30. 1. 2018

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Již jen pár měsíců do účinnosti: Připravte se na GDPR!

Jak již jistě víte, v květnu 2018 vstoupí v účinnost nové evropské Obecné nařízení o ochraně osobních údajů, zkráceně GDPR (General Data Protection Regulation). Ačkoliv pro legislativu ochrany osobních údajů představuje spíše evoluci než revoluci, jeho vyšší sankce a zpřísnění úpravy vyvolávají mnohé diskuse a nezřídka působí až zděšení. Panika přitom není na místě, pokud se organizace s GDPR zavčasu seznámí a přizpůsobí mu své procesy nakládání s osobními údaji. Protože se jedná o velmi komplexní úkol, připravili jsme přehled nejdůležitějších kroků, které by bylo třeba podniknout ještě před účinností GDPR.

Jak začít?

Ještě předtím, než organizace přistoupí k samotné úpravě činností, je potřeba seznámit sebe a své kolegy s obecnými dopady, které GDPR bude mít. Prvním krokem by měl být přehled o všech rizicích, příležitostech, nezbytných krocích a nákladech s implementací GDPR spojených. Organizace by měla věnovat čas také přípravě harmonogramu implementace, aby získala neustálý přehled o podstatných termínech a návaznosti jednotlivých kroků.

Dalším krokem by mělo být rozhodnutí, zda bude zajišťovat soulad s GDPR svépomocí nebo zda využijete asistence odborníků v daných oblastech. Jelikož ohledně změn, které GDPR přináší, panuje i mezi odbornou veřejností mnoho mýtů a nepřesností, doporučujeme zapojit minimálně specialisty z oblasti práva, procesů, bezpečnosti a IT. Ve většině případů není zajištění souladu s GDPR záležitostí jedné nebo dvou osob, ale vyžaduje spolupráci managementu IT, marketingu, lidských zdrojů a dalších a jde tedy o personálně náročnou záležitost. Náhledem externího odborníka z oblasti ochrany osobních údajů je tak možné zabránit potenciální vnitropodnikové slepotě, či hůře vynakládání času a prostředků na nesmyslné kroky nezajišťující soulad s GDPR, a předejít případným sankcím za nesoulad s GDPR. Externista také může pomoci s projektem implementace a s odhadem celkových nákladů.

V každém případě doporučujeme vždy vybírat odborníka, který má s implementací GDPR praktické zkušenosti a má z těchto projektů kladné a ověřitelné reference. Poptávka po odbornících z této oblasti je nyní tak vysoká, že počet „GDPR expertů“ roste raketovým tempem, ne vždy však skutečně pomohou.

Mapujte, posuzujte, evidujte

Jakmile z přípravné fáze vyplyne přehled o obecných změnách, které GDPR přináší, může se začít s vlastní implementací. Nejprve doporučujeme zmapovat, jaké údaje jsou uvnitř organizace zpracovávány, za jakým účelem a na jakém právním základu k tomu dochází. GDPR přináší povinnost tyto informace kdykoli doložit dozorovému úřadu. Mapování by mělo pokrýt celý cyklus zpracování včetně toho, jaké procesy jej pokrývají. Závěrem tohoto kroku by měl být vytvořen přehled, jak a od koho jsou údaje získávány, k čemu jsou využívány, komu je organizace předává a jak probíhá jejich likvidace ve chvíli, kdy pominou důvody pro další uchovávání. Tento krok bývá součástí auditu ochrany osobních údajů.

Až budou údaje zmapované, následuje posouzení, zda nedochází ke zpracování více údajů, než je nutné, a tedy i více, než je možné. Jedním ze základních principů GDPR je tzv. princip minimalizace – možné je zpracovávat pouze nezbytné množství údajů a pouze po nezbytnou dobu. Minimalizace přirozeně souvisí s principem zákonnosti, tedy že každé takové zpracování musí mít zároveň právní základ. Také nezbytnost zpracování je potřeba před dozorovým úřadem kdykoliv obhájit. Samozřejmě je též nutno posoudit, zda jsou v rámci každého procesu plněny veškeré další povinnosti uložené GDPR – pouhý jejich výčet by však vydal na samostatný článek.

Po provedení výše uvedeného posouzení je nutné identifikovat mezery mezi stávajícím stavem a stavem souladným s požadavky GDPR, navrhnout opatření pro dosažení souladu a identifikovat jejich možné dopady do fungování společnosti. Po diskusi mezi odbornými poradci a vedením společnosti by měla být dosažena shoda na tom, která z možných opatření budou implementována, popř. identifikována akceptovatelná rizika zpracování.

Hurá na implementaci

Po zmapování veškerých procesů, odhalení mezer mezi stávajícím stavem a požadavky GDPR a zvolení konkrétních opatření k implementaci je namístě zajistit implementaci všech těchto opatření. Bude se jednat zejména o změnu procesů, dokumentů (formulářů pro klienty, interních směrnic, smluv se zpracovateli, informací o zpracování apod.) a opatření ochrany osobních údajů.

Pokyny pro konkrétní zaměstnance by přitom měly být co nejvíce praktické. Jistě nikoho nepotěší, pokud mu bude sděleno, aby postupoval při předávání údajů do třetích zemí v souladu s čl. 44-49 GDPR. Pokud však bude instruován k tomu, aby v případě možného předávání údajů do třetích zemí kontaktoval právní oddělení společnosti, bude spíše ochoten tuto změnu přijmout.

Aby bylo možné prokázat zákonnost postupů, je nutná důkladná evidence toho, jaké údaje jsou zpracovávány, za jakým účelem a na jakém právním základu k tomu dochází. Není pravdou, že nejlepším právním základem je vždy souhlas subjektu údajů – naopak se ve většině případů jedná o nejhorší možný titul. Nezřídka jsou správci ke zpracování oprávněni či dokonce povinni na základě plnění smlouvy nebo ze zákona, často také může být svobodnost souhlasu prakticky nedosažitelná, například v případě zpracování osobních údajů zaměstnanců (byť jeho získání bývá některými mylně doporučováno).

Respektujte práva subjektů údajů

Kromě povinností přináší GDPR také práva, a to v prvé řadě subjektům osobních údajů. Jde především o právo na přístup k údajům a jejich opravu, možnost podání námitky vůči zpracování, právo omezení zpracování, právo na přenositelnost údajů (tzv. portabilita) a právo na výmaz údajů. Rozšířená obava, že výkon těchto práv prakticky znemožní pracovat s údaji klientů nebo

zaměstnanců, je zpravidla zbytečná.

Všichni, kdo komunikují se zákazníky nebo mají k údajům alespoň přístup, by měli být s právy subjektů dostatečně obeznámeni, aby mohli subjekty řádně informovat a případně jim pomoci tato práva vykonat. Každý subjekt údajů by měl být dále dostatečně informován o způsobu, účelu a rozsahu zpracování. Informace přitom musí být podány srozumitelně a stručně, aby je bylo možné bez problémů pochopit.

Podobný standard musí mít i případné získávání souhlasů se zpracováním. Pakliže v průběhu procesu implementace dojde ke zjištění, že pro některé formy zpracování budou souhlasy potřebné, je nutné se při jejich získávání držet podmínek, jejichž splnění Nařízení vyžaduje. Souhlas by měl být snadno identifikovatelný a oddělitelný, nesmí být podmínkou k poskytnutí služby (pokud není skutečně nezbytný), musí být odvolatelný a příslušný správce osobních údajů musí být schopen prokázat, že souhlas řádně získal.

Podobně jak bylo uvedeno výše, i zde by měly být instrukce pro zaměstnance související s výkonem těchto práv maximálně jednoduché a srozumitelné. Například pokyn k zajištění práva na přístup podle čl. 15 GDPR, bez dalšího upřesnění, může být pro pověřeného zaměstnance nadlidským úkolem s potenciálními dopady do chodu celé společnosti. Pokud však bude zpracování řádně evidováno (jak co do zpracovávaných údajů, tak co do účelu, kategorií zpracovávaných údajů apod.) a pro zaměstnance bude stanoven jednoduchý proces (údaje o osobě lze získat způsobem X, informace o parametrech zpracování jsou dostupné v interním dokumentu Y, formulář pro odpověď je dostupný v C), může být vypořádání takové žádosti doslova otázkou několika minut.

Kdo potřebuje „pověřence“?

Součástí implementace GDPR by měla být také úvaha o potřebnosti pověřence pro ochranu osobních údajů, neboli DPO (Data Protection Officer). Ten bude kontaktním místem v otázkách ochrany osobních údajů a to jak uvnitř, tak navenek organizace, bude monitorovat soulad s organizace s GDPR a bude styčnou osobou pro potřeby dozorového úřadu. Koho se bude týkat povinnost pověřence jmenovat, určuje článek 37 Nařízení. Půjde především o organizace, které vykonávají veřejnou moc nebo systematicky zpracovávají velké množství údajů, pokud se jedná o zpracování citlivých osobních údajů nebo pokud přitom dochází k monitorování osob.

Oproti všeobecnému přesvědčení lze uvést, že velká většina společností tohoto pověřence vůbec nebude muset mít. Pokud však v rámci organizace existuje podezření, že by se tato povinnost mohla aplikovat, doporučujeme obrátit se na odborníky. I když si posouzení, zda tato povinnost na organizaci dopadá, vyžádá určité náklady, ty se v případě, kdy pověřence nebude nutné jmenovat, mohou vrátit již za jediný měsíc činnosti pověřence, ne-li dříve (značné náklady si vyžádá již samotné nastavení výkonu funkce pověřence).

Pověřenec může být buď interní, tedy zaměstnanec, nebo externí, tedy fyzická či právnická osoba, vykonávající tuto činnost na základě smlouvy o poskytování služeb. Interní pověřenec může být výhodný z důvodu znalosti procesů a podnikové reality, avšak je u něj omezena odpovědnost a dají se předpokládat vyšší náklady na získání patřičné kvalifikace. Externí pověřenec by měl příslušnou kvalifikaci již mít a náhradu škody je v jeho případě možné smluvně stanovit prakticky bez omezení, může být ale obtížné seznámit jej se všemi procesy zpracování ve společnosti.

Dobře o data pečujte

Osobní údaje je nutné zabezpečit nejen v rámci společnosti, ale v případě outsourcingu i u smluvních

partnerů. Pokud správce údajů využívá externí zpracovatele, je povinen zajistit, aby s údaji i oni zacházeli v souladu s GDPR, a aby smlouvy s nimi obsahovaly některá povinná ustanovení. Smlouvy se zpracovateli by měly být upraveny tak, aby byly plně v souladu s čl. 28 GDPR. Při předávání údajů mimo území EU by pak měla být zajištěna dostatečná ochrana dat alespoň jedním z odpovídajících GDPR nástrojů (smluvní doložky, podniková pravidla, atd.).

Pokud i přes veškerou péči dojde k ohrožení bezpečnosti údajů, incidenty musí být zaevidovány a je povinností organizace posoudit, zda je nezbytné je ohlásit dozorovému úřadu či v případě vysokého rizika i dotčeným subjektům.

Za nedodržení povinností vyplývajících z GDPR jsou stanoveny extrémní pokuty, až půl miliardy Kč nebo 4 % celosvětového ročního obratu firmy. Podcenit přípravu se tak opravdu nemusí vyplatit.

A co dál?

Úprava zpracování do souladu s GDPR je však pouze začátek. Soulad procesů, opatření ochrany a dokumentů s GDPR je potřeba kontrolovat pravidelně, stejně jako je potřeba pravidelně proškolovat příslušné zaměstnance. GDPR však nemusí být pouze administrativní zátěží, ale může představovat příležitost zmapovat činnosti probíhající v podniku, udělat pořádek v datech a optimalizovat vnitropodnikové procesy. Pro zákazníky a zaměstnance pak může skutečnost, že procesy organizace jsou plně v souladu s GDPR, znamenat posílení důvěry a v konečném důsledku i větší ochotu osobní údaje svěřovat, což může pomoci získat podstatnou konkurenční výhodu.

Mgr. Michal Nulíček, LL.M.

Mgr. Bohuslav Lichnovský

ROWAN LEGAL, advokátní kancelář s.r.o.

GEMINI A
Na Pankráci 1683/127
140 00 Praha 4

Tel.: +420 224 216 212
Fax: +420 224 215 823
e-mail: praha@rowanlegal.com

Další články:

- Dvě kiwi denně: EU schválila první zdravotní tvrzení pro čerstvé ovoce
- Digital Omnibus: Revoluce v datech, nebo jen nová zátěž pro podnikatele?
- Nová pravidla pro ground handling v EU a jejich dopady na letecký sektor
- Novinky z české a evropské regulace finančních institucí za měsíc březen 2026
- Novelizace nařízení EU o odlesňování (EUDR)
- Zneužití práva na přístup podle GDPR
- Doručování soudních písemností ze zahraničí do ČR
- Novinky z české a evropské regulace finančních institucí za měsíc únor 2026
- Digital Fairness Act a influencer marketing – cesta ke konci roztříštěnosti regulace?
- Novinky z české a evropské regulace finančních institucí za měsíc leden 2026
- IATA Travel & Cargo akreditace v letectví – v čem spočívají její výhody?