Spolky a GDPR – východiska pro přípravu na účinnost Nařízení

Mgr. Alena Hájková

www.crdm.cz

Spolky a GDPR – východiska pro přípravu na účinnost Nařízení

Obecné nařízení o ochraně osobních údajů – General Data Protection Regulation (dále jen „GDPR“) navazuje na současnou právní úpravu ochrany osobních údajů směrnicí 95/46/ES (a zákona č. 101/2000 Sb. o ochraně osobních údajů, který tuto problematiku upravuje až do května letošního roku na území ČR). Jeho cílem je především sjednotit pravidla ochrany osobních údajů v rámci členských států EU a reagovat na aktuální trendy panující v oblasti zpracování osobních údajů, a tedy i stále se vyvíjející prostředky, které jsou ke zpracování osobních údajů využívány.

Nemá jít a nejde o převrat v ochraně osobních údajů, ale především o zpřesnění a aktualizaci pravidel zpracování osobních údajů v rámci členských států EU. Pro subjekty, které jsou správci nebo zpracovateli osobních údajů a již nyní zpracovávají osobní údaje v souladu s platnou legislativou, nepřináší tedy GDPR zcela zásadní změny, na druhou stranu úplně beze změn se jejich činnost při zpracování osobních údajů také neobejde, protože zpřesněním pravidel ochrany osobních údajů byly definovány nové požadavky, které jsou na správce, popř. zpracovatele osobních údajů kladeny. K tomu podrobněji dále.

Ochrana osobních údajů podle GDPR je vystavěna na dvou **základních principech**:

1) princip odpovědnosti správce/zpracovatele osobních údajů za dodržení zásad zpracování osobních údajů, a to včetně jeho schopnosti shodu se zásadami kdykoliv doložit dozorovému úřadu, a
2) princip rizika – tj. správce/zpracovatel musí v každém okamžiku zpracování osobních údajů brát v úvahu rozsah, kontext, povahu a účel zpracování osobních údajů a zároveň průběžně reagovat na možná rizika, která může zpracování znamenat pro práva a svobody fyzických osob tak, aby v maximální možné míře zajistil bezpečnost zpracovávaných osobních údajů.

Ani jeden z principů není uplatněn nově, u prvního z nich je ale nově kladen důraz na schopnost správce/zpracovatele kdykoliv prokázat soulad svých činností se zásadami GDPR. Projevem tohoto nového přístupu v rámci GDPR pak je podstatná změna, kterou představuje zrušení registrační povinnosti u Úřadu na ochranu osobních údajů – dále jen „ÚOOÚ“. Ode dne účinnosti GDPR zanikne povinnost registrovat se jako správce/zpracovatel osobních údajů u ÚOOÚ a současně vznikne nová povinnost správců/zpracovatelů zajistit/vytvořit si pro svou činnost při zpracování osobních údajů takové podklady, aby byli schopní dozorovému úřadu kdykoliv prokázat soulad svých činností s GDPR.

Ke splnění povinnosti prokázat soulad zpracování s GDPR budou sloužit především „Záznamy o činnostech“, které si každý správce/zpracovatel může vypracovat sám a dále Kodexy a Osvědčení, které by měli být dalšími prostředky pro splnění této povinnosti. Přitom Kodexy budou sloužit na sektorové úrovni – jako vodítko správné praxe vypracované „shora“ zastřešujícím orgánem nebo organizací a všeobecně uznané za správné (předpokládá se vznik pro sektory jako bankovnictví, telekomunikace, zdravotnictví, školství…). Pokud správce/zpracovatel pak prokáže, že jeho činnost je v souladu s příslušným Kodexem, svou povinnost prokázat soulad zpracování s GDPR tím splní. Osvědčení pak má být samo o sobě prostředkem k prokázání souladu zpracování s GDPR, protože získat je samozřejmě nepůjde jinak, než právě splněním všech podmínek stanovených pro zpracování osobních údajů v GDPR. V této souvislosti je však třeba upozornit na to, že systém orgánů, které budou oprávněné vydávat osvědčení, zatím není připravený, natož funkční. Možnost získat „osvědčení“ je tedy prozatím v nedohlednu a správci/zpracovatelé nemají zatím jinou možnost, než postupovat při přípravě na účinnost GDPR každý samostatně až do doby, kdy budou Kodexy, popř. Osvědčení zavedeny do praxe.

Stávajícím správcům/zpracovatelům tedy nezbývá, než **provést podrobný rozbor svých činností při kterých zpracovávají osobní údaje a posoudit, do jaké míry jsou v souladu se zásadami zpracování a podmínkami** podle GDPR, **a pokud v některých ohledech nejsou v souladu s GDPR, pak je přiměřeně upravit**.

Zásady zpracování (čl. 5 GDPR)

Správce/zpracovatel je odpovědný za to, že bude při zpracování osobních údajů dodržovat tyto základní zásady (všechny uvedené zásady je správce/zpracovatel povinen dodržovat již nyní, nově ale musí být schopen sám aktivně kdykoliv prokázat jejich dodržování):

- Zákonnost, správnost a transparentnost – správce musí zpracovávat osobní údaje na základě nejméně jednoho právního (zákonného) důvodu a vůči subjektu údajů transparentně.
- Omezení účelu – osobní údaje musí být shromažďovány pro určité a legitimní účely (účel musí být určen předem a subjektu údajů sdělen) a nesmějí být zpracovávány způsobem s těmito účely neslučitelným.
- Minimalizace údajů – osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány.
- Přesnost – správce smí zpracovávat jen přesné osobní údaje; jejich přesnost musí průběžně zajišťovat.
- Omezení uložení – osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány, a po té by měly být smazány (nejsou-li uloženy v souvislosti s dalším účelem).
- Integrita a důvěrnost – správce je povinen přijmout taková technická opatření (např. pseudonymizace osobních údajů, šifrování) a organizační opatření (např. vnitřní předpisy, školení zaměstnanců, omezení počtu osob, které mají přístup ke zpracovávaným osobním údajům), aby zajistil v maximální možné míře bezpečnost zpracovávaných osobních údajů (viz shora „princip rizika“).

K zajištění souladu zpracování se shora uvedenými zásadami aktuálně platné předpisy (a do budoucna GDPR) stanoví celý výčet práv a povinností správců/zpracovatelů a práv subjektů údajů[1] (přičemž některá práva a povinnosti se samozřejmě mohou vztahovat k několika ze shora uvedených zásad), a to:

Práva subjektu údajů (tj. osoby, jejíž údaje jsou zpracovávány)

- Právo na přístup k osobním údajům
  Subjekt údajů má právo na to, aby mu správce potvrdil, zda zpracovává jeho osobní údaje, a pokud ano, má právo získat přístup k nim i k informacím, které se tohoto zpracování týkají (tomuto právu subjektu údajů odpovídá povinnost správce sdělit informace – viz informační povinnost správce).
- Právo na opravu a doplnění neúplných osobních údajů
  Aktivita musí vzejít od subjektu údajů. Pokud se ale subjekt údajů obrátí na správce s tím, že o něm zpracovávané údaje jsou nepřesné nebo nesprávné, musí je správce bez zbytečného odkladu opravit nebo doplnit.
- Právo na výmaz, resp. právo „být zapomenut“
  NOVÉ! Nejčastěji připadá v úvahu v případě, kdy je správce povinen zlikvidovat osobní údaje, protože již dále neexistuje právní důvod, aby je dále zpracovával. Taková situace nastane typicky,

[1] Z hlediska správců/zpracovatelů je tento výčet vlastně sám o sobě vodítkem, co všechno minimálně musí správce/zpracovatel dělat, aby zpracování osobních údajů bylo v souladu s předpisy.

pokud bylo dosaženo účelu, pro který byly údaje zpracovávány nebo pokud subjekt údajů odvolal souhlas se zpracováním (pokud byly údaje zpracovávány na základě jeho souhlasu).

- Právo na omezení zpracování
  K omezení zpracování osobních údajů musí správce přistoupit, pokud subjekt údajů namítne jejich nepřesnost nebo nesprávnost, pokud vznese námitku proti zpracování svých osobních údajů apod.
- Právo na přenositelnost údajů
  NOVÉ! Subjekt údajů má právo (pokud jsou jeho údaje zpracovávány na základě souhlasu subjektu údajů, na základě uzavřené smlouvy nebo pokud je zpracování prováděno automatizovaně) získat od správce bezplatně své osobní údaje (ve strukturovaném, běžně užívaném a strojově čitelném formátu), a také má právo je bez omezení předat jinému správci.
- Právo vznést námitku
  Právo subjektu údajů vznést námitku proti zpracování osobních údajů z důvodu plnění úkolu prováděného ve veř. zájmu nebo při výkonu veř. moci a z důvodu oprávněných zájmů správce či třetí strany (viz čl. 6 odst. 1 písm. e) a f) GDPR). Správce je pak povinen prověřit oprávněnost zpracování osobních údajů a podle výsledků prověření pak zpracování osobních údajů konkrétní osoby dále upravit, popř. v něm nepokračovat, není-li k němu ospravedlnitelný zvlášť závažný důvod.

Povinnosti správce

Obecné povinnosti

- Zajistit, aby zpracování bylo v souladu s GDPR, a to s využitím vhodných technických a organizační opatření, Kodexů, Osvědčení. Vhodnost opatření (jejich počet, druh…) musí správce určit podle povahy, rozsahu, kontextu a účelů zpracování, a také s ohledem na pravděpodobná a různě závažná rizika pro práva a svobody subjektu údajů.
- Vést záznamy o činnostech zpracování, nebo jinak zajistit, aby byl schopen soulad zpracování s GDPR doložit. Záznamy o činnostech nemusí vést podnik nebo organizace, které zaměstnávají méně než 250 zaměstnanců, pokud zároveň zpracování, které provádí, nepředstavuje riziko pro práva a svobody subjektů údajů, je příležitostné[2] nebo nezahrnuje zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů dle čl. 10 GDPR[3].
- Uvést činnosti do souladu s Kodexem (byl-li pro jeho sektor vytvořen), získat osvědčení o souladu zpracování s GDPR (až bude vydáváno).

Ve vztahu k subjektům údajů je správce povinen plnit všechny povinnosti, které jsou protipólem práv subjektu údajů, tj.:

Informační povinnost (čl. 12 GDPR)

- Na dotaz sdělit subjektu údajů, jaké osobní údaje o něm zpracovává.
- Poskytnout (aktivně, spolu s informacemi o zpracovávaných údajích) subjektu údajů informace, které se týkají zpracování – tj. informace o účelu zpracování, o kategoriích dotčených osobních údajů, o plánované době uložení osobních údajů, o příjemcích zpracovávaných osobních údajů,

[2] Toto vymezení prakticky vylučuje užití výjimky z povinnosti vypracovat záznamy o činnostech na jakýkoliv subjekt, který zpracovává údaje pravidelně nebo dlouhodobě, tj. i spolky, protože zpracování osobních údajů členů, přinejmenším za účelem jejich evidence nebo rozesílání informací o aktivitách spolku rozhodně nelze označit jako „příležitostné“.
[3] viz čl. 30 odst. 5. GDPR

o dalších právech subjektu údajů (požadovat opravu nebo výmaz osobních údajů, vznést námitku, podat stížnost u dozorového úřadu), o zdroji osobních údajů (pokud je správce nezískal přímo od subjektu údajů), o skutečnosti, že dochází (pokud k němu dochází) k automatizovanému rozhodování, včetně profilování, o totožnosti správce a o oprávněných zájmech správce pro zpracování osobních údajů.

Administrace žádostí a námitek subjektu údajů

- Zajistit bez zbytečného odkladu (= nejdéle do 1 měsíce; v odůvodněných případech možno prodloužit max. o dva měsíce, subjekt údajů musí být informován o prodloužení i jeho důvodech) administraci žádostí subjektu údajů o opravu, výmaz nebo omezení zpracování osobních údajů a provedení opravy, výmazu nebo omezení zpracování provést, pokud byla žádost důvodná.
- Zajistit přenositelnost zpracovávaných údajů – ve strukturovaném, běžně používaném a strojově čitelném formátu.
- Zajistit administraci podaných námitek – pokud správce zpracovává osobní údaje z důvodu dle čl. 6 odst. 1 písm. e) a f) GDPR.

NOVÉ povinnosti podle GDPR

- Posouzení vlivu na ochranu osobních údajů a konzultace s dozorovým úřadem.
- Ohlašování porušení zabezpečení osobních údajů (dozorovému úřadu nebo subjektu údajů).
- Jmenování pověřence na ochranu osobních údajů.

Všechny tyto nové povinnosti vycházejí z uplatňování principu rizika v rámci GDPR. Vztahují se proto především na ty správce/zpracovatele, kteří provádějí zpracování osobních údajů, které představuje vysoké riziko pro práva a svobody subjektu údajů a podobně na situace, které při zpracování osobních údajů mohou nastat a rovněž představují vysoké riziko. Do jaké míry je konkrétní správce povinen tyto povinnosti plnit, je vždy třeba posuzovat ve vztahu ke konkrétnímu zpracování osobních údajů, popř. ve vztahu ke konkrétní situaci.

Příprava spolků na účinnost GDPR

Pro přípravu na účinnost GDPR je klíčové mít na paměti, že Nařízení především směřuje k tomu, aby byly osobní údaje zpracovávány systematicky a vědomě bezpečně. Situace všech současných správců/zpracovatelů osobních údajů je, oproti těm, kteří se stanou správci/zpracovateli s předchozí znalostí GDPR, specifická v tom, že musí své postupy a systémy doplnit o další prvky, které GDPR zavádí (a se kterými nebylo možné v minulosti počítat). To nemusí být úplně jednoduché, ale také to neznamená, že je třeba všechno změnit. Každý správce/zpracovatel proto musí své činnosti posoudit sám a zohlednit jen pro něj relevantní skutečnosti. Je rozdíl v tom, co bude muset udělat malý spolek, a co bude potřeba u velkého spolku, popř. spolku hlavního, který je zastřešujícím pro činnost pobočných spolků.

Z hlediska nevelkých spolků (popř. i pobočných spolků, u nichž hlavní spolek plní úlohu zastřešující organizace) zabývajících se klasickou spolkovou činností – tj. činností vzájemně prospěšnou svým členům nebo veřejně prospěšnou, prováděnou členy spolku, které nezpracovávají jiné osobní údaje než osobní údaje svých členů pro účely realizace činnosti spolku a nezpracovávají žádné zvláštní kategorie osobních údajů kromě toho, že evidují své členy[4], lze říci, že se opravdu nijak zvlášť připravovat nemusí. Posouzením

[4] **POZOR!** Údaj o členství ve spolku je sám o sobě osobním údajem zvláštní kategorie podle čl. 9 GDPR, neboť vypovídá (může vypovídat) o politických názorech, náboženském vyznání či filozofickém přesvědčení subjektu údajů.

jejich nemnoha činností při zpracování osobních údajů podle GDPR, uvedením těchto činností do souladu se zásadami GDPR a sepsáním Záznamů o činnostech, velmi pravděpodobně splní veškeré požadavky, které na ně GDPR klade, protože vzhledem k tomu, jak jsou malé a jak omezený je rozsah jejich činností při zpracování osobních údajů a jak (ne)velké je riziko pro práva a svobody subjektů údajů, jejichž osobní údaje jsou zpracovávány, nebudou povinny:

- jmenovat pověřence pro ochranu osobních údajů,
- absolvovat předchozí konzultace činností zpracování s dozorovým úřadem, popř. absolvovat zvláštní posuzování vlivu zpracování na ochranu osobních údajů (pokud nezavedou nějakou novou, vysoce rizikovou činnost zpracování osobních údajů).

Pochopitelně je mohou, v rámci uvádění činností zpracování do souladu s GDPR, kromě vypracování Záznamů o činnostech, čekat nějaké další administrativní úkony[5] a změna v přístupu při rozhodování o činnostech spolku, jejichž součástí je také zpracování osobních údajů fyzických osob[6], nic dalšího ale nebudou muset dělat.

U spolků s velkým počtem členů, resp. spolků, které v rámci své činnosti zpracovávají velký objem osobních údajů svých členů nebo i subjektů údajů, které nejsou členy spolku, zpracovávají citlivé údaje, popř. zvláštní kategorie osobních údajů, apod., bude situace samozřejmě odlišná. Každý takový spolek musí rovněž posoudit rozsah svých činností při zpracovávání osobních údajů a míru rizika, které zpracování osobních údajů představuje pro subjekty údajů, jejichž údaje spolek zpracovává a na základě toho pak stanovit, jaké kroky podniknout, aby uvedl své činnosti při zpracování osobních údajů do souladu s GDPR, výsledkem ale pravděpodobně bude časově i organizačně náročnější výčet opatření a úkonů, které bude nutné realizovat.

Postup přípravy na účinnost GDPR

Pokud by měl být postup přípravy na účinnost GDPR vyjádřený jednoduchým výčtem základních kroků, pak bychom jej definovali jako tyto 4 body:

1) Zmapování všech činností organizace (spolku), při nichž dochází ke zpracovávání osobních údajů fyzických osob a vytvoření/uvědomění si schématu zpracovávání (jak se shromažďují, kam a kdo je zapisuje – pokud jsou zapisovány, kdo má k osobním údajům při zpracování přístup a odkud, jak a kdo může s osobními údaji dále nakládat…).
2) Revize zpracovávaných osobních údajů – rozbor právních důvodů zpracování a posouzení kategorií osobních údajů (osobní/citlivé údaje), ověření zda jsou zpracovávány jen nezbytné údaje, pořízení/aktualizace souhlasů se zpracováním, je-li souhlas třeba, případně oprava či doplnění osobních údajů a vymazání osobních údajů zpracovávaných neoprávněně nebo nadbytečně.

Zpracovávání údaje o členství ve spolku je možné jen na základě výjimky zakotvené v čl. 9 odst. 2. písm. d), tj. jestliže ho v rámci svých oprávněných činností a s vhodnými zárukami provádí nadace, spolek nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy tohoto subjektu nebo osoby, které s ním udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt.

[5] nejčastěji v podobě doplnění souhlasu členů se zpracováním osobních údajů (protože dříve udělené souhlasy již nebudou z hlediska GDPR dostatečné), nebo bude nezbytné aktualizovat/doplnit informace, které o zpracování osobních údajů dávají svým členům jako subjektům údajů

[6] s ohledem na povinnost správce/zpracovatele osobních údajů být schopen doložit soulad zpracovávání osobních údajů v souladu se zásadami GDPR by měla taková rozhodnutí být určitě písemně zachycená (např. v zápise ze zasedání rozhodujícího orgánu) a pečlivě archivovaná

3) Revize organizačních a technických opatření, které mají zajistit práva fyzických osob (splnění informační povinnosti správce) a chránit zpracovávané osobní údaje – ověření dostatečnosti opatření, která organizace (spolek) používá, případně doplnění dalších opatření, nejsou-li stávající dostatečná (např. omezení počtu osob, které mají přístup k osobním údajům, zavedení školení pro ty, kdo osobní údaje zpracovávají…).
4) Doplnění náležitostí činností zpracování zaváděných GDPR (záznamy o činnostech zpracování, posouzení vlivu na ochranu osobních údajů, jmenování pověřence pro ochranu osobních údajů, příprava na administraci žádostí fyzických osob – opravy a doplnění osobních údajů a výmaz osobních údajů, podání informace o zpracovávaných údajích, omezení zpracování osobních údajů, zajištění přenositelnosti údajů).

Ke shora uvedenému výčtu:

Ad 2.
Souhlas se zpracováním osobních údajů (dále jen „souhlas“)

GDPR klade na udělený souhlas vyšší nároky než dosavadní právní úprava, a to jak na formu, tak na obsah souhlasu.

Souhlas je podle čl. 4 odst. 1 bod 11 GDPR svobodný, konkrétní, informovaný a jednoznačný projev vůle – musí jít o aktivní a dobrovolný projev vůle, vždy se poskytuje ke konkrétnímu účelu zpracování (osoba udělující souhlas musí účel prokazatelně znát).

Aby byl udělený souhlas v souladu s GDPR, musí také splňovat podmínky vyjádření souhlasu (viz čl. 7 GDPR), přičemž zásadní je odlišitelnost souhlasu, tj.:

- souhlas (pokud je součástí prohlášení, které se týká i jiných skutečností) musí být odlišen od jiných skutečností, ke kterým se subjekt údajů vyjadřuje (např. pokud by měl být udělen společně s uzavřením smlouvy nebo vyjádřením souhlasu s obchodními podmínkami, musí od nich být jednoznačně oddělený. Souhlas udělený zaškrtnutím jednoho okénka ve webovém formuláři, a zároveň pro obsah obchodních podmínek i souhlas samotný, by nebyl považovaný za závazný);
- souhlas dále nesmí být podmínkou pro uzavření smlouvy (i když za účelem plnění smlouvy k určitému zpracování osobních údajů dojde, k tomuto zpracování není výslovný souhlas třeba, protože právním důvodem zpracování těchto údajů je plnění smlouvy samo o sobě, proto má-li být s uzavřením smlouvy dán zvlášť souhlas, musí být konkrétně uvedeno, k čemu se dává – např. souhlas se zápisem osobních údajů do seznamu členů spolku).

Ad 3.
Splnění informační povinnosti správce (dále jen „informační povinnost“)

Vzhledem k tomu, že se výčet práv fyzických osob při zpracování osobních údajů rozšířil, je třeba také aktualizovat dokumenty, kterými sděluje správce fyzické osobě povinné informace o činnostech zpracování a jejích právech – viz „povinnosti správce“ shora.

Ad. 4.
Výčet náležitostí, které bude třeba doplnit, závisí v mnohém na podrobném posouzení situace konkrétního spolku.

Podstatou přípravy na účinnost GDPR je posoudit a rozhodnout se, co všechno organizace (spolek) musí udělat, aby její činnost jako správce osobních údajů byla v souladu s GDPR. Při posuzování je třeba vycházet z textu GDPR a výkladových stanovisek a metodik Úřadu na ochranu osobních údajů (dále jen „ÚOOÚ“).

Považuji za nutné ještě dodat, že spolek – jakkoliv velký – určitě není subjektem, který by byl ve středu zájmu dozorového úřadu (tj. ÚOOÚ), a proto lze předpokládat, že žádnému spolku nehrozí, že bude úderem 25. 5. 2018 přísně a bez milosti kontrolován, zda při zpracovávání osobních údajů bezezbytku splňuje a průběžně dodržuje zásady a podmínky GDPR, a pokud je nesplní, bude nemilosrdně pokutován nejvyšší možnou pokutou. Připravit se plně na účinnost GDPR ale nepovažuji za zbytečné, určitě je to důležitý krok ke změně v přístupu k osobním údajům, které spolky zpracovávají. Taková změna je podle mě žádoucí, protože není jedno, jak se s osobními údaji fyzických osob nakládá, ani v případě spolků. Na druhou stranu není třeba bezhlavě rušit všechno, co je již zavedeno a zavádět všechno nové, co bylo vymyšleno. Důležité je posoudit okolnosti a s jejich znalostí postupovat v souladu s GDPR a zároveň co nejrozumněji. Takový postup bude jistě velmi dobře obhajitelný, až jednou dozorový úřad případně přijde na kontrolu.

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