Devět kroků k zajištění souladu s právní úpravou na ochranu osobních údajů

Předložený materiál není komplexním návodem k řešení problematiky. Jedná se pouze o rámcový doporučený postup, jehož důsledné provedení při znalosti problematiky může vést k zajištění souladu s právní úpravou na ochranu osobních údajů. Materiál se nezaobírá základním pojmoslovím a věnuje se pouze případům, které podléhají právní úpravě na ochranu osobních údajů, a zaměřuje se na soukromé osoby nevykonávající veřejnou moc. Stranou tedy nechává například nakládání s osobními údaji pro osobní potřebu, které je mimo působnost této právní úpravy, stejně jako související občanskoprávní konotace související s ochranou osobnosti.

Vzhledem k tomu, že platný zákon č. 101/2000 Sb., o ochraně osobních údajů, dosud nebyl odpovídajícím způsobem novelizován, nezbývá než odkazovat přímo na nařízení Evropského parlamentu a Rady č. 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 (dále jen „obecné nařízení")

1. Mapování

Výchozím krokem k zajištění souladu s právní úpravou na ochranu osobních údajů, pokud prozatím tato problematika nebyla řešena, je zmapování nakládání s osobními údaji. V rámci tohoto mapování je třeba se zaměřit zejména na zjištění:

a. s osobními údaji jakých osob je nakládáno (například zaměstnanci, spotřebitelé, členové společenství vlastníků jednotek, osoby zaznamenané kamerovým systémem);

b. s jakými osobními údaji dotyčných osob je nakládáno (například identifikační – jméno, příjmení, bydliště, datum narození, kontaktní – jméno, příjmení, bydliště, telefonní spojení, adresa el. pošty, dále například údaje o pracovním výkonu, o majetkových poměrech, o rodinném stav, včetně počtu dětí, záznam z kamerového systému atp.);

c. v jaké formě (listinné, IT systém), resp. na jakých nosičích jsou údaje vedeny (například v listinné kartotéce, v počítačovém programu/souboru);

d. jaké operace se s údaji provádí (například kopírování, zpřístupňování, předávání, včetně předávání do třetích zemí);

e. jaké osoby a kdy s údaji pracují (například personalistka či mzdová účetní při výpočtu mezd, bezpečnostní technik při zjišťování identity osoby, která poškodila věci sledované kamerovým systémem, ale třeba i externí poskytovatel služeb, který má postavení zpracovatele).

2. Účel

Každé nakládání s osobními údaji musí mít svůj legitimní a legální účel. Účel zpracování osobních údajů je cíl, kterého má být s osobními údaji dosaženo. Může se jednat o splnění právní povinnost (například vedení knihy úrazů podle předpisů pracovního práva) nebo jen o obecně deklarovaný cíl (například ochrana majetku – tento účel je obvyklý u kamerových systémů). Nemá-li vedení určitého údaje ke konkrétní osobě žádný účel, jde o protiprávní nakládání s osobními údaji dotyčného člověka.

Účel je jako jednotící prvek rozhodný z hlediska právní úpravy. Od účelu je nebo může být odvislých řada povinností správce osobních údajů; například doba uchování, rozsah údajů, přístup k údajům.

Mapování podle bodu 1 je tudíž třeba zakončit s tím, že se zjištěné informace přiřadí pod příslušné účely. Lze doporučit formulaci obecnějších účelu zpracování, jako je například:

a. personální a mzdová agenda;
b. kamerový systém;
c. odběratelé a dodavatelé;
d. marketing;
e. správa bytového domu.

Údaje zpracovávané pro jednotlivé účely musí být vedeny odděleně. Může tudíž nastat situace, že jeden údaj bude veden v několika evidencích.

Údaje musí být zpracovávány pouze za účelem, pro který byly shromážděny. Využití údajů k jinému účelu je možné pouze při splnění zákonných podmínek.

3. Právní podklad

Každé zpracování osobních údajů musí být v plném rozsahu, tedy z hlediska zejména (a) dotčených lidí (subjektů údajů), jejichž osobní údaje jsou zpracovávány, (b) osobních údajů, které se zpracovávají, (c) doby, po kterou se zpracovávají a (d) jednotlivých operací s údaji, pokryto některým z šesti právních titulů pro zpracování; musí být pokryta každá osoba, každý údaj, každá operace a vždy po celou dobu.

Právní důvody pro zpracování jsou:

a. souhlas dotyčného člověka (subjektu údajů);
b. plnění právní povinnosti správce založené právním předpisem nebo rozhodnutím (například vedení evidence pro daňové účely nebo pro účely sociálního pojištění) – při využívání tohoto právního důvodu je vhodné evidovat, který právní předpis konkrétně povinnost ukládá;
c. plnění smlouvy s dotyčným člověkem (subjektem údajů) včetně nezbytných opatření před uzavřením smlouvy na žádost takového člověka (například nájemní smlouva, pracovní smlouva);
d. oprávněný zájem správce nebo třetí strany (například ochrana majetku, kontaktování obchodního partnera), kdy tyto zájmy mají větší váhu než dotčené zájmy (soukromí a ochrana osobních údajů) člověka, s jehož údaji se nakládá (subjektu údajů);
e. životně důležitý zájem subjektu údajů nebo jiné fyzické osoby;
f. výkon veřejné moci nebo plnění úkolu ve veřejném zájmu.

Při běžné činnosti soukromé osoby neúčastnící se výkonu veřejné moci by neměly připadat v úvahu důvody podle písm. e. a f.

Je vhodné v co nejmenší míře spoléhat na souhlas. Získání platného souhlasu je relativně komplikované, navíc je souhlas odvolatelný; souhlas nemusí být (vyjma citlivých údajů) výslovný, musí však být vždy prokazatelný.

Souhlasem není možné rozšířit zákonné účely. Není možné využít souhlas, pokud se jedná o údaje, které mají být získány a zpracovávány na základě zákona; takové jednání by mohlo být kvalifikováno jako nesprávní informování dotčeného člověka (subjektu údajů) a mohlo by být sankcionováno. I souhlas je limitován principem nezbytnosti.

Po určení účelu je třeba identifikovat právní titul zpracování.

4. Nezbytnost

V návaznosti na účel a právní podklad nakládání (zpracování) s osobními údaji je třeba určit, jaké osobní údaje jsou nebytné; legálně lze nakládat pouze s údaji, bez nichž není možné dosáhnout účelu, a které jsou kryty právním podkladem zpracování.

Stejné platí i ohledně doby uchování údajů; doba nesmí být ani delší (jednalo by se o neoprávněn zásah) a ani kratší (nebylo by možné dosáhnout účelu). Po uplynutí doby musí být údaje vymazány nebo alespoň trvale vylou2čeny z dalšího zpracování. Případně lze, při splnění zákonných podmínek, navázat dalším zpracováním osobních údajů.

5. Přesnost

Osobní údaje musí být z hlediska účelu zpracování přesné. Přesností se v tomto případě míní i komplexnost údajů, pokud je například rozsah určen právním předpisem. S nepřesnými údaji není možné dosáhnout sledovaného účelu (například u seznamu členů spolku, aby bylo takové zpracování osobních údajů funkční, tedy bylo možné v případě potřeby členy kontaktovat a sezvat, je třeba, aby byl seznam kompletní, a aby byly kontaktní údaje aktuální).

Je třeba určit proces k zajištění přesnosti údaji. Přesnost lze zajistit například uložením povinnosti oznamovat změnu údajů, při komunikaci s dotyčným, jeho aktivním oslovením nebo i jinak (ve shora uvedeném případě například na členské schůzi).

6. Bezpečnost

Na základě úvahy o možných rizicích v jednotlivých fázích nakládání s údaji (shromáždění, uložení, zpracování, likvidace) je třeba ke každému jednomu účelu a zpracování určit a následně provést odpovídající bezpečnostní opatření tak, aby byla rizika minimalizována a aby se pokud možno předešlo nepříznivým důsledkům.

Bezpečnostní opatření musí být přiměřená charakteru údajů, které jsou zpracovávány (jiná opatření budou přijata ve vztahu ke zdravotnické dokumentaci a jiná k seznamu vizitek) rizikům a jejich pravděpodobnosti (ztráta dat z PC v důsledku poškození HDD – pravděpodobné atp.), možným negativním důsledkům, ale i možnostem dotyčného správce (prostorovým, finančním, personálním atp.); například živnostník (instalatér), který má místo podnikání ve svém bytě a nemá žádného zaměstnance, dostojí svým povinnostem, uloží-li dokumentaci doma do skříně, hrozí-li její zničení či poškození (ze strany dětí nebo zvířat), zabezpečí-li přístup do PC heslem, PC opatří antivirovým programem, bude pořizovat zálohy dat a tyto zabezpečovat a bude-li dodržovat pravidla bezpečné komunikace.

V základu je třeba uvažovat o bezpečnosti:

a. **Osobní** – řízení přístupu k osobním údajů, tj. určení kdo, kdy a z jakého důvodu k údajům bude mít přístup a určení oprávnění k nakládání s nimi (například personalista při zpracování mezd) – přístup musí být jen v odůvodněných případech;
b. **Prostorové** – řízení přístupu k údajům, tj. je-li to možné přenesení kritérií z oblasti osobní bezpečnosti (například klíče od spisovny pouze osobám oprávněným přistoupit ke spisům), a další potřebná bezpečnostní opatření (zámky, kamery, mříže);
c. **Výpočetní techniky** - řízení přístupu k údajům, tj. přenesení kritérií z oblasti osobní bezpečnosti (rozdělení uživatelských oprávnění), a další potřebná bezpečnostní opatření (hesla, antivirové programy atp.).

Mezi prvky k zajištění bezpečnosti spadá i přijetí smlouvy se zpracovatelem. Smlouva má předepsané náležitosti podle čl. 28 odst. 3 obecného nařízení. Měla by však obsahovat i pravidla pro komunikaci, spolupráci stran, rozdělení úkolů ve vztahu k plnění povinností vůči subjektům údajů, pravidla k zajištění bezpečnosti informací o zabezpečení a informací o parametrech zpracování atp. Do budoucna by měly existovat (schválené Komisí EU nebo Úřadem pro ochranu osobních údaj) tzv. standardní smluvní doložky, které by měly pokrývat základní náležitosti smlouvy.
Dále je třeba zajistit bezpečnost vůči třetím osobám (poskytovatelům služeb), které se pohybují (fyzicky nebo online) ve sféře správce, jejichž úkolem však není zpracovávat osobní údaje, ale mohou mít k údajům přístup nebo mohou mít přístup k informacím o jejich zabezpečení nebo informacím o zpracování jako takovém. S těmito osobami (například IT podpora, úklidová služba) je taktéž vhodné zakotvit smluvní garance k zajištění bezpečnosti.

Ve složitějších provozech a společnostech/organizacích je vhodné organizačně technická opatření k zajištění bezpečnosti údajů a informací sepsat a vyhlásit ve formě bezpečnostní směrnice; pro tyto účely bude možné do budoucna (nejméně částečně) využít tzv. kodexy chování.

Součástí bezpečnostních opatření je i pravidelné školení osob, které přichází do kontaktu s údaji a informacemi o bezpečnostních pravidlech a ověřování jejich znalostí.

Bezpečnostní opatření, jejich efektivita a spolehlivost, by měla být pravidelně prověřována a bezpečnostní opatření by případně měla být upravována, obnovována a doplňována dle potřeby.

Ve stanovených případech bude třeba provádět tzv. posouzení vlivu na ochranu osobních údajů (čl. 35 an. obecného nařízení)

Samostatnou oblastí vyžadující zvláštní záruky (například standardní smluvní doložky) je využití služeb mimo EU – zde jde o tzv. předávání osobních údajů do třetích zemí.

Částečně jako prvek k zajištění bezpečnosti zpracování osobních údajů lze vnímat i institut pověřence pro ochranu osobních údajů. Soukromé osoby neúčastnící se na výkonu veřejné moci budou mít pověřence pouze výjimečně – ledaže by jejich hlavní činností (součástí takové činnosti) bylo rozsáhlé zpracování citlivých údajů (více jak 5000 záznamů, například nemocnice), nebo by bylo jejich hlavní činností (součástí takové činnosti) rozsáhlé pravidelné a systematické monitorování osob (například systematické sledování spotřebitelského chování v souvislosti s hlubokými marketingovými praktikami). Pověřence pro ochranu osobních údajů je možné si ustanovit i dobrovolně.

7. Informace

Vyjma případů, kdy je zjevné, že člověk, s jehož údaji je nakládáno (subjektu údajů), již tyto informace má, je třeba mu poskytnout informace v rozsahu čl. 13 obecného nařízení; uvedené platí obdobně pro případ, kdy nebyly údaje získány přímo od subjektu údajů (viz čl. 14 obecného nařízení). Informace obsahuje krom jiného i poučení o právech, které mu v souvislosti se zpracováním vůči správci náleží a o způsobu, jak se tato práva uplatňují.

V této fázi je tedy třeba formulovat informaci pro jednotlivá zpracování a určit vhodný způsob plnění informační povinnosti. Informace musí být formulována srozumitelně, jednoduchým jazykem; v této souvislosti je vhodné využívat jednak mnohovrstevnost informací a jednak, až budou vydány, standardizované ikony.

8. Práva

Subjektu údajů vůči správci v souvislosti se zpracováním osobních údajů náleží řada práv (právo na informace, právo přístup k osobním údajů, včetně kopie zpracovávaných osobních údajů, právo na opravu údajů, právo na výmaz údajů, právo na omezení zpracování, právo na námitku atd.). V návaznosti na povahu jednotlivých zpracování (zda se realizují elektronicky nebo v listinné formě, zda jsou povinná podle právního předpisu nebo se realizují na základě souhlasu subjektu údajů) může být rozsah práv různý. K žádosti (uplatnění práva) musí správce reagovat v zákonné lhůtě. Uplatňování práv je bezplatné. Jen v předepsaných případech je možné žádost odmítnout či vyřízení žádosti zpoplatnit.

Je tudíž třeba ve vztahu ke každému ze zpracování osobních údajů určit práva, která člověku náleží. Tuto informaci je třeba zahrnou do informační povinnosti (bod 7). Dále je třeba určit proces, jehož prostřednictvím bude žádost o uplatnění práva vyřizována, včetně procesu, jímž budou realizována opatření, kterými se bude reagovat na žádost subjektu údajů (například se provede oprava). Subjektu údajů náleží mj. právo podat stížnost k Úřadu pro ochranu osobních údajů ohledně vyřízení jeho žádosti o uplatnění práv.

9. Úřad pro ochranu osobních údajů – komunikace

Správce musí být schopen po celou dobu zpracování osobních údajů prokázat (v případě kontroly), že řádně plní jednotlivé povinnosti plynoucí z právní úpravy (zásada odpovědnosti), jak jsou popsány v bodech 1 až 8 shora. Vyžaduje-li to struktura a složitost organizace, lze doporučit vést si dokumentaci k jednotlivým zpracováním, jak budou rozděleny podle účelů (viz bod 2). V dokumentaci je vhodné evidovat základní parametry zpracování a zaznamenávat zde další podstatné skutečnosti, jako je například uplatnění práva ze strany subjektu údajů a související reakci a opatření správce.

Právě popsaná evidence není záznamem o činnostech zpracování. Záznamy o činnostech zpracování (čl. 30 obecného nařízení) jsou speciální evidence jednotlivých zpracování s předepsanou strukturou, kterou musí správce (až na předepsané výjimky) vést primárně pro případ kontroly ze strany Úřadu pro ochranu osobních údajů; jedná se o evidenci obdobnou stávajícím záznamům ve veřejném registru zpracování (viz www.uoou.cz – sekce registr).

Správce musí zaznamenat každé porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů (například ztrátu zabezpečeného nosiče s osobními údaji, který neobsahuje jejich jedinou kopii).

Pokud takový bezpečnostní incident představuje riziko pro práva a svobody subjektu údajů (například odeslání elektronické pošty na nesprávnou adresu, kdy přílohou je jmenné rozpočítání spotřeby vody, tepla a elektřiny v bytovém domě), je povinností jej způsobem určeným Úřadem pro ochranu osobních údajů (zatím nebyl způsob určen) oznámit jmenovanému úřadu; oznamované informace se uvádí v čl. 33 odst. 2 obecného nařízení. Oznámení se činí bez zbytečného odkladu, nejpozději však do 72 hodin od chvíle, kdy se o něm správce dozví.

Pokud by takový bezpečnostní incident představovat vysoké riziko pro subjektu údajů (například nahlédnutí do personálního spisu neoprávněnou osobu, kdy spis obsahuje krom jiného jméno, příjmení, datum narození, rodné číslo a bydliště subjektu údajů, nebo ztráta přístupových údajů do elektronického bankovnictví subjektu údajů), oznámí se vedle úřadu i dotyčnému člověku, včetně opatření, která by měl přijmout k tomu, aby předešel možným negativním důsledkům.

Zejména pokud se jedná o správce se složitější organizační strukturou, je vhodné vnitřním předpisem/směrnicí nastavit procesy pro oznamování bezpečnostních incidentů.

Je třeba dbát důsledně toho, že oznamování bezpečnostních incidentů může být také zpracováním osobních údajů a je třeba určit taková pravidla, aby i v tomto případě byla respektována právní úprava na ochranu osobních údajů (viz shora); zejména je třeba dbát na to, jelikož v této souvislosti může dojít k určité stigmatizaci či viktimizaci dotčených osob, aby byla při oznamování incidentů uvnitř správce zachovávána maximální diskrétnost.

V Praze dne 2. května 2018

Materiál vznikl ve spolupráci Felix a spol, advokátní kanceláře s.r.o. a Hospodářské komory České republiky