



## 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-00371/20-5

### PŘÍKAZ

Úřad pro ochranu osobních údajů, jako příslušný správní orgán podle § 64 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů, a podle čl. 58 odst. 2 písm. i) 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), vydává dne 29. června 2020 v souladu s § 150 odst. 1 zákona č. 500/2004 Sb., správní řád, a § 90 odst. 1 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, tento příkaz:

Statutární město [REDACTED]

- I. se uznává vinným ze spáchání přestupku podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb., neboť porušilo některou z povinností podle čl. 8, 11, 25 až 39, 42 až 49 nařízení (EU) 2016/679, kterého se, jako správce osobních údajů svých dlužníků podle čl. 4 bodu 7 nařízení (EU) 2016/679, dopustilo tím, že nezajistilo, aby dne 13. ledna 2020 nedošlo k předání osobních údajů 150 členů Společenství vlastníků domů ve [REDACTED] ulici v [REDACTED] (v rozsahu jméno, příjmení, adresa trvalého bydliště a rodné číslo) zaměstnankyní města nájemci nebytových prostor u tohoto společenství, a to za účelem získání souhlasu dotčených členů se změnou užívání jím pronajatých prostor,

čímž porušilo povinnost stanovenou v čl. 32 odst. 1 nařízení (EU) 2016/679, tedy povinnost s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provést vhodná technická a organizační opatření k zajištění úrovně zabezpečení odpovídající danému riziku,

- II. přičemž se podle § 62 odst. 5 zákona č. 110/2019 Sb.

**upouští od uložení správního trestu.**

## Odůvodnění

Podkladem pro vydání tohoto příkazu je spisový materiál shromážděný na základě ohlášení porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů (dále jen „Úřad“) ze dne 17. ledna 2020 učiněného Statutárním městem [REDAKCE], [REDAKCE] (dále jen „obviněný“).

Ze spisového materiálu vyplývá, že pracovnice obviněného dne 13. ledna 2020 předala nájemci nebytových prostor u Společenství vlastníků domů ve [REDAKCE] ulici v [REDAKCE] za účelem získání souhlasu se změnou užívání jím pronajatých prostor seznam 150 členů tohoto společenství, který obsahoval jejich jméno, příjmení, adresu trvalého bydliště a rodné číslo. Uvedený seznam tak zahrnoval i osobní údaje (rodná čísla), které byly pro zamýšlený účel (vyžádání souhlasu dotčených subjektů) nerelevantní a nadbytečné.

Z učiněného ohlášení vyplývá, že obviněný prověřil oprávněnost přístupu zaměstnankyně k databázi obsahující osobní údaje, a na základě tohoto případu opětovně poučil zaměstnance zařazené do Magistrátu města [REDAKCE] o zásadách zpracování osobních údajů zejm. s ohledem na rozsah zpracovávaných dat a jejich předávání nebo jiné zpřístupňování na základě existujícího a relevantního právního důvodu.

K předmětu řízení lze konstatovat, že dle čl. 4 bodu 1 nařízení (EU) 2016/679 se osobním údajem rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. Ze shromážděné dokumentace vyplývá, že obviněný v rámci své činnosti (činnost orgánu veřejné moci) nakládá s osobními údaji dotčených subjektů, a to minimálně v rozsahu jméno, příjmení, adresa trvalého bydliště a rodné číslo. Tyto informace, které obviněný zpracovává, jsou nepochybně osobními údaji ve smyslu čl. 4 bod 1 nařízení (EU) 2016/679, neboť se jedná o informace o identifikovaných osobách.

Dle čl. 4 bodu 2 nařízení (EU) 2016/679 se zpracováním rozumí jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů 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. Obviněný v postavení orgánu veřejné moci nepochybně zpracovává osobní údaje dotčených dlužníků, neboť je systematicky shromažďuje, uchovává a v případě potřeby dále používá. Současně je tedy v této souvislosti i správcem údajů výše uvedených subjektů ve smyslu čl. 4 bodu 7 nařízení (EU) 2016/679, neboť v rámci své činnosti určil účel i prostředky zpracování.

Dle čl. 32 odst. 1 nařízení (EU) 2016/679 správce, popř. zpracovatel musí s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob provést vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení

odpovídající danému riziku, případně včetně opatření uvedených pod písm. a) až d) tohoto článku.

Je tedy zřejmé, že správce musí nejprve posoudit pravděpodobnost a závažnost rizik, která při zpracování osobních údajů hrozí, a následně s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování vybrat a následně zavést vhodná technická a organizační bezpečnostní opatření ke zmírnění těchto rizik. Riziko pro práva a svobody fyzických osob přitom lze považovat za kritérium, na němž závisí uplatnění nebo míra uplatnění řady institutů upravených v nařízení (EU) 2016/679. Riziko pro práva a svobody fyzických osob musí být hodnoceno na základě objektivního posouzení, kdy východiskem pro jeho posouzení je hrozba narušení důvěrnosti a integrity zpracování. Pro posouzení bezpečnostních rizik a volbu vhodných opatření k jejich zmírnění platí stejné zásady jako pro posuzování obecného rizika zpracování. Posouzení by nemělo být jednorázovým procesem, nýbrž by se mělo jednat o pravidelný proces vyhodnocování vnitřních a vnějších okolností, které mohou mít na míru rizika vliv, a v případě změny rizika pak musí správce bezpečnostní opatření zrevidovat a případně přijmout vhodnější.

Lze tedy shrnout, že splnění této povinnosti, tj. povinnosti provést vhodná technická a organizační opatření, aby byla zajištěna úroveň zabezpečení odpovídající danému riziku, aby osobní údaje nebyly vystaveny riziku neoprávněného zpracování či využití, předpokládá, že účastník řízení důsledně zváží veškerá rizika, která jsou s jím prováděným zpracováním osobních údajů spojená, a přijme odpovídající opatření k jejich maximálnímu vyloučení.

Z výše uvedeného je zřejmé, že obviněný nesplnil svou povinnost stanovenou v článku 32 odst. 1 nařízení (EU) 2016/679, když nedostatečným poučením svých zaměstnanců nezajistil, aby jedna z pracovníků nepředala neoprávněné osobě, nájemci nebytových prostor u Společenství vlastníků domů ve [REDAKCE] ulici v [REDAKCE] za účelem získání souhlasu se změnou užívání jím pronajatých prostor seznam 150 členů tohoto společenství, který obsahoval osobní údaje těchto osob vč. rodných čísel, která byla pro zamýšlený účel nerelevantní a nadbytečná. V důsledku tohoto jednání došlo k porušení důvěrnosti uvedených údajů, které pro dotčené subjekty může představovat riziko, neboť rodná čísla fyzických osob nejsou v katastru nemovitostí běžným nahlédnutím přístupná. Správní orgán navíc konstatuje, že ani přístupnost určitých údajů v jiném informačním systému nezbavuje správce odpovědnosti za jím prováděné zpracování osobních údajů a jejich odpovídající zabezpečení, přičemž tato odpovědnost je objektivní.

Podle § 5 zákona č. 250/2016 Sb. je přestupkem škodlivý protiprávní čin, který je v zákoně za přestupek výslovně označen a který vykazuje znaky stanovené zákonem, nejde-li o trestný čin.

Správní orgán považuje ve smyslu § 150 odst. 1 správního řádu skutkové zjištění za dostatečné a na základě výše uvedeného považuje za prokázané, že obviněný porušil svým jednáním povinnost stanovenou v čl. 32 odst. 1 nařízení (EU) 2016/679, tedy povinnost s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provést vhodná technická a organizační opatření k zajištění úrovně zabezpečení odpovídající danému riziku, a proto rozhodl podle § 150 odst. 1 správního řádu ve spojení s § 90 odst. 1 zákona č. 250/2016 Sb. ve věci příkazem.

Z čl. 83 odst. 7 nařízení (EU) 2016/679 vyplývá, že aniž jsou dotčeny nápravné pravomoci dozorových úřadů podle čl. 58 odst. 2 tohoto nařízení, může každý členský stát stanovit pravidla týkající se toho, zda a do jaké míry je možno ukládat správní pokuty orgánům veřejné moci a veřejným subjektům usazeným v daném členském státě. Podle § 62 odst. 5 zákona č. 110/2019 Sb. Úřad upustí od uložení správního trestu také tehdy, jde-li o správce a zpracovatele uvedené v čl. 83 odst. 7 nařízení (EU) 2016/679. S ohledem na skutečnost, že obviněný je orgánem veřejné moci, tedy správcem uvedeným v čl. 83 odst. 7 nařízení (EU) 2016/679, upustil správní orgán od uložení správního trestu.

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

Příkaz je doručen dnem převzetí stejnopisu, nejpozději ale desátým dnem od jeho uložení na poště. V případě doručování do datové schránky je dnem doručení okamžik přihlášení oprávněné osoby do datové schránky, nejpozději ale desátý den ode dne dodání příkazu do datové schránky.

Praha, 29. června 2020

otisk  
úředního  
razítka

JUDr. Jiří Žůrek  
ředitel odboru dozoru  
(podepsáno elektronicky)