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-05251/19-8

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 20. dubna 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 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXX

I. se uznává vinnou ze spáchání přestupku podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb., neboť porušila některou z povinností podle čl. 8, 11, 25 až 39, 42 až 49 nařízení (EU) 2016/679, nebo hlavy II, kterého se jako zpracovatel osobních údajů bývalých zaměstnanců společnosti XXXXXXXXXXXXXXXX podle čl. 4 bodu 8 nařízení (EU) 2016/679 propuštěných v období od roku 1995 do roku 2015, dopustila tím, že nezajistila přibližně 15 ks archivních krabic obsahujících osobní údaje přibližně 30 subjektů údajů, a to v přesně nezjištěném rozsahu osobních údajů, minimálně v rozsahu jméno, příjmení, datum narození, rodné číslo, adresa trvalého pobytu, telefonní číslo, e-mailová adresa, číslo bankovního účtu, údaje o trestním odsouzení, údaje o spáchání přestupku a další osobní údaje potřebné k vedení zaměstnanecké agendy a veškeré informace obsažené v nejrůznějších písemnostech včetně osobních složek zaměstnanců (pracovní smlouvy, dodatky k pracovním smlouvám, vstupní dotazníky, dohody o rozvázání pracovního poměru, výpovědi z pracovního poměru, mzdové výměry, přihlášky ke zdravotnímu a sociálnímu pojištění, evidenční listy důchodového pojištění, podepsaná prohlášení poplatníků k dani ze závislé činnosti, souhlasy se zpracováním osobních údajů, zápočtové listy, školení zaměstnanců, osobní listy bezpečnosti a ochrany zdraví při práci, lékařské prohlídky, osobní ochranné pracovní prostředky včetně předávacích protokolů, prostředků osobního pojištění a osobních karet na svěřené předměty, penzijní připojištění zaměstnanců, životní pojištění zaměstnanců a kompletní mzdy za roky 2011, 2016, 2017), které byly dne 2. prosince 2019 převáženy na přívěsném vozíku, přičemž tento vozík se uvolnil a zůstal mezi obcemi Kyselovice a Žalkovice, odkud byl neznámým pachatelem odcizen,

čímž porušila povinnost stanovenou v čl. 32 odst. 1 nařízení (EU) 2016/679, tedy povinnost zpracovatele provést vhodná technická a organizační opatření,

II. za což se jí podle § 35 písm. b) zákona č. 250/2016 Sb. a v souladu s čl. 83 odst. 4 písm. a) nařízení (EU) 2016/679 ukládá

pokuta ve výši 15.000 Kč
(slovy patnáct 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 ohlášení porušení zabezpečení osobních údajů, které bylo Úřadu pro ochranu osobních údajů (dále jen „Úřad“) doručeno dne 4. prosince 2019 zpracovatelem osobních údajů, u kterého došlo k porušení zabezpečení, a to obviněnou společností XXXXXXXXXXXXXXXXXX.

Ze spisového materiálu vyplývá, že obviněná Úřadu ohlásila v souladu s čl. 33 nařízení (EU) 2016/679, dne 4. prosince 2019 porušení zabezpečení osobních údajů. K tomu došlo dne 2. prosince 2019, když obviněná společnost XXXXXXXXXXXXXXXXXXX která měla uzavřenu se společností XXXXXXXXXXXXXXX. smlouvu o skladování a archivaci ze dne 2. prosince 2019, převážela listinnou dokumentaci, kterou jí předala společnost XXXXXXXXXXXXXXXX jako správce osobních údajů. Obviněná uvedla, že při převozu listinné dokumentace došlo k uvolnění přívěsného vozíku a jeho odpojení od vozidla, kdy tuto skutečnost zjistila až po ujetí cca 10 km. Po vrácení se na místo bylo zjištěno, že vozík i s nákladem archivních krabic byl odcizen. Obviněná dále uvedla, že hned v den ztráty listinné dokumentace byla přijata opatření k řešení porušení zabezpečení, a to podáním trestního oznámení na Policii České republiky, a též byla věc telefonicky oznámena majiteli listinných dokumentů.

Obviněná v rámci oznámení porušení zabezpečení osobních údaje uvedla, že dotčenými osobními údaji byly identifikační údaje (jméno, příjmení, datum narození, rodné číslo, jiný identifikátor), kontaktní údaje (např. adresa, e-mail, telefon), ekonomické a finanční údaje, údaje o trestním odsouzení, o spáchání přestupku a jiné. Dále obviněná doplnila, že se jednalo o listinnou dokumentaci zaměstnanců nebo osob v pracovněprávním vztahu ke správci, zejména osobní složky, včetně lékařských prohlídek ke způsobilosti a mzdová dokumentace, přičemž přibližný počet dotčených subjektů údajů byl maximálně 30. K důsledkům, resp. povaze pravděpodobného dopadu na ohrožení subjektů údajů, obviněná uvedla, že jde zejména o ztrátu kontroly nad osobními údaji, kdy data mohou být spojena s dalšími informacemi. Na závěr obviněná uvedla, že relevantními dokumenty, kterými je mezi správcem a obviněnou jako zpracovatelem řízeno zpracování osobních údajů, jsou vnitřní předpisy a smlouva o zpracování osobních údajů.

Správní orgán zaslal dne 5. února 2020 společnosti XXXXXXXXXXXXXXX, jako správci osobních údajů, žádost o podání vysvětlení, a to zasláním zpracovatelské smlouvy mezi touto společností a společností XXXXXXXXXXXXXXXXXXX, a sdělením přesného počtu zaměstnanců s uvedením rozsahu osobních údajů ve ztracených dokumentech. Dále byla

společnost požádána o uvedení adresy obvodního oddělení Policie České republiky, ke kterému byla ztráta přívěsného vozíku spolu s listinami ohlášena a které provádí v současnosti šetření.

Dne 19. února 2020 byla správnímu orgánu doručena odpověď společnosti XXXXXXXXXXXXXXXX, ve které uvedla, že byly ztraceny archivní krabice s osobními složkami odhadem maximálně 30 zaměstnanců, kdy číslo již nelze nijak přesně určit. Jednalo se o složky bývalých zaměstnanců, kteří byli propuštěni v období let 1995 až 2015. Dále společnost uvedla, že ve složkách byly pracovní smlouvy, dodatky k pracovním smlouvám, dohody o rozvázání pracovního poměru, výpovědi z pracovního poměru, mzdové výměry, přihlášky ke zdravotnímu a sociálnímu pojištění, evidenční listy důchodového pojištění, a to za dobu trvání zaměstnání u jejich společnosti, podepsaná prohlášení poplatníků k dani ze závislé činnosti, souhlasy se zpracováním osobních údajů, lékařské prohlídky, školení, zápočtové listy, životní a penzijní připojištění zaměstnanců a kompletní mzdy za roky 2011, 2016, 2017 (kompletní měsíční i roční výstupy/sestavy). Ke své odpovědi společnost XXXXXXXXXXXXXXXX přiložila jako důkaz kopii Smlouvy o skladování a archivaci písemností ze dne 2. prosince 2019 uzavřenou mezi společností XXXXXXXXXXXXXXXX jako ukladatelem a společností XXXXXXXXXXXXXXXXXXX, jako skladovatelem, ze které mimo jiné vyplývá, že: *„Ukladatel předá písemnosti k archivaci na základě protokolu o předání písemností. Skladovatel uloží převzaté písemnosti…“.*

Dále společnost XXXXXXXXXXXXXXXX správnímu orgánu zaslala dokumenty Policie České republiky, Krajského ředitelství policie Zlínského kraje, Územního odboru Kroměříž, obvodního oddělení policie Hulín, a to kopii Potvrzení o šetřené věci sepsané s jednatelem společnosti obviněné XXXXXXXXXXXXX a Potvrzení o přijatém oznámení ekonomky společnosti XXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXX ze dne 17. prosince 2019 a Vyrozumění podle § 74 odst. 4 zákona číslo 250/2016 Sb. ze dne 14. února 2020. Z těchto dokumentů vyplývá, že dne 2. prosince 2019 v 15:42 hod. XXXXXXXXXXXXXXX oznámila na linku 158, že okolo 10:30 hod. v obci Kyselovice v objektu družstva naložili do dodávky a přípojného vozíku účetní dokumenty končící společnosti XXXXXXXXXXXXXXXX. Tyto dokumenty následně řidič XXXXXXXXX odvezl do Zlína k jejich uložení. Po příjezdu do Zlína řidič zjistil, že přívěsný vozík již za dodávkou nemá, a tedy se někde v průběhu jízdy musel odpojit. Poté bylo zjištěno, že se musel přípojný vozík odpojit mezi obcemi Kyselovice a Žalkovice, kdy jej poté doposud neznámý pachatel odcizil i se všemi účetními dokumenty. Policie České republiky uvedla, že provedeným šetřením nebyly zjištěny skutečnosti odůvodňující podezření, že jej spáchala určitá osoba a z tohoto důvodu byla věc dne 28. prosince 2019 odložena podle § 74 odst. 3 písm. b) zákona č. 250/2016 Sb.

Dne 27. února 2020 požádal správní orgán společnost XXXXXXXXXXXXXXXX o zaslání protokolu o předání písemností ke skartaci společnosti XXXXXXXXXXXXXXXXXXX. Dne 3. března 2020 byl správnímu orgánu doručen požadovaný dokument, kopie Protokolu o předání a převzetí písemností ze dne 2. prosince 2019, který mj. obsahoval 15 ks krabic s osobními údaji zaměstnanců v těchto písemnostech:

- osobní složky zaměstnanců za období od roku 1995 až do roku 2015, kteří ukončili pracovní poměr v celkovém počtu 7 ks krabic;
- školení zaměstnanců za období od roku 1997 do roku 2019, včetně osobních listů bezpečnosti a ochrany zdraví při práci (dále jen „BOZP“) a lékařských prohlídek v celkovém počtu 6 ks krabic;
- osobní ochranné pracovní prostředky (dále jen „OOPP“) za období od roku 1997 až do roku 2019, včetně předávacích protokolů, prostředků osobního pojištění, osobních karet na svěřené předměty a lékařských potvrzení v celkovém počtu 1 ks krabic;

- smlouvy o půjčce, penzijní připojištění zaměstnanců a životní pojištění zaměstnanců za období od roku 2001 až do roku 2019 v celkovém počtu 1 ks krabic.

Dne 4. března 2020 správní orgán telefonicky kontaktoval XXXXXXXXXXXXX, o čemž pořídil dne 5. března 2020 úřední záznam čj. UOOU-05251/19-6, která je v ohlášení porušení zabezpečení osobních údajů označena jako pověřenec správce nebo jiná kontaktní osoba, s dotazem, zda může sdělit, jaký rozsah osobních údajů byl ve ztracených dokumentech obsažen, případně, zda může Úřadu zaslat písemné vyjádření, ve kterém je specifikován rozsah osobních údajů obsažených v jednotlivých ztracených dokumentech. XXXXXXXXXXXXX uvedla, že ztracenou dokumentaci společnost XXXXXXXXXXXXXXX vedla pouze v písemné podobě a rozsah osobních údajů již není schopna dohledat, neboť neexistuje o tom žádný dokument. K tomu dodala, že ztracené písemnosti obsahovaly vstupní dotazníky, bankovní účty zaměstnanců a veškeré osobní údaje, které jsou potřebné pro vedení zaměstnanecké agendy.

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 zpracovávala společnost XXXXXXXXXXXXXXXX. o svých bývalých zaměstnancích a které na základě smlouvy o skladování a archivaci písemností předala obviněné jako zpracovateli těchto osobních údajů minimálně v rozsahu jméno, příjmení, datum narození, rodné číslo, adresa trvalého pobytu, telefonní číslo, e-mailová adresa, číslo bankovního účtu a veškeré informace obsažené v nejrůznějších písemnostech uvedených ve výroku tohoto příkazu, 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. Obviněná v rámci své činnosti, především v souvislosti s archivací a následnou likvidací výše uvedených písemností týkající se zaměstnanecké agendy společnosti XXXXXXXXXXXXXXXX nepochybně zpracovává osobní údaje bývalých zaměstnanců v písemnostech uvedených ve výroku tohoto příkazu, neboť je shromažďuje, uchovává, ukládá a v konečné fázi likviduje.

Dle čl. 4 bodu 8 nařízení (EU) 2016/679 je zpracovatelem fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. Vzhledem k tomu, že obviněná měla se správcem osobních údajů bývalých zaměstnanců, tj. se společností XXXXXXXXXXXXXXXX, uzavřenu smlouvu o skladování a archivaci písemností, na základě které archivovala pro tuto společnost zaměstnaneckou agendu a následně zajišťovala její likvidaci, je tedy v této souvislosti zpracovatelem osobních údajů těchto bývalých zaměstnanců společnosti XXXXXXXXXXXXXXXX.

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 zpracovatel 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 zpracovatel 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 obviněná 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 bývalých zaměstnanců obviněnou zpracovávány způsobem, který by zajistil jejich náležité zabezpečení. Obviněná nedostatečně vyhodnotila rizika pro práva a svobody bývalých zaměstnanců, a tedy ani nepřijala odpovídající bezpečnostní opatření k jejich ochraně před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením, když došlo k uvolnění přívěsného vozíku a jeho odpojení od vozidla, kdy po vrácení se na místo bylo zjištěno, že vozík i s nákladem archivních krabic byl odcizen doposud neznámým pachatelem, přičemž vzhledem k tomu, že písemnosti nebyly nalezeny, mohly se dostat do dispozice širokému počtu osob, které s nimi mohou neomezeně nakládat.

Správní orgán tedy na základě výše uvedeného považuje za prokázané, že obviněná porušila svým jednáním povinnost stanovenou v čl. 32 odst. 1 nařízení (EU) 2016/679, tedy povinnost zpracovatele provést vhodná technická a organizační opatření.

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 charakteru osobních údajů, které byly ve ztracených listinách, tedy, že se jednalo o zaměstnaneckou agendu, která obsahuje široký rozsah osobních údajů zaměstnanců, a dále to, že ztracené 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 to, že nebyly nalezeny, zneužít prakticky kdokoli a dále období za které byly listiny ztraceny. Na druhou stranu správní orgán při stanovení sankce přihlédl jako k okolnosti snižující závažnost jednání obviněné k tomu, že obviněná sama nahlásila ztrátu listinné dokumentace. 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 povinnost stanovenou v čl. 32 odst. 1 nařízení (EU) 2016/679, 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, 20. dubna 2020

otisk
úředního
razítka

Mgr. Lucie Lakatošová
pověřená řízením přestupkové agendy
(podepsáno elektronicky)