Jak na GDPR?

Nařízení EU č. 2016/679 (známé jako GDPR – *General Data Protection Regulation*, [1]) se stává velkým strašákem, a to hned ze dvou důvodů. Tím prvním jsou obrovské sankce za jeho porušení. Druhým, mnohem vážnějším důvodem je, že jen málokdo ví, jak požadavky GDPR realizovat. Realizace GDPR nebude vůbec snadná ani laciná.

Ucelené řešení, které by bylo možné pořídit podobně jako systém pro EET, totiž neexistuje. Je to dáno tím, že každý subjekt, přestože zpracovává stejná data, je trochu jiný. Například všechny internetové obchody mají něco společného (databázi zákazníků), ale současně i podstatně rozdílného (kde ji mají uloženou, jak ochráněnou a jak s ní pracují). Navíc každý subjekt funguje v trochu jiném právním režimu, a tak na realizaci GDPR je třeba mít odborníky ve dvou oborech současně: v informatice a ve správním právu.

Obecně vzato, každý subjekt se může k realizaci GDPR postavit zhruba pěti způsoby.

Ignorovat

Zde je situace podobná jako u BOZP: je to nejsnadnější a nejlevnější cesta. Ovšem jen do okamžiku, než nastane bezpečnostní incident nebo než se najde první kverulant. Pak je to zničující.

Postavit své řešení na cloudu

Poskytovatelé cloudů se předhánějí v marketingovém velebení [3] cloudového řešení. Ovšem to je nesmyslné. Z hlediska GDPR totiž zůstane poskytovatel cloudu vždy v roli zpracovatele, zatímco firma v roli správce údajů. Připomeňme, že odpovědnost vždycky nese správce. Kdyby došlo k bezpečnostnímu incidentu, správce by musel dokazovat příslušnému úřadu, že má s cloudovým poskytovatelem tak precizně postavené smlouvy, že se z odpovědnosti vyviní. Následně se může soudit o náhradu škody, např. s Googlem a Microsoftem, navíc v zahraničí...

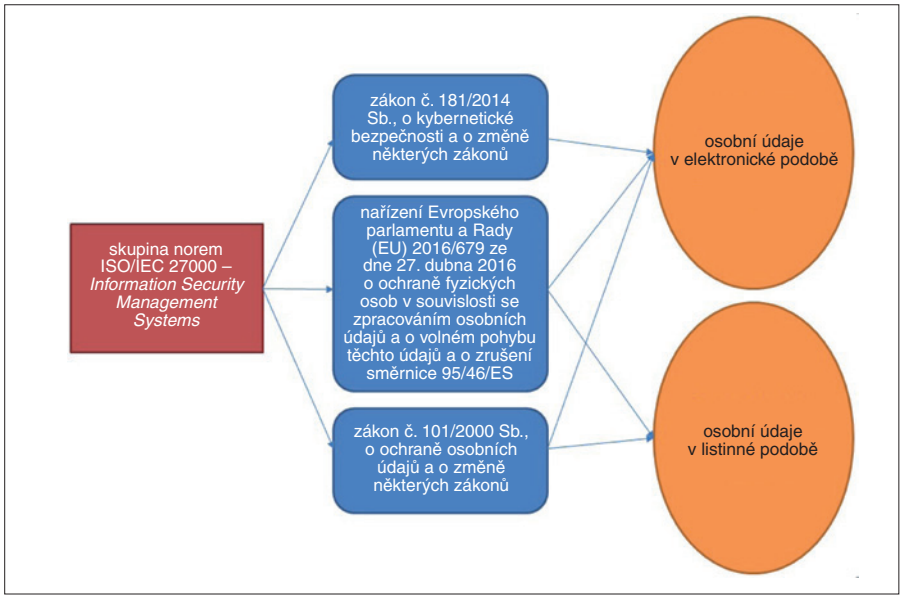
Avšak především: cloudové řešení by znamenalo, že firma nesmí mít žádné doklady v papírové podobě. GDPR totiž platí jak pro elektronické, tak i pro papírové doklady.

Právní řešení

Právní řešení je řešení, které se chystají nabízet všechny velké advokátní kanceláře. V podstatě jde o vyvedení všech osobních údajů za brány firmy, ke zpracovatelům. S vírou, že smlouvy se zpracovateli budou postaveny tak dokonale, že firmu při případném incidentu ochrání. Jde tedy v podstatě o řešení obdobné cloudu, jenže „naruby“. Zatímco cloud řeší kyberbezpečnost a nezajímá se o papírové doklady, u právního řešení je tomu přesně naopak. Většina právníků má totiž o počítačích jen velmi naivní a mlhavé představy. Navíc právní řešení vychází jako dosti nákladné.

Vlastní technické řešení

Vlastní technické řešení je metodicky i fakticky jediné správné. Znamená to, že firma sama provede všechny kroky k realizaci GDPR, od věcné a právní analýzy přes nastartování příslušných procesů až k závěrečnému auditu. Jedině pracovníci firmy totiž přesně vědí, jaké soubory dat se používají, kde a k čemu. Ani cenově nemusí být toto řešení špatné. Problémem ovšem je, že málokterá firma má fundované právníky specializované na správní právo (veškerá řízení před Úřadem na ochranu osobních údajů probíhají v režimu podle správního řádu) a současně odborníky na informatiku schopné upravovat existující software. Že problém není jednoduchý, ukazuje příklad na *obr. 1*, který znázorňuje vzájemný vztah základních právních předpisů.



Obr. 1. Vztah základních právních předpisů týkajících se ochrany osobních údajů

Outsourcing

V současné době se téměř výlučně prosazuje trend nechat si GDPR „udělat na klíč“ formou outsourcingu. Touto cestou jdou jak velké nadnárodní společnosti, tak i např. nejmenší jednotky veřejné správy (obce prvního a druhého typu). Výhody tohoto řešení jsou stejné jako u vlastního technického řešení podle předcházejícího odstavce, ale navíc je zde ještě zvýšení bezpečnosti. Kdyby došlo k bezpečnostnímu incidentu, zodpovídá za něj v každém případě firma jako správce údajů, to nelze změnit. Ale jestliže si správce objednal provedení GDPR u externí firmy, přece jen se odpovědnost poněkud „rozptýlí“, protože správce snadno prokáže, že udělal maximum pro to, aby incidentu zabránil. Jsou-li správcem malé a střední subjekty, které si jsou navzájem podobné (např. lékárny, internetové obchody, obce, školy a mnoho dalších), vychází outsourcing dokonce relativně levně, protože některé náklady je možné mezi ně rozdělit.

Literatura:

[1] *Nařízení Evropského parlamentu a Rady 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES*. In: Úřední věstník Evropské unie, 2016, číslo 119.

[2] ODBOR LEGISLATIVY, PRÁVA A ANALÝZ ÚŘADU HK ČR, ed. *Obecné nařízení na ochranu osobních údajů* [online]. 2017 [cit. 2017-09-11]. Dostupné z: www.komora.cz/pro-podnikani/legislativa-a-normy/aktuality-z-legislativy/obecne-narizeni-na-ochranu-osobnich-udaju.aspx

[3] ŠKORNIČKOVÁ, Eva. Google Cloud a G Suite se připravují na GDPR. *GDPR.cz* [online]. 2017 [cit. 2017-09-11]. Dostupné z: https://www.gdpr.cz/blog/google-cloud-a-g-suite-se-pripravuji-na-gdpr/

Josef Kokeš, GDPR Systems – Služby pro vědu a výzkum, s. r. o.