ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 111, fax: 234 665 444
posta@uoou.cz, www.uoou.cz

Čj. UOOU-00120/20-4

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 23. ledna 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:

Společnost [redacted] se sídlem [redacted], IČO: [redacted],

I. se uznává vinnou ze spáchání přestupku podle § 62 odst. 1 písm. b) zákona č. 110/2019 Sb., neboť porušila některou ze základních zásad pro zpracování osobních údajů podle čl. 5 až 7 nebo 9 nařízení (EU) 2016/679, kterého se, jako správce osobních údajů svých zaměstnanců a dalších osob (pronajímatelů, věřitelů, rodinných příslušníků zaměstnanců) podle čl. 4 bodu 7 nařízení (EU) 2016/679, dopustila tím, že nezajistila osobní údaje přibližně 170 subjektů údajů v různém rozsahu osobních údajů u jednotlivých subjektů údajů, kdy osobními údaji bylo jméno, příjmení, datum narození, rodné číslo, číslo občanské průkazu, státní příslušnost, adresa trvalého pobytu, telefonní číslo, e-mailová adresa, informace o zdravotní pojišťovně, rodné příjmení, místo narození, rodinný stav, dosažené vzdělání, informace o tom, zda subjekt pobírá důchod a případně jaký, číslo bankovního účtu, informace o případných srážkách ze mzdy, titul, pohlaví, informace o tom, od kdy je subjekt zaměstnán, informace o mzdových položkách, číslo pojištěnce, informace o tom, od kdy je subjekt zdravotně pojištěn, podpis a veškeré informace obsažené v nejrůznějších písemnostech (ukončení dohody o provedení práce, potvrzení zaměstnání, prohlášení poplatníka daně z příjmů fyzických osob ze závislé činnosti a z funkčních požitků, dotazník zaměstnance, dohoda o provedení práce, rozsudek o úpravě rodičovské zodpovědnosti na dobu před i po rozvodu manželství, čestné prohlášení o neevidování daného subjektu v určité době u jiného zaměstnavatele, rozsudek o rozvodu manželství, rodný list dítěte, podací arch na poštu obsahující jméno, příjmení a adresu daných osob, potvrzení o zaregistrování smlouvy o penzijním pojištění se státním příspěvkem, dohoda o ukončení nájmu, smlouva o nájmu,

předávací protokol, mandátní smlouva, předání vstupních karet, dohoda o zániku podnájmu bytu, výpověď z nájemní smlouvy, protokol o převzetí nebytových prostor, mzdový list, dohoda o zániku nájmu nebytových prostor, smlouva o podnájmu, protokol o předání nebytových prostor, výpočtový list nájmu, dohoda o převzetí ručitelského závazku, oznámení o nástupu do zaměstnání, přehled registrovaných zaměstnanců, hromadné oznámení zaměstnavatele vůči zdravotní pojišťovně, plná moc a dopisy od Pražské správy sociálního zabezpečení), které byly dne 20. prosince 2019 v dopoledních hodinách nalezeny ve tříděném odpadu v obci [redacted]

čímž porušila povinnost stanovenou čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679, tedy zásadu, že osobní údaje musí být zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením,

II. za což se jí podle § 35 písm. b) zákona č. 250/2016 Sb. a v souladu s čl. 83 odst. 5 písm. a) nařízení (EU) 2016/679 ukládá

pokuta ve výši 180.000 Kč
(slovy sto osmdesát tisíc korun českých)

splatná do 30 dnů ode dne nabytí právní moci tohoto příkazu bezhotovostním převodem na účet vedený u ČNB, č. ú. 19-5825001/0710, variabilní symbol IČO obviněné, konstantní symbol 1148.

Odůvodnění

Podkladem pro vydání tohoto příkazu je podnět Obecní policie [redacted] doručený Úřadu pro ochranu osobních údajů (dále jen „Úřad“) dne 2. ledna 2020 a doplněný dne 8. ledna 2020.

Ze spisového materiálu vyplývá, že dne 20. prosince 2019 v dopoledních hodinách byla Obecní policie [redacted] informována o tom, že ve tříděném odpadu v obci [redacted] se nachází dokumenty společnosti [redacted], přičemž tyto dokumenty byly vyzvednuty a předány str. [redacted] Jednalo se o 5 šanonů a 1 desky, které obsahovaly nejrůznější dokumenty a písemnosti související s činností společnosti (vše následně předáno Úřadu). Většina osobních údajů se týkala zaměstnanců dané společnosti (mzdové listy, dotazníky zaměstnanců, prohlášení poplatníka daně z příjmů fyzických osob ze závislé činnosti a z funkčních požitků, dohody o provedení práce apod.). Další osobní údaje byly obsaženy v nejrůznějších smlouvách (o nájmu či podnájmu bytových nebo nebytových prostor) a s nimi souvisejícími další dohody, výpovědi, předávací protokoly apod. Správní orgán zjistil, že se jednalo o osobní údaje minimálně 170 subjektů údajů, a to v rozsahu uvedeném ve výroku tohoto rozhodnutí.

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 (dále jen „subjekt údajů“); 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. Informace, které zpracovává účastník řízení o svých zaměstnancích a dalších osobách, se kterými měl různé smluvní vztahy (jméno, příjmení, datum narození, rodné číslo, číslo občanské průkazu, státní příslušnost, adresa trvalého pobytu, telefonní číslo, e-mailová adresa, informace o zdravotní pojišťovně, rodné příjmení, místo narození, rodinný stav, dosažené vzdělání, informace o tom, zda subjekt pobírá důchod a případně jaký, číslo bankovního účtu, informace o případných srážkách ze mzdy, titul, pohlaví, informace o tom, od kdy je subjekt zaměstnán, informace o mzdových položkách, číslo pojištěnce, informace o tom, od kdy je subjekt zdravotně pojištěn, podpis a veškeré informace obsažené v nejrůznějších písemnostech) využívaných pro potřeby fungování jeho společnosti, jsou 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. Účastník řízení v rámci své činnosti, především v souvislosti se zaměstnáváním osob a uzavíráním různých smluvních vztahů pro své potřeby, tj. k zajištění svého fungování, nepochybně zpracovává osobní údaje svých zaměstnanců a dalších osob, neboť je shromažďuje, uchovává a v případě potřeby dále používá. Současně je tedy v této souvislosti i správcem údajů svých zaměstnanců a dalších osob ve smyslu čl. 4 bodu 7 nařízení (EU) 2016/679, neboť v rámci své činnosti určil účel a prostředky zpracování.

Zpracování osobních údajů musí být vždy v souladu se základními zásadami, které jsou zakotveny v čl. 5 nařízení (EU) 2016/679. Tyto zásady představují základní pravidla, od nichž se odvíjejí všechny procesy zpracování, a zároveň jsou též nejdůležitějšími principy, které správci určují, jak má s osobními údajů nakládat. Jednou z těchto zásad je zásada integrity a důvěrnosti stanovená v čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679, která stanoví, že osobní údaje musí být zpracovány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

Výše uvedená zásada integrity a důvěrnosti je pak podrobněji specifikována v dalších ustanoveních nařízení (EU) 2016/679, zejména v čl. 32 tohoto nařízení, kde jsou stanoveny konkrétní požadavky na zabezpečení osobních údajů. 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.

Správní orgán musí konstatovat, že v daném případě nebyly osobní údaje zaměstnanců a dalších osob účastníkem řízení zpracovávány způsobem, který by zajistil jejich náležité zabezpečení. Účastník řízení nedostatečně vyhodnotil rizika pro práva a svobody svých zaměstnanců a dalších osob, a tedy ani nepřijal odpovídající bezpečnostní opatření k jejich ochraně před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením, když byly dokumenty obsahující osobní údaje nalezeny v kontejneru na tříděný odpad v obci [redacted] přičemž do doby nálezu se mohly dostat do dispozice širokému počtu osob, které s nimi mohly neomezeně nakládat.

Správní orgán tedy na základě výše uvedeného považuje za prokázané, že účastník řízení porušil svým jednáním zásadu stanovenou v čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679, tedy zásadu, že osobní údaje musí být zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

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.

Podle čl. 83 odst. 2 nařízení (EU) 2016/679 se při rozhodování o uložení sankce a její výši přihlédne zejména k povaze, závažnosti a délce trvání porušení, k povaze, rozsahu a účelu dotčeného zpracování, k počtu dotčených subjektů údajů a míře škody, která jim byla způsobena, a k dalším okolnostem porušení stanoveným v tomto článku.

Při stanovení sankce tak správní orgán přihlédl, jako k okolnosti zvyšující závažnost jednání, zejména k tomu, že jednáním účastníka řízení byla porušena základní zásada, která představuje základní principy, na jejichž řádném dodržování spočívá každé zpracování osobních údajů. Dalšími přitěžujícími skutečnostmi při stanovení výše sankce bylo i to, že osobní údaje se týkaly většího počtu subjektů údajů a širokého rozsahu osobních údajů a současně i ta skutečnost, že nalezené listiny obsahovaly i rodná čísla, která slouží jako

obecný identifikátor občanů. Jako další okolnost zvyšující závažnost protiprávního jednání vyhodnotil správní orgán skutečnost, že obsah písemností mohl s ohledem na místo nálezu listin zneužít prakticky kdokoli. V neposlední řadě vzal správní orgán v potaz jako přitěžující okolnost, že se v několika případech jednalo o osobní údaje rodinných příslušníků jeho zaměstnanců včetně nezletilých osob. Po souhrnném zhodnocení všech okolností byla pokuta uložena při samé dolní hranici sazby, kterou nařízení (EU) 2016/679 stanoví a která, jak je výše uvedeno, činí 20 000 000 eur.

Správní orgán považuje ve smyslu § 150 odst. 1 správního řádu skutkové zjištění za dostatečné a na základě výše uvedeného považuje za prokázané, že obviněná porušila svým jednáním povinnosti stanovené v čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679, tedy zásadu, že osobní údaje musí být zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením, a proto rozhodl podle § 150 odst. 1 správního řádu ve věci příkazem.

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, 23. ledna 2020

otisk
úředního
razítka

Mgr. Martina Šnajderová, DiS.
pověřená řízením přestupkové agendy
(podepsáno elektronicky)