NEMOVITOST PROFI

VERLAG DASHÖFER

Manuál k aplikaci obecného nařízení o ochraně osobních údajů (GDPR) pro společenství vlastníků

13.4.2018, Mgr. Adriana Kvítková, Mgr. Alexandra Javoreková, Zdroj: Verlag Dashöfer

Tento manuál představuje praktickou pomůcku určenou zejména pro předsedy společenství a členy výborů společenství vlastníků a jeho účelem je seznámit tyto statutární orgány (či jejich členy) s povinnostmi, které pro společenství vlastníků, a tedy i pro ně, přináší nařízení Evropského parlamentu a Rady (EU) 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 (obecné nařízení o ochraně osobních údajů), (dále jen „GDPR").

Tento manuál si neklade za cíl přinést vyčerpávající informaci týkající se implementace GDPR do vnitřních postupů fungování společenství vlastníků, ale spíše má sloužit jako základní přehled jím stanovených povinností, kterým by statutární orgány společenství vlastníků měly při zpracování osobních údajů věnovat větší pozornost.

Co je GDPR a jak se projeví ve vztahu ke společenstvím vlastníků

GDPR je nařízením Evropského parlamentu a Rady (EU), tedy přímo použitelným předpisem Evropské unie, které nabude účinnosti dne 25. 5. 2018 a které spolu se zákonem o zpracování osobních údajů (jehož návrh se v současné době nachází v legislativním procesu) bude tvořit základní právní rámec pro zpracování osobních údajů. Zmíněné právní předpisy tak nahradí dosavadní právní úpravu, kterou v České republice představoval zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů").

S ohledem na brzké nabytí účinnosti výše popsané právní úpravy je nezbytné, aby subjekty, které zpracovávají osobní údaje, zkontrolovaly své procesy při zpracování osobních údajů a přizpůsobily je novým (nebo spíše podrobnějším) pravidlům v této oblasti.

Společenství vlastníků jakožto právnická osoba založená za účelem zajišťování správy domu a pozemku při své činnosti zpracovává osobní údaje subjektů údajů (tedy zejména svých členů, tedy vlastníků bytových a nebytových jednotek v domě, členů jejich domácností, nájemců, podnájemců, příp. dalších osob, které se v domě zdržují), a vystupuje ve vztahu k těmto subjektům údajů jako správce osobních údajů.

I přes skutečnost, že GDPR vychází především z principu kontinuity právní úpravy ochrany osobních údajů, přináší pro správce některé nové povinnosti, jiné povinnosti upřesňuje, či je doplňuje. Za nedodržení povinností správců a zpracovatelů pak hrozí dle GDPR poměrně citelné sankce. Z těchto důvodu je nezbytné, aby společenství vlastníků provedlo ještě před nabytím účinnosti GDPR a souvisejících předpisů vnitřní audit, tedy posouzení a vyhodnocení stávajících procesů zpracování osobních údajů subjektů údajů, přizpůsobilo tyto procesy nové právní úpravě a zajistilo dodržování zmíněných právních předpisů do budoucna.

Níže tedy uvádíme přehled povinností statutárních orgánů společenství vlastníků ve vztahu k GDPR a souvisejícím předpisům na poli ochrany osobních údajů.

Povinnosti společenství vlastníků před nabytím účinnosti GDPR

Statutární orgán společenství vlastníků by měl před nabytím účinnosti GDPR a souvisejících předpisů provést vnitřní audit, tedy podrobnější analýzu týkající se aktuálního stavu zpracování osobních údajů tímto společenstvím.

Ve vztahu ke zpracovávaným osobním údajům je nutné prověřit zejména:

a. které osobní údaje subjektů údajů společenství vlastníků zpracovává,
b. na základě kterého zákonného důvodu společenství tyto osobní údaje zpracovává (nezbytnost pro plnění právní povinnosti, oprávněný zájem, plnění smluvní povinnosti apod.),

c. zda společenství nezpracovává některé osobní údaje nad rámec zákona (tedy ověření, zda je zpracování některých osobních údajů pro společenství vlastníků nezbytné, např. zpracování rodných čísel),
d. zda společenství zpracovává některé z osobních údajů ze zákonného důvodu spočívajícího v udělení souhlasu subjektem údajů.

Pokud společenství vlastníků dospěje k závěru, že zpracovává víc osobních údajů subjektů údajů, než je nezbytné pro naplňování účelu správy domu a pozemku, zajistí náležitý výmaz nadbytečných osobních údajů, anebo pokud bude trvat na zpracovávání takových osobních údajů, získá souhlas subjektů údajů.

V případě, že společenství vlastníků zpracovává některé osobní údaje na základě souhlasu subjektu údajů (např. rodná čísla), společenství vlastníků je povinno prozkoumat poskytnuté souhlasy a zjistit, zda mají tyto souhlasy veškeré náležitosti vyžadované GDPR. Souhlasy subjektů údajů by měly být uděleny písemně, a to s ohledem na povinnost správce osobních údajů doložit, že subjekt údajů souhlas udělil, nejlépe tedy ve formě prohlášení, které bude odlišitelné od jiných skutečností (pokud bude souhlas součástí jiného dokumentu), srozumitelné a snadno přístupné (za použití jasných a jednoduchých jazykových prostředků). Statutární orgán společenství musí počítat i s tím, že subjekt údajů může svůj souhlas kdykoliv vzít zpět.

Po zjištění, které osobní údaje a na základě čeho společenství vlastníků jakožto správce osobních údajů, zpracovává, je nezbytné se zaměřit na jejich zabezpečení, příp. i posouzení vlivu na ochranu osobních údajů[1], tedy vyhodnocení zamýšlených operací zpracování na ochranu osobních údajů.

Statutární orgán společenství by měl posoudit, zda stávající zabezpečení osobních údajů je v souladu s povinnostmi stanovenými GDPR. Statutární orgán společenství by se měl v této souvislosti zaměřit na tyto oblasti:

a. které osoby mají přístup ke zpracovávaným osobním údajům,
b. kde jsou osobní údaje uloženy (jak papírově, tak i elektronicky),
c. jakým způsobem je zamezeno přístupu třetích osob k těmto osobním údajům (šifrování, zaheslování, anonymizace),
d. zda a jak společenství vlastníků osobní údaje člena tohoto společenství zpřístupňuje ostatním členům společenství,
e. zda a jakým způsobem společenství vlastníků poskytuje osobní údaje členů společenství, příp. dalších osob, jiným subjektům, např. správcovské společnosti, externí účetní apod.

Následně by statutární orgán společenství měl zkontrolovat smlouvy uzavřené s osobami, které pro společenství vlastníků vykonávají určitou konkrétní činnost, při které zpracovávají osobní údaje členů společenství, příp. i dalších osob, a to zejména smlouvy se správcovskými společnostmi. Tyto osoby, které zpracovávají osobní údaje z pokynu společenství vlastníků, vystupují ve vztahu k subjektům údajů jako zpracovatelé osobních údajů.

Výběru zpracovatelů osobních údajů (tedy subjektů, s nimiž společenství vlastníků spolupracuje a poskytuje jim osobní údaje svých členů, členů jejich domácností, příp. dalších osob) by měly statutární orgány společenství věnovat zvýšenou pozornost, jelikož v souladu s GDPR je správce osobních údajů povinen využívat pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky GDPR a aby byla zajištěna ochrana práv subjektů údajů.

GDPR rovněž uvádí náležitosti, které musí obsahovat smlouva mezi správcem osobních údajů a zpracovatelem, tedy hlavně následující údaje:

a. předmět a dobu trvání zpracování,
b. typ osobních údajů a kategorie subjektů údajů,
c. povinnosti a práva správce a další.

Výše uvedeným skutečnostem by statutární orgány měly při kontrole smluv se zpracovateli osobních údajů, a dále pak při uzavírání nových smluv s těmito, příp. novými, zpracovateli, věnovat zvýšenou pozornost. Pokud by některé ze smluv, uzavřených mezi společenstvím vlastníků a příslušnou správcovskou společností, účetním apod. nevyhovovaly požadavkům GDPR, anebo by příslušný zpracovatel neposkytoval veškeré nezbytné záruky vhodného zpracování osobních údajů, statutární orgán by měl přijmout náležitá opatření (např. uzavřít novou smlouvu se zpracovatelem, kde by byly obsaženy požadované skutečnosti, příp. i ukončit spolupráci s takovým subjektem, který neposkytuje dostatečné záruky zpracování dle GDPR).

Statutární orgán společenství by dále měl zajistit proškolení svých zaměstnanců a osob, které z pokynu společenství zpracovávají osobní údaje, a to tak, aby při zpracovávání osobních údajů postupovali v

souladu s GDPR a uměli promptně řešit situace spojené s narušením zabezpečení osobních údajů, chybami při zpracování osobních údajů a požadavky subjektů údajů v souvislosti s uplatněním jejich práv dle GDPR. Statutární orgán v této souvislosti zajistí i mlčenlivost těchto osob.

V této souvislosti by statutární orgán měl připravit/zapracovat/přijmout vnitřní směrnici, která bude obsahovat základní pravidla zpracování osobních údajů společenstvím vlastníků.

GDPR dále upřesňuje (a částečně doplňuje, či stanoví nově) práva subjektů údajů - mnohá z nich však byla upravena i stávajícím zákonem o ochraně osobních údajů. Statutární orgán společenství vlastníků v souvislosti s povinností společenství vlastníků umožnit uplatnění práv subjektům údajů zkontroluje následující postupy (příp. pokud tak společenství vlastníků již nečiní, tyto postupy zavede):

a. postup při poskytování informací subjektům údajů, tj. členům společenství a dalším osobám, jejichž osobní údaje společenství zpracovává, a to zejména prostřednictvím prohlášení o ochraně osobních údajů určené pro jednotlivé subjekty údajů, ve kterém jsou obsaženy zejména tyto informace:
    - uvedení osobních údajů, které o nich společenství zpracovává,
    - kontaktní údaje správce (na koho se mohou subjekty údajů v případě potřeby obracet),
    - účely zpracování jejich osobních údajů a právní základ tohoto zpracování (souhlas, oprávněný zájem, nezbytnost pro plnění právní povinnosti apod.),
    - uvedení, jaká práva jim podle GDPR náleží,
    - uvedení příp. příjemců osobních údajů apod.
b. postup pro vydávání potvrzení o zpracování osobních údajů na žádost subjektů údajů a zajištění přístupu subjektů údajů k informacím o:
    - účelech zpracování,
    - kategoriích dotčených osobních údajů,
    - příjemcích nebo kategoriích příjemců, kterým osobní údaje byly nebo budou zpřístupněny,
    - plánované době, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby,
    - existenci práva požadovat od společenství vlastníků opravu nebo výmaz osobních údajů týkajících se subjektu údajů, omezení jejich zpracování a práva vznést námitku proti tomuto zpracování,
    - právu podat stížnost u Úřadu pro ochranu osobních údajů,
    - veškerých dostupných informacích o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,
c. postup pro provedení opravy osobních údajů subjektu údajů,
d. postup pro provedení výmazu osobních údajů subjektu údajů,
e. postup pro omezení zpracování osobních údajů subjektu údajů,
f. postup pro řešení námitek subjektů údajů.

Výsledkem všech výše uvedených opatření by mělo být vytvoření funkčního systému ochrany osobních údajů a kontrolních mechanismů, které by bránily rizikům spojeným se zpracováním osobních údajů (zejména ztrátě, porušení zabezpečení údajů apod). O všech výše uvedených krocích by měl statutární orgán společenství vyhotovit písemné zápisy/protokoly/jiné písemné dokumenty, které budou sloužit v případě kontroly ze strany Úřadu pro ochranu osobních údajů k prokázání činnosti společenství vlastníků ve vztahu k ochraně osobních údajů a doložení souladu zpracování osobních údajů s GDPR, a to s ohledem na skutečnost, že dle GDPR nestačí, že správce osobních údajů řádně tyto osobní údaje zpracovává (tj. dodržuje povinnosti stanovené GDPR), ale správce musí být schopen správnost tohoto zpracování (a tedy soulad s GDPR) i doložit.

Průběžné povinnosti společenství vlastníků dle GDPR

Společenství vlastníků by mělo zpracovávat osobní údaje v souladu se základními zásadami zpracování, a to:

a. „zákonnost, korektnost a transparentnost",
b. „účelové omezení" – tedy zpracování osobních údajů jen pro konkrétní, legitimní účely a způsobem slučitelným s těmito účely,
c. „minimalizace údajů" – tedy zpracování by mělo být omezeno na nezbytný rozsah a mělo by být přiměřené a relevantní a jen k účelům, pro které jsou osobní údaje zpracovávány,
d. „přesnost" – tedy zpracování pouze aktuálních osobních údajů, které jsou bezchybné,
e. „omezení uložení" – tedy zpracování ne delší, než je nezbytné pro plnění příslušného účelu,
f. „integrita a důvěrnost" – tedy zajištění náležitého zabezpečení osobních údajů.

Společenství vlastníků by mělo být schopno dodržení souladu s výše uvedenými zásadami dokázat (princip odpovědnosti), a to učiní především řádným dodržováním pravidel ochrany osobních údajů a vedením o tom náležité dokumentace.

Statutární orgán společenství by měl pravidelně kontrolovat zejména:

a. trvání zákonných důvodů zpracování osobních údajů a nezbytnosti jejich zpracování,
b. zda disponuje souhlasy ke zpracování osobních údajů, ke kterému jsou tyto souhlasy vyžadovány (tj. když se neuplatní jiný zákonný důvod zpracování),
c. možnost subjektů údajů uplatňovat svá práva v souladu s GDPR,
d. činnost zpracovatelů osobních údajů (zejména správcovských firem) a smlouvy s těmito zpracovateli,
e. aktuálnost zabezpečení osobních údajů, a to zejména s ohledem na nové technologie, či hrozby s nimi související.

Statutární orgán společenství by měl dále pravidelně zajišťovat:

a. aktualizaci zabezpečovacích instrumentů osobních údajů, zejména s ohledem na technologický posun a nová rizika s ním spojená,
b. opravu a výmazy osobních údajů,
c. proškolování zaměstnanců a osob, které zpracovávají osobní údaje na pokyn společenství.

Plnění výše uvedených povinností statutárnímu orgánu společenství ulehčí tvorba záznamů o činnostech zpracování, které je rovněž povinen vést, a za které společenství vlastníků odpovídá. Tyto záznamy musí obsahovat informace o činnostech souvisejících se zpracováním osobních údajů (identifikační a kontaktní údaje společenství vlastníků, účely zpracování, popis kategorií subjektů údajů a kategorií osobních údajů, kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, je-li to možné, pak i obecný popis technických a organizačních bezpečnostních opatření k zabezpečení osobních údajů a plánované lhůty pro výmaz jednotlivých kategorií údajů). Záznamy o činnostech zpracování statutární orgán společenství poskytne na vyžádání Úřadu pro ochranu osobních údajů.

V neposlední řadě je pak statutární orgán společenství povinen ohlašovat jakékoli porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů (ledaže je nepravděpodobné, že by porušení mělo za následek riziko pro práva a svobody fyzických osob), a to bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se společenství vlastníků o tomto porušení zabezpečení dozvědělo (pokud tak učiní později, uvede spolu s tímto ohlášením i důvody pozdního ohlášení). Každé porušení zabezpečení musí společenství vlastníků zdokumentovat. Pokud společenství vlastníků vyhodnotí, že toto porušení přináší vysoké riziko pro práva a svobody fyzických osob, oznámí dané porušení i subjektu údajů, tj. tomu, koho se dané osobní údaje týkají.
