Spolky a ochrana osobních údajů ve světle GDPR

Mgr. Alena Hájková

www.crdm.cz

Spolky a ochrana osobních údajů ve světle GDPR

Obecné nařízení o ochraně osobních údajů (GDPR, dále jen „Nařízení“) bylo přijato v dubnu 2016 a vstupuje v účinnost **od 25. května 2018**.

S přijetím Nařízení je spojena neopodstatněná panika a množství „poplašných zpráv“. Ve skutečnosti nová unijní úprava většinou spíše zpřesňuje a rozvádí úpravu stávající. Pokud Nařízení přináší větší a podstatnější změny, jsou tyto mířeny na jiné subjekty, než kterými jsou standardní tuzemské spolky či podobné organizace. Reálně dopad Nařízení pocítí především velcí správci a zpracovatelé osobních údajů, kteří v rámci své činnosti pracují s velkým množstvím osobním údajů. Dále pak společnosti zabývající se marketingem a cílenou reklamou, sociální sítě apod. Zvýšenou pozornost přinášeným změnám budou muset také věnovat zaměstnavatelé, veřejné subjekty a subjekty, které pracují s citlivými údaji (zvláštní skupinou osobních údajů).

Hlavní změny:

- zvýšený dosah nových pravidel, který plyne z obsahu i ze samotné povahy Nařízení;
- značné posílení práv subjektů osobních údajů, které se zrcadlově promítají do povinností správců a zpracovatelů, které vyplývá ze zesíleného důrazu na bezpečnost a odpovědnost při správě a zpracování osobních údajů;
- konkretizace a zpřesnění pravidel pro mezinárodní zpracování a správu osobních údajů, směřující především k harmonizaci pravidel v členských státech EU;
- některé nové instituty a povinnosti, jako je například předběžné posouzení přijatých opatření k ochraně osobních údajů, povinnost vést záznamy o zpracování osobních údajů, ohlašování případů porušení zabezpečení osobních údajů či jmenování pověřence pro ochranu osobních údajů.

Lze konstatovat, že **na obecných základech ochrany osobních údajů Nařízení nic nemění**. Zůstává tak zachován koncept, že primárním podkladem ke zpracování osobních údajů by měl být informovaný a svobodný souhlas uživatele či výjimečná okolnost, za které souhlas vyžadován není. Zůstává rovněž zachována definice osobního údaje jako takového, jen je rozšířena o další kategorie.

Definice a dělení subjektů odpovědných za zpracování – správců a zpracovatelů osobních údajů – zůstávají zachovány společně se zákonnými důvody pro zpracování osobních údajů.

Jelikož by se postavení spolků, jakožto prostých správců osobních údajů ve vztahu ke členům, nemělo Nařízením nijak principiálně měnit, lze dovozovat, že stávající povinnosti dopadající na spolky v této oblasti nebudou podstatně rozšířeny a maximálně doznají lehkých zpřesňujících změn.

Tedy i po účinnosti Nařízení zůstanou v platnosti následující povinnosti spolků při zpracování osobních údajů jejich členů:

Spolky **nemají oznamovací povinnost** vůči úřadu (ÚOOÚ) podle ustanovení § 16 zákona č. 101/2000 Sb. o ochraně osobních údajů. Protože dle stanoviska úřadu se oznamovací povinnost podle § 16 nevztahuje na zpracování osobních údajů, jde-li o zpracování, které

sleduje politické, filosofické, náboženské nebo odborové cíle, prováděné v rámci oprávněné činnosti sdružení (spolků), a které se týká pouze členů sdružení nebo osob, se kterými je sdružení v opakujícím se kontaktu souvisejícím s oprávněnou činností sdružení, a osobní údaje nejsou zpřístupňovány bez souhlasu subjektu údajů.

Spolky jsou povinny zajistit **souhlas svého člena ke zpracování osobních údajů** pro účely činnosti spolku (vedení seznamu členů apod.). Nařízení definuje, že souhlas musí být **svobodný** (dobrovolný, nevázaný na přijetí nabídky), **konkrétní** (jasně a srozumitelně popsaný účel, pro který se souhlas uděluje), **informovaný** (ten kdo souhlas uděluje, dostal předem všechny informace předpokládané Nařízením[1]) a **jednoznačný** a musí být udělen prohlášením nebo zjevným potvrzením (subjekt musí učinit nějakou akci, nestačí například ukrytí souhlasu do obchodních podmínek). Souhlas bez těchto náležitostí bude neplatný.

Spolky jsou rovněž povinny splnit **informační povinnost vůči svým členům**, tj. informovat členy zejména o tom, že jsou shromažďovány jejich osobní údaje pro účely činnosti spolku, v jakém rozsahu (jméno, příjmení, rodné číslo atd.) a komu mohou být zpřístupněny (např. hlavnímu spolku v případě pobočného spolku, nadřízené organizaci apod.).

Na spolky také dopadají **obecné povinnosti k ochraně osobních údajů**, kterými disponují. Zde lze obecně doporučit cestu zdravého rozumu a základní IT gramotnosti a vždy brát v potaz možná rizika s přihlédnutím k množství zpracovávaných údajů. Zabezpečení by vždy mělo vycházet z konkrétní situace a technických a finančních možností správce těchto údajů. *„Například spolek s dvaceti členy nebude nucen k ochraně svého seznamu členů zakoupit sofistikované šifrovací programy apod.“*

---

[1] Článek 13 GDPR: „1. Pokud se osobní údaje týkající se subjektu údajů získávají od subjektu údajů, poskytne správce v okamžiku získání osobních údajů subjektu údajů tyto informace: a) **totožnost a kontaktní údaje správce a jeho případného zástupce**; b) případně **kontaktní údaje případného pověřence pro ochranu osobních údajů**; c) **účely zpracování**, pro které jsou osobní údaje určeny, a právní základ pro zpracování; d) oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f); e) případné **příjemce nebo kategorie příjemců osobních údajů**; f) případný **úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci** a existenci či neexistenci rozhodnutí Komise o odpovídající ochraně nebo, v případech předání uvedených v článcích 46 nebo 47 nebo čl. 49 odst. 1 druhém pododstavci, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny. 2. Vedle informací uvedených v odstavci 1 poskytne správce subjektu údajů v okamžiku získání osobních údajů tyto další informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování: a) **doba, po kterou budou osobní údaje uloženy**, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby; b) **existence práva požadovat** od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich **opravu nebo výmaz**, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů; c) pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním; d) **existence práva podat stížnost u dozorového úřadu**; e) skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů; f) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.“

Navzdory tomu, že Nařízení není žádnou revolucí v pravém slova smyslu, koluje v souvislosti s blížící se účinností řada nepřesných informací. Mezi obvykle „démonizované" novinky, které Nařízení přináší, patří například:

> ***„Povinnost jmenovat pověřence na ochranu osobních údajů"*** – tato povinnost v Nařízení skutečně stanovena je, ale týká se pouze situací, kde zpracování provádí orgán veřejné moci nebo veřejný subjekt, hlavní činnost správce nebo zpracovatele spočívá v operacích vyžadujících rozsáhlé pravidelné a systematické monitorování subjektů údajů nebo kde hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů (jako je rasový a etnický původ, politické názory, náboženské vyznání, údaje o sexuální orientaci, zdravotním stavu apod.).
>
> ***„Všechny osobní údaje se budou muset šifrovat"*** – Nařízení uvádí šifrování jako jedno z možných bezpečnostních opatření. To však neznamená, že všechna zpracování a všechny údaje budou muset podléhat šifrování. Nadále platí, že zpracovatel musí přijmout vhodná technická a organizační opatření k ochraně zpracovávaných osobních údajů, vzhledem k rizikům, která toto zpracování představuje a s ohledem na technické a finanční možnosti.
>
> ***„Souhlas bude nutný pro veškeré zpracování osobních údajů"*** – stále platí, že náležitě udělený souhlas bude pouze jedním z více „právních titulů" ke zpracování osobních údajů. Nařízení zachovává další právní základy zpracování, jako je dodržení právní povinnosti správce (zaměstnavatel předá informace správě sociálního zabezpečení), nezbytnost pro plnění smlouvy (podnikatel si uchová originál smlouvy, která obsahuje osobní údaje) atd.

Jelikož účinnost Nařízení je poměrně vzdálená a odborná debata na toto téma se neustále vyvíjí, je otázkou, jak se bude **do budoucna** měnit interpretace jednotlivých ustanovení Nařízení. Je možné, že výkladem dojde například k rozšíření informační povinnosti správců či stanovení dalších náležitostí udělovaného souhlasu. Lze doporučit sledovat stanoviska Úřadu na ochranu osobních údajů a legislativní změny přijaté v důsledku účinnosti Nařízení.

Ve vztahu k zaměstnavatelům (kterým může být a nezřídka je i spolek) je v současné době možno uvést především to, že čl. 88 Nařízení stanoví, že *„právním předpisem, anebo kolektivní smlouvou, lze stanovit konkrétnější pravidla k zajištění ochrany práv a svobod ve vztahu ke zpracování osobních údajů zaměstnanců v souvislosti se zaměstnáním…".* Toto ustanovení umožňuje členským státům přijmout speciální vnitrostátní právní úpravu týkající se zpracování osobních údajů zaměstnanců ze strany zaměstnavatelů. Zatím není zřejmé, zda tato úprava bude přijata, případně v jaké podobě, a proto není možné nyní přesně uvést, jak budou tyto vztahy upraveny. Pokud by zvláštní právní úprava přijata nebyla a ochrana osobních údajů v pracovněprávních vztazích by vycházela z Nařízení, je třeba upozornit na následující: Zaměstnavatel zpracovává osobní údaje zaměstnanců většinou z několika různých „zákonných právních důvodů", jednak se osobní údaje vyskytnou typicky na pracovní smlouvě a ta bude jistě uložena v elektronické či listinné podobě u zaměstnavatele, dále zaměstnavatel poskytuje ze zákona osobní údaje zaměstnanců například správě sociálního zabezpečení za účelem řádné evidence apod. V tomto ohledu nezavádí Nařízení pro zaměstnavatele žádné nové povinnosti. Naproti tomu například pro zveřejnění osobních údajů zaměstnanců na webových stránkách zaměstnavatele bude třeba, aby zaměstnavatel získal výslovný souhlas zaměstnanců, a pokud ho nezíská, osobní údaje zveřejnit nebude moci. Ani

v tomto případě nejde o něco zcela nového, zaměstnavatele by ale čekal horší postih, pokud by toto pravidlo porušil.

Dalším aspektem Nařízení, který je třeba v souvislosti s postavením zaměstnavatele zmínit, je že Nařízení zvyšuje ochranu osob, které jsou v nerovnovážném vztahu k tomu, kdo po nich vyžaduje souhlas se zpracováním osobních údajů. Za takový nerovnovážný vztah bude pravděpodobně považován i vztah pracovněprávní (při výkonu závislé práce). Jak široce se tato ustanovení budou aplikovat a na jaké vztahy se skutečně nakonec budou vztahovat, ale není zatím definitivní. Zaměstnavatelé tedy musí shora uvedenou problematiku nadále průběžně sledovat.

Závěrem uvádíme, že je důvod k obezřetnosti, avšak nikoli k panice. Pokud byla problematika ochrany osobních údajů až doposud přehlížena, dochází k porušování předpisů pravděpodobně již nyní a uvedené Nařízení pouze vyvolalo náhlý zvýšený zájem o agendu, které se mělo dostat zasloužené pozornosti už dávno. Uvedou-li spolky svou agendu do souladu s aktuálně platnou právní úpravou, je prakticky jisté, že dále nemusí kvůli nadcházející účinnosti Nařízení podnikat žádné zvláštní kroky, aby pravidlům stanoveným v Nařízení vyhověly.

Česká rada dětí a mládeže
Senovážné nám. 977/24
110 00 Praha 1

telefon: 211 222 860
fax: 272 049 680
datová schránka: vfq5xz4
e-mail: sekretariat@crdm.cz

web: www.crdm.cz