



ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ

Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 111, fax: 234 665 444
posta@uouu.cz, www.uouu.cz



Čj. UOOU-04516/19-2

PŘÍKAZ

Úřad pro ochranu osobních údajů, jako příslušný správní orgán podle čl. 58 odst. 2 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 a § 60 zákona č. 110/2019 Sb., o zpracování osobních údajů, rozhodl dne 23. října 2019 v souladu s § 150 odst. 1 zákona č. 500/2004 Sb., správní řád takto:

Účastníku řízení Společenství vlastníků domu [REDAKCE], se sídlem [REDAKCE], se v souvislosti s porušováním povinnosti správce osobních údajů při zpracování osobních údajů členů SVD, rodinných příslušníků členů, nájemníků a třetích osob bydlících v domech spravovaných SVD, ukládá povinnost:

1. Nezveřejňovat v rámci úložiště SVD dokumenty vzniklé v rámci činnosti SVD, které obsahují osobní údaje, které nejsou nezbytné pro uplatnění práv a povinností člena SVD dle § 1175 a násl. zákona č. 89/2012 Sb., občanský zákoník, jako je jméno (název), číslo běžného účtu, název banky, příp. SIPO plátce a příjemce,

a to ve lhůtě 40 dnů ode dne právní moci tohoto příkazu.

2. Nezveřejňovat dehonestující osobní údaje [REDAKCE] na webových stránkách [REDAKCE] jejichž provozovatelem je účastník řízení,

a to ve lhůtě 40 dnů ode dne právní moci tohoto příkazu.

3. Podle čl. 15 odst. 1 nařízení (EU) 2016/679 zpracovat a předat [REDAKCE] informace obsahující:

- a) účely zpracování;
- b) kategorie dotčených osobních údajů o příjemci/příjemcích nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny;

- c) plánované době, po kterou byly nebo budou osobní údaje zpracovány, resp. uloženy;
 - d) o existenci práva požadovat od správce opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování, anebo vznést námitku proti tomuto zpracování;
 - e) o právu podat stížnost u dozorového úřadu;
 - f) veškeré dostupné informace o zdroji/zdrojích osobních údajů, pokud nejsou/nebyly získány od subjektu údajů;
 - g) o skutečnosti/skutečnostech, že dochází k automatizovanému rozhodování, včetně profilování, uvedeném v čl. 22 odst. 1 a 4,
- tedy podat stěžovatelce zprávu zároveň v souladu s Vnitřní směrnicí SVD k ochraně osobních údajů,

a to ve lhůtě 20 dnů ode dne nabytí právní moci tohoto příkazu.

4. Podle čl. 32 odst. 2 nařízení (EU) 2016/679 přijmout taková technicko-organizační opatření, aby přístup k uloženým dokumentům SVD byl umožněn pouze členům SVD, na základě přístupového jména a hesla.

a to ve lhůtě do 40 dnů ode dne nabytí právní moci tohoto příkazu.

5. Přijmout technickoorganizační opatření umožňující kontrolu přístupu k osobním údajům prostřednictvím logovacího systému,

a to ve lhůtě 40 dnů ode dne nabytí právní moci tohoto příkazu.

6. Podat Úřadu pro ochranu osobních údajů zprávu o splnění uložených opatření uvedených ve výroku č. 1, 2, 3, 4 a 5,

a to ve lhůtě 15 dnů ode dne jejich splnění.

Odůvodnění

Podkladem pro vydání tohoto příkazu je spisový materiál shromážděný v rámci kontroly sp. zn. UOOU-06362/18, uskutečněné inspektorkou Úřadu PaedDr. Janou Rybínovou ve dnech 15. února 2019 až 25. září 2019, včetně vyřízení námitek předsedkyně Úřadu č.j. UOOU-06362/18-41.

Kontrola byla provedena na základě podnětu, který Úřad pro ochranu osobních údajů (dále jen „Úřad“) obdržel od stěžovatelky [REDAKCE]. Předmětem kontroly byla kontrola dodržování povinností správce osobních údajů stanovených nařízením (EU) 2016/679 v souvislosti se zaměřením na zpracování osobních údajů členů SVD, rodinných příslušníků členů, nájemníků a třetích osob bydlících v domech spravovaných SVD, zejména se zaměřením na dodržování:

- zásad zpracování osobních údajů (čl. 5)

- zákonnost zpracování osobních údajů, se zaměřením na právní titul zpracování (čl.6)
- informační povinnosti (čl. 12, 13 a 14)
- práva subjektu údajů na přístup a opravu k osobním údajům a právo na výmaz (čl. 15, 16, 17)
- práva vznést námitku (čl. 21)
- povinnosti správce osobních údajů (čl. 24 a 25)
- povinnosti při zabezpečení zpracování (čl. 32)

Kontrola byla zahájena dne 15. února 2019 písemným Oznámením o zahájení kontroly, č.j. UOOU-06362/18-19. Protokol o kontrole č.j. UOOU-06362/18-36 byl účastníkovi řízení předán dne 28. května 2019. Účastník řízení podal dne 11. června 2019 námitky proti protokolu o kontrole. Celkem bylo podáno 6 námitek. V rámci vyřízení námitek, předsedkyně Úřadu všech šest námitek zamítla jako nedůvodné. Přípis Vyřízení námitek č.j. UOOU-06362/18-41 byl účastníkovi řízení doručen dne 25. září 2019.

Kontrolou bylo prokázáno, že účastník řízení zpracovává osobní údaje svých členů, jejich rodinných příslušníků a nájemníků – fyzických osob za účelem plnění zákonné povinnosti podle § 1175 a násl. zákona č. 89/2012 Sb., občanský zákoník, zákona č. 67/2013 Sb., o službách, zákona č. 586/1992 Sb., o dani z příjmů a zákona č. 133/2000 Sb., o evidenci obyvatel a v případě zaměstnanců SVD dle pracovně právních předpisů a předpisů v oblasti sociálních, zdravotních a fiskálních předpisů. Na uvedené zpracování se tak vztahuje podmínka zákonného zpracování osobních údajů uvedená v čl. 6 odst. 1 písm. c) nařízení (EU) 2016/679. V případě podmínky uvedené v čl. 6 odst. 1 písm. f) Nařízení EU („Zpracování je nezbytné pro účely oprávněných zájmů příslušného správce, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě“). V rámci kontrolního řízení bylo prokázáno, že SVD může zpracovávat rovněž i číslo bankovního účtu členů SVD a nájemníků – fyzických osob za účelem jeho oprávněných zájmů zpracovávat, nikoliv však zveřejňovat širokému okruhu subjektů, a to ani subjektům (členům SVD) v rámci SVD. Kontrolou bylo dále prokázáno, že účastník řízení tím, že zveřejňuje prostřednictvím vzdáleného přístupu do úložiště všechny dokumenty vzniklé v rámci činnosti SVD, které obsahují osobní údaje, které nejsou nezbytné pro uplatnění práv a povinností člena SVD dle § 1175 a násl. zákona č. 89/2012 Sb. a pro plnění povinností uložených zákonem, tedy i jméno (název) číslo běžného účtu, název banky, případně SIPO, plátce a příjemce, porušuje zásadu zpracování osobních údajů uvedenou v čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679, tedy že osobní údaje musí být zpracovány přiměřeně a omezeně na nezbytný rozsah k účelu, pro který jsou zpracovávány.

Správní orgán stanovil u výroku č. 1 lhůtu pro splnění opatření k nápravě v délce 40 dnů ode dne právní moci tohoto příkazu s tím, že tato doba je zcela dostačující k odstranění dokumentů, které nesouvisí s plněním právních povinností, které účastník řízení, je povinen plnit dle právních předpisů.

V případě stěžovatelky ██████████, zveřejnilo SVD minimálně od 28. března 2019 (zahájení provozu nových webových stránek) na svých webových stránkách u přihlašovacích údajů text: „Pro přístup do této sekce webové stránky musíte zadat své přihlašovací údaje. UPOZORNĚNÍ Z důvodu splnění požadavku ÚOOÚ na udán ██████████ je web dočasně nedostupný“.

Rozsah zveřejňovaných osobních údajů, jako je jméno, příjmení zveřejněné v souvislosti s konkrétně identifikovatelným SVD, jsou informacemi, které jsou identifikačními údaji minimálně pro všechny členy, jejich rodinné příslušníky a bydlící v bytovém domě spravovaném v SVD a jsou tedy osobními údaji ve smyslu čl. 4 odst. 1 Nařízení (EU). Současně správní orgán považuje za prokázané, že účelem zpracování těchto informací nebylo informování oprávněných členů SVD o provozu webových stránek, ale účelem byla dehonestace stěžovatelky.

Účastník řízení zveřejnil na svých webových stránkách [REDAKCE] osobní údaje stěžovatelky v rozsahu jméno a příjmení u přihlašovacích údajů, včetně dehonestujícího sdělení, a to bez jejího souhlasu širokému okruhu subjektů. Toto jednání bylo v protokolu o kontrole vyhodnoceno, jako porušení čl. 6 odst. 1 písm. a) Nařízení (EU) 2016/679, přičemž zákonné podmínky pro zpracování osobních údajů uvedené v čl. 6 odst. 1 písm. b) – f) Nařízení EU se na zveřejnění osobních údajů stěžovatelky na webových stránkách SVD nevztahují.

Správní orgán stanovil u výroku č.2 lhůtu pro splnění opatření k nápravě v délce 40 dnů ode dne právní moci tohoto příkazu s tím, že tato doba je zcela dostačující k odstranění dehonestujících osobních údajů [REDAKCE].

Stěžovatelka [REDAKCE] dne 29. června 2018 podala u účastníka řízení žádost o poskytnutí informací o zpracování jejich osobních údajů, konkrétně požadovala:

- a) které kategorie osobních údajů jsou zpracovávány a za jakým účelem jsou údaje zpracovávány
- b) bezplatné poskytnutí kopie zpracovávaných osobních údajů (elektronickou formou)
- c) informaci, kdo jsou příjemci jejich osobních údajů, kterým byly nebo budou její osobní údaje zpřístupněny
- d) Dále stěžovatelka požádala, aby SVD ze svých webových stránek odstranilo veškeré její osobní údaje, včetně údajů její rodiny a nepřeje si, aby na výtahových dveřích a nástěnkách byly zveřejňovány osobní údaje její a její rodiny, jelikož k tomu ona, ani nikdo z její rodiny nedal souhlas.

K žádosti stěžovatelky směřované k SVD dne 2. července 2018 SVD sdělilo pouze, že její osobní údaje jsou zpracovávány SVD v souladu se zákonem a Nařízením (EU.) 2016/679. Dále jí výbor SVD sdělil, že ke zpracování jejích osobních údajů na webových stránkách SVD nepotřebují souhlas subjektu údajů, a to platí i o usneseních výboru apod., které stěžovatelka v podané žádosti uvedla, neboť se jedná o zpracování v rámci plnění zákonných povinností SVD, která vyplývají ze správy domu. V závěru odpovědi SVD uvedlo, že veškeré osobní údaje, které o stěžovatelce SVD zpracovává má stěžovatelka k dispozici na webových stránkách SVD [REDAKCE] nebo ve vyúčtování služeb.

V dokumentu „Vnitřní směrnice SVD k ochraně osobních údajů dle GDPR“ samo SVD uvádí, že poskytne subjektu údajů na jeho žádost následující informace:

identifikační a kontaktní údaje SVD a případného zástupce SVD; účely zpracování, pro které jsou osobní údaje určeny a právní základ pro zpracování, oprávněné zájmy SVD nebo třetí strany v případě, že je zpracování nezbytné pro účely oprávněných zájmů SVD či třetí osoby; případné příjemce nebo kategorie příjemců osobních údajů, pokud je to nezbytné pro zajištění spravedlivého a transparentního zpracování, poskytne SVD subjektu údajů i další informace, zejména dobu zpracování osobních údajů, příp. kritéria pro její

stanovení; dále pak informace o právu subjektu údajů na opravu osobních údajů, jejich výmaz apod.

SVD ve své odpovědi ze dne 2. července 2018 tak odkázalo stěžovatelku pouze obecně na své webové stránky namísto toho, aby stěžovatelku informovalo konkrétně o zpracování jejích osobních údajů tak, jak stěžovatelka ve svých dotazech požadovala. SVD mělo stěžovatelku informovat o konkrétních kategoriích zpracovávaných osobních údajů; účelech jejich zpracování a o jejich příjemcích. Dále ji mělo poskytnout požadované kopie zpracovávaných osobních údajů a další informace týkající se jejího požadavku na odstranění jejích osobních údajů z webových stránek SVD tak, jak samo uvádí ve Vnitřní směrnici SVD k ochraně osobních údajů.

Kontrolou bylo konstatováno, že právu přístupu k osobním údajům podle čl. 15 odst. 1 Nařízení EU 2016/679 odpovídá povinnost správce podat subjektu údajů sdělení o zpracování jeho osobních údajů podle čl. 15 až 22 (čl. 12 odst. 1 nařízení (EU) 2016/679, a to stručným, transparentním, srozumitelným a snadno přístupným způsobem, což pouhý odkaz na webové stránky SVD (obsahují 21 složek a další podsložky) nebo na vyúčtování služeb a obecná informace, že SVD zpracovává osobní údaje stěžovatelky v souladu se zákonem a nařízením (EU) 2016/679 nesplňuje.

Lhůta pro splnění povinnosti k povinnosti uložené pod výrokem č. 3, v délce 20 dnů ode dne nabytí právní moci tohoto příkazu je s ohledem na charakter požadavku na přístup k osobním údajům stěžovatelky [REDAKCE] zcela dostačující, neboť se jedná o relativně malý soubor dat, který je v rámci činnosti účastníka řízení opakující se u každého subjektu údajů a nevyžaduje zvláštní nároky na personální zabezpečení.

V rámci kontroly bylo zjištěno, že SVD minimálně od dubna 2018, kdy rozeslalo členům SVD informaci o zprovoznění nových webových stránek, a to minimálně do doby zahájení kontroly dne 15. února 2019, průběžně zveřejňovalo na svých webových stránkách čísla bankovních účtů fyzických osob, které SVD prováděly bezhotovostní platby na jeho účet za služby, nájem a další platby. K jednotlivým bankovním účtům je přitom přiřazeno jméno a příjmení plátce a finanční částka. Čísla účtů a jména plátců tak byla zveřejněna širokému okruhu subjektů. Kontrolou bylo konstatováno, že informace o číslech účtů není určena ani členům SVD, ani třetím osobám, jelikož zveřejnění této informace odporuje účelům zpracování, které jsou SVD stanoveny zvláštními předpisy.

Dále SVD ve výše uvedeném období zveřejňovalo širokému okruhu subjektů, tedy kromě členů SVD i dalším osobám, **zázpisy ze schůzí výboru SVD, které obsahují osobní údaje členů SVD a dalších subjektů údajů. Tyto zázpisy ze schůzí výboru SVD, které obsahují osobní údaje, jsou interními dokumenty účastníka řízení a byly určeny pouze členům SVD, nikoli široké veřejnosti, třetím osobám. Účelem tohoto zpracování mělo být informovat členy SVD o vlastní činnosti, nikoli zázpisy z činnosti zpřístupňovat široké veřejnosti mimo působnost účastníka řízení.**

Správní orgán má za prokázané, že účastník řízení tím, že minimálně v období od dubna 2018 do 15. února 2019 umožňoval neoprávněné přístupy nezjištěnému okruhu lidí tím, že k uloženým dokumentům bylo možno přistoupit i bez znalosti přístupových údajů (viz Úřední záznam č.j. UOUU-06362/18-17 ze dne 6. února 2019) k úložišti dokumentů na svých webových stránkách [REDAKCE] a současně tím, že nemá zajištěnu kontrolu přístupů prostřednictvím logovacího systému porušilo čl. 32 odst. 2 nařízení (EU) 2016/679 a

s přihlédnutím ke konkrétní povaze, rozsahu, kontextu, postupům a účelům zpracování, včetně zvážení rizika při zpracování je konstatováno, že přijatá technická a organizační opatření nezajišťují dostatečnou úroveň zabezpečení ve smyslu čl. 32 nařízení (EU) 2016/679, a zpracování není v souladu se zásadou vyjádřenou v čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679.

Lhůta pro splnění povinností výroků č. 4 a č. 5 tohoto příkazu, v délce 40 dnů byla stanovena s ohledem na povinnost účastníka řízení, jako správce osobních údajů, zajistit, aby byly umožněny přístupy k uloženým dokumentům SVD pouze členům SVD a dále vzhledem ke skutečnosti, že zpracovává osobní údaje elektronickou formou, pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní zaznamenány nebo jinak zpracovány, přičemž správní orgán přihlédl ke skutečnosti, že tato povinnost byla stanovena účastníkovi řízení v okamžiku zahájení zpracování v elektronické formě.

Správní orgán považuje ve smyslu § 150 odst. 1 správního řádu skutkové zjištění za dostatečné, a proto byla účastníku řízení uložena opatření k odstranění zjištěných nedostatků v rozsahu ve výrokové části tohoto příkazu.

Správní orgán považuje lhůtu stanovenou pro podání zprávy o splnění uložených opatření v délce 15 dnů za přiměřenou.

Poučení: V souladu s § 150 odst. 3 správního řádu lze u Úřadu pro ochranu osobních údajů proti tomuto příkaz podat ve lhůtě 8 dnů ode dne jeho doručení odpor, kterým se příkaz ruší a řízení pokračuje.

Příkaz je doručen dnem převzetí stejnopisu, nejpozději však desátým dnem od jeho uložení u provozovatele poštovních služeb. V případě doručování do datové schránky je příkaz doručen okamžikem přihlášení oprávněné osoby do datové schránky, nejpozději však desátý den ode dne dodání příkazu do datové schránky.

Praha 23. října 2019

otisk
úředního
razítka

PaedDr. Jana Rybínová
inspektorka
(*podepsáno elektronicky*)