NEWSLETTER 5/2017

Nová právní úprava ochrany osobních údajů – nařízení GDPR

I. Nařízení GDPR

- **Dne 25. května 2018** nabude **účinnosti** ve všech členských státech EU **Obecné nařízení o ochraně osobních údajů**, tj. nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (*General Data Protection Regulation*), tzv. **nařízení GDPR**.

- Nařízení GDPR představuje **nejvýznamnější změnu v oblasti ochrany soukromí a osobních údajů** od přijetí původní směrnice (95/46/ES), **sjednocuje tuto oblast na úrovni EU** a bude mít velký dopad na všechny subjekty, které osobní údaje zpracovávají.

- **Hlavním cílem** nového nařízení je posílit ochranu fyzických osob v souvislosti s rozšířením internetu a moderních sledovacích nástrojů a zároveň usnadnit volný pohyb osobních údajů v rámci jednotného digitálního trhu.

- Nová právní úprava byla přijata v podobě **nařízení**, bude tedy **účinná v celé EU** a nebudou vznikat národní právní předpisy. V ČR **nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů**.

II. Základní pojmy dle GDPR

- **Osobními údaji** dle GDPR jsou i nadále veškeré informace o identifikované nebo přímo či nepřímo identifikovatelné fyzické osobě (subjekt údajů). Nová definice však zdůrazňuje, že při posuzování, zda je osoba identifikovatelná, je třeba hledět také na lokalizační údaje a elektronické identifikátory, jako jsou síťové adresy či cookies.

- **Zpracováním osobních údajů** se jako doposud rozumí jakákoliv operace nebo soubor operací s osobními údaji, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení, vyhledání, nahlédnutí, použití, šíření, omezení, výmaz, zničení atd.

- **Správcem** je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, jenž sám nebo společně s jinými určuje účel, prostředky a podmínky zpracování.

- **Zpracovatelem** je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

III. Souhlas se zpracováním osobních údajů

- **Souhlas se zpracováním osobních údajů** je podle GDPR definován jako „*jakýkoliv* ***svobodný, konkrétní, informovaný a jednoznačný*** *projev vůle*“, kterým subjekt údajů dává, a to buď prostřednictvím prohlášení, nebo jiným zjevným potvrzením, své svolení k tomu, aby osobní údaje, které se jej týkají, byly předmětem zpracování.

- Souhlas bude muset být prezentován **samostatně** od ostatních podmínek předkládaných danému subjektu údajů ke schválení a nebude moci být podmínkou poskytování služby, pokud pro její poskytování nebude zpracování daných údajů pro konkrétní účel nezbytné.

- Je-li zpracování údajů založeno na souhlasu, musí být správce schopen doložit, že subjekt údajů souhlas se zpracováním svých údajů udělil.

- V rámci souhlasu budou muset být jednotlivé subjekty informovány o svých právech dle GDPR, souhlas bude moci být kdykoliv **odvolatelný**.

- Souhlas získaný před účinností GDPR, který nebude odpovídat požadavkům GDPR, již nebude nadále považován za aktuální a použitelný.

IV. Práva subjektů údajů podle GDPR

- Jedním z největších dopadů GDPR v praxi bude **výrazné posílení práv subjektů údajů**. Těmito právy jsou zejména:

  (i) **právo na informovanost a přístup** dává subjektům údajů právo vědět a být informován zejména o tom, za jakým účelem se osobní údaje zpracovávají, znát dobu, po kterou budou údaje uchovávány, znát příjemce jeho osobních údajů, vědět, v čem spočívá logika automatizovaného zpracování a jaké mohou být důsledky takového zpracování;

  (ii) **právo na opravu** spočívá v právu subjektu údajů na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají;

  (iii) **právo na výmaz** je zcela novým právem podle GDPR a rozumí se jím právo subjektů na to, aby správce bez zbytečného odkladu vymazal jejich osobní údaje, pokud je dán jeden z následujících důvodů: (a) osobní údaje již nejsou potřebné pro účel, pro který byly shromažďovány nebo zpracovávány, (b) subjekt údajů odvolá souhlas, pokud je zpracování založeno na souhlasu a neexistuje žádný další právní důvod pro zpracování, (c) subjekt údajů vznese námitku proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování, (d) osobní údaje byly zpracovány protiprávně;

(iv) **právo být zapomenut** je rozšířeným právem na výmaz. Spočívá v provedení přiměřených kroků, včetně technických opatření, k vymazání veškerých odkazů na osobní údaje a jejich kopie. Zde však GDPR uvádí řadu výjimek (např. z důvodů veřejného zájmu v oblasti veřejného zdraví či pro statistické účely apod.);

(v) **právo na omezení zpracování** znamená právo na to, aby správce omezil zpracování v případech, kdy (a) subjekt popírá přesnost údajů, (b) zpracování bylo protiprávní, ale subjekt odmítá výmaz údajů a požaduje omezení jejich použití, (c) správce osobní údaje již nepotřebuje, ale subjekt je potřebuje pro obhajobu svých právních nároků (d) vznesl námitku proti zpracování. Skutečnost, že zpracování osobních údajů je omezeno, by měla být v systému jasně vyznačena;

(vi) **právo na přenositelnost** může být subjektem uplatněno, pokud (a) je zpracování založeno na souhlasu nebo na smlouvě a (b) je prováděno automatizovaně. Zahrnuje právo subjektu získat své osobní údaje, které poskytl správci, **ve strukturovaném, běžně používaném a strojově čitelném formátu**, a právo ponechat si je pro další osobní užití nebo předat tyto údaje jinému správci. Pokud je to technicky proveditelné, má právo, aby osobní údaje byly předány přímo jedním správcem správci druhému;

(vii) **právo vznést** kdykoliv **námitku** proti zpracování údajů z důvodů týkajících se konkrétní situace subjektu;

(viii) **právo nebýt předmětem rozhodnutí založeného výhradně na automatizovaném zpracování**, které má pro subjekt údajů právní účinky.

V. Zrušení registrační povinnosti u Úřadu pro ochranu osobních údajů a zavedení principu tzv. zodpovědnosti

- Nařízení GDPR opouští princip registrace správců u Úřadu pro ochranu osobních údajů a nově zavádí **princip tzv. zodpovědnosti**, který spočívá v povinnosti správců a zpracovatelů údajů bez ohledu na jejich velikost nebo počet zaměstnanců zavést vhodná technická, organizační a procesní opatření za účelem prokázání souladu s principy GDPR.

- Aby mohl správce doložit soulad s GDPR, měl by přijmout vnitřní koncepce, provést procesní změny a zavést opatření, která dodržují zejména zásady **záměrné a standardní ochrany osobních údajů**. Tato opatření by měla mj. spočívat v **minimalizaci** zpracování osobních údajů, v jejich co nejrychlejší **pseudonymizaci**, v **transparentnosti** s ohledem na účely zpracování osobních údajů a v **umožnění přístupu** občanů k jejich údajům.

- Jedním ze způsobů, jimiž mohou správci prokazovat svůj soulad s GDPR je i dodržování **tzv. kodexů chování** vypracovaných odbornými organizacemi.

VI. Pověřenec pro ochranu osobních údajů

- Zcela **novým institutem** je pozice **pověřence pro ochranu osobních *údajů*** *(Data Protection Officer* - DPO). Správce nebo zpracovatel osobních údajů je **povinen** jmenovat pověřence pro ochranu osobních údajů v případě, že:
  (i) zpracování provádí orgán veřejné moci či veřejný subjekt (s výjimkou soudů jednajících v rámci svých soudních pravomocí);
  (ii) jeho hlavní aktivity spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů; nebo
  (iii) jeho hlavní činnosti spočívají v rozsáhlém zpracování zvláštních kategorií údajů (např. údajů o zdravotním stavu).

- Pověřence pro ochranu osobních údajů lze jmenovat **i dobrovolně**.

- **Kvalifikační předpoklady** na pozici pověřence jsou poměrně **vysoké**, požaduje se od něj odborná znalost práva a praxe v oblasti ochrany osobních údajů.

- Pověřenec může svou činnost vykonávat jak **v pracovním poměru**, tak **na základě smlouvy o poskytování služeb**. Správce je povinen zajistit, aby byl pověřenec informován o všech aktivitách správce spojených se zpracováním osobních údajů, pověřenec musí být ohledně své činnosti nezávislý a odpovídat přímo nejvyššímu vedení.

VII. Zabezpečení osobních údajů

- GDPR klade **velký důraz** i na oblast zabezpečení zpracování osobních údajů. V případě jakéhokoliv porušení zabezpečení osobních údajů bude správce povinen bez zbytečného odkladu, nejpozději však do 72 hodin, toto **porušení ohlásit Úřadu pro ochranu osobních údajů** a v závažných případech i dotčeným subjektům údajů.

VIII. Dozor nad správci a zpracovateli působících ve více zemích EU

- Velkou změnu přináší GDPR také ohledně výkonu dozoru nad správci a zpracovateli, kteří působí ve více členských zemích zároveň. Dozor nad zpracováním ve všech zemích, kde správce či zpracovatel sídlí, bude vykonávat pouze jeden orgán dohledu, a to ze země, kde má správce či zpracovatel **hlavní provozovnu,** tj. místo centrální administrativy. Pokud je však o účelu a prostředcích zpracování osobních údajů rozhodováno na jiném místě, bude za hlavní provozovnu považováno toto místo.

IX. Sankce

- GDPR rovněž zavádí **vysoké sankce** za porušení nařízení, které mohou podle závažnosti porušení dosáhnout **10 až 20 mil. eur** nebo jedná-li se o podnik, až výše **2 až 4 % celkového celosvětového ročního obratu** za předchozí finanční rok, podle toho, která hodnota bude vyšší.

Věříme, že výše uvedené shrnutí usnadní Vaši orientaci v nové právní úpravě. V případě potřeby jsme Vám plně k dispozici pro poskytnutí doplňujících informací nebo právní asistenci v dané oblasti.

Editor: JUDr. Magda Stárková, advokát, e-mail: starkova@akvk.cz

---