezpečnosti ochrany osobních údajů minimalizována (čl. 24 a 25 GDPR). Kromě toho bude také muset aktualizovat svoje smlouvy s poskytovateli služeb.

5. Kromě výše uvedeného musím mít také plán, kdo a jak bude informovat Úřad pro ochranu osobních údajů, pokud by mělo dojít k úniku / narušení bezpečnosti osobních údajů (tzv. leak/breach), tedy že by se osobní údaje dostaly neoprávněně na veřejnost. Dle nařízení GDPR musí být tato povinnost splněna nejpozději do 72 hodin od narušení bezpečnosti, a to bez ohledu na víkendy či státní svátky.

Nařízení GDPR obsahuje celou řadu dalších povinností, kterými jsou správci, resp. zpracovatelé povinni se řídit. V tuto chvíli je proto maximálně žádoucí nechat si prověřit stav ochrany osobních údajů ve vlastní společnosti externími odborníky, kteří se orientují také v oblasti pracovního práva, aby mohly být identifikovány rozpory a následně implementovány vhodné metody pro zlepšení stávajícího stavu. I pro dobře vedené společnosti nastal nejvyšší čas pro zahájení přípravy na účinnost nařízení GDPR. Není však důvod propadat panice.