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-00472/19-5

PŘÍKAZ

Úřad pro ochranu osobních údajů, jako věcně příslušný orgán podle § 46 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, a 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 8. února 2019 v souladu s § 150 odst. 1 zákona č. 500/2004 Sb., správní řád, tento příkaz:

I. Je prokázáno, že účastník řízení: společnost [redacted] se sídlem [redacted], v souvislosti se zprostředkováním pojištění, jako správce osobních údajů podle čl. 4 bodu 7 nařízení (EU) 2016/679, tím, že nezajistil osobní údaje 4 subjektů údajů, a to [redacted] a [redacted] uvedené v pojistných smlouvách, které byly odcizeny v blíže nezjištěné době mezi 12. a 19. prosincem 2018 z osobního automobilu [redacted] jednatelky účastníka řízení,

porušil základní zásadu zpracování osobních údajů 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 mu v souladu s čl. 58 odst. 2 písm. b) nařízení (EU) 2016/679 ukládá

napomenutí.

Odůvodnění

Podkladem pro vydání tohoto příkazu je spisový materiál Krajského ředitelství policie [redacted], obvodní oddělení [redacted], čj. K[redacted] doručený Úřadu pro ochranu osobních údajů (dále jen „Úřad“) dne 24. ledna 2019.

Ze spisového materiálu vyplývá, že jednatelka účastníka řízení na adrese svého současného bydliště (ulice [redacted]í, [redacted]) uložila dne 12. prosince 2018 do svého služebního vozidla za sedadlo řidiče aktovku s pojistnými smlouvami, které obsahovaly osobní údaje [redacted], [redacted] [redacted] a [redacted] v rozsahu jméno, příjmení, rodné číslo, adresa bydliště a telefonní číslo. Ve stejný den se s vozidlem pohybovala a parkovala na různých místech po území hlavního města Prahy a následně jej večer zaparkovala u svého bydliště. Dne 19. prosince 2018 jednatelka společnosti zjistila, že došlo k odcizení výše uvedených smluv. Poškození vozidla nebylo zjištěno a jednatelka účastníka řízení dle svého tvrzení automobil pokaždé uzamkla.

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. Odcizené pojistné smlouvy nepochybně obsahovaly osobní údaje 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 shromažďuje osobní údaje osob, jímž zprostředkoval pojištění, používá tyto údaje k sepsání smluv a uchovává originály nebo kopie smluv s osobními údaji atd.; provádí tedy zpracování osobních údajů.

Dle čl. 4 bodu 7 nařízení (EU) 2016/679 se správcem rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení. Dle těchto kritérií je účastník řízení v postavení správce osobních údajů, protože určil účel (zprostředkování pojištění a dalších služeb) předmětného zpracování osobních údajů.

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 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 zajistili 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 revidovat a případně přijmout opatření 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 klientů účastníkem řízení zpracovávány způsobem, který by zajistil jejich náležité zabezpečení. Účastník řízení nedostatečně vyhodnotil rizika pro práva a svobody svých klientů, a tedy ani nepřijal odpovídající bezpečnostní opatření k jejich ochraně před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením, když byly jednatelkou účastníka řízení ponechány v prostoru motorového vozidla, přičemž jejich ztrátu zjistila až s odstupem jednoho týdne.

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 čl. 83 odst. 2 nařízení (EU) 2016/679 správní orgán při rozhodování o uložení napomenutí přihlédl 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. Vzal přitom v úvahu zejména nízký počet dotčených subjektů údajů, omezený rozsah údajů, které byly součástí pojistných smluv, a skutečnost, že k jednání jednatelky účastníka řízení nedošlo úmyslně.

Správní orgán považuje ve smyslu § 150 odst. 1 správního řádu skutkové zjištění za dostatečné a na základě výše uvedeného považuje za prokázané, že účastník řízení porušil svým jednáním povinnost stanovenou v čl. 5 odst. 1 písm. f) 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 8. února 2019

otisk
úředního
razítka

Vanda Foldová
ředitelka odboru kontrolního