Jednatelé a jejich zodpovědnost za **GDPR** (I.)



Mgr. Ing. Martin Lukáš
Mgr. Barbora Kudrhalt Suchá
Mgr. David Hlaváček, LL.M.
Advokátní kancelář Weinhold Legal

GDPR je přelomovou legislativou Evropské unie, která zakotvuje nový jednotný právní rámec ochrany osobních údajů v celé EU. Čas na přípravu na účinnost nařízení se rychle krátí. Žádné další přechodné období nebylo stanoveno, a tak již od 25. 5. 2018 budou muset být všechny společnosti, v souladu s novou zásadou odpovědnosti, **schopny prokázat, že řádně plní veškerá nařízení podle GDPR, jinak jim budou hrozit vysoké sankce**. Zrevidujte díky následujícímu článku své povinnosti a ujistěte se, že znáte nová pravidla!

Nařízení Evropského parlamentu a Rady (EU) 2016/679 z 27. 4. 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále také jen „GDPR" či „nařízení"), přijaté v dubnu 2016, nabude účinnosti 25. 5. 2018 a zruší stávající českou právní úpravu obsaženou v zákoně o ochraně osobních údajů – zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, jenž implementoval směrnici Evropského parlamentu a Rady 95/46/ES z 24. 10. 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, která bude s účinností GDPR taktéž zrušena. V českém právním řádu tak zůstanou pouze ustanovení upravující fungování Úřadu pro ochranu osobních údajů (ÚOOÚ) a některá národní specifika povolená GDPR, a to pravděpodobně ve zcela novém zákoně o zpracování osobních údajů, jenž se v současnosti projednává v připomínkovém řízení.

Nový zákon upravující národní specifika ČR se nyní projednává v připomínkovém řízení

Hlavní cíle nařízení

Hlavními cíli přijetí nařízení bylo prohloubit a sjednotit právní rámec a standardy ochrany osobních údajů v celé Unii, zajistit jejím občanům (nařízení pracuje s pojmem „subjekt údajů", tedy osoba, jejíž osobní údaje jsou zpracovávány) co nejvíce práv a ochrany proti neoprávněnému nakládání a zacházení s jejich osobními údaji a reagovat na rozvoj nových technologií, které umožňují stále širší zásahy do soukromí jednotlivců. Základní principy ochrany osobních údajů však zůstanou i po účinnosti GDPR zachovány.

GDPR rozšíří okruh subjektů, které musejí při zpracování osobních údajů dodržovat práva a povinnosti vyplývající z práva EU. Nařízení se obecně vztahuje na každého – ať už jednotlivce, obchodní společnosti, nebo insti-

tuce –, kdo zpracovává osobní údaje fyzických osob nacházejících se na území Evropské unie, včetně obchodních společností a jiných institucí nacházejících se mimo území EU, které aktivně působí na evropském trhu. Z působnosti nařízení je vyloučeno zpracování osobních údajů pro výkon výlučně osobních či domácích prací, tj. pouze pro osobní potřebu.

Nařízení přinese společnostem a jejich jednatelům některé zcela nové povinnosti, jako například povinnost vést záznamy o zpracování osobních údajů, provést posouzení vlivu na ochranu osobních údajů, zavést záměrnou a standardní ochranu osobních údajů či v jistých případech jmenovat pověřence pro ochranu osobních údajů. Některé stávající povinnosti, jako je například informační povinnost či povinná smlouva o zpracování osobních údajů, budou rozšířeny.

Na jaké oblasti se zaměřit

Jednatelé by proto nyní měli intenzivně pracovat na zajištění souladu s nařízením, a to zejména v následujících 3 oblastech:

- oblast procesů – zmapování datových toků a implementace požadavků nařízení do procesů společnosti;
- oblast IT – revize automatizovaných procesů správy a zpracování osobních údajů a zabezpečení těchto údajů, implementace opatření podle GDPR;
- oblast právní – úprava právní dokumentace související se správou a zpracováním osobních údajů v souladu s GDPR.

V článku se dále zaměříme na právní oblast, a to na příkladu zaměstnaneckých osobních údajů, protože ty se v praxi týkají všech společností. Obdobné povinnosti pro společnosti platí i při zpracování osobních údajů o zákaznících či dodavatelích, při provozování věrnostních programů atp.

Osobním údajem se rozumí jakákoliv informace, která se týká určené nebo přímo či nepřímo určitelné fyzické osoby. Osobním údajem bude tedy jméno, pohlaví, věk, datum narození, rodné číslo, osobní stav, údaj o vlastnictví určité věci, údaj o výši mzdy, ale také například IP adresa, lokační údaje (např. z GPS instalované ve služebním automobilu či telefonu), fotografie osoby a řada dalších.

Do zvláštní kategorie osobních údajů (nynější citlivé osobní údaje), pro jejichž zpracování je nutné splnit ještě přísnější podmínky, patří například biometrické údaje, údaje o členství v odborových organizacích či údaje o zdravotním stavu.

Pod pojmem zpracování osobních údajů je pak třeba si představit jakoukoliv operaci či soubor více operací s osobními údaji nebo soubory osobních údajů – ať už jsou prováděny automatizovaně, či ručně –, jako je například shromáždění, uložení, vyhledání, použití, šíření, výmaz atd.

> Za jednu z nejvýznamnějších zásad ochrany osobních údajů lze označit zásadu zákonnosti. Plyne z ní, že zpracování osobních údajů musí vždy probíhat na základě alespoň jednoho z právních titulů vyjmenovaných v nařízení.

Nejdůležitější právní tituly a účel zpracování

Nejdůležitějšími právními tituly jsou:

- plnění právní povinnosti správce – povinnost zpracovávat osobní údaje o zaměstnancích stanoví hned několik právních předpisů (např. zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů; zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů; § 95 zákona č. 187/2006 Sb., o nemocenském pojištění, ve znění pozdějších předpisů; § 37 zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů);
- nezbytnost pro uzavření či plnění smlouvy, jejíž stranou je subjekt údajů – například pro uzavření pracovní smlouvy je nutné uvést identifikační údaje zaměstnance, pro vyplacení mzdy na bankovní účet zaměstnance je nutné sdělit zaměstnavateli číslo tohoto účtu atp.;
- nezbytnost pro účely oprávněných zájmů správce či třetí strany – správce si sám určí, co považuje za oprávněný zájem.

něný zájem: například pořizování kamerových záznamů může být prováděno na základě oprávněného zájmu správce na ochraně majetku; správce však musí být schopen prokázat, že nad jeho oprávněným zájmem nepřevažují zájmy nebo základní práva a svobody subjektů údajů;

» souhlas subjektu údajů – oproti současné úpravě, kdy je souhlas uveden jako hlavní právní titul, dochází ke změně a souhlas by naopak měl být vyžadován až v případě, kdy pro zpracování osobních údajů nelze využít žádný jiný titul; ve vztahu k zaměstnancům je při používání souhlasů nutná ještě větší opatrnost, neboť závislé postavení zaměstnance může vylučovat svobodu souhlasu, která je jednou ze základních podmínek jeho platnosti; na tuto skutečnost upozorňuje i evropská Pracovní skupina pro ochranu osobních údajů ve svém novém stanovisku (stanovisko Pracovní skupiny 29 ke zpracování osobních údajů v práci z 8. 6. 2017); souhlas navíc může subjekt údajů kdykoliv odvolat (GDPR možnost odvolání podrobně upravuje), a nelze se na něj tedy příliš spoléhat.

Kromě právního titulu je správce před započetím jakéhokoliv zpracování osobních údajů povinen stanovit účel zpracování (např. vedení personální a mzdové agendy). Účel musí být stanoven tak určitě, aby z něj vyplývalo, jaká zpracování na jeho základě budou probíhat, a aby mohl být posouzen soulad těchto zpracování s právními předpisy. Zpracovávat pak správce může pouze údaje nezbytné k dosažení stanoveného účelu a jen po dobu nezbytnou k jeho dosažení.

Povinnosti společností a jejich jednatelů podle GDPR

Informační povinnost

Základní praktickou povinností, která se týká všech správců osobních údajů, je povinnost informovat subjekt údajů o zpracování jeho osobních údajů. Informační povinnost má správce jak v případě, že osobní údaje získal přímo od subjektu údajů, tak tehdy, získá-li je jiným způsobem. Ke splnění informační povinnosti musí dojít nejpozději v okamžiku získání osobních údajů.

Nařízení nově upravuje i způsob a formu plnění informační povinnosti a další komunikace se subjekty údajů. Všechny informace a sdělení musejí být poskytovány stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jednoduchých jazykových prostředků. Měly by tak být využívány různé vizualizační metody, text by měl být přehledně členěný, psaný například ve formě otázek a odpovědí či v několika vrstvách (základní stručné shrnutí s odkazy na podrobnější informace k jednotlivým oblastem). Zapomínat nelze ani na poskytování informací v rámci osobní či telefonické komunikace, při které jsou získávány osobní údaje.

Povinný rozsah informační povinnosti se oproti současné právní úpravě významně rozšiřuje. Dříve poskytnuté informace proto nebudou dostačující a je třeba je subjektům před účinností GDPR poskytnout znovu. V obvyklých případech je správce povinen sdělit subjektu údajů svou totožnost a kontaktní údaje (pokud má pověřence, pak i kontaktní údaje tohoto pověřence), účel a právní titul (příp. i důvod) zpracování, dobu uložení osobních údajů a práva subjektu údajů; je-li to relevantní, tak rovněž informace o příjemcích osobních údajů, ohledně předávání údajů do třetích zemí, možnosti odvolat souhlas, automatizovaného rozhodování atd.

!

Ke splnění informační povinnosti o právech subjektu údajů nepostačí, pokud správce pouze odkáže na úpravu obsaženou v GDPR. Jednotlivá práva je třeba vyjmenovat – tedy uvést, že subjekt údajů má právo na přístup k osobním údajům, právo na opravu, právo na výmaz („právo být zapomenut"), právo na omezení zpracování, právo na přenositelnost údajů, právo vznést námitku, právo nebýt předmětem automatizovaného individuálního rozhodování včetně profilování a právo podat stížnost u dozorového úřadu.

Ideálně by měl správce i vysvětlit podstatu jednotlivých práv tak, aby jim subjekt údajů porozuměl: Například že zcela nové právo na přenositelnost údajů znamená, že je zaměstnavatel povinen na žádost zaměstnance předat jeho osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu novému zaměstnavateli, je-li to technicky proveditelné.

Povinnost vést záznamy o činnostech zpracování

Další novou povinností správců a zpracovatelů je vedení záznamů o činnostech zpracování, za něž odpovídají. Každý správce či zpracovatel bude povinen na žádost dozorového orgánu mu tyto záznamy zpřístupnit. Dalo by se říci, že záznamy o činnostech zpracování nahradí současnou ohlašovací povinnost vůči ÚOOÚ, neboť obsah těchto záznamů je prakticky totožný se současným ohlášením. Ohlašovací povinnost bude s účinností GDPR zrušena.

Záznamy musejí obsahovat minimálně: kontaktní údaje správce, účel zpracování, kategorie subjektů údajů, kategorie osobních údajů, kategorie příjemců údajů, případně informaci o předávání informací do zahraničí, je-li to možné, tak také lhůty pro vymazání jednotlivých kategorií údajů, a rovněž popis technických a organizačních opatření, která správce či zpracovatel přijal v souvislosti se zabezpečením osobních údajů.

Povinnost ohlásit porušení zabezpečení osobních údajů

Dojde-li k porušení zabezpečení osobních údajů, je správce povinen takovýto bezpečnostní incident bez zbytečného odkladu (do 72 hodin) ohlásit ÚOOÚ. Správci jsou dále povinni vést registr porušení a přijatých opatření. Ohlášení není správce povinen provádět, pokud je nepravděpodobné, že by porušení mělo za následek riziko pro práva a svobody fyzických osob; vždy je však povinen porušení zabezpečení alespoň zdokumentovat. Pokud by naopak bezpečnostní incident mohl mít za následek vysoké riziko pro práva a svobody subjektů údajů, musí jej ohlásit i jednotlivým subjektům.

Povinnost provést posouzení vlivu na ochranu osobních údajů je další z novinek, které GDPR přináší. Cílem je, aby otázky ochrany osobních údajů byly zvažovány již v okamžiku zavádění jakýchkoliv opatření v rámci společnosti.

Povinnost vypracovat posouzení vlivu v rozsahu stanoveném GDPR bude dopadat na správce či zpracovatele, kteří provádějí systematické a rozsáhlé zpracování osobních údajů, systematické a rozsáhlé vyhodnocování osobních údajů, jež je založeno na automatizovaném zpracování, či systematické monitorování veřejně přístupných prostorů. Jedná se tak například o banky, pojišťovny, finanční instituce, ale také o společnosti poskytující věrnostní programy, on-line nebo telekomunikační služby založené na lokalizačních datech či o správce využívající cílenou behaviorální reklamu.

Dospěje-li správce či zpracovatel po prvotním posouzení k závěru, že na něj povinnost provést posouzení vlivu na ochranu osobních údajů nedopadá, měl by toto zjištění v souladu se zásadou odpovědnosti přiměřeně zdokumentovat, aby byl schopen prokázat soulad s nařízením. Pokud by naopak z provedeného posouzení vlivu vyplynulo, že zamýšlené zpracování je vysoce rizikové a riziko nelze zmírnit přiměřenými prostředky, bude správce povinen zamýšlené zpracování konzultovat s ÚOOÚ.

Záměrná a standardní ochrana, bezpečnost údajů

Aby byl správce schopen doložit soulad s nařízením, je povinen při-

tip

Výjimka z této povinnosti platí pro společnosti s méně než 250 zaměstnanci, pokud zpracování osobních údajů není jejich hlavní činností, neexistuje riziko pro práva a svobody subjektů údajů a nedochází ke zpracování „citlivých údajů".

jmout určité interní koncepce, provést změny ve svých procesech a zavést taková opatření, která budou naplňovat zásady záměrné a standardní ochrany osobních údajů. Správce i zpracovatel musejí přijmout taková organizační a technická opatření, aby zajistili dodržování všech zásad zpracování osobních údajů. Rovněž jsou povinni přijmout adekvátní bezpečnostní opatření k zamezení nežádoucím jevům, jako je náhodné nebo protiprávní zničení, ztráta či pozměnění údajů, neoprávněné zpřístupnění údajů třetím osobám anebo neoprávněný přístup k údajům při přenosu, uložení či jiném zpracování.

Je třeba zajistit důvěrnost, integritu, dostupnost a odolnost systémů, například pomocí šifrování a zálohování zpracovaných osobních údajů. Bezpečnostní opatření by podle GDPR měla být pravidelně testována, posuzována a jejich účinnost hodnocena.

Pseudonymizace osobních údajů

Novým bezpečnostním opatřením, doporučovaným nařízením, je pseudonymizace osobních údajů. Například osobní údaje zaměstnanců jsou při ní upraveny takovým způsobem, že je každému zaměstnanci přidělen určitý kód a databáze je vedena tak, že z ní nelze určit, kterému zaměstnanci daný osobní údaj (kupř. výše mzdy) patří. Klíč je bezpečně uložen mimo tuto databázi a jeho pomocí lze ke kódům přiřadit osobní údaje a (identifikovat) tím i konkrétního zaměstnance.

Někteří správci či zpracovatelé budou dále nově povinni jmenovat pověřence pro ochranu osobních údajů. Tuto a další povinnosti přiblížíme v dalším čísle časopisu.