Praktická příručka, jak na Obecné nařízení o ochraně osobních údajů

GDPR

pro společenství vlastníků jednotek a bytová družstva

Obsah

Ochrana osobních údajů byla poslední rok jednou z oblastí, kterou se zabýval snad každý od velkých obchodních korporací, až po malé živnostníky, od ministerstev až po malé obce či školy. Téměř každá organizace dnes pracuje s nějakými osobními údaji a musí tak plnit příslušná pravidla. Týká se to i společenství vlastníků jednotek a bytových družstev bez ohledu na jejich velikost.

Důvodem, proč každý ochranu osobních údajů najednou řešil, bylo nabytí účinnosti ***obecného nařízení o ochraně osobních údajů*** *(tzv. GDPR). To s sebou přineslo některé nové povinnosti, ale v možná ještě větší míře se veřejnost seznámila s povinnostmi, které již dlouho platily, ale často nebyly tak úplně respektovány.*

Bohužel veřejná debata přiživovaná strašením ze strany těch, kteří chtěli na GDPR vydělat, s sebou přinesla řadu mýtů, což často ***vedlo k přijímání zbytečných opatření, která GDPR vůbec nevyžaduje.*** *Představa o složitosti celé právní úpravy pak v mnoha případech naopak vedla k ignorování právní úpravy s tím, že bude lepší riskovat případné postihy.*

Cílem této příručky je zaměřit se na ***implementaci GDPR v společenstvích vlastníků jednotek (SVJ) a bytových družstvech (BD).*** *Velkou výhodou je, že agenda je zde velmi podobná a to umožňuje, abychom byli v příručce maximálně praktičtí a návodní. Výhodou také je, že během našeho projektu, v rámci něhož příručka vychází, jsme měli již možnost podílet se na celé řadě implementací GDPR, což nám dalo* ***řadu praktických zkušeností.***

Naším cílem není mít z předsedů SVJ a BD odborníky na ochranu osobních údajů. Je nám jasné, že často jsou to lidé, kteří vykonávají špatně placenou či neplacenou práci pro dům prostě proto, že zde nebyl nikdo jiný, kdo by byl ochoten funkci vzít. Mají málo času, a čím praktičtější návod dostanou, tím jim to více ušetří práci.

Příručka je členěna tak, že v úvodní kapitole seznamujeme čtenáře s důležitými pojmy, v další kapitole pak s jednotlivými povinnostmi souvisejícími s GDPR a v poslední kapitole potom s typickými příklady zpracování osobních údajů v SVJ a BD. Kromě doprovodného textu přinášíme v příručce ***i sadu praktických vzorů dokumentů,*** *které implementaci GDPR usnadní.*

Mgr. Jan Vobořil, Ph.D., advokát a výkonný ředitel IuRe,
autor textu
říjen 2018

Důležité pojmy

Osobní údaj

Osobním údajem je jakákoliv informace týkající se identifikované nebo identifikovatelné fyzické osoby. Pokud tedy je možno z údaje zjistit identitu osoby, případně ho bez vynaložení nějakého velkého úsilí propojit s dalšími údaji, které jsou třeba veřejně dostupné (zejména na internetu), bude se o osobní údaj jednat. Je třeba také pamatovat, že osobním údajem nemusí být pouze identifikační údaje osob (jméno, bydliště, datum narození, apod.), ale všechny informace, které s identitou osoby jsme schopni propojit.

Jak je to třeba s údaji o spotřebách v bytech? Jsou to osobní údaje?
Mohou být a nemusí. Pokud máme údaj o spotřebě v bytě, který obývá více osob, tak vlastně nějakou novou informaci, kterou lze vstáhnout ke konkrétní osobě nedostáváme. Pokud by ale v bytě bydlela pouze jedna osoba, tak už o osobní údaj půjde, protože spotřeba se zjevně týká dané osoby. Vzhledem k tomu, že s konkrétní kategorií údajů, ať už jsou osobní nebo nikoli, je praktické nakládat stejně, tak lze v tomto případě doporučit, aby se jako k osobním údajům přistupovalo i k údajům o spotřebě, které osobní nebudou.

V praxi SVJ a BD se setkáme s osobními údaji různých skupin osob. Předně půjde o členy SVJ nebo BD, dále o funkcionáře, případně zaměstnance. Dalšími skupinami mohou být nájemníci či podnájemníci BD či členů SVJ či BD, kteří byty obývají. Dále může jít o další osoby, které bydlí v domě. Dále půjde o osobní údaje osob, které přicházejí do smluvního vztahu s SVJ a BD a jejich zaměstnanců, půjde například o úklidové či správcovské firmy, účetní atd.

Vedle pojmu osobní údaj se v praxi setkáte i s pojmem **subjekt údajů.** Jde o jedince (tedy fyzickou osobu), k němuž se dané osobní údaje vztahují.

Zpracování osobních údajů

Dalším důležitým pojmem je zpracování osobních údajů. Zpracování je *„jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení“.*

Zjednodušeně řečeno zpracováním může být prakticky cokoli, co s osobními údaji děláte. Ne všechna zpracování ale budou regulována GDPR. **To se totiž vztahuje pouze na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do evidence mají být zařazeny.** To tedy znamená, že se GDPR bude řídit zpracování údajů, které jsou nějak uspořádány, typicky tak, aby se v nich dalo nějak orientovat či hledat. Můžeme si tedy představit spisy, které jsou neuspořádaně uloženy třeba ve sklepě domu bez nějakého systému, a prakticky s nimi nelze pracovat. Toto zřejmě nebude zpracování ve smyslu GDPR, ačkoli spisy obsahují osobní údaje. Může zde ale být relevantní například ochrana osobnosti dle občanského zákoníku. V každém případě stojí za zvážení, zda takové nepotřebné spisy není možné zlikvidovat, pokud s nimi stejně reálně pracovat nelze a nějaká forma jejich systematizace by byla náročná a vlastně není třeba.

Jak je to se zesnulými osobami?
GDPR se vztahuje pouze na osobní údaje osob, které žijí. Netýká se tedy osob zesnulých. Zde je nicméně třeba pamatovat, že údaje těchto osob mohou být chráněny například ustanoveními o ochraně osobnosti, která najdeme v § 81 a následujících občanského zákoníku.

GDPR se také nebude vztahovat na **zpracování osobních údajů pro osobní potřebu.** Zde je ovšem třeba si uvědomit, že jde skutečně pouze o potřebu konkrétní fyzické osoby. Tedy pokud si třeba předseda SVJ vede svůj osobní adresář kontaktů na sousedy, nebude se na něj GDPR vztahovat. Pokud by ale tento adresář už využíval ve věcech SVJ, například k rozesílání informací o odečtech vody, tak už o osobní potřebu nepůjde a je třeba postupovat v souladu s GDPR.

To kde zpravidla se s osobními údaji v SVJ a BD můžeme setkat, se více dočtete v kapitole Typická zpracování osobních údajů v SVJ a BD.

Správce, zpracovatel a příjemce

Správce je ten, kdo určuje účel a prostředky zpracování osobních údajů, případně komu ukládá zákon povinnost údaje zpracovávat. Toto zpracování také zpravidla provádí. Některými úkoly nebo i celým zpracováním ale může pověřit **zpracovatele.**

SVJ nebo BD tedy budou v drtivé většině případů správci. Zpracovatelem by se mohly stát tehdy, kdyby třeba vykonávaly na základě smlouvy nějakou agendu pro jiné SVJ nebo BD.

Typickými příklady zpracovatelů budou různé **správní firmy, externí účetní, firmy, které provádí odečty** atd. Tedy každý, kdo na základě smlouvy s SVJ nebo BD provádí nějakou činnost, kde nakládá s osobními údaji.

Proč je potřeba tyto pozice rozlišovat? Je to hlavně proto, že správce i zpracovatel mají různé povinnosti uložené GDPR. Správce by pak měl vždy mít se zpracovatelem uzavřenou smlouvu o zpracování osobních údajů, k níž se dostaneme později. Je to pak právě správce, kdo za zpracování odpovídá, včetně třeba možné odpovědnosti za pochybení zpracovatele.

Vedle správce a zpracovatele zde máme i další subjekty, které jsou označovány jako **příjemci.** Jde o ty, kteří mají obvykle ze zákona k osobním údajům přístup, ale nejsou zpracovateli. Půjde tedy například o zdravotní pojišťovny, Českou správu sociálního zabezpečení či finanční úřady pokud jde o údaje zaměstnanců, může jít o členy SVJ či BD, kteří využijí svého práva získat údaje ostatních ze seznamu členů vedeného ze strany SVJ či BD. Může jít třeba také o exekutora, insolvenčního správce, policii, soudy a řadu dalších subjektů, které mohou získat k údajům přístup.

Co nového GDPR přinese

GDPR přináší řadu novinek, ale je jich méně, než si lidé zpravidla myslí. První důležitou změnou je už forma právní regulace. Dříve jsme měli evropskou směrnici, která byla transponována do našeho zákona o ochraně osobních údajů, s nímž se v praxi pracovalo. GDPR má naproti tomu formu evropského nařízení. To platí rovnou a není třeba ho transponovat do českých zákonů, byť některé detaily budou v doprovodných (a stále neschválených)zákonech upraveny.

Novou povinností, která se dotkne i SVJ a BD je vedení tzv. **záznamů o činnostech zpracování,** což je jakýsi přehled toho, co a jak se s osobními údaji v BD či SVJ děje. Naproti tomu ale **zaniká povinnost zpracování osobních údajů registrovat** u Úřadu pro ochranu osobních údajů. To se týkalo zejména případů, kdy se údaje nezpracovávaly na základě zákona.

V oblasti zabezpečení osobních údajů se prosadil přístup založený na **riziku,** který hodnotí rizika zneužití údajů z pohledu jejich hodnoty pro útočníka i možného zásahu do práv subjektu údajů a tomu přizpůsobuje úroveň zabezpečení. Tím se oproti starší legislativě lépe vyjasnilo, jak se má k zabezpečení dat přistupovat v situacích, kdy sice existují nákladnější a lepší způsoby zabezpečení, ale citlivost dat či riziko jejich úniku jsou relativně malé.

SVJ a BD se může dotknout i nová povinnost **ohlašovat případy porušení zabezpečení osobních údajů** ať už Úřadu pro ochranu osobních údajů nebo samotným subjektům údajů, o jejichž osobní údaje jde.

Naopak SVJ a BD se zpravidla **nebude týkat povinnost zpracovávat tzv. posouzení vlivu na ochranu osobních údajů,** případně povinnost mít **pověřence pro ochranu osobních údajů.** O povinnosti zavedení pověřence ve smyslu zákona by bylo na místě uvažovat například u velkých bytových družstev s desítkami či stovkami bytových domů. Je ale třeba zdůraznit, že je dobré mít v každém SVJ a BD nějakou konkrétně určenou osobu, která za agendu odpovídá, či má o ní největší přehled. Je to dobré zejména pro komunikaci s ÚOOÚ, případně se subjekt údajů, pokud by třeba žádali o sdělení, jaké osobní údaje jsou o nich zpracovávány. Je ale také dobré mít vždy někoho, kdo na tuto problematiku bude myslet a pokud například dojde k nějakým změnám v nakládání s osobními údaji, tak ji promítne do příslušné dokumentace i samotné činnosti SVJ či BD.

Co je v GDPR oproti předchozí právní regulaci zdůrazněno, je povinnost správce či zpracovatele **prokazovat, že mají vše v pořádku a v souladu s GDPR,** proto bude potřeba více než dříve dokumentovat přijatá opatření a postupy.

Novinkou jsou také **sankce.** Což je velmi pravděpodobně jeden z hlavních důvodů, proč se GDPR stalo takovým tématem. Přináší totiž výrazné zvýšení sankci za nedodržování pravidel. Ty mohou v některých případech dosáhnout až 20 milionů euro, případně 4% celosvětového obratu. Na první pohled děsivé sankce jsou samozřejmě takto vysoké zejména proto, aby se k dodržování pravidel donutily i velké nadnárodní společnosti. Přestože GDPR zřejmě přinese zvýšení udělovaných sankcí ze strany ÚOOÚ, tak ve vztahu k běžným SVJ či BD lze počítat s nižšími sankcemi obvykle v řádu jednotek či maximálně desítek tisíc korun.

Jak na GDPR implementaci?

Každá impementace GDPR má několik kroků, které by měly následovat po sobě. Prvním krokem by měl být audit a jeho vyhodnocení. Po něm by pak měly následovat kroky spočívající v přijetí různých organizačních (určit kdo za co odpovídá a kdo co kontroluje, likvidace nepotřebných údajů), technických (zabezpečení počítačového i listinného zpracování) a právních opatření (vnitřní směrnice, aktualizované souhlasy a informace, smlouvy se zpracovateli, záznamy o činnostech zpracování)

Audit zpracování osobních údajů a jeho vyhodnocení

První co je potřeba udělat je provést audit zpracování osobních údajů v SVJ nebo BD. Povinnosti při zpracování osobních údajů z větší části nejsou nové a navazují na povinnosti upravené například v zákoně o ochraně osobních údajů, který je účinný téměř 18 let. Problémem je, že ne všechny povinnosti, které již dnes ze zákona vyplývaly, byly v praxi dodržovány. I proto audit může odhalit nejen to, co je potřeba přizpůsobit GDPR, ale i to, na co se třeba nepamatovalo v minulosti.

Máme řadu dokumentů z minulosti, budou se na ně vztahovat pravidla GDPR?

Ano, pokud budou osobní údaje zpracovávány po květnu 2018, kdy GDPR nabylo účinnosti, je třeba GDPR aplikovat i na osobní údaje, jejichž zpracování začalo před nabytím účinnosti. To znamená také to, že pokud jsou údaje zpracovávány třeba na základě souhlasu, který už neodpovídá GDPR, bude třeba získat souhlas nový a odpovídající. Naopak třeba povinnosti, které se mají plnit v okamžiku získávání údajů, např. informační povinnost dle čl. 13 GDPR, není třeba plnit znovu, protože okamžik, kdy měl být subjekt informován byl před nabytím účinnosti tehdy platné legislativy (ovšem i ta informování subjektu v určitém rozsahu vyžadovala).

Co bychom tedy měli při auditu zjišťovat?:

1. Zjistit **jaká zpracováním osobních údajů provádíme,** zejména s ohledem na

    a. Typ subjektu osobních údajů (členové BD či SVJ, nájemníci či podnájemníci, dodavatelé, zaměstnanci, funkcionáři orgánů atd.)
    b. Zpracovávané osobní údaje
    c. Účel zpracování a právní titul
    d. Způsob zpracování
    e. Kdo přichází s údaji do styku (v rámci SVJ či BD, zpracovatel a další subjekty)
    f. Způsob informování subjektu údajů
    g. Zabezpečení osobních údajů

2. Zjistit, co je třeba dodělat či změnit, aby bylo zpracování v souladu s GDPR

Výsledky auditu je dobré si zapisovat například do tabulky. Poslouží nám nejen při vyhodnocení auditu, ale následně i při tvorbě záznamů o činnostech zpracování, jejichž vedení je jedna z nových povinností podle GDPR.

Pro praktický příklad si vezměme například zpracování spočívající ve vedení seznamu členů BD. Tabulka, kterou si sestavíme, by pak mohla vypadat zhruba následovně:

Audit-vedení seznamu členů BD

Název zpracování	Vedení seznamu členů BD
Typ subjektu údajů	Členové BD
Zpracovávané osobní údaje	Jméno, příjmení, bydliště, den vzniku či zániku členství, výše členského vkladu a jeho splacení
Účel zpracování a právní titul	Přehled o členech BD – Plnění právní povinnosti (§6 odst. 1 písm. c) GDPR) dle § 580 a násl. zákona č. 90/2012 Sb., o obchodních korporacích.
Způsob zpracování	Elektronicky – cloudové úložiště, PC správcovské firmy
Kdo přichází s údaji do styku	Předseda družstva a členové představenstva BD (logovaný přístup do cloudového úložiště), členové BD na základě oprávnění přístupu dle §§ 582 a 583 ZoOK, zpracovatel – správcovská firma ABCD, s.r.o.
Způsoby informování subjektu údajů	Není – je třeba dodělat
Zabezpečení osobních údajů	PC předsedy – zabezpečení přístupu k počítači login/heslo, PC umístěno v bytě předsedy opatřeném bezpečnostními dveřmi PC správcovské firmy – je třeba doplnit smlouvu o zpracování osobních údajů

Opatření, která bude třeba provést	**Organizační:** Vést evidenci, komu byly osobní údaje z evidence členů předány, zjistit, zda jsou vedeny záznamy o přístupech k údajům v rámci cloudového úložiště **Technická:** Vytvořit zálohu seznamu členů na PC předsedy BD a tuto při změnách aktualizovat **Právní:** Zpracovat informaci pro členy o zpracování na webové stránky do členské sekce, Zpracování vnitřní směrnice s úpravou odpovědnosti, Zpracování záznamu do Záznamů o činnostech zpracování, Uzavřít dodatek o zpracování osobních údajů do smlouvy se správcovskou firmou, Zjistit jestli je vybrané cloudové úložiště kompatibilní s pravidly GDPR (zejména obsah smlouvy o zpracování, umístění serverů v EU)

Při jakémkoli zpracování osobních údajů je třeba mít na paměti zásady, které najdeme vyjádřeny v čl. 5 GDPR. Předně jde o účelnost zpracování, kterou rozvedeme v další kapitole. Vždy je třeba dále pamatovat na nutnost **minimalizace údajů,** tedy zpracovávat jen to, co potřebuji nebo ze zákona mám zpracovávat. Jakékoli neúčelné zpracování údajů může být jednak nezákonné, ale zároveň s sebou nese náklady a rizika spojená s nutným zabezpečením údajů. Osobní údaje by dále měly být **přesné.** To neznamená, že je v rozporu s GDPR, když máme v databázi zastaralý údaj, ale měli bychom mít nastaveny mechanismy, jak údaje aktualizovat. Důležité je i zachování **důvěrnosti a integrity** zpracovávaných osobních údajů. Musíme zabránit jak neoprávněným přístupům, tak ale i například ztrátě či zničení osobních údajů. Správce by měl být také schopen **doložit plnění povinností.** I proto je nutno věnovat se nejen zavedení opatření týkající se implementace GDPR, ale i jejich dokumentaci.

K tomu, abychom dokázali určit, co vše musíme při implementaci udělat, by nám mohl posloužit následující přehled konkrétních povinností, které dle GDPR správce má.
Kromě dodržování výše uvedených zásad jde zejména o následující:

- Stanovení účelu a právního titulu
- Zpracování záznamu o činnostech zpracování
- Příprava vnitřní směrnice
- Plnění informační povinnosti
- Naplňování práv subjektů údajů
- Smlouvy se zpracovateli
- Zabezpečení dat a hlášení incidentů

Stanovení účelu a právního titulu zpracování

U každého zpracování osobních údajů **bychom měli vědět jaký je jeho účel a o jaký ho opíráme právní titul.** Proč osobní údaje zpracováváme? To je základní otázka, kterou si musíme položit. Tam, kde nám ukládá zpracování zákon, nemusíme nic řešit a účelem je pro nás povinnost postupovat v souladu se zákonem. Půjde například o povinnost vést seznam členů BD. V případech, kdy osobní údaje nezpracováváme na základě zákona, může být situace složitější. Až překvapivě často se shromažďují nějaké osobní údaje dlouhodobě a nikdo už vlastně neví proč. Pokud nejsme v konkrétním případě schopni říci, proč nějaké údaje zpracováváme, bude na místě vážně pouvažovat o tom, že s takovým zpracováním skončíme. Základním pravidlem totiž je, že u každého zpracování údajů musíme vždy být schopni účel uvést.

Vedle účelu by každé zpracování mělo být opřeno také o nějaký z **právních titulů.** Jednotlivé právní tituly, které přicházejí v úvahu, najdeme v čl. 6 odst. 1 GDPR. Předně je třeba vyvrátit **častý omyl, že by základním právním titulem zpracování měl být souhlas.** Je tomu právě naopak, **souhlas vyžadujte až tam, kde žádný jiný titul zpracování nenajdete.** Ušetříte si tím řadu starostí. Už třeba proto, že souhlas lze kdykoli odvolat. Navíc vyžadování souhlasu tam, kde ho není třeba **je v rozporu s GDPR.**

Nejčastější právní tituly zpracování OÚ u SVJ a BD

- Souhlas subjektu údajů (čl. 6 odst. 1 písm. a) GDPR)
- Plnění smlouvy, jejíž smluvní stranou je subjekt údajů (čl. 6 odst. 1 písm. b) GDPR)
- Plnění právní povinnosti, která se na správce vztahuje (čl. 6 odst. 1 písm. c) GDPR)
- Zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů (čl. 6 odst. 1 písm. f GDPR)

Nejčastějšími právními důvody zpracování bude plnění právní povinnosti nebo dojednávání či následné plnění smlouvy. Specifický je právní titul dle čl. 6 odst. 1 písm. f) GDPR. Ten bude přiléhavý tehdy, kdy existuje nějaký významný zájem, pro nějž je například potřeba zpracovávat osobní údaje z důvodu ochrany zájmů SVJ nebo jeho jednotlivých členů. Typicky půjde třeba o provoz kamerového systému. U tohoto právního titulu je ale potřeba vždy pamatovat na to, že zájmy SVJ nebo třetích osob **je třeba vyvažovat s právy subjektů údajů.** Proto bude potřeba věnovat zvýšenou pozornost nastavení zpracování a přísné účelnosti a minimalizaci zásahů do soukromí.

Každá implementace GDPR začne skartací všech dokumentů obsahujících osobní údaje, u nichž nebudeme schopni určit účel a právní titul jejich zpracování.

Zpracování záznamu o činnostech zpracování

Jde o novou povinnost zakotvenou v čl. 30 GDPR, která do jisté míry nahrazuje spolu s posílenou informační povinností dřívější povinnost registrovat některá zpracování osobních údajů u Úřadu pro ochranu osobních údajů. Záznamy o činnostech zpracování budou vycházet z auditu po provedení kroků k dosažení souladu zpracování s GDPR. Jejich smysl je jednak vnitřní, tedy mít zdokumentována jednotlivá zpracování. Druhým účelem je předložení záznamů ÚOOÚ v případě kontroly.

Záznam o činnosti zpracování nemá nějakou předepsanou formu, vhodné je ale například připravit si jednu tabulku v tabulkovém editoru (např. Excel), kam se vedle sebe vypíší jednotlivá zpracování. Ta je vhodné třídit podle evidencí nebo informačních systémů, případně podle účelů nebo kategorií subjektů údajů. Může jít tak například o vedení seznamu členů, vedení účetnictví, vedení zaměstnanecké agendy, provoz kamerového systému apod.

Co by mělo být v záznamech evidováno

- jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů – tedy údaje o SVJ či BD, jakožto správci, případně o osobě, která je v rámci SVJ a BD pověřena dohlížet na zpracování osobních údajů v dané agendě
- účely zpracování – účel by měl být určen jednoznačně, v případě, že je plněna právní povinnost, tak není třeba dovozovat účelnost a stačí odkaz na příslušný právní předpis, který ukládá zpracovávat osobní údaje
- popis kategorií subjektů údajů a kategorií osobních údajů – půjde o členy BD, SVJ, nájemníky či podnájem-

níky, členy orgánů SVJ či BD, zaměstnance, rodinné příslušníky, případně další osoby

- kategorie příjemců, kterým byly nebo mohou být osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích – půjde o osoby, které mohou mít k osobním údajům přístup (např. další členové SVJ či BD v případě vedení seznamu členů), není třeba vypisovat veškeré možné příjemce typu policie, jejichž oprávnění vyplývá ze zvláštních zákonů

- informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace – zde pravděpodobně k žádným předáním docházet nebude, nicméně je třeba pamatovat například, že takovým předáním může být i lokalizace údajů na počítačovém serveru umístěném v zahraničí

- je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů – zde stanovit lhůty buď číslem, nebo alespoň uvést mechanismus, který vede ke stanovení délky zpracování (např. u souhlasu, že bude zpracováváno tak dlouho, dokud nebude souhlas odvolán)

- obecný popis technických a organizačních bezpečnostních opatření - uvést, jaká opatření byla přijata k ochraně osobních údajů (k tomu viz kapitola věnovaná zabezpečení osobních údajů)

Vedle toho, co v záznamech být dle GDPR musí, je dobré doplnit do záznamů i další informace.

Co je dobré také v záznamech evidovat

- Způsob informování subjektu údajů o zpracování

- Využití a identifikace zpracovatele osobních údajů

- Pokud je právním titulem souhlas, tak kde a jak je uchovávána listina k jeho prokázání

- Fyzické umístění osobních údajů – tedy nejen umístění fyzických kopií, ale například i umístění serverů, na nichž jsou uloženy osobní údaje v cloudu

- Kdo v rámci SVJ či BD má k údajům přístup

- Kdo má na starost naplňování práv subjektu údajů (např. na přístup k údajům, na opravu atd.)

Vzory záznamu o činnosti zpracování zde:

Příprava vnitřní směrnice

Vnitřní směrnice o zpracování osobních údajů v rámci SVJ a BD je dalším „papírem“, který je vhodné při implementaci GDPR zpracovat. **Mít směrnici není povinnost, která by vyplývala z GDPR přímo výslovně,** nicméně vzhledem k tomu, že je nezbytné dokumentovat přijatá opatření, tak je to jedna z možností, jak nastavit pravidla nakládání s osobními údaji.

Směrnice by neměla pouze mechanicky opakovat povinnosti správce, ale měla by být praktickým dokumentem, který zachycuje toky osobních údajů (např. mezi správcem a zpracovateli), jednotlivá organizační a technická opatření k ochraně osobních údajů a to, kdo je za co při zpracování odpovědný. Slouží zejména pro vnitřní potřebu osob, které s osobními údaji pracují, tedy zejména členy orgánů SVJ či BD, zaměstnance, případně externí dodavatele, jako je správcovská firma či účetní.

Vzor vnitřní směrnice je k dispozici zde:

Plnění informační povinnosti

Důraz na transparentnost zpracování je jedním z principů GDPR. Subjekt údajů by měl být obecně vždy informován o zpracování svých osobních údajů. Klíčový problém, který tedy budou muset SVJ a BD řešit je, jak **sladit povinnost informovat subjekty údajů s tím, aby to pokud možno co nejméně zatěžovalo fungování SVJ či BD** a činnost jejich orgánů.

Způsob informování se bude odvíjet od kategorií subjektů údajů. Jinak lze informovat u členů SVJ či BD, jinak u dalších osob. Povinnost prokazovat, že byl subjekt údajů s informací seznámen, má správce. Jednoznačně lze samozřejmě prokázat informování v případě, že toto máme od subjektů údajů podepsáno. To nicméně nemusí být úplně praktické už proto, že může docházet ke změnám ve zpracování, kdy bychom museli vždy znovu shánět podpisy, případně je to v zásadě nemožné, jako třeba u zpracování osobních údajů při používání kamerového systému. Podle okolností se tak nabízí i další způsoby, jako je vložení informací do stanov či smluv, vyvěšení na domovní nástěnce či na webových stránkách, ústní seznámení na schůzích, které je následně uvedeno v zápise ze schůze.

Povinnost informovat subjekty údajů lze najít v čl. 13 a 14 GDPR. Zatímco čl. 13 se věnuje případům, kdy **získáváte osobní údaje od subjektu údajů** (např. vedení seznamu členů), tak čl. 14 případům, kdy je získáváte **jiným způsobem** (např. kamerové záznamy).

Pro většinu zpracování osobních údajů v SVJ či BD bude právním titulem plnění právní povinnosti. U plnění těchto povinností by do budoucna mělo postačovat uveřejnit informace na webových stránkách BD či SVJ. Toto vyplývá z návrhu zákona o zpracování osobních údajů, konkrétně z jeho navrhovaného § 8. Bohužel v současné době neprošel ještě tento zákon legislativním procesem, nicméně lze předpokládat, že toto pravidlo bude obsahovat.

Pořizujeme zápisy ze schůzí SVJ. Musím na schůzi vždy znovu informovat o zpracování osobních údajů, které se objeví v zápise ze schůze?
Informační povinnost není třeba plnit v případech, kdy subjekt údajů už má informace o zpracování osobních údajů z minulosti. Pokud tedy nedochází ke změnám, tak informování nebude třeba. V daném případě doporučujeme uveřejnit informaci o zpracování na webových stránkách a zároveň například dát do zápisu z některé ze schůzí SVJ, případně i vyvěsit v domě na nástěnce.

Pokud zpracováváme údaje na základě souhlasu subjektu údajů, tak by informace měla být podána ještě před udělením souhlasu, protože jednou z náležitostí souhlasu je i informovanost s parametry zpracování, k němuž souhlas dávám. Pokud by šlo o plnění smluvní povinnosti, je vhodné informaci včlenit do smlouvy.

A co by měla **informace obsahovat?**

1. Označení správce ideálně s kontaktními údaji na osobu zodpovědnou za dané zpracování
2. Kategorie osobních údajů
3. Účel a právní titul, k němuž jsou osobní údaje zpracovávány, včetně podrobností pokud by byl právním titulem oprávněný zájem správce nebo třetí osoby
4. Kategorie příjemců osobních údajů a případný záměr předávat údaje do třetích zemí mimo země EU

Vedle výše uvedených informací je vhodné poskytnout i další informace, nicméně jejich poskytnutí je povinné pouze pokud je to nutné pro zajištění „spravedlivého a transparentního zpracování“. Jde například o následující informace:

1. Doba, po níž budou údaje zpracovány (může být stanovena buď pevně, nebo vázána na určitou skutečnost – např. odvolání souhlasu)
2. Informace o právu a způsobu odvolání souhlasu, pokud je zpracování na něm založeno
3. Informace, zda má subjekt údajů zákonnou či smluvní povinnost údaje poskytnout
4. Informace o právech subjektu údajů (zejména právo na přístup, opravu, vznesení námitky, právo obrátit se na dozorový úřad)
5. Informaci, zda dochází k automatizovanému rozhodování či profilování (na činnost SVJ a BD se vztahovat prakticky nebude).

Z informační povinnosti jsou i výjimky. Tou hlavní je, že **není třeba poskytovat informaci, pokud ji subjekt údajů už má.** Další skupina výjimek se vztahuje na zpracování, kde získáme údaje jiným způsobem, než od subjektu údajů. Tyto další výjimky uvedené v čl. 14 odst. 5 GDPR se ale v praxe SVJ a BD příliš neuplatní.

Důležité je řešit i **způsob informování.** GDPR totiž přináší jeden zdánlivý paradox. Na jednu stranu klade důraz na transparentnost a poměrně široké spektrum informací, které by měl subjekt údajů dostat. Na druhou stranu ale zdůrazňuje i srozumitelnost těchto informací. Do budoucna se zřejmě objeví sady obecně srozumitelných piktogramů, které nám prostřednictvím obrázků popíší parametry daného zpracování. Do té doby lze využívat vrstvení informací, pokud je to vhodné.

Provozujeme kamerový systém, jak mám informovat subjekty údajů, že pořizujeme záznam?
Nejpraktičtější forma, je často používaná informační tabulka. Problém je, že se na ní vejde poměrně málo informací. Bude tedy vhodné informaci strukturovat tak, že na samotné ceduli bude informace, že dům je sledován kamerami se záznamem, že správcem je SVJ či BD, dále informace, že důvodem je ochrana majetku správce a osob bydlících v domě a nakonec informace, že další informace lze získat na webových stránkách BD či SVJ případně na nějakém kontaktním telefonním čísle. Zde by pak měla být umístěna, respektive předána informace například o tom, jak dlouho je záznam uchováván, případně informace o právech subjektů údajů.

Vzor informace pro vyvěšení na webové stránky je k dispozici zde:

Naplňování práv subjektů údajů

Subjekt údajů má dle GDPR řadu práv, která může vůči správci nebo zpracovateli uplatňovat. Tato práva mají zajistit, aby měl přístup k informacím, jak jsou jeho údaje zpracovány, případně aby mohl jejich zpracování ovlivnit.

Prvním právem je právo na přístup k osobním údajům zakotvené v čl. 15 GDPR. Jestliže informace dle čl. 13 GDPR by měla zpracování osobních údajů předcházet nebo dle čl. 14 GDPR následovat v krátké době po zahájení zpracování, tak právo na přístup lze uplatnit kdykoli během trvání zpracování. Jde zejména o právo dozvědět se od správce, jaké údaje jsou zpracovávány, včetně informace o účelu a právním titulu zpracování, dále o tom, komu údaje mohou být předávány, či po jakou dobu budou zpracovávány.

Zároveň s obecnými informacemi správce musí poskytnout i kopie zpracovávaných osobních údajů. Při tom je třeba dbát, aby nedošlo k zásahu do práv jiných osob, což s sebou může nést **dosti náročné úpravy nosičů osobních údajů.** Pokud například máme kamerový záznam, na němž je zachycen subjekt údajů, tak by mu tyto záznamy měly být poskytnuty až po anonymizování, dalších osob na záznamu. V případě předání kopií dokumentů by se zase měly začernit pasáže týkající se osobních údajů dalších osob. Pokud bychom to neudělali, mohlo by jít o porušení povinnosti zabezpečit osobní údaje. Toto se ale samozřejmě nebude týkat případů, kdy má ze zákona subjekt údajů přístup ke kompletním dokumentům na základě jiných právních předpisů, jako bude třeba přístup k zápisům ze schůzí orgánů SVJ či BD.

Jeden z členů družstva se na nás obrátil s požadavkem, abychom mu sdělili veškeré osobní údaje, které o něm vedeme. Ve sklepě máme na hromadě staré spisy, s nimiž nepracujeme a nikdo se v nich nevyzná. To je opravdu budu muset všechny procházet a hledat, kde je co o tom člověku napsáno?
Zde je nutné si říci, na jaká zpracování osobních údajů se GDPR vztahuje. U manuálního zpracování by mělo jít o osobní údaje, které jsou nebo mají být v určité evidenci. Tedy měly by být nějakým způsobem uspořádány, mělo by v nich být možno hledat. Domníváme se tedy, že na spisy o nichž mluvíte se dle čl. 2 odst. 1 GDPR tento předpis vztahovat nebude a člen BD tak nebude mít právo toto požadovat. Na druhou stranu, pokud jde o spisy, s nimiž stejně nejde pracovat, tak bych doporučil zvážit jejich likvidaci.

V případě opakovaných žádostí lze požadovat administrativní poplatek za náklady spojené s poskytnutím informace, případně pokud by šlo o šikanózní žádosti, které se opakují v krátkých časových intervalech a jejich smyslem je pouze zatížit správce, tak by bylo na místě takovou žádost i odmítnout s odkazem na zneužití práva ze strany subjektu údajů.

Vedle práva na přístup má subjekt údajů dále **právo na opravu** nepřesných osobních údajů. Vyhovění takové žádosti o opravu údajů je nutné vyhovět i proto, že GDPR vyžaduje zároveň zpracovávat přesné osobní údaje, respektive zavést mechanismy pro jejich aktualizaci.

V nájemních smlouvách vyplňujeme i rodná čísla nájemníků, členů BD. Neporušujeme tím zákon?
Používání rodného čísla se řídí pravidly, která se liší od ostatních osobních údajů a jsou upravena v zákoně č. 133/2000 Sb., o evidenci obyvatel a rodných číslech. Tento zákon umožňuje v zásadě dva režimy. Buď vyplývá vaše povinnost rodné číslo evidovat ze zákona. Nebo k tomu potřebujete souhlas nositele rodného čísla. Proto by se rodná čísla neměla v nájemních smlouvách uvádět. K identifikaci stran postačuje plně jméno, bydliště a datum narození.

Určitý mediální mýtus vznikl kolem tzv. **„práva být zapomenut“.** To bylo často prezentováno jako novinka, s kterou GDPR přichází. V řadě případů bylo toto právo považováno za absolutní, tedy jako právo subjektů dosáhnout likvace jakýchkoli jeho osobních údajů. Toto samozřejmě pravda není. Fakticky jde pouze o zdůraznění povinnosti správce likvidovat osobní údaje, u nichž už nejsou splněny podmínky pro jejich zpracování a právo subjektu údajů požadovat likvidaci těchto údajů. Tato povinnost zde byla již dříve, ale často ji správci nedodržovali dostatečně důsledně. Rozhodně neplatí, že SVJ či BD musí například vyhovět požadavku subjektu údajů zlikvidovat i údaje, které zpracovává ze zákona.

Subjekt údajů má dále právo na **omezení zpracování osobních údajů.** To se týká případů, kdy například již pominuly účely původního zpracování a správně by mělo dojít k likvidaci osobních údajů, nicméně subjekt údajů například žádá, aby správce údaje dále zpracovával z důvodu využitelnosti údajů pro obhajobu oprávněných zájmů subjektu údajů. Ten by mu měl vyhovět, nicméně zpracování (tedy například předání údajů subjektu údajů místo jejich likvidace) by mělo probíhat pouze za požadovaným účelem.
Dále například může jít o omezení zpracování po dobu ověření, zda jsou zde dostatečné oprávněné zájmy správce (tedy právní titul dle čl. 6 odst. 1 písm. f) GDPR), které odůvodňují zpracování osobních údajů i po vznesení **námitky** dle čl. 21 GDPR.

O vyřízení jednotlivých žádostí souvisejících s uplatněním práv subjektů údajů by měla být vedena **jednoduchá evidence,** která by obsahovala, kdo o co žádal, kdo věc vyřizoval a jakým způsobem.

Smlouvy se zpracovateli

Povinnost mít písemnou smlouvu se zpracovatelem osobních údajů je něčím, na co bude třeba při implementaci GDPR v SVJ či BD dobře pamatovat. Tato povinnost sice není nová a byla již ve starém zákoně o ochraně osobních údajů, v řadě případů ale nebyla plně respektována a tak je zpravidla potřeba smlouvy předělat nebo napsat úplně znovu.

V praxi SVJ a BD půjde zejména o **smlouvy se správcovskými firmami, externími účetními, ale i o smlouvy s provozovateli serverů,** na nichž jsou zpracovávány osobní údaje (např. webové stránky, cloudové zpracování).
Tyto společnosti obvykle mají samy připravené smlouvy o zpracování osobních údajů, které lze po kontrole použít, nicméně je třeba pamatovat na to, že je odpovědností správce, aby smlouva obsahovala veškeré závazky zpracovatele, které dle GDPR obsahovat má. Ty jsou konkrétně rozvedeny v čl. 28 odst. 3 GDPR. Jde zejména o závazek zpracovatele, že se bude řídit při zpracování pokyny správce a přijme stanovená opatření k zabezpečení osobních údajů.

Důležité je upravit i **zapojení různých subdodavatelů.** Zpracovatel by se ve smlouvě měl zavázat k tomu, že bude informovat s předstihem o zapojení subdodavatelů, kteří se zapojí do zpracování osobních údajů s tím, že by SVJ a BD měla zůstat možnost konkrétního subdodavatele odmítnout. To bude připadat v úvahu zejména, pokud by měly osobní údaje být předávány mimo území EU. Zároveň by ve smlouvě měl být závazek, že zpracovatel tyto subdodavatele smluvně zaváže k zachování stejné úrovně ochrany dat, jaká vyplývá ze smlouvy o zpracování osobních údajů, a že bude odpovídat za případná pochybení těchto subdodavatelů.

Chceme sdílet osobní údaje prostřednictvím cloudu a poskytovatel cloudových služeb s námi nechce uzavřít zvláštní smlouvu o zpracování osobních údajů. Můžeme tyto služby využívat?

Zejména u velkých poskytovatelů cloudových služeb se lze setkat s tzv. adhezními smlouvami, tedy smlouvami, v nichž nemůžete jako druhá smluvní strana nic měnit, ale pouze smlouvu akceptovat nebo služby nevyužívat. Obvykle tedy nemáte jako správce možnost uzavírat specifickou smlouvu a třeba měnit smluvní podmínky, nicméně i tento typ smlouvy je dostačující, pokud je uzavřena jasnými projevy vůle a má písemnou formu. Samozřejmě musí splňovat také veškeré náležitosti stanovené v GDPR.

Vzor smlouvy se zpracovatelem je k dispozici zde:

Zabezpečení – organizační a technická opatření

Zabezpečení osobních údajů je jednou z nejdůležitějších povinností, které musí správce zajistit. Často je dokonce zabezpečení vnímáno jako povinnost jediná, což, jak je zřejmé z předchozích řádků, není pravda.
Důležité je uvědomit si, **před čím mám vlastně data chránit.** Cílem bezpečnostních opatření je nejen to, aby nedošlo k úniku nebo zneužití dat ze strany někoho neoprávněného, ale ani k jejich ztrátě, pozměnění či zničení. Proto je vedle různých bezpečnostních opatření nezbytné nastavit třeba i zálohování.

Dobrým zabezpečením je zabezpečení, při němž nedojde k ničemu z toho, před čím data chráníme. GDPR nepřináší výčet povinných způsobů zabezpečení, což je jediným možným řešením v době rychlého rozvoje technologií, kdy by třeba jedno přikázané technické řešení mohlo být za pár měsíců nepoužitelné. Na správce to ale samozřejmě klade **zvýšené nároky.**

Jedním z mýtů je, že by zabezpečení osobních údajů mělo být na maximální možné úrovni. GDPR naopak říká, že **úroveň zabezpečení by se měla odvíjet od charakteru zpracování a hrozících rizik.** Obecně platí, že bychom samozřejmě mohli do zabezpečení dávat stále větší a větší peníze a míra zabezpečení by se vždy zvýšila. Nakonec by ovšem už investice byla tak velká a zlepšení tak nepatrné, že by přijímání takových opatření nedávalo smysl.

Předně tedy zhodnotíme, o jak citlivé údaje se bude jednat. Samozřejmě nejcitlivějšími budou zvláštní kategorie údajů, nicméně ty SVJ ani BD zpracovávat zpravidla nebudou. Dále je důležitým kritériem, jaké nepříjemnosti by subjektům údajů hrozily, pokud by se údaje dostaly do nepovolaných rukou a jaká by například mohla být motivace někoho osobní údaje neoprávněně získat. Na druhé straně pak hodnotíme náklady a přínosy přijatých opatření.

Nájemník, kterému naše BD pronajímá byt, chce přesně vědět, kde máme uloženy jeho osobní údaje. Musíme mu tuto informaci dát?
Subjekt údajů má právo vědět, jaké údaje jsou zpracovávány, včetně informace o účelu a právním titulu zpracování, dále o tom, komu údaje mohou být předávány, či po jakou dobu budou zpracovávány. Má také právo na kopie osobních údajů. Sdělení o způsobu zabezpečení osobních údajů nemáte povinnost předávat a v řadě případů je to i nevhodné, protože to může zabezpečení ohrozit.

Obecně lze říci, že zpracování prováděná SVJ a BD budou spíše méně riziková a náklady na zabezpečení by neměly být nijak vysoké. Vždy bychom měli přijímat taková opatření, aby byla funkční a aby se skutečně dodržovala. Jsou nesmyslná opatření, která ztěžují běžné fungování SVJ a BD natolik, že je nutné je obcházet.

Pokud jde o **papírové zpracování,** pak by mělo být vždy zřejmé, kdo má k osobním údajům přístup, údaje by ideálně měly být v uzamčené místnosti, případně alespoň v uzamčené skříni. Není třeba naopak pořizovat například trezorové skříně. Měla by být vedena evidence vydaných klíčů. Zejména v menších SVJ či BD jsou údaje uloženy v bytě předsedy nebo jiného člena vedení. Je třeba pamatovat, že i zde by se mělo zamezit přístupu neoprávněných osob, kterými mohou být nejen třeba návštěvy, ale i rodinní příslušníci.

Počítače, na nichž jsou zpracovávány osobní údaje či přístupy do cloudových úložišť, by měly být chráněny **uživatelským jménem a heslem,** které používá pouze konkrétní osoba. Mělo by být rovněž stanoveno, kdo může údaje pouze prohlížet a kdo je může měnit. Mělo by být dohledatelné, kdo jaké změny prováděl. Podobně jako se zaheslovávají počítače, je třeba zaheslovat i přenosná média (externí disky, flashky, CD). Počítače by samozřejmě měly mít běžnou úroveň zabezpečení, tedy aktualizované antiviry či firewally. Nelze spoléhat pouze na zabudované zabezpečení od výrobce operačního systému.

U nastavení hesla by měla být vybírána ideálně hesla, která na první pohled nedávají smysl, využívají různých druhů znaků (velká a malá písmena, čísla, speciální znaky), nejsou nějak úzce spojena s osobou, která heslo využívá (jméno dítěte, datum narození, apod.)

Důležité je stanovit si rovněž **pravidla pro e-mailovou komunikaci.** Často členové orgánů BD a SVJ používají své soukromé e-maily umístěné u různých poskytovatelů. Pro běžnou komunikaci to nemusí být problém, nicméně je dobré se vyvarovat třeba zasílání citlivějších dokumentů v přílohách. Už proto, že při zasílání e-mailů reálně hrozí odeslání jiné osobě, než je zamýšlený adresát. Vhodnější je tyto umisťovat třeba do již zmíněných cloudových úložišť, kde si je může adresát vyzvednout. Řešením může být také zaheslování dokumentu. Pro zasílání informací členům SVJ či BD lze doporučit uveřejnění informace v členské sekci webu a zaslání informačního e-mailu s obecným popisem dokumentu a odkazem do členské sekce e-mailem.

Se zabezpečením souvisí přijetí různých **organizačních opatření,** které minimalizují zpracování osobních údajů, protože obecně platí, že jediným stoprocentním zabezpečením osobních údajů je to, když tyto údaje vůbec nezpracováváte. Důležitým organizačním opatřením by tak mělo být stanovení pravidel pro likvidaci osobních údajů. Je vhodné myslet i na možnosti snížení rizikovosti zpracování. Už pouhá pseudonymizace osobních údajů, tedy například vedení si databáze kontaktních telefonů pod čísly bytů a nikoli pod jmény majitelů, je poměrně jednoduchým nástrojem, který ale snižuje rizika.

Dalším organizačním opatřením by měla být pravidelná revize osobních údajů a jejich aktualizace. Lze doporučit aktualizovat například kontaktní údaje průběžně dle oznámení členů, a pak třeba jednou ročně při schůzi členů.

Při nastavování pravidel je třeba pamatovat i na **proměnu oprávnění konkrétních osob.** Typickým příkladem může být volba nového představenstva BD, kdy by starému představenstvu mělo být znemožněno nadále využívat stará přístupová oprávnění, ať už jde o počítačová hesla nebo klíče od archivu.

Proč mám chránit seznam vlastníků jednotek, když v něm jsou údaje, které si každý může najít v katastru nemovitostí?

Podle GDPR neplatí, že pokud jsou údaje zveřejněné a někdo jiný je zároveň zpracovává, tak je nemusí chránit. Může to vypadat paradoxně, když máme chránit osobní údaje, které jsou dostupné volně na internetu, nicméně ačkoli jde o stejné údaje, tak účel zveřejnění, správce i právní titul jsou rozdílné. Na druhou stranu zabezpečení údajů bychom měli přizpůsobit rizikům s ohledem na to, jak závažný zásah do práv subjektů údajů by například neoprávněný přístup k seznamu znamenal, ale také s ohledem na to, nakolik je pravděpodobné, že k takovému neoprávněnému zásahu dojde. Samozřejmě zde zásah vzhledem k tomu, že údaje jsou veřejné v katastru nemovitostí, bude malý a pravděpodobnost, že bude někdo motivován se vám třeba dostat do počítače a seznam si zkopírovat je s ohledem na jeho legální dostupnost v katastru také minimální.

Hlášení bezpečnostních incidentů

Novou povinností je povinnost hlásit bezpečnostní incidenty, tedy porušení zabezpečení osobních údajů. Tato povinnost zde byla již dříve, ale vztahovala se pouze na určité sektory. Podle GDPR jde o povinnost, která se vztahuje na všechny správce.

To kdy a komu je potřeba porušení zabezpečení hlásit závisí na tom, **jak velké riziko pro práva a svobody osob tento incident znamená.** SVJ či BD tedy musí posoudit, jaká data unikla (nebo třeba byla omylem smazána), za jakých okolností (např. méně rizikové může být, pokud jde o nedbalost, než pokud by šlo o úmysl data získat neoprávněně) a zejména, co by mohl útočník s daty dělat (např. zneužití údajů ke krádeži identity) případně jaký zásah do práv subjektu údajů ať už v majetkové či nemajetkové sféře to může znamenat. V zásadě mohou existovat tři varianty postupu:

1. Pokud je vyhodnoceno, že zde pravděpodobně **není riziko pro práva a svobody** subjektu údajů, tak zde ani nevznikne povinnost hlášení provádět. V praxi si lze například představit únik seznamu členů SVJ s údaji, které jsou veřejně dostupné v katastru nemovitostí. Pokud například takový seznam omylem zašleme osobě, která vůbec nemá s SVJ nic společného, tak to nebude znamenat žádné nové ohrožení pro subjekty údajů, protože i pokud by tato osoba chtěla informace nějak zneužít, tak se k nim může jednoduše a na dálku dostat pohledem do katastru nemovitostí. To nicméně už nemusí platit u seznamu členů BD, který nikde veřejně dostupný není.

2. Pokud dojdeme k tomu, že zde potenciálně **může být nějaké riziko,** tak máme povinnost ohlásit bezpečnostní incident Úřadu pro ochranu osobních údajů, a to do 72 hodin od chvíle, kdy je únik dat zjištěn. Náležitosti, co by mělo hlášení obsahovat, jsou uvedeny v čl. 33 odst. 3 GDPR.

3. Poslední možností je, že by unikla data, kde hrozí **velké nebezpečí** pro práva subjektů údajů, pokud jde o riziko zneužití osobních údajů. To by se týkalo zejména úniku zvláštních kategorií údajů (dříve citlivých údajů). V takovém případě čl. 34 GDPR ukládá správci oznámit bezpečnostní incident přímo subjektu údajů.

Typická zpracování osobních údajů v SVJ a BD

Z naší dosavadní poradenské praxe vyplynulo, že okruh druhů zpracování se v SVJ a BD opakuje. Praxe se tak neliší obvykle ani tak v druzích zpracování, ale spíše ve způsobu zpracování, ať už jde o zapojení zpracovatelů do procesu zpracování nebo otázku nakolik jsou při zpracování využívány informační technologie. Rozdíly pak samozřejmě jsou i v tom jak velké SVJ či BD je a zda je výkon činností pro družstvo profesionalizován.

Vedení seznamu členů SVJ či BD

Vedení seznamu členů BD a SVJ je jedna ze základních povinností, které vyplývají ze zákona. V případě SVJ jde o ustanovení § 1177 a násl. občanského zákoníku, v případě BD pak o § 580 zákona č. 90/2012 Sb., o obchodních korporacích. Vedení příslušného seznamu je samozřejmě nezbytné pro správu domu, realizaci převodů bytů v BD, rozpočítávání nákladů atd. Právním titulem zde tedy bude plnění právní povinnosti a rozhodně není třeba žádat o souhlas se zpracováním osobních údajů.

Máme pohledávku vůči jednomu členovi družstva za nezaplacený nájem. Ten se teď ocitnul v oddlužení. Můžeme zpracovávat informace o průběhu oddlužení? Dlužník nám tvrdí, že k tomu potřebujeme jeho souhlas.

Jakožto dobrý hospodáře předpokládám, že se BD přihlásilo do oddlužení se svojí pohledávkou. Vymáhání pohledávek samozřejmě je legitimním oprávněným zájmem dle čl. 6 odst. 1 písm. f) GDPR, na základě něhož lze zpracovávat osobní údaje i bez souhlasu subjektu údajů. Často se lze setkat s tím, že SVJ či BD zpracovávají za účelem prověřování dlužníků jejich rodná čísla. Zde je ovšem nutno upozornit, že to lze na základě zákona o evidenci obyvatel a rodných číslech dělat pouze se souhlasem nositele rodného čísla.

Důležité je zde upozornit, že v obou případech, tedy jak u BD, tak u SVJ tyto údaje ze seznamu také mají být poskytovány na vyžádání dalším členům BD či vlastníkům jednotek. Toto vyplývá z § 1178 občanského zákoníku (pro SVJ), respektive z § 582 odst. 1 zákona o obchodních korporacích. V případě bytového družstva dokonce představenstvo umožní nahlédnout do příslušné části seznamu každému (tedy i nečlenovi družstva), jestliže osvědčí právní zájem na tomto nahlédnutí nebo doloží písemný souhlas člena, kterého se zápis týká (§ 582 odst. 2 zákona o obchodních korporacích).

Evidence dalších kontaktních údajů

Vedle seznamu členů BD a SVJ obvykle evidují i další údaje týkající se členů či vlastníků jednotek. Zejména půjde o e-mailové kontakty či telefonní čísla. Na rozdíl od jména či adresy, v tomto případě nevyplývá povinnost vedení těchto údajů ze zákona, ale z mnoha důvodů je samozřejmě praktické, aby BD či SVJ tyto kontaktní údaje mělo. Důvodem může být potřeba řešit například havárie, kdy třeba vlastníkovi bytu teče v bytě voda a on je na dovolené. Může ujít ale i o mnohem méně naléhavé případy, jako je domluva termínů odečtů vody, informování o konání schůzí, nebo jen obecné informace o dění v domě.

Pokud jde o právní titul pro zpracování údajů, tak v případě uchovávání kontaktních telefonních čísel pro případ havárie by připadal v úvahu právní důvod dle čl. 6 odst. 1 písm. f) GDPR, tedy oprávněný zájem správce, který převyšuje zájem na ochraně soukromí subjektů údajů. V takovém případě by tedy nebylo potřeba žádat souhlas se zpracováním osobních údajů.

Získání souhlasu lze nicméně doporučit například u uchovávání e-mailových kontaktů za účelem sjednání revizí, odečtů případně zasílání informací o dění v domě. Pokud jde o pozvánky na schůze, pak i zde by měl být vysloven souhlas. V takovém případě by bylo možno například uvažovat o uplatnění právního titulu oprávněného zájmu správce, který převyšuje zájem na ochraně soukromí. Totéž, co je uvedeno výše se pak bude vztahovat například i na nájemníky vlastníků jednotek.

Ve stanovách máme uvedeno, že pozvánka na schůzi bytového družstva se zasílá e-mailem na adresu sdělenou jednotlivými členy BD. Jaký bude titul pro zpracování e-mailů v tomto případě?
V takovém případě by zřejmě šlo o právní titul spočívající v oprávněném zájmu správce, kterým je plnění pravidel stanovených ve stanovách. Je zde ale třeba dát pozor na rozesílání dalších informací e-mailem, kde oprávněný zájem převyšující zájem na ochraně soukromí třeba dovodit nepůjde a bude třeba vyžadovat souhlas. Tedy i pokud údaje zpracováváme k jednomu účelu, nemůžeme je automaticky využívat k jiným účelům.

Vzor poskytnutím telefoního čísla a e-mailu je k dispozici zde:

Zápisy ze schůzí

Vedení zápisů ze schůzí je nezbytné pro fungování BD či SVJ a povinnost vytvářet zápis vyplývá ze zákona. V případě SVJ se používá podpůrně úprava fungování spolku v občanském zákoníku (dle § 1221 OZ) včetně povinnosti statutárního orgánu vyhotovit zápis (§ 254 OZ). V případě BD je pak povinnost vyhotovovat zápis ze všech jednání orgánů BD obsažena přímo v zákoně (§ 634 ZOK). Zápisy ze schůzí přitom budou často obsahovat osobní údaje, ať už údaje z prezenčních listin, tak informace zachycené přímo v zápise. Proto i na ně se vztahuje povinnost chránit osobní údaje.

Otázkou tedy bude zejména, komu mají být zápisy ze schůzí zpřístupněny a jakou formou je to nejlepší. Pokud není ve stanovách SVJ upraveno jinak, tak členové mají právo nahlížet do zápisů ze schůzí. Ideální pro fungování SVJ je uveřejnění zápisů ve členské sekci webových stránek SVJ, která je přístupná pouze členům.

Mohu jako předseda SVJ vyvěsit zápis ze schůze SVJ na nástěnce v domě?
Pokud zápis obsahuje osobní údaje, tak by měl být přístupný pouze osobám, které na to mají ze zákona nárok. Problémem je, že v domě na nástěnce uvidí zápis i široký okruh osob, které nejsou členy SVJ, ať už jde o rodinné příslušníky, nájemníky nebo osoby, které s domem nic společného nemají (pošťák, návštěvy, řemeslníci). To, že by tyto osoby měly k osobním údajům přístup, by tedy mohlo znamenat porušení povinnosti zabezpečit osobní údaje před náhodným přístupem. Určitě by ale řešením mohlo být zveřejnění anonymizovaného zápisu beze jmen, například pouze v podobě přijatých usnesení.

V případě BD jsou práva širší, protože podle § 659 odst. 1 ZOK má každý člen družstva právo na vydání kopie zápisu z členské schůze. I zde lze doporučit výše zmíněný postup při publikaci zápisu ve členské sekci webu BD. Na vyžádání člena by pak mělo BD poskytnout i tištěnou kopii zápisu.

Webové stránky

Již v předchozí kapitole jsme naznačili, že webové stránky, kterými dnes již většina BD i SVJ disponuje, je vhodné rozdělit na sekci, která je dostupná všem a na sekci, která je dostupná pouze členům. V sekci dostupné všem je vhodné mít vedle obecných informací i kontaktní údaje na osoby, které za BD či SVJ jednají (pokud jde o soukromé kontakty, tak se souhlasem těchto osob) či na správcovskou firmu, stanovy, případně domovní řád. Většinu obsahu nicméně bude vhodné vložit do členské sekce, která bude přístupná pouze členům po zadání přihlašovacího jména a hesla. Půjde o pozvánky na schůze, zápisy ze schůzí, může jít i o údaje o hospodaření družstva, formuláře plných mocí apod.

V členské sekci je třeba pohlídat, aby obsah nebyl přístupný jiným osobám, než členům. Je třeba, aby v případě, že osoba přestane být vlastníkem jednotky a tedy i členem SVJ nebo BD, již neměla aktivní přístup do členské sekce.

U webových stránek je třeba rovněž pamatovat na to, že zde bude zpravidla docházet k zapojení zpracovatele osobních údajů, pokud budou webové stránky umístěny na serverech poskytovatele hostingových služeb. Zde je třeba uzavřít písemnou smlouvu o zpracování osobních údajů, která by měla mít veškeré náležitosti dle GDPR. Vybírat by se mělo rovněž podle toho, kde budou fyzicky data umístěna, tedy kde jsou servery, na nichž budou osobní údaje umístěny. Pokud půjde o státy EU, tak nemusíte nic dalšího řešit, u států mimo EU by však mohly vznikat další povinnosti a pro SVJ a BD je lepší se takového předávání dat do třetích zemí vyvarovat.

Zaměstnanci

Zejména u větších SVJ či BD se lze setkat s tím, že mají své zaměstnance, kteří vykonávají činnost. Nemusí jít přitom nutně o pracovní poměr, ale i o zaměstnance z dohod o pracovní činnosti nebo dohod o provedení práce. Právě prostřednictvím těchto dohod jsou často odměňování členové orgánů SVJ či BD. Se zaměstnaneckou agendou je samozřejmě spjato zpracování osobních údajů zaměstnanců, které se nijak nebude odlišovat například od zpracování údajů zaměstnanců ve veřejné či v soukromé sféře.

Celá řada právních předpisů v čele se zákoníkem práce či předpisy upravujícími sociální a zdravotní pojištění obsahují povinnosti zaměstnavatele určité osobní údaje shromažďovat, uchovávat či předávat třetímu subjektu. Vedle adresných osobních údajů půjde zejména o údaje o mzdě, pracovní době, kvalifikaci, počtu dětí, povinných odvodech pojištění, údaje evidované pro plnění povinností v oblasti bezpečnosti práce, požární ochrany a mnoho dalších. Zaměstnanec by měl být informován o zpracování osobních údajů, které se ho týká. Tuto informaci lze buď začlenit přímo do pracovní smlouvy, z hlediska operativnosti je nicméně lepší ji předat zaměstnanci samostatně a nechat si od něj rovněž podepsat, že s ní byl seznámen.

Lhůty pro zpracování osobních údajů dle platné legislativy

Typ dokumentu	Doba archivace	Právní úprava
Stejnopisy evidenčních listů	3 roky	§ 35a odst. 4 a § 37 odst. 1 zákona o organizaci a provádění sociálního zabezpečení
Mzdové listy	30 let (10 let u poživatelů starobního důchodu)	
Údaje potřebné pro stanovení a odvod pojistného	10 let	§ 22c zákona o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti

Účetnictví, vyúčtování služeb

Údaje o hospodaření, které SVJ či BD vede, obsahují samozřejmě také celou řadu osobních údajů. Vedle údajů členů BD či SVJ může jít například o osobní údaje nájemníků, kteří nejsou členy BD, o osobní údaje členů orgánů BD či SVJ, případně zaměstnanců.

I zde je nezbytné pamatovat na to, že členové BD a SVJ mají právo na přístup k informacím o hospodaření. V souladu s § 1179 OZ se například může vlastník jednotky, tedy člen SVJ, seznamovat s informacemi, jak osoba odpovědná za správu domu dům spravuje, může nahlížet do smluv, do účetních knih i dokladů. To platí I pro dokumenty, v nichž budou uvedeny osobní údaje. Právo seznamovat se s podklady vyúčtováním je zakotveno i v zákoně č. 67/2013 Sb., kterým se upravují některé otázky související s poskytováním plnění spojených s užíváním bytů a nebytových prostorů v domě s byty. Ten upravuje práva a povinnosti při vyúčtování služeb. V § 8 pak dává vlastníkům jednotek i nájemníkům (včetně členů BD, kteří jsou nájemníky) právo nahlížet do podkladů pro vyúčtování služeb, stejně mají právo činit si kopie podkladů pro vyúčtování.

Jak je to s osobními údaji dodavatelů, třeba na fakturách?

I údaje o dodavatelích, kteří jsou fyzickými osobami, případně o osobách jednajících jménem právnických osob, budou osobními údaji, které bude SVJ či BD zpracovávat. Právním titulem zpracování zde bude zejména plnění právní povinnosti (zejména povinnost vést v určité podobě účetní záznamy dle zákona o účetnictví) a samozřejmě také půjde o údaje nezbytné k plnění smlouvy a evidenci případných závazků ze smlouvy plynoucích. Informace o zpracování osobních údajů je vhodné dát jednak na webové stránky, jednak je vložit do podepisovaných smluv, na základě nichž je plněno.

Spornou otázkou je, nakolik při výkonu tohoto práva lze poskytovat i osobní údaje, například údaje o platbách či odpočtech v bytech dalších vlastníků či nájemníků. Vzhledem k tomu, že při rozúčtování služeb je nezbytné znát počty osob v bytě, podlahovou plochu, případně umístění bytu v rámci domu, je zřejmé, že tyto údaje povedou k identifikaci konkrétních bytových jednotek. K tomu je dobré zmínit i stanovisko Úřadu pro ochranu osobních údajů, který došel k závěru, že člen SVJ má právo seznamovat se s podklady relevantními pro společné hospodaření domu, včetně třeba údajů o úhradách do fondu oprav, které se týkají ostatních členů SVJ (k tomu viz rozhodnutí ÚOOÚ čj. 9/04/SŘ-OSR).

Lhůty pro uchovávání účetní dokumentace dle § 31 a § 35a zákona o účetnictví

Typ dokumentu	Doba archivace
Účetní závěrky a výroční zprávy	10 let
Účetní doklady, účetní knihy, odpisové plány, inventurní soupisy, účtový rozvrh, přehledy	5 let
Účetní záznamy, daňové doklady	5 let

Rozúčtování služeb a vedení účetnictví je často realizováno s pomocí různých externistů, ať už jde o externí účetní či správcovskou firmu. Vedení SVJ a BD by tedy ani zde nemělo zapomenout na uzavření písemných smluv o zpracování osobních údaj.

Bezpečnostní kamery

Bezpečnostní kamery jsou stále častějším způsobem zabezpečení bytových domů. Ponechme stranou otázku, nakolik je volba zabezpečení kamerovými systémy vhodná a soustřeďme se na pravidla, která by mělo BD či SVJ při instalaci kamerového systému splnit. V zásadě existují tři varianty využití kamer. První jsou klasické kamery se záznamem, kterým se budeme věnovat. Dalšími variantami mohou být kamery, které přenášejí obraz, ale tento nenahrávají. Těchto kamer se GDPR nedotkne, protože zde nedochází ke zpracování osobních údajů, protože nevzniká záznam. Alespoň tak se k těmto kamerám v současnosti staví ÚOOÚ. Každopádně zde je třeba pamatovat na ochranu osobnosti upravenou v občanském zákoníku. Třetí variantou, která určitě stojí za zvážení, jsou atrapy kamer. Pro jejich instalaci neplatí žádná omezení. Vyrábějí se velmi věrné atrapy, které mohou mít zejména na osoby, které se v domě pohybují poprvé, slušný preventivní účinek a mohou je odradit od páchání trestné činnosti.

My se nicméně budeme věnovat výlučně kamerovým systémům se záznamem. Pokud se SVJ nebo BD rozhoduje pro jejich instalaci, je dobré si nastudovat [1]Stanovisko ÚOOÚ č. 1/2016 .

Budu potřebovat k provozování kamerového systému souhlas všech vlastníků bytů?

Nikoli. Právním titulem pro instalaci kamerového systému v podstatě nikdy nemůže být souhlas. Ten by byl totiž potřeba od všech osob, které se na záznamech objeví, tedy nejen od vlastníků bytů, ale i jejich návštěv, řemeslníků, pošťáka apod. Nelze ani dovodit, že ten, kdo vstoupí do domu s monitorováním souhlasí, pokud je na něj upozorněn. Už třeba zmíněný pošťák do domu musí docházet za účelem plnění jeho pracovních povinností, dovozovat tedy z jeho vstupu do domu, že souhlasí s nahráváním na kameru, by bylo nesprávné. U kamerových systémů tak bude zpravidla právním titulem ochrana oprávněných zájmů správce či třetích osob, zejména vlastníků bytů, účelem pak ochrana majetku.

Právním titulem k instalaci kamerového systému, bude zpravidla ochrana majetku BD, SVJ nebo jejich členů, tedy ochrana oprávněných zájmů dle čl. 6 odst. 1 písm. f) GDPR. To s sebou přináší i potřebu klást větší důraz na přiměřenost. To začíná už při rozhodování o instalaci kamer, což by mělo být odůvodněno nějakými událostmi v minulosti, které také jsou prokazatelné. Může jít třeba o policejní protokoly o tom, že došlo k vykradení sklepa, bytu apod. Proto je dobré tyto incidenty hlásit policii a protokoly si uschovat pro případnou kontrolu ze strany ÚOOÚ.

Záběry kamery by neměly nepřiměřeně monitorovat veřejné prostory (ulici, náměstí), zároveň by ale neměl monitorovat prostory, kde lze v rámci domu očekávat větší míru soukromí (například dveře do bytů). Naopak možné za splnění dalších podmínek může být třeba monitorování vstupních dveří do domu, prostor sklepů, schránek, případně vnějšího pláště budovy včetně jeho bezprostředního okolí. Na tom, co a jak má být v domě vlastně monitorováno, závisí například výběr typu kamery a nastavení jejího záběru. Důležitá je nastavení pravidel provozu kamerového systému. Předně jde o dobu uchovávání záznamu. Ideální je kamerový systém nastavit tak, aby se záznam po určité době, např. po 24 hodinách sám promazával. Doba by měla být taková, aby dostačovala ke zjištění nějakého incidentu (např. vykradení sklepa). Nemělo by jít ale o více než několik dní. Následně lze samozřejmě uchovávat záznamy, které zachycují incident pro potřeby policie delší dobu.

Důležitá je také transparentnost. Tedy kamery by měly být viditelné, na domě by měla být informace o sledování spolu s informací, kdo je správce a jaké prostory v domě jsou monitorovány. Měl by zde být i kontakt na správce pro uplatnění práv subjektu údajů (např. na přístup ke kamerovému záznamu). V neposlední řadě je nezbytné věnovat se i zabezpečení. A to jak technickým, tak organizačním. Častou chybou zejména u malých

[1] Stanovisko je dostupné zde:
https://www.uoou.cz/stanovisko-c-1-2016-umisteni-kamerovych-systemu-v-bytovych-domech/d-18866#_ftnref1

kamerových systémů třeba bývá ponechání továrního nastavení hesla pro přístup ke kameře. Dnes si tak lze na internetu dohledat stránky se záběry z tisíců kamer po celém světě, které jsou volně dostupné. To samozřejmě pak bezpečnost spíše snižuje, než by ji to zvyšovalo. Důležité je i jasné nastavení toho, kdo má k záznamům z kamer přístup. Ideálně by to měla být pouze jedna osoba.

Vstup do domu na čipy

Další novou technologií, která se stále více rozšiřuje, je používání různých druhů kontaktních či bezkontaktních čipů pro otevírání domovních dveří. Tyto čipy mohou být na přívěsku na klíčích nebo třeba na kartě. Vstup na čip má svoje výhody, ale je potřeba zvážit i rizika a minimalizovat hned na začátku rozsah zpracování osobních údajů. Proto je potřeba si především stanovit účel, tedy proč chci vstup na čip. Nejčastějším důvodem bude kontrola toho, kdo čip má a může tedy vstupovat do budovy. Tedy evidence vydaných čipů, ale například i možnost konkrétní čipy zablokovat v případě, že se třeba dotyčný odstěhuje, prodá byt, ztratí čip apod.

Problémem je, že čipy umožňují i mnohem více, zejména evidenci jednotlivých vstupů do domu. Z nich zjistíte, kdy se kdo vrací z práce, kdy odchází z domova, kdy se chodí večer bavit a kdy se vrací. Toto jsou informace, kde bychom jejich účelnost hledali opravdu obtížně. Vedení BD a SVJ do tohoto nic není a mělo by respektovat soukromí obyvatel domu a omezit zpracování osobních údajů pouze na evidenci čísel vydaných čipů za účelem jejich možné blokace.

Je problém, že naše BD označuje domovní zvonky a poštovní schránky jménem?

Teoreticky i toto by mohlo být porušením povinností dle GDPR, pokud chybí souhlas subjektu údajů. Je na každém obyvateli bytu, aby si sám zvolil, zda chce být na zvoncích či schránce uveden a případně jakou formou. Existuje řada legitimních důvodů, proč někdo na schránce být uveden nechce (třeba se skrývá před exekutorem, násilnickým partnerem apod.) Ideální tedy je, aby BD či SVJ samo označování zvonků a schránek jmény neiniciovalo a označilo je třeba jen číslem bytu. Buď si mohou následně jednotliví obyvatelé domu zvonky označit sami, případně na jejich žádost tak může učinit BD či SVJ, nicméně to už pak nebude správcem takového zpracování a nebude za něj odpovídat, protože účel bude určovat sám subjekt údajů.

GDPR pro společenství vlastníků jednotek a bytová družstva
Vydalo Iuridicum Remedium, z.s.

Iuridicum Remedium, z.s.
Sídlo Přístavní 1236/35, 170 00 Praha 7
Kancelář U Výstaviště 3, 170 00 Praha 7
Tel. +420 776 703 170
e-mail: iure@iure.org
www.iure.org, www.slidilove.cz, www.bigbrotherawards.cz
Facebook: Ceny Velkého bratra ČR
Twitter: @iure_cz

Příručka byla vydána v rámci realizace projektu **Právní podpora pro hlavní výzvy v bydlení v roce 2018- GDPR, bydlení v platformách a nájmy.** Projekt je realizován za přispění prostředků státního rozpočtu ČR z programu Ministerstva pro místní rozvoj.

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR