12. 3. 2018

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

GDPR – základní postup v praxi

O problematice GDPR bylo napsáno již mnoho. K dispozici je nespočet více či méně odborných publikací, probíhají školení, množí se specializované weby. Ačkoliv se lze setkat s názory některých odborníků, že Česká republika podlehla v souvislosti s Obecným nařízením o ochraně osobních údajů (GDPR) hysterii, skutečností je, že do 25. května zbývají necelé 3 měsíce, a ačkoliv aktivity podnikatelských uskupení, veřejné správy i regiónů začínají být viditelné, nejsou často dostatečně koordinované, funkční a jednotné. Přestože děsivé předpovědi, že 80 % společností nebude ke květnovému datu na GDPR připraveno (Forrester) je skutečně nutné brát s přiměřeným nadhledem, zůstává faktem, že pro ty, kteří ještě připraveni nejsou, se od teď již každý den počítá. Nastala tedy chvíle mluvit a psát o GDPR v holých větách.

ADVOKÁTNÍ KANCELÁŘ
KŘÍŽ A PARTNEŘI

Pokud mnoha zástupcům správců a zpracovatelů vadilo, že dostupné informace o tom, co se od nich bude očekávat, byly obecné, pak tento krátký popis implementace GDPR již bude naopak obecný úvod i vysvětlení postrádat. Lze předpokládat, že v tuto chvíli již o nařízení mají všichni čtenáři alespoň základní povědomí. Cílem textu tedy není vykládat předpis jako takový, kontext národních právních úprav ani vybrané instituty GDPR, které mohou v praxi působit problémy. Jediným cílem textu je být pomocným checklistem toho, na co při přípravě není možné zapomenout. Proto ani text neobsahuje odkazy na konkrétní články Nařízení GDPR, ale pouze na již všeobecně známé pojmy, principy a povinnosti. Nejedná se však o vyčerpávající univerzální plnohodnotný návod, protože pokud je vhodné přidržet se jen jediné rady, bude jí to, že obecný postup lze aplikovat v zásadě na všechny subjekty, ale konkrétní rozsah přijatých kroků a způsob jejich provedení je nezbytné rozhodovat se znalostí procesů zpracování osobních údajů, jejich kategorií a množství u každého subjektu individuálně. Pro zjednodušení se v tomto článku nebudeme zabývat mezinárodním předáváním osobních údajů a pozicí mimoevropských subjektů, zpracovávajících osobní údaje z EU. Pro upřesnění je pak vhodné ještě dodat, že pro entitu, zavádějící GDPR, je v článku užíváno označení subjekt, a to za účelem sjednocení označení pro soukromé a veřejnoprávní organizace. Pro žijící fyzickou osobu je, ve smyslu terminologie GDPR, pak užíván v článku pojem subjekt údajů.

Na samém začátku implementace GDPR je nezbytné sestavit tým pracovníků, kteří budou na implementaci GDPR pracovat. Jedná se o časově náročný proces, a tedy je třeba najít osoby, které budou schopny tuto problematiku dostatečně soustředěně řešit nad rámec svých běžných pracovních povinností. Nezbytné pak je, aby byly jasně určené úkoly, odpovědnosti a hierarchie týmu v rámci projektového řízení. Z dosavadních zkušeností lze z těchto důvodů jako nanejvýš vhodné objektivně vyhodnotit zajištění implementace externí společností. Jedinou myslitelnou nevýhodou je, že cizí lidé budou trávit dlouhý čas prověřováním chodu společnosti a dotazováním vedoucích pracovníků a přicházet s návrhy řešení, měnících zaběhnutou praxi. Pokud je audit však prováděn správně, není jeho cílem pouze vyhodnotit, co vše je nutné přestavět od základu a jaký software je absolutně nezbytné pořídit, ale spíše, jak upravit činnost subjektu tak, aby došlo ke změnám, narušujícím

dosavadní praxi pouze v míře nutné, bez zbytečných nákladů a v kontextu zpracování osobních údajů dostatečně, nikoliv nepřiměřeně. Na druhou stranu přání subjektu „nastehovat“ jen systém, který je absolutně minimalistický, může být zrádné, neboť v tuto chvíli nic nebrání kontrolám u kterýchkoliv subjektů, přestože ideově bylo Nařízení koncipováno na určitý typ podniků, vykazujících znaky rozsáhlého komerčního zpracování osobních údajů a historicky také nezřídka laxnost k ochraně práv subjektu údajů.

Nejprve lze jistě doporučit vypracovat rozbor aktuálního stavu ochrany osobních údajů u subjektu. Klíčovým v tomto ohledu bude, zda se řídil zákonem č. 101/2000 Sb., o ochraně osobních údajů, či nikoliv. Vhodné je také zjistit, zda jsou zavedeny nástroje např. podle ISO 27001. Přestože pokud v obou případech bude odpověď kladná, práce tím nekončí, bude takový výchozí stav představovat jednak značnou časovou a finanční úsporu při implementaci, jednak lze očekávat, že nikoho nepřekvapí, že je konkrétními způsoby třeba osobní údaje chránit a komunikace se tím značně zefektivní. Na druhou stranu subjekty, které tento stupeň přípravy mají, budou v praxi spíše provozy, kde dochází k rozsáhlému zpracování osobních údajů zvláštní kategorie či kde to vyžaduje povaha provozu (technologie, finance, telekomunikace atp.) a v těchto případech pak implementace bude často obnášet také obsazení DPO nebo provádění DPIA. Na tomto místě je nutné také připomenout, že podle konkrétní činnosti subjektu je nezbytné hodnotit také rozsah aplikovatelných právních předpisů a kroky tak zavádět nikoliv výhradně podle GDPR, ale také v návaznosti na další právní předpisy.

To zcela podstatné, co však zůstává někdy opomíjeno, je určení harmonogramu prací, časového horizontu plnění jednotlivých kapitol a rozpočtu. To je nezbytné i z důvodu nutnosti dostupnosti některých pracovníků či zajištění jejich zastupitelnosti. I pokud bude audit prováděn externí společností, je třeba určit minimálně jednoho pracovníka pro zajištění součinnosti v rámci subjektu a o auditu dostatečně informovat klíčové pracovníky. Očekávat lze nezbytnost komunikace zejména s vedoucími pracovníky HR, IT, finančního a právního oddělení. Každý z nich se musí připravit na nezbytnost zejména informovat o chodu oddělení ve smyslu pohybu dat, technického a organizačního zabezpečení, stavu dokumentace (a nutnosti jejího dohledání), dodržování interních směrnic (pokud jsou zavedeny). Ideální potom je, pokud je, na základě prvního pohovoru nad vyplněnými úvodními formuláři auditu, pro každé oddělení vypracován seznam úkolů a informací, které je třeba doplnit.

Prvním krokem bude zmapování toho, jaké kategorie osobních údajů jsou zpracovávány a jakých subjektů údajů se týkají. Jinak bude přistupováno k osobním údajům klientů, jinak k údajům zaměstnaneckým a jinak k osobním údajům jejich rodinných příslušníků. Rozhodné bude také množství osobních údajů, které je zpracováváno. Častým omylem je posuzování závažnosti dopadu Nařízení pouze podle velikosti společnosti, resp. počtu zaměstnanců. Obvykle sice přímá úměra může platit, pokud na ni však budete spoléhat, můžete být nepříjemně překvapeni. Ačkoliv, nařízením blíže specifikovaná výjimka z povinnosti vést záznamy o zpracování se vztahuje na společnosti s méně, než 250 zaměstnanci, neznamená to, že nemůže existovat malý podnik, který pro povahu svého provozu a množství zpracovávaných údajů přesto bude muset na soulad s GDPR klást značný důraz. Již zmiňované záznamy o činnosti mohou v této kapitole implementace plnit praktický dvojí účel – jednak je na jejich základě možné přehledně zmapovat výchozí stav zpracování osobních údajů, jednak je možné po úpravách na základě implementace použít i u subjektů, které povinnost jejich vedení nemají, jako archivovaný záznam s potenciálem doložit dodržování principu zodpovědnosti.

Podstatné bude dále zatřídění jednotlivých procesů zpracování podle právních důvodů, na jejichž základě k němu dochází. Obecná praktická poučka zní, že cokoliv jde podčlenit pod jakýkoliv jiný důvod, než souhlas, je výhra. Lze však předpokládat, že i tak se najde téměř v každé společnosti alespoň jedno zpracování, které bude souhlas subjektů údajů požadovat. K souhlasům se ale vrátíme

později.

Vhodné, nikoliv nutné, je vést deník implementace, do kterého budou zaznamenávány nejen jednotlivé kroky, ale také přijatá rozhodnutí s odůvodněními. Tento materiál může pomoci při komunikaci s ÚOOÚ v případě kontroly. Bude totiž obsahovat odůvodnění, s odkazem na Nařízení, proč např. nebyla zřízena funkce DPO nebo proč některé zpracování bylo podčleněno pod oprávněný zájem společnosti. Takto bude prokazatelné, že byla rozhodnutí přijímána nikoliv nahodile, ale na základě posouzení právního předpisu, včasně a že je o implementaci vedena evidence. Podobný materiál může být také vhodným nástrojem při kontrole implementace v pozdější době a revizi dodržování zavedených postupů a jejich adekvátnosti k aktuální podobě procesů zpracování.

Ve chvíli, kdy existuje přehled osobních údajů a jejich zpracování, je vhodné zamyslet se kriticky nad jejich potřebností. V souladu s principem minimalizace by měly být zavedeny změny vylučující zpracování osobních údajů, které není nezbytné pro splnění účelu procesu. Výsledná sestava procesů pak musí projít dalším sítem úprav, a to oddělením procesů rizikových pro subjekt údajů. Zde je pak vhodné se zamýšlet nad změnami, které by toto riziko mohly eliminovat. Je potřeba zdůraznit, že dosažitelným cílem implementace není stav, který absolutně vyloučí jakékoliv riziko, ale stav, který rizika co nejvíce minimalizuje, a tam, kde zcela odstranitelná nejsou, budou přijata odpovídající opatření.

K DPO je v tuto chvíli třeba připomenout pouze dva podstatné body, které bývají často nesprávně vykládány: 1. DPO není „děvče pro všechno“ v oblasti ochrany osobních údajů. Není možné, ani fakticky a ani právně, na něj přenést veškerou datovou agendu a odpovědnost za chod zpracování osobních údajů v rámci subjektu. DPO, mimo jiné, komunikuje s ÚOOÚ a subjekty údajů, školí zaměstnance, doporučuje řešení a monitoruje zpracování osobních údajů ve společnosti, nicméně nařízení mu vytyčuje poměrně důrazně (ačkoliv ve vztahu k subjektům, které budou muset tuto funkci obsadit bolestně obecně) nároky na zajištění odpovídajících podmínek pro výkon jeho činnosti. Proto je pak naopak pro subjekt nezbytné nepodceňovat formulaci smlouvy, uzavírané mezi DPO a subjektem. 2. DPO je nezbytné vybírat v návaznosti na specifika činnosti společnosti, týkající se osobních údajů. Na jednu stranu je nepřiměřeným rizikem pouhé formální obsazení funkce osobou postrádající kvalifikační kritéria podle Nařízení GDPR a stanoviska, vydaného WP29, zároveň však nelze spoléhat pouze na komerční certifikaci, která není Nařízením uvedena jako povinnost. Zjednodušeně řečeno: DPO musí být znalý věci. Pokud bude mít certifikát, bude to certifikát komerční. Certifikát může prokázat větší znalosti právní a technické problematiky, zároveň však v tuto chvíli v České republice neplatí, že certifikovaný DPO musí být nutně kvalitnější než necertifikovaný.

Dalším podstatným krokem bude modifikace nebo vypracování nových interních směrnic pro zpracování osobních údajů. Směrnice by měly být konzultovány jak z jednotlivými odděleními, tak především s IT. Při nastavování organizačních a technických opatření pak nelze zapomínat na to, že takovými opatřeními bude nejen např. ochrana datových sítí, zaheslování zařízení a sjednocení autorizace přístupu k souborům, ale také zajištění bezpečného uložení papírových kartoték, úprava vedení spisové agendy v papírové podobě a skartace. S tím souvisí i načasování a zajištění likvidace osobních údajů. Zde lze doporučit spárovat, pokud tak subjekt doposud neučinil, konkrétní proces se zákonnou lhůtou podle národní úpravy. V některých případech tak bude možné pro konkrétní účely uchovávat osobní údaje po skutečně dlouhou dobu. Tam, kde ale zákonná lhůta chybí, bude třeba retenční lhůty nastavit přiměřeně účelu zpracování a zajistit jejich dodržování ve formě připomínek či automatizovaného třídění dokumentů (se schválením), připravených ke skartaci.

Nutné bude také vytvořit seznam zpracovatelů osobních údajů a společných správců. Každý z těchto právních vztahů vyžaduje ve vztahu k GDPR jiné řešení, řešit je však nutné oba. U zpracovatelů je

nezbytné zjistit jejich stav připravenosti na GDPR. Správce musí dbát na to, aby zpracovatelé, kteří pro něj osobní údaje zpracovávají, poskytovali dostatečné záruky ochrany osobních údajů z pohledu GDPR. V tomto smyslu bude nutná úprava existující zpracovatelské smlouvy a v některých případech dokonce nezbytná změna zpracovatele. U společných správců je pak nutné jasně vymezit rozsah oprávnění a odpovědností každého ze správců, opět smluvní úpravou.

Samostatnou kapitolou je pak poučení o zpracování osobních údajů. Jeho obsah a technické řešení bude záviset na jeho umístění a případných specificích okruhu jeho adresátů. Oproti prostému textu je někdy doporučována např. strukturovaná informace, zajišťující trvalou pozornost čtenáře. Nařízení v tomto smyslu klade opět poněkud zrádně definované, ač pochopitelné, podmínky jednoduchosti sdělení, které musí být subjektu údajů srozumitelné. Myšlenkou zde byla snaha uchránit uživatele zejména velkých společností, podnikajících na internetu, před nekonečnými nepřehlednými texty miniaturní velikosti. Jak v praxi závazek dodržet, bude nutné posuzovat ve vztahu ke konkrétní situaci. Nároky na většinu společností nemusí být tak podstatné, nicméně znění a podobu poučení si bude muset subjekt obhájit. Je tedy vhodné opět popis a odůvodnění volby zavést do deníku implementace. Dále bude nutné, tam, kde nelze jinak, upravit souhlasy. Pokud již bude potřeba souhlas získat, je třeba klást maximální důraz na splnění všech požadavků obsahových, i týkajících se jeho poskytnutí subjektem údajů.

S implementací souvisí zejména dva typy činností, které budou mít dlouhodobý přesah. První činností je úprava listin. Mimo smluv zpracovatelských, se společnými správci a DPO, bude třeba připravit také dodatky pracovních smluv, často také smluv s klienty a dodavateli. Druhou činností bude úprava postupů, které subjekt doposud zavedeny neměl. Bude to např. příprava postupu monitoringu aktuálnosti a přesnosti zpracovávaných osobních údajů nebo, tam, kde není DPO, úprava postupu pro případ porušení ochrany osobních údajů (rozhodnutí o rizikovosti incidentu, postup včasného řešení, hlášení ÚOOÚ, případně subjektu údajů, postup vytvoření záznamu). Upravit je třeba i postupy pro komunikaci se subjektem údajů, resp. řešení jeho požadavků. Zde lze výhledově předpokládat mnoho komplikací, které mohou vyvstat nedostatečným proškolením pracovníků nebo nepochopením práv subjektu údajů. Je nutné apelovat na všechny subjekty, aby formou informačních rozcestníků nebo školením na praktických příkladech předcházeli situacím, kdy subjektu údajů buď nebude včasně či adekvátně vyhověno, nebo mu bude naopak vyjito vstříc nad rámec povinnosti správce. Obě situace mohou mít na subjekt závažný negativní dopad.

Školení bude obecně nezbytnou součástí implementace GDPR do provozu. Zaměstnanci, kteří osobní údaje zpracovávají, by měli být prokazatelně proškoleni k dodržování pravidel zaváděných vnitřními směrnicemi. Tato školení by se měla v budoucnosti opakovat. Na obdobnou činnost zaměstnavatele jsou zaměstnanci zvyklí, nicméně v tomto případě by se nemělo jednat o formální úkon, bez skutečného seznámení se s pravidly, jak tomu někdy bývá např. při školení BOZP. U větších společností lze pak nad rámec nezbytného doporučit využít interní komunikace k obecnému informování všech zaměstnanců o GDPR tak, aby se po společnosti nešířila panika, vyvolaná přebíráním kusých informací z médií. Pokud je to součástí politiky společnosti, lze pochopitelně připravit také školení zaměstnanců o jejich právech coby subjektů údajů. Potenciální komplikace, které takové školení může však přinést, je třeba kriticky zohlednit oproti přínosu maximálního komfortu zaměstnanců.

Závěrem je třeba shrnout, že i po implementaci GDPR a úspěšném otestování zavedených opatření, práce v této oblasti nekončí. Ochrana osobních údajů je kontinuální činností. Ustavení procesů zpracování do souladu s GDPR je pouhým vstupem na cestu modifikovaných sjednocených pravidel pro ochranu osobních údajů, které správce a zpracovatele může připravit na, prozatím více tušenou než zcela jasnou, novou realitu. Spíše než národní právní úpravy, doplňující GDPR, na které se v mnoha zemích, včetně ČR stále čeká, nás v budoucnu mohou překvapit první rozhodnutí ÚOOÚ a

Evropského sboru pro ochranu osobních údajů, první žaloby subjektů údajů a první spory o náhradu škody z porušení smlouvy mezi správcem a chráněným DPO.

JUDr. Veronika Křížová LL.M.,
advokát

Advokátní kancelář Kříž a partneři s.r.o.

Rybná 9
110 00 Praha 1

Tel.: +420 224 819 334
Fax: +420 224 819 343
e-mail: info@ak-kp.cz

2017 právnická firma roku

_____
[*] Aktualizace textu, 15.3.2018

© EPRAVO.CZ – Sbírka zákonů, judikatura, právo | www.epravo.cz

Další články:

- Jaké klíčové změny přináší návrh novely stavebního zákona?
- Nový zákon o zbraních a střelivu
- Novela zákona o pyrotechnice: likvidace profesionálů namísto zmírnění negativních vlivů
- Nový zákon o zbraních – hlavní a vedlejší držitelé a změny v posuzování zdravotní způsobilosti
- Klientská zóna Jenda – právní účinky činění podání a doručování písemností
- Kdo vlastní mosty a kdo má povinnost je udržovat?
- Změny zápisu zástavního práva do katastru nemovitostí už nejsou tabu. ČÚZK mění dlouholetou praxi
- Nenápadná novela SŘS s velkým potenciálem: urychlí změny ve správním soudnictví výstavbu?
- Jedno užívání, dvě platby: Neudržitelnost souběžného zpoplatnění nájmu a poplatku za užívání veřejného prostranství
- Zákon o přístupnosti

- Nejvyšší soud k zásadě reformationis in peius v insolvenčním řízení