Čj. UOOU-07097/16-27

ROZHODNUTÍ

Úřad pro ochranu osobních údajů, jako příslušný správní orgán podle § 10 zákona č. 500/2004 Sb., správní řád, § 2 odst. 2 a § 46 odst. 4 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, rozhodl dne 10. srpna 2016 takto:

Je prokázáno, že účastník řízení: společnost T-Mobile Czech Republic a.s., se sídlem Tomíčkova 2144/1, 148 00 Praha 4 – Chodov, IČO: 64949681, jako správce osobních údajů svých klientů podle § 4 písm. j) zákona č. 101/2000 Sb., nepřijal dostatečná opatření k zabezpečení osobních údajů obsažených v elektronické interní databázi účastníka řízení, která ke dni 30. června 2016 obsahovala osobní údaje 1 193 497 zákazníků – fyzických osob, čímž nezajistil, aby v blíže nezjištěné době, nejméně však od [redacted] do [redacted], nedošlo k ohrožení těchto osobních údajů v rozsahu jméno, příjmení, datum narození, adresa, telefonní číslo, kód zákazníka, tarif, název, kategorie a značka zařízení, údaj o průměrné útratě, platební metodě, popř. číslu účtu a kódu banky, a v důsledku toho k odcizení uvedených dat jeho zaměstnancem,

čímž porušil povinnost stanovenou v § 13 odst. 1 zákona č. 101/2000 Sb., tedy přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů, přičemž tato povinnost platí i po ukončení zpracování osobních údajů,

a tím spáchal správní delikt podle § 45 odst. 1 písm. h) a odst. 2 písm. a) zákona č. 101/2000 Sb., neboť nepřijal opatření pro zajištění bezpečnosti zpracování osobních údajů, a při zpracování osobních údajů ohrozil větší počet osob svým neoprávněným zasahováním do soukromého a osobního života, za což se mu v souladu s § 45 odst. 4 zákona č. 101/2000 Sb. ukládá

pokuta ve výši 3.600.000 Kč
(slovy tři miliony šest set tisíc korun českých)

a dále podle § 79 odst. 5 správního řádu povinnost nahradit **náklady řízení ve výši 1.000 Kč**,

obojí splatné do 30 dnů ode dne nabytí právní moci tohoto rozhodnutí bezhotovostním převodem na účet vedený u ČNB, č. ú. 19-5825001/0710, variabilní symbol IČO účastníka řízení, konstantní symbol 1148.

Odůvodnění

Správní řízení pro podezření ze spáchání správního deliktu podle § 45 odst. 1 písm. h) a odst. 2 písm. a) zákona č. 101/2000 Sb. v souvislosti s nezajištěním bezpečnosti osobních údajů zákazníků, fyzických osob, vedených v elektronické databázi účastníka řízení bylo zahájeno oznámením Úřadu pro ochranu osobních údajů, které bylo účastníku řízení, společnosti T-Mobile Czech Republic a.s., doručeno dne 30. června 2016. Podkladem pro zahájení řízení bylo oznámení účastníka řízení ze dne 13. června 2016 a jeho doplnění zaslané Úřadu pro ochranu osobních údajů (dále jen „Úřad").

Ze spisového materiálu vyplývá, že dne 13. června 2016 zaslal účastník řízení Úřadu oznámení o narušení bezpečnosti osobních údajů jako povinný subjekt ve smyslu § 88 odst. 4 zákona č. 127/2005 Sb. K narušení bezpečnosti osobních údajů účastník řízení uvedl, že [redacted]

[redacted]

Dne 14. června 2016 zaslal účastník řízení Úřadu doplnění oznámení o narušení bezpečnosti osobních údajů, v němž uvedl, že [redacted]

Dne 15. června 2016 zaslal účastník řízení Úřadu doplnění oznámení, v němž uvedl [redacted]

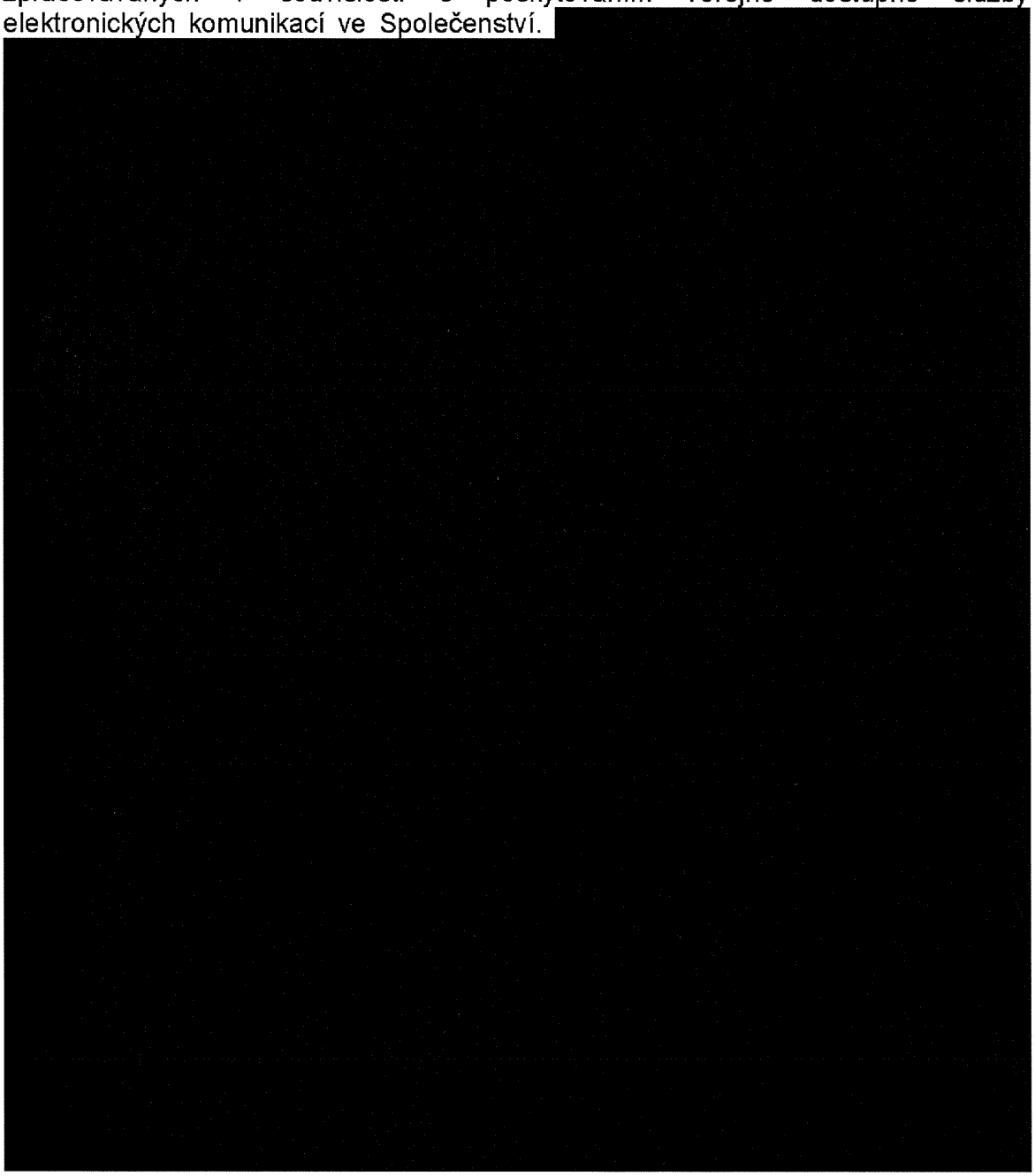
[redacted]

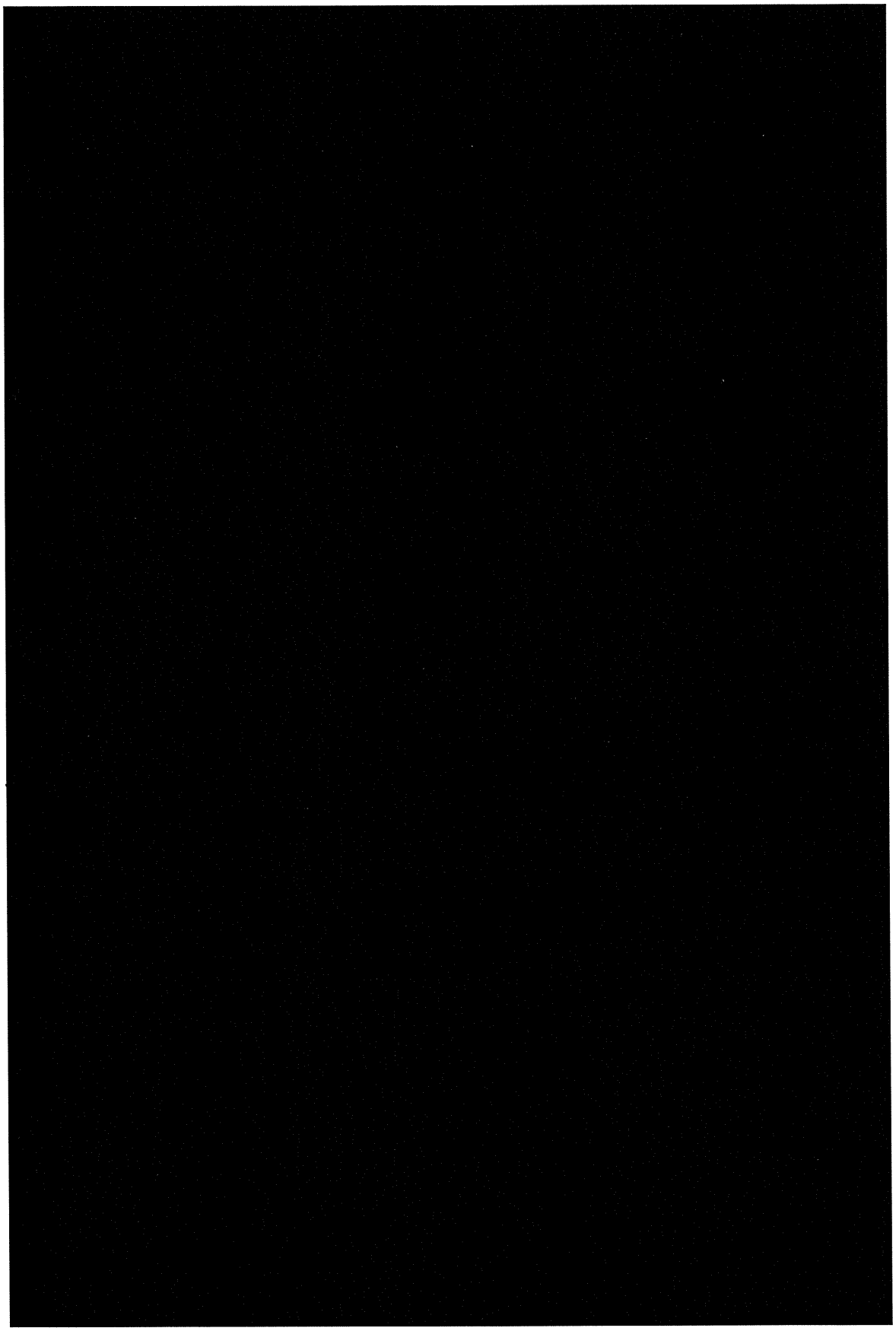
Dne 16. června 2016 zaslal účastník řízení Úřadu doplnění oznámení obsahující vzorky souboru, které byly předmětem šetřeného incidentu (tj. vzorky s reálnými daty jeho zákazníků), [redacted]

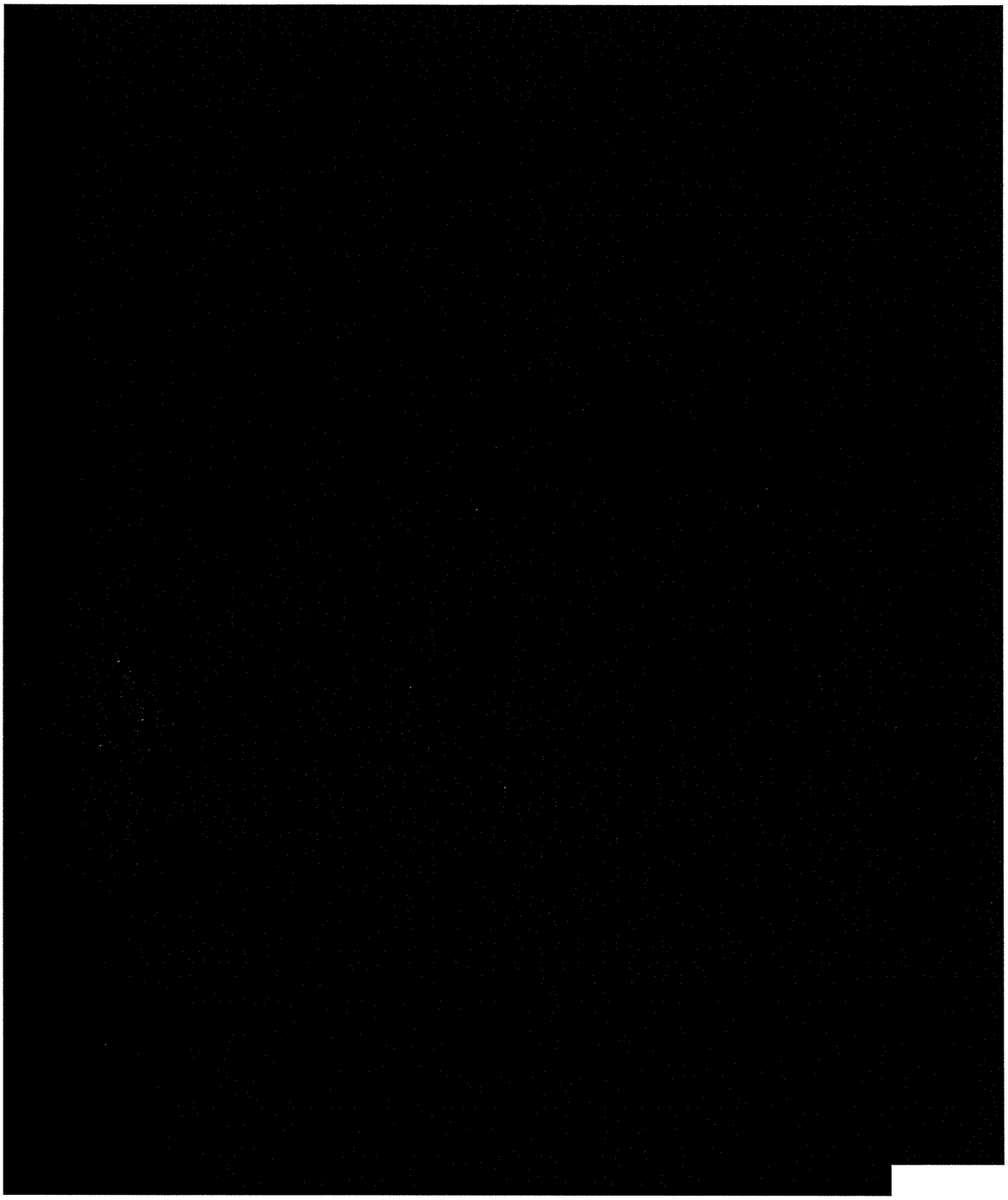
Dne 20. června 2016 zaslal Úřad účastníku řízení výzvu, v níž bylo konstatováno, že z oznámení učiněného účastníkem řízení jednoznačně nevyplývá přesný rozsah zasažených údajů a přesný počet zasažených subjektů, jakým způsobem došlo k úniku dat, rozsah technicko-organizačních opatření uplatněných na zasažená data a v jakém rozsahu došlo k narušení dostupnosti, integrity a důvěrnosti údajů. Účastník řízení byl vyzván, aby se vyjádřil k nedodržení lhůty podle čl. 2 nařízení Komise (EU) č. 611/2013 o opatřeních vztahujících se k oznámení o narušení bezpečnosti osobních údajů podle směrnice Evropského parlamentu a Rady 2002/58/ES, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, a aby zdůvodnil, proč nebyly o incidentu bezodkladně po jeho zjištění informovány dotčené subjekty. Dále byl vyzván, aby upřesnil popis narušení bezpečnosti osobních údajů (zejména postup a způsob jakým se osobní údaje zákazníků dostaly mimo informační systémy účastníka řízení a jak bylo narušení zjištěno). Dále pak byl vyzván k upřesnění počtu zasažených subjektů, vzhledem k celkovému počtu ohrožených subjektů, a ke sdělení, zda byly údaje zaměstnancem odcizeny a zda byly následně někomu prodány (s odkazem na tiskovou zprávu vydanou účastníkem řízení, v níž bylo uvedeno, že zaměstnanec se pokusil odcizit a následně prodat zákaznická data), případně v jakém počtu. [redacted]

Dne 23. června 2016 zaslal účastník řízení v reakci na výše uvedenou výzvu vyjádření, v němž uvedl, že samo přijetí speciální právní úpravy obsažené ve směrnici 2002/58/ES („ePrivacy směrnice“) reagovalo na vývoj technologií v sítích elektronických komunikací, které opodstatňovaly definování speciálních sektorově specifických požadavků ve vztahu k ochraně osobních údajů a soukromí jednotlivců

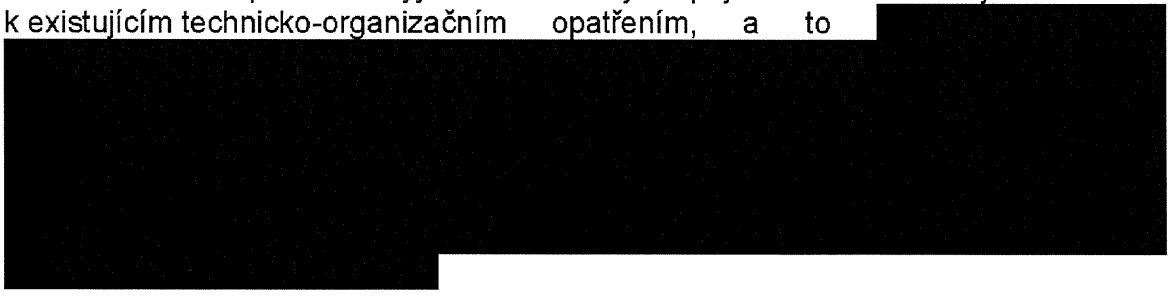
(viz čl. 5 „ePrivacy směrnice"). Jedná se tak o sektorově specifickou právní úpravu, která si klade za cíl nad rámec směrnice 95/46/ES uložit další specifické požadavky na ochranu osobních údajů a soukromí v souvislosti s provozováním sítí elektronických komunikací a poskytováním služeb elektronických komunikací. Za tímto účelem „ePrivacy směrnice" definuje provozní a lokalizační údaje, které mají potenciál vypovídat detailně o soukromí subjektů údajů, dále potom cílí na zajištění ochrany obsahu přenášených zpráv a souvisejících provozních údajů (viz např. čl. 21 „ePrivacy směrnice"). Obdobně rovněž tak v čl. 2 písm. i) „ePrivacy směrnice" jasně definuje „narušení bezpečnosti osobních údajů" jako narušení bezpečnosti, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně či neoprávněnému vyzrazení nebo zpřístupnění osobních údajů přenášených, uchovávaných nebo jinak zpracovávaných v souvislosti s poskytováním veřejně dostupné služby elektronických komunikací ve Společenství.

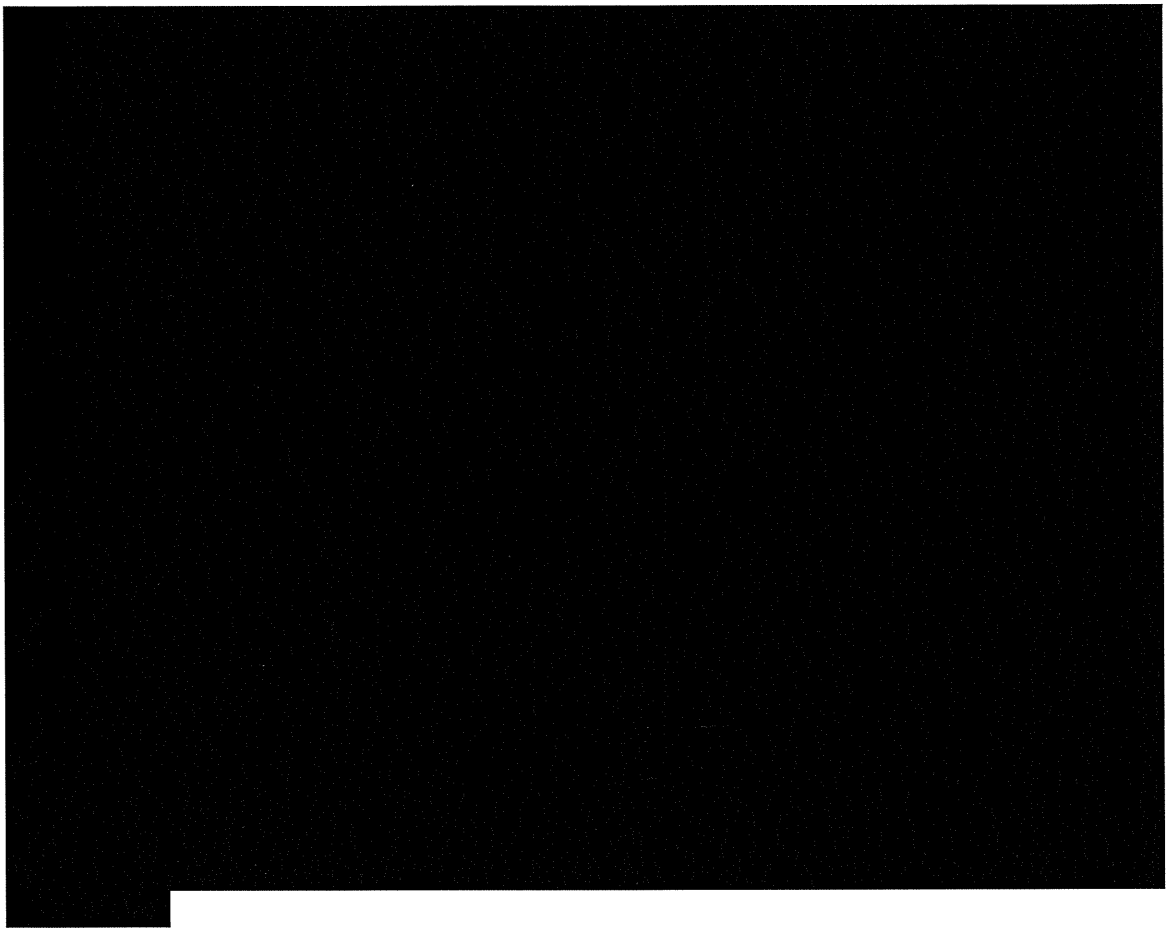




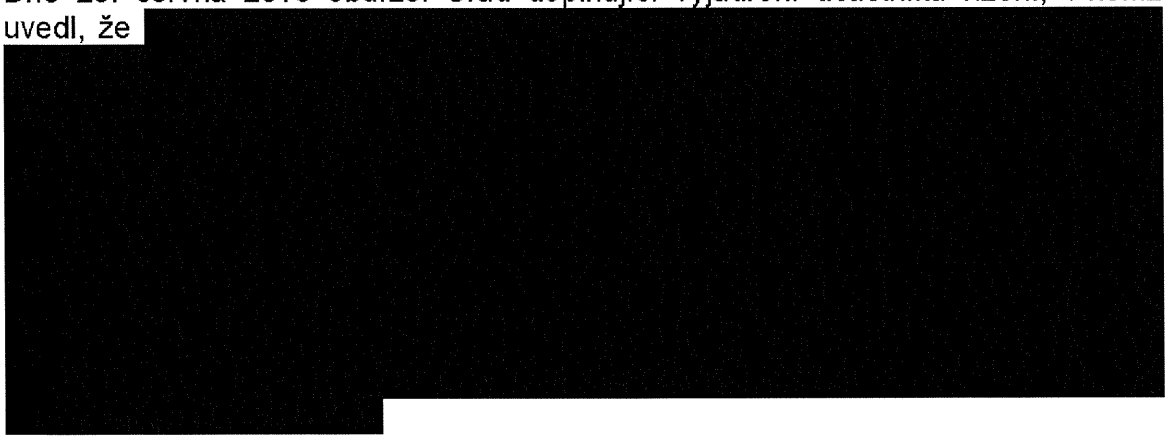


Účastník řízení přiložil k vyjádření další jím přijaté interní normy ve vztahu k existujícím technicko-organizačním opatřením, a to

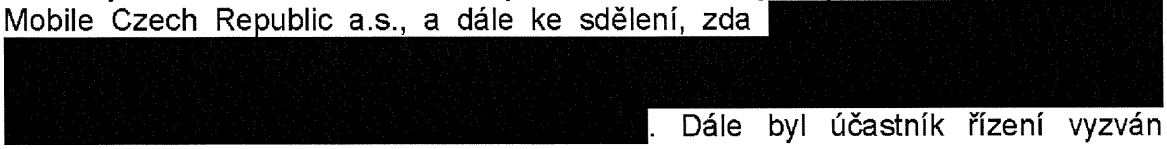




Dne 28. června 2016 obdržel Úřad doplňující vyjádření účastníka řízení, v němž uvedl, že



Dne 30. června 2016 zaslal správní orgán účastníku řízení oznámení o zahájení řízení, které mu bylo doručeno téhož dne. V oznámení o zahájení řízení byl účastník řízení vyzván ke sdělení aktuálního počtu zákazníků, fyzických osob, společnosti T-Mobile Czech Republic a.s., a dále ke sdělení, zda



. Dále byl účastník řízení vyzván

ke sdělení, zda mohl výše uvedený zaměstnanec osobní údaje zákazníků, ke kterým měl přístup, kopírovat na externí datové nosiče, příp. jaké, popř. zda je mohl odeslat elektronickou poštou a za jakých podmínek. Dále bylo požadováno sdělení počtu zákazníků, fyzických osob, jejichž osobní údaje získané z elektronické databáze účastníka řízení byly nabízeny k prodeji jeho zaměstnancem. Účastník řízení byl vyzván k identifikaci policejního útvaru, který provádí šetření v dané věci včetně sdělení čísla jednacího, pod nímž je věc projednávána. [redacted] Dále pak byl vyzván k předložení relevantních vnitřních předpisů společnosti T-Mobile Czech Republic a.s. majících vztah k předmětu řízení.

Dne 30. června 2016 zaslal správní orgán žádost o součinnost Policejnímu prezidiu České republiky, v níž žádal o sdělení konkrétního policejního útvaru, který provádí šetření v dané věci.

Dne 1. července 2016 obdržel správní orgán sdělení Policejního prezidia České republiky, z něhož vyplývá, že předmětný spis zpracovává [redacted].

Dne 1. července 2016 zaslal správní orgán žádost o poskytnutí součinnosti Policii České republiky, [redacted], v němž žádal sdělení, zda [redacted]

Dne 11. července 2016 obdržel správní orgán vyjádření účastníka řízení, v němž uvedl [redacted]

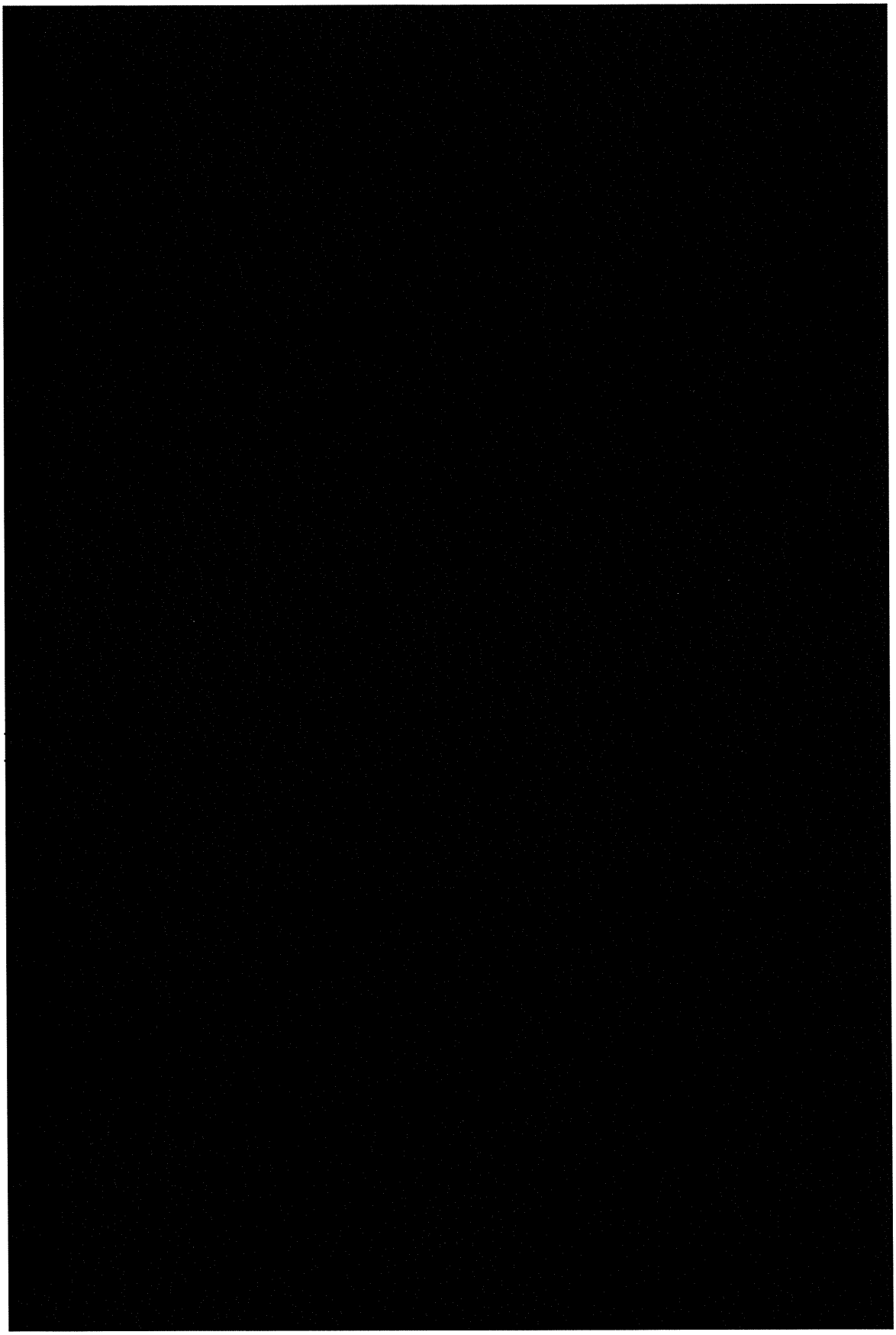
[redacted]

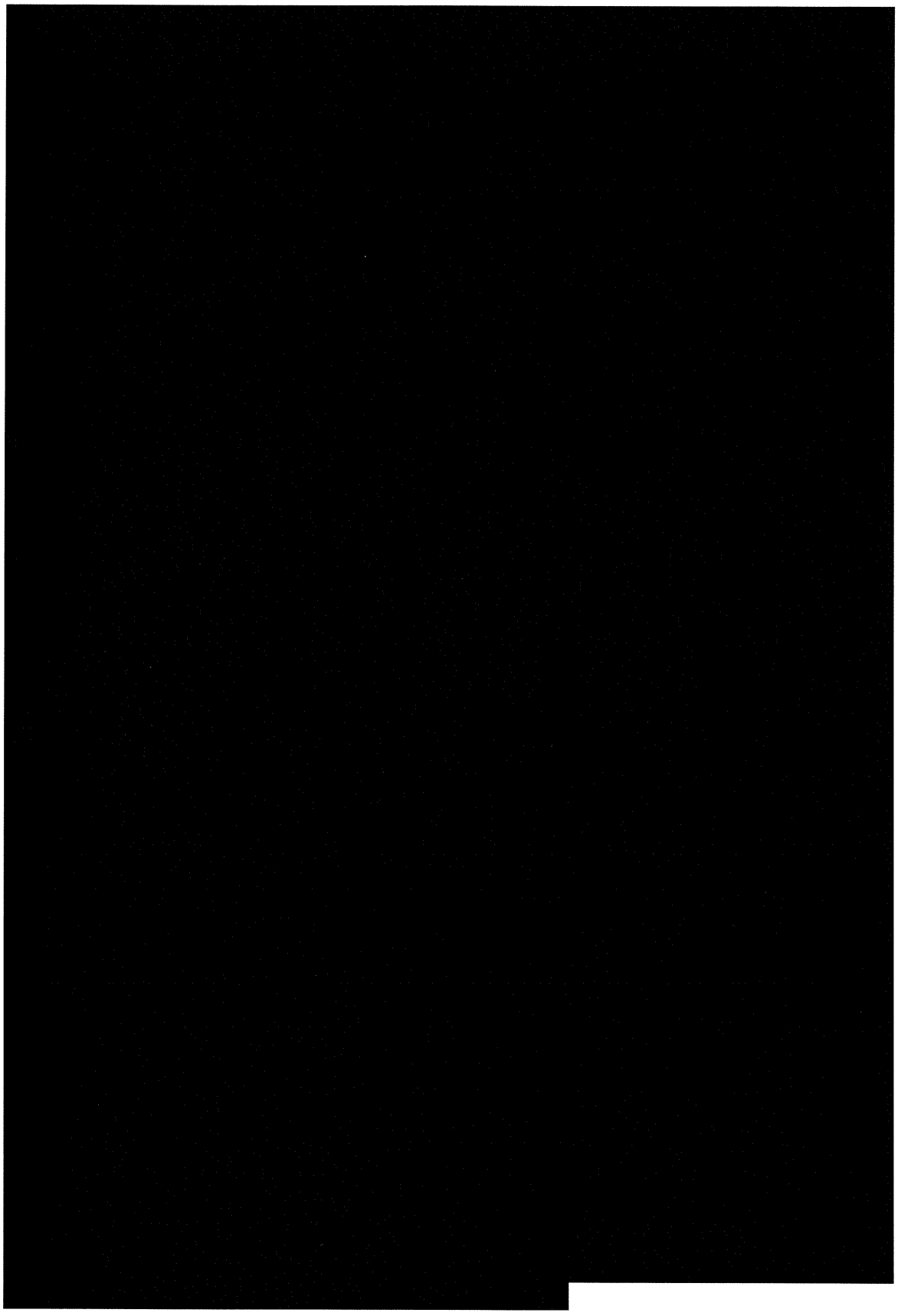
Dne 13. července 2016 obdržel správní orgán vyjádření [redacted], v němž uvedl k dotazům položeným správním orgánem v žádosti o součinnost ze dne 1. července 2016 následující.

[redacted]

[redacted]

Dne 18. července 2016 obdržel správní orgán vyjádření účastníka řízení, v němž uvedl, že [redacted]





Dne 20. července 2016 zaslal správní orgán výzvu k předložení listin účastníku řízení, v níž jej vyzval k předložení listin dokládajících skutečnost, že [redacted] Dále jej vyzval k předložení listin, z nichž je zřejmé, že na základě výše uvedeného zjištění byla prostřednictvím oddělení bezpečnosti provedena analýza neobvyklého chování všech oprávněných uživatelů databáze, včetně data zahájení a ukončení uvedené analýzy. Dále vznesl správní orgán požadavek na zaslání listin dokládajících výstup interního šetření včetně výsledku provedené analýzy logů, na základě kterých došlo k identifikaci konkrétního uživatele (zaměstnance společnosti), který se měl dopustit bezpečnostního incidentu, včetně data, kdy došlo k určení tohoto uživatele. Dále správní orgán požadoval zaslání listin, z nichž je patrné, kdy přesně společnost T-Mobile Czech Republic a.s. kontaktovala v dané věci Policii České republiky (kopie trestního oznámení apod.).

Dále správní orgán dne 20. července 2016 zaslal žádost o poskytnutí součinnosti [redacted], v níž žádal o sdělení následujících skutečností v případě, vyplývají-li ze shromážděného spisového materiálu, příp. jejich doložení relevantními podklady. Správní orgán žádal o sdělení, zda [redacted]

Dne 20. července 2016 byl vyhotoven správním orgánem úřední záznam týkající se pořízení výtisku tiskové zprávy ze dne 13. června 2016 označené „T-Mobile – vyjádření k úniku dat" dostupné na internetové adrese http://www.t-press.cz/cs/novinky/t-mobile-vyjadreni-k-uniku-dat.html prostřednictvím webových stránek společnosti T-Mobile Czech Republic a.s. z rubriky „O T-Mobile" – „Pro média". Dále byly pořízeny výtisky článků zveřejněných dne 13. června 2016 v internetových denících, a to článku s názvem „Zaměstnanec T-Mobile ukradl a prodal osobní údaje 1,5 milionu klientů" dostupného z internetové adresy http://zpravy.idnes.cz/masivni-unik-dat-z-ceskeho-t-mobile-dt3-/domaci.aspx?c=A160612_215016_domaci_neh, článku s názvem „Obří únik dat z T-Mobile: Zaměstnanec ukradl a prodával údaje 1,5 milionu klientů" dostupného z internetové adresy

https://zpravy.aktualne.cz/ekonomika/pracovnik-t-mobilu-ukradl-a-prodaval-data-1-5-milionu-klient/r~8c70c474312411e68afb002590604f2e/ a článku s názvem „'Ajťák' z T-Mobilu ukradl data 1,5 milionu klientů. Zloděje prozradilo, že údaje nabídl obchodnímu partnerovi operátora" dostupného z internetové adresy http://domaci.ihned.cz/c1-65329380-zamestnanec-t-mobilu-ukradl-a-prodaval-data-1-5-milionu-klientu-mohla-mezi-nimi-byt-i-cisla-bankovnich-uctu.

Z článku „Zaměstnanec T-Mobile ukradl a prodal osobní údaje 1,5 milionu klientů" (dostupného na internetovém portálu http://www.idnes.cz/) vyplývá, že Mladou frontou DNES mělo být zjištěno, že jeden ze zaměstnanců firmy ukradl pečlivě střežené osobní údaje klientů a prodával je dál. K tomu bylo uvedeno, že zaměstnanec byl dopaden a únik dat vyšetřuje policie, která v souvislosti s kauzou už obvinila dva lidi a stíhá je na svobodě. Dále bylo citováno vyjádření tiskové mluvčí společnosti T-Mobile Czech Republic a.s. Martiny Kemrové, která měla uvést k dotazu deníku: „Bohužel musíme potvrdit, že došlo ke zcizení a prodeji zákaznických dat." Dále deník uvedl, že prý ani společnost T-Mobile Czech Republic a.s. neví, kolika klientů se únik týkal, s tím, že podle informací deníku se únik týká zhruba 1,5 milionu zákazníků. Na to měla tisková mluvčí Martina Kemrová reagovat: „Je to předmětem šetření policie, údaj nemůžeme potvrdit." Dále deník uvedl, že to, zda český zaměstnanec T-Mobilu prodával pouze jména, telefonní čísla, e-mailové adresy nebo ještě citlivější údaje, jako jsou čísla kont, nechce operátor prozradit, s tím, že na dotazy svých zákazníků na Twitteru se firma odkazuje na tiskovou zprávu, kterou vydala. Dále deník uvedl, že tisková mluvčí Martina Kemrová uvedla: „Ihned poté, co jsme díky důkladným bezpečnostním mechanismům zjistili, že došlo ke stažení zákaznických dat, zasáhli naši bezpečnostní experti. Případ jsme předali policii, zaměstnanec byl okamžitě propuštěn, data jsou zpět v majetku naší společnosti. V současné chvíli je případ v šetření, a proto nemůžeme poskytnout detailní informace." Tisková mluvčí následně doplnila, že postiženým zákazníkům hrozí přinejhorším marketingové nabídky od společností, které osobní data skupují (tisková mluvčí Martina Kemrová uvedla: „Nešlo o data lokalizační či provozní ani o citlivé údaje typu hesel. Jediné nebezpečí, které by hypoteticky mohlo našim zákazníkům hrozit, je případně oslovení nevyžádanými marketingovými nabídkami."). Dále deník uvedl, že dle jeho informací vyšetřuje případ Útvar pro odhalování organizovaného zločinu, přičemž v dané věci měl deníku sdělit mluvčí útvaru Pavel Hanták, že probíhá vyšetřování pro podezření z podílnictví a z neoprávněného přístupu k počítačovému systému a nosiči informací, ze kterého byly obviněny dvě osoby, které jsou stíhány na svobodě, s tím, že bližší informace poskytovat nebudou.

Z článku „Obří únik dat z T-Mobile: Zaměstnanec ukradl a prodával údaje 1,5 milionu klientů" (dostupného na internetovém portálu http://www.aktualne.cz/) je zřejmé, že článek vycházel z informací získaných a zveřejněných Mladou frontou DNES (viz výše popsaná vyjádření tiskové mluvčí společnosti T-Mobile Czech Republic a.s. a mluvčího Útvaru pro odhalování organizovaného zločinu). V úvodu bylo uvedeno, že únik dat vyšetřuje policie, která už obvinila dva lidi, s tím, že zloděje dat prozradilo, že databázi nabídl firmě, která se společností T-Mobile Czech Republic a.s. spolupracuje. Podle tiskové mluvčí společnosti T-Mobile Czech Republic a.s. šlo o data pro marketing a nešlo o citlivé údaje typu hesel. K tomu deník doplnil, že podle Mladé fronty DNES se případ stal v dubnu a jde v něm

o údaje zhruba 1,5 milionu zákazníků. Zloděje dat prozradilo, že databázi nabídl firmě, která se společností T-Mobile Czech Republic a.s. spolupracuje. Deníkem bylo uvedeno, že tisková mluvčí společnosti T-Mobile Czech Republic a.s. uvedla: "Případ se podařilo odhalit díky spolupráci s obchodním partnerem, který nás informoval, že mu někdo nabízí k odkoupení databázi údajně našich klientů. Prošetřili jsme, zda jde o reálná data, a po zjištění, že ano, jsme informovali policii a podnikli patřičné kroky." V článku je dále uvedeno, že Mladá fronta DNES píše, že se zpočátku mluvilo o škodě v řádu stamilionů korun, kterou krádeží dat mohla společnost T-Mobile Czech Republic a.s. utrpět. K tomu bylo konstatováno, že firma uvedla, že žádná škoda jí ani zákazníkům nevznikla. K tomu bylo doplněno, že generální ředitel společnosti T-Mobile Czech Republic a.s. Milan Vašina uvedl: "Chci zákazníky ujistit, že reálně k úniku dat nedošlo a že jejich data jsou v bezpečí." Tisková mluvčí společnosti T-Mobile Czech Republic a.s. doplnila: "Pokus byl podchycen v samotném začátku." Podle tiskové mluvčí šlo o selhání jednotlivce, nikoli o systémovou či procesní chybu. Dle zjištění deníku Aktuálně.cz to samé říkají klientům společnosti T-Mobile Czech Republic a.s. operátoři na zákaznické lince, přičemž redaktorovi bylo sděleno operátorem, že společnost neví, koho přesně se únik dat týkal, s tím, že data byla ale zničena, a k tomu bylo dále operátorem doplněno, že podvodník se je snažil prodat, ale nevyšlo mu to. Pracovníka IT oddělení T-Mobilu, který data zkopíroval, už policie obvinila. Šlo o člena malého týmu, který se zákaznickými daty běžně pracoval. Krádež dat vyšetřuje Útvar pro odhalování organizovaného zločinu.

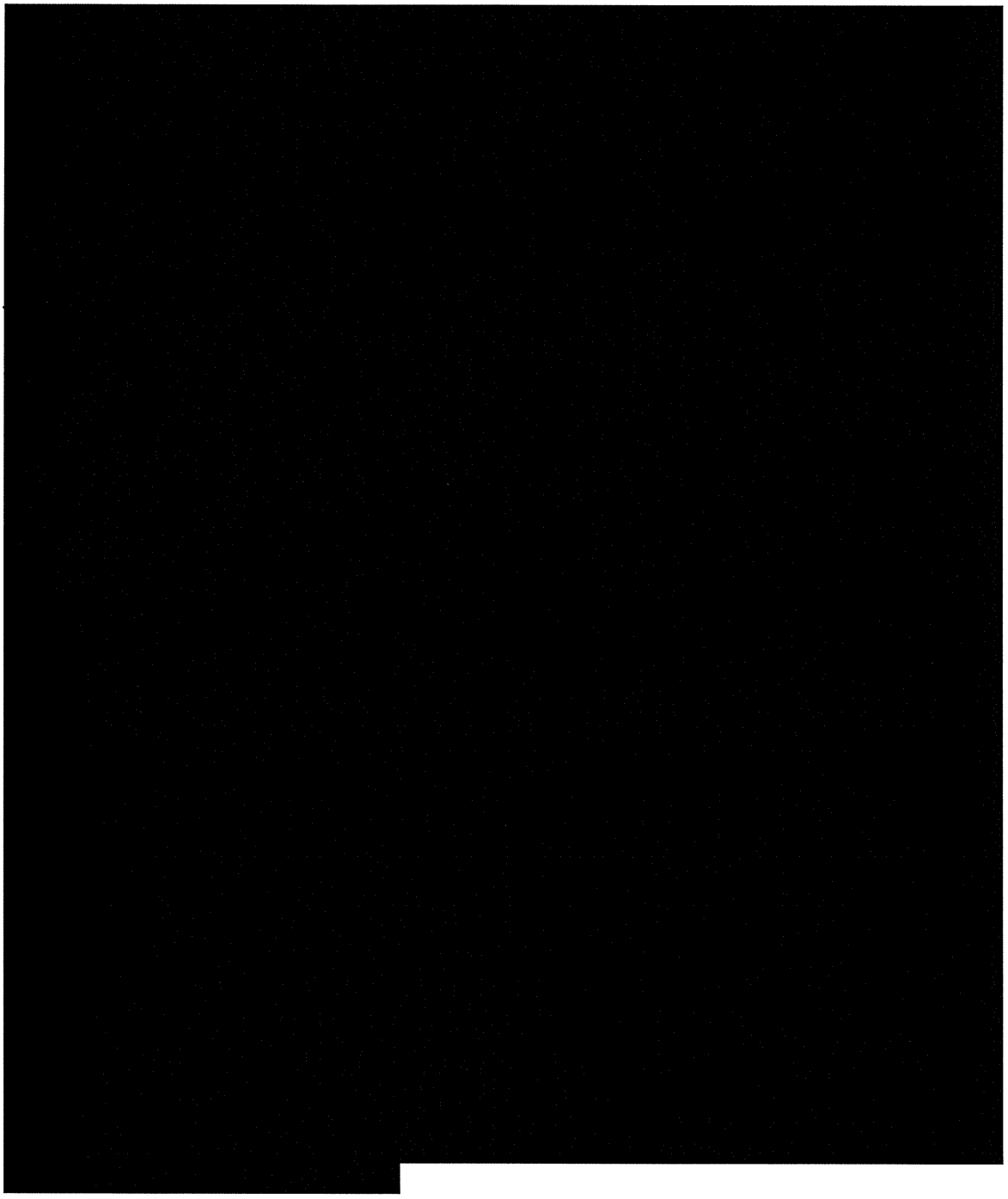
V úvodu článku „'Ajťák' z T-Mobilu ukradl data 1,5 milionu klientů. Zloděje prozradilo, že údaje nabídl obchodnímu partnerovi operátora" (dostupného na internetovém portálu http://ihned.cz/) je konstatováno, že zaměstnanec IT oddělení společnosti T-Mobile Czech Republic a.s. ukradl a následně prodal data 1,5 milionu klientů. Dále je konstatováno, že pracovník měl data stáhnout 19. dubna 2016, s tím, že operátor, který má v Česku na šest milionů zákazníků, však únik přiznal až poté, co o něm informovala média, tedy po téměř dvou měsících. Podle firmy nevznikla ani jí, ani zákazníkům žádná škoda, a proto o incidentu neinformovala. Policie však již obvinila dva lidi. Následně je uvedeno, že jeden ze zaměstnanců telekomunikačního operátora společnosti T-Mobile Czech Republic a.s. ukradl osobní údaje klientů a prodával je dál, přičemž únik dat vyšetřuje policie, jak napsala Mladá fronta DNES, která přišla s hypotézou, že únik souvisel s výpadkem sítě společnosti T-Mobile Czech Republic a.s. Zatímco únik dat mluvčí operátora Martina Kemrová potvrdila, souvislost s technickými problémy odmítá. Opětovně bylo deníkem konstatováno, že k úniku dat došlo v dubnu a jde v něm o údaje zhruba 1,5 milionu zákazníků. Rovněž bylo opětovně konstatováno, že zloděje dat prozradilo, že databázi nabídl firmě, která se společností T-Mobile Czech Republic a.s. spolupracuje (shodným způsobem bylo citováno v této souvislosti vyjádření tiskové mluvčí společnosti T-Mobile Czech Republic a.s., viz výše uvedený článek zveřejněný na internetovém portálu http://www.aktualne.cz). Dále bylo doplněno vyjádření tiskové mluvčí, která uvedla: "Zaměstnanec byl okamžitě propuštěn, data jsou zpět v majetku naší společnosti.", a dále uvedla k dotazu Hospodářských novin: "Byly zajištěny všechny nosiče, na nichž data byla stažena. Existuje teoretická možnost, že existují také jiné nosiče, ale zatím nemáme indikace, že by tomu tak bylo." K charakteru odcizené databáze bylo uvedeno, že podle společnosti T-Mobile Czech Republic a.s. je čistě marketingový, k čemuž bylo připojeno vyjádření tiskové mluvčí, jak je popsáno výše

v článku dostupném na internetovém portálu http://www.idnes.cz/). Dále bylo uvedeno, že na otázku, kdy chtěla firma o úniku informovat, tisková mluvčí uvedla, že šlo o neúspěšný pokus, kdy zákazníkům nevznikla žádná újma, a z toho důvodu by proto společnost T-Mobile Czech Republic a.s. "informaci aktivně nešířila". Dále bylo poukázáno na to, že podle Mladé fronty DNES se zpočátku mluvilo o škodě v řádu stamilionů korun, kterou mohla krádeží dat společnost T-Mobile Czech Republic a.s. utrpět, s tím, že firma uvedla, že žádná škoda jí ani zákazníkům nevznikla (viz vyjádření tiskové mluvčí, že pokus byl podchycen v samotném začátku). Podle Mladé fronty DNES pracovníka IT oddělení společnosti T-Mobile Czech Republic a.s., který data zkopíroval, už policie obvinila. Podle jedné z verzí data stáhl 19. dubna 2016 a způsobil tím výpadky signálu po celém Česku, jak bylo uvedeno Mladou frontou DNES, přičemž společnost T-Mobile Czech Republic a.s. to popírá (k tomu připojil vysvětlení podané tiskovou mluvčí, která uvedla: „Výpadek signálu s únikem dat spolu nijak nesouvisí. Z technologického pohledu je taková spojitost naprosto vyloučena."). Celkem policie v souvislosti s únikem dat stíhá dva lidi. I když podle společnosti T-Mobile Czech Republic a.s. šlo pouze o selhání jednotlivce, firma preventivně prověří své systémy. K tomu bylo doplněno, že ředitel společnosti T-Mobile Czech Republic a.s. Milan Vašina uvedl: "Chci zákazníky ujistit, že reálně k úniku dat nedošlo a že data našich zákazníků jsou v bezpečí." Dále uvedl: "Po prozkoumání našeho systému zvážíme případné zavedení dalších preventivních opatření." Podle tiskové mluvčí uvedené společnosti se objem dat, s nímž "lupič" pracoval, nevymykal běžnému provozu. Zaměstnanec měl k datům řádně přidělená přístupová práva. Dále tisková mluvčí uvedla: "Nemůžete chránit data před člověkem, který s nimi pracuje."

Z výše uvedené tiskové zprávy vydané účastníkem řízení vyplývá, že účastník řízení k věci uvedl, že jeden z jeho zaměstnanců (člen malého týmu, který se zákaznickými daty běžně pracoval) se pokusil odcizit a následně prodat zákaznická data. Dále účastník řízení uvedl, že ihned po zjištění podezření na trestnou činnost podnikl všechny nutné kroky v součinnosti s Policií České republiky. Zaměstnanci byl bez prodlení zrušen pracovní poměr a bylo zahájeno vyšetřování orgánů činných v trestním řízení, s tím, že právě v souvislosti s tímto bohužel nejsou oprávněni poskytovat žádné konkrétní informace. Dále účastník řízení zdůraznil, že jde o případ selhání jednotlivce, nikoli o systémovou, či procesní chybu. Dále uvedl, že díky důkladným bezpečnostním mechanismům byli schopni okamžitě zareagovat a databázi zajistit. Charakter odcizené databáze byl čistě marketingový, nešlo o data lokalizační či provozní, ani o citlivé údaje typu hesel. Jediné nebezpečí, které by hypoteticky mohlo zákazníkům hrozit, je případné oslovení nevyžádanými marketingovými nabídkami. Dále byl v tiskové zprávě citován generální ředitel T-Mobile Czech Republic a.s. Milan Vašina, který uvedl, že chce zákazníky ujistit, že reálně k úniku dat nedošlo a že jejich data jsou v bezpečí, k čemuž doplnil, že důvěra zákazníků a jejich bezpečnost jsou pro ně naprostou prioritou, přičemž dle jeho slov, přestože při důkladné kontrole neshledali systémové pochybení, znovu celý systém přezkoumají a zváží případné zavedení dalších preventivních opatření. Účastník řízení se dále vyjádřil v tom smyslu, že by rád vyvrátil spekulace o tom, že únik dat byl spojen s výpadkem signálu dne 19. dubna 2016, s tím, že tyto dva incidenty spolu nikterak nesouvisí, přičemž z technologického pohledu je taková spojitost naprosto vyloučena.

Dne 26. července 2016 obdržel správní orgán vyjádření Útvaru [redacted] k žádosti o součinnost ze dne 20. července 2016, který uvedl, že [redacted]

Dne 26. července 2016 obdržel správní orgán vyjádření účastníka řízení zaslané v reakci na výzvu správního orgánu ze dne 20. července 2016, v němž uvedl [redacted]



Dále účastník řízení předložil výpis [redacted]

Z textu trestního oznámení učiněného účastníkem řízení [redacted]

Dne 26. července 2016 zaslal správní orgán účastníku řízení výzvu k seznámení s podklady rozhodnutí, která mu byla doručena téhož dne. Dne 1. srpna 2016 se dostavil pověřený zaměstnanec účastníka řízení k nahlédnutí do spisu.

Dne 4. srpna 2016 obdržel správní orgán doplňující vyjádření účastníka řízení, [redacted]

K předmětu řízení lze konstatovat, že údaje zákazníků v rozsahu jméno, příjmení, datum narození, adresa, telefonní číslo, kód zákazníka, tarif, název, kategorie a značka zařízení, údaj o průměrné útratě, platební metodě, popř. číslu účtu a kódu banky (v případě zákazníků majících zřízenou inkasní platbu), jsou nepochybně osobní údaje ve smyslu § 4 písm. a) zákona č. 101/2000 Sb., neboť se vztahují k jednoznačně určenému subjektu údajů.

Za zpracování osobních údajů je podle § 4 písm. e) zákona č. 101/2000 Sb. považována jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace. Osobní údaje zákazníků společnosti T-Mobile Czech Republic a.s. jsou shromažďovány účastníkem řízení, následně jsou uchovávány v elektronické podobě v databázi spravované účastníkem řízení a používány pro účastníkem řízení vymezené účely, jedná se tedy o zpracovávání osobních údajů ve smyslu zákona č. 101/2000 Sb.

Účastník řízení je správcem osobních údajů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb., který stanoví, že správcem osobních údajů je každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Účelem zpracování osobních údajů v elektronické databázi účastníka řízení je evidence zákazníků pro potřeby účastníka řízení a v souvislosti s jím zajišťovanými telekomunikačními a dalšími službami. Prostředky zpracování osobních údajů stanovil účastník řízení mj. prostřednictvím svých vnitřních předpisů. Účastník řízení je tedy správcem těchto osobních údajů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb., a odpovídá za dodržování povinností stanovených pro jejich zpracování zákonem č. 101/2000 Sb. Jednou z těchto povinností je povinnost stanovená v § 13 odst. 1 tohoto zákona, tj. povinnost přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

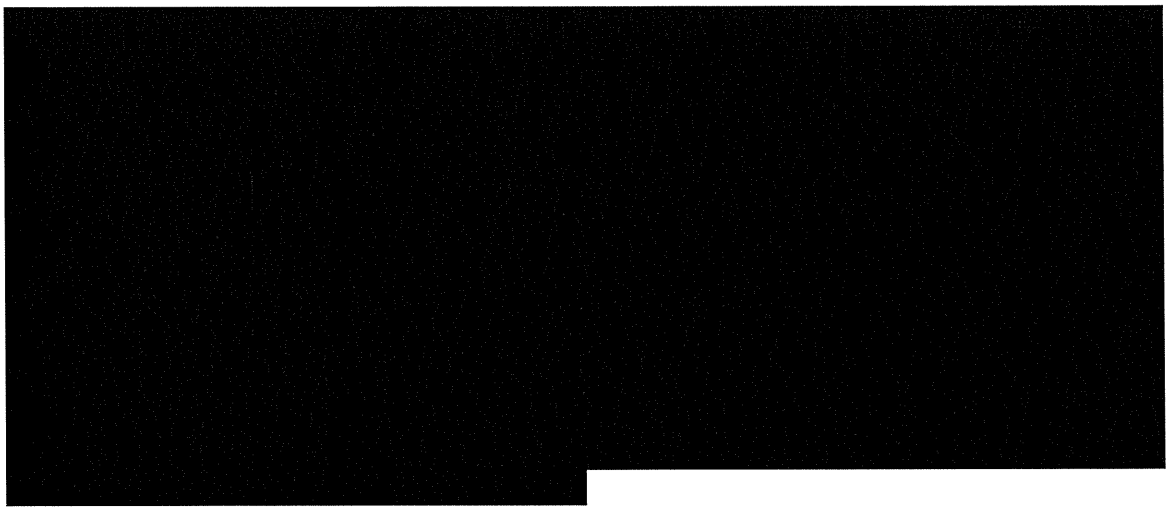
Povinnost dle § 13 odst. 1 zákona č. 101/2000 Sb. a této povinnosti odpovídající skutková podstata správního deliktu je formulovaná jako odpovědnost za následek.

Dojde-li tedy k následku předvídanému v § 13 odst. 1 zákona č. 101/2000 Sb. (neoprávněnému přístupu k osobním údajům apod.), což je v této věci nepochybné, znamená to, že se správce osobních údajů dopustil také správního deliktu.

Správní orgán v této souvislosti odkazuje na argumentaci Nejvyššího správního soudu k problematice objektivní odpovědnosti za správní delikt v rozsudku čj. 9 As 36/2007-59 (byť v jiné oblasti veřejného práva a bez výslovného zakotvení liberačního ustanovení). Dle názoru správního orgánu je pojem „přijmout taková opatření" v normě ukládající primární povinnosti (tj. v § 13 odst. 1 zákona č. 101/2000 Sb.) nutno považovat za synonymum pojmu zajistit. Oba tyto pojmy je poté třeba dle názoru správního orgánu interpretovat jako garanci správce osobních údajů za bezpečnost zpracování osobních údajů, tedy za to, že se s osobními údaji např. neseznámí žádná nepovolaná osoba. Jedině tento výklad je schopen zajistit efektivní fungování právní normy a naplnění jejího elementárního smyslu a účelu, kterým je naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí (viz opět rozsudek Nejvyššího správního soudu čj. 9 As 36/2007-59, www.nssoud.cz).

Skutková podstata správního deliktu podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. je naplněna již v situaci, kdy zpracovávaným osobním údajům hrozí (v důsledku nepřijetí či neprovedení dostatečných organizačních a technických opatření) riziko nesprávného či neoprávněného zpracování. V případě, kdy jsou osobní údaje bez jakéhokoli právního titulu již zpřístupněny třetím osobám (v daném případě byly nabídnuty, včetně vzorku, ke koupi třetímu subjektu), nelze o naplnění uvedené skutkové podstaty pochybovat.

Ze spisového materiálu vyplývá, že ke zjištění úniku dat zákazníků z interní databáze



Vzhledem k výše uvedenému má správní orgán důvod se domnívat, že [redacted] Reakce účastníka řízení na zjištěné neobvyklé chování uživatele databáze tak nebyla dostatečná ani včasná (tj. neboť včasnost nelze odvíjet od okamžiku, kdy se účastník řízení o úniku dozvěděl od spolupracující agentury).

Ze spisového materiálu je dále zřejmé, že účastník řízení měl přijata opatření k zabezpečení osobních údajů klientů, nicméně uvedená opatření nebyla dostatečná. V důsledku toho měly osoby s oprávněným přístupem do informačního systému a k osobním údajům zákazníků bez dalšího možnost kopírovat data zákazníků na datové nosiče, popř. v omezeném rozsahu rovněž posílat prostřednictvím e-mailových zpráv. K tvrzení účastníka řízení, že bezpečnostní incident nenastal v důsledku nedostatečných technicko-organizačních opatření, případně jejich selhání, ale v důsledku protiprávního excesivního chování jedince, tak správní orgán uvádí, že příčinou, že k bezpečnostnímu incidentu a k ohrožení osobních údajů došlo, je skutečnost, že nedostatečným způsobem zabezpečil ochranu osobních údajů obsažených v uvedené databázi. V důsledku nedostatečného zabezpečení osobních údajů bylo možné a proveditelné odcizení osobních údajů zákazníků z interní databáze zaměstnancem, který měl oprávněný přístup do systému a s předmětnými daty pracoval.

Účastníkem řízení byly předloženy vnitřní předpisy přijaté ve vztahu k zabezpečení ochrany osobních údajů zákazníků. Předmětné vnitřní předpisy se zaměřují na ochranu osobních údajů před jejich získáním neoprávněnými uživateli [redacted] Vnitřní předpisy upravují základní oprávnění a povinnosti ve vztahu k zabezpečení informací obsažených v informačních systémech a databázích včetně přístupových oprávnění. Předmětná pravidla se zaměřují především na zamezení přístupu neoprávněných osob do informačních systémů, popř. zamezení přístupu zaměstnanců, kteří nepotřebují informace nezbytně nutně k výkonu práce (řízení přístupu k citlivým informacím). Účastník řízení však nedoložil

žádný dokument, vnitřní předpis, ani nedoložil přijetí opatření, která by byla schopna účinným způsobem zamezit osobě oprávněné k přístupu k osobním údajům zákazníků v neoprávněném ukládání takovýchto údajů na externí média, popř. jejich zaslání e-mailem. [redacted]

Ze spisového materiálu je tedy zřejmé, že zaměstnanec účastníka řízení oprávněný k přístupu k osobním údajům zákazníků vedeným v elektronické interní databázi [redacted]

Správní orgán tedy na základě výše uvedeného konstatuje, že účastník řízení nepřijal dostatečná opatření k ochraně osobních údajů zákazníků obsažených v jeho interní databázi, čímž došlo nepochybně k porušení povinnosti stanovené § 13 odst. 1 zákona č. 101/2000 Sb., tedy povinnosti přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům nebo k jejich neoprávněnému zpracování.

Odpovědnost za správní delikt je přitom postavena na objektivní odpovědnosti (tedy bez ohledu na zavinění), přičemž zákon č. 101/2000 Sb. upravuje v § 46 odst. 1 liberační důvod, jehož naplněním se pachatel správního deliktu může odpovědnosti zprostit. Účastník řízení tedy za správní delikt neodpovídá, jestliže prokáže, že vynaložil veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránil. Posuzování naplnění liberačního ustanovení je přitom závislé vždy na konkrétních okolnostech daného případu a nelze jej předem jakkoliv zobecnit (při současném respektování limitu vyjádřeného v § 2 odst. 4 správního řádu).

Důkazní břemeno se přitom přenáší na účastníka řízení a je to on, kdo musí k prokázání liberace navrhovat důkazy (srov. Mates P. a kolektiv: Základy správního práva trestního, 3. vydání, Praha: C. H. Beck, 2002, str. 12; dále také § 52 správního řádu).

Správní orgán tedy na základě shora uvedeného posuzoval jednání účastníka řízení z hlediska ustanovení § 46 odst. 1 zákona č. 101/2000 Sb. Správní orgán v této souvislosti uvádí, že vynaložení veškerého úsilí, které bylo možno požadovat, neznamená jakékoliv úsilí, které správce vynaloží, ale musí se ve vztahu ke každému, konkrétně posuzovanému případu, jednat o úsilí maximálně možné, které je správce objektivně schopen vynaložit (zákon používá kritérium veškeré úsilí,

které bylo možno požadovat, a nikoliv např. spravedlivě požadovat, požadovat s ohledem na poměry atp.).

Přes tvrzení účastníka řízení, že neshledal v daném případě selhání jeho systémů, či interních technicko-organizačních bezpečnostních mechanismů a že se jednalo o typický případ selhání jednotlivce, přijal účastník řízení dodatečná nápravná opatření, jak vyplývá z jeho vyjádření ze dne 28. června a 18. července 2016, která mají zamezit dalšímu úniku osobních údajů, což významně podporuje závěr správního orgánu týkající se neaplikovatelnosti liberačního ustanovení, který bude popsán níže. Správní orgán však tuto skutečnost posoudil jako polehčující okolnost.

Správní orgán po zhodnocení výše uvedeného dospěl k závěru, že v případě účastníka řízení § 46 odst. 1 zákona č. 101/2000 Sb. nelze aplikovat. V daném případě je správní orgán názoru, že se ze strany účastníka řízení nejednalo o vynaložení maximálně možného úsilí k ochraně osobních údajů, tj. zabránění porušení jeho právní povinnosti spočívající v zabezpečení zpracovávaných údajů; vnitřní předpisy přijaté účastníkem řízení, stanovení přístupových práv k osobním údajům zákazníků a do systému účastníka řízení včetně vymezení pravidel pro export dat na externí média zaměstnanci účastníka řízení, nelze považovat v daném případě za dostatečné. Vyústěním uvedených skutečností pak bylo ohrožení osobních údajů jeho zákazníků, které byly následně odcizeny zaměstnancem účastníka řízení, tak, jak bylo popsáno výše.

K vyjádření účastníka řízení ve vztahu k plnění povinností dle zákona č. 127/2005 Sb. správní orgán uvádí, že jejich výklad není předmětem tohoto správního řízení.

Podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. se právnická osoba jako správce dopustí správního deliktu tím, že při zpracování osobních údajů nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů. V daném případě účastník řízení svým jednáním naplnil rovněž kvalifikovanou skutkovou podstatu správního deliktu podle § 45 odst. 2 písm. a) zákona č. 101/2000 Sb., který stanoví, že právnická osoba jako správce nebo zpracovatel osobních údajů se dopustí správního deliktu tím, že při zpracování osobních údajů některým ze způsobů podle § 45 odst. 1 téhož zákona ohrozí větší počet osob svým neoprávněným zasahováním do soukromého a osobního života. Ze spisového materiálu je patrné, že došlo k ohrožení osobních údajů v databázi účastníka řízení, která v době, kdy došlo k incidentu vyvolanému zaměstnancem účastníkem řízení ([redacted]), obsahovala údaje více než jednoho milionu zákazníků – fyzických osob. Na základě výše uvedeného považuje správní orgán za nepochybné, že při zpracování osobních údajů ohrozil účastník řízení větší počet osob (svých zákazníků) neoprávněným zasahováním do jejich soukromého a osobního života v souvislosti s přijetím nedostatečných opatření k zabezpečení jejich osobních údajů.

Podle § 46 odst. 2 zákona č. 101/2000 Sb. se při rozhodování o výši pokuty přihlíží k závažnosti, způsobu, době trvání, následkům protiprávního jednání a k okolnostem, za nichž bylo protiprávní jednání spácháno. Správní orgán v souladu s tímto ustanovením při stanovení výše pokuty vycházel z následujících skutečností.

Při stanovení výše sankce bylo z hlediska závažnosti jednání přihlédnuto jako k přitěžující okolnosti k rozsahu osobních údajů, které byly protiprávním jednáním účastníka řízení ohroženy. V případě, že by takový rozsah údajů skutečně získaly k volné dispozici třetí subjekty, mohli být lidé, o jejichž osobní údaje se jednalo, vystaveni velmi obtěžujícím situacím spočívajícím s největší pravděpodobností v opakovaném obtěžování nabídkami zboží či služeb. Nelze však vyloučit ani závažné zneužití těchto osobních údajů například pro uzavření různého typu smluv, bez vědomí dotčených subjektů údajů.

Počet dotčených subjektů údajů (ke dni 30. června 2016 se jednalo o 1 193 497 zákazníků – fyzických osob) správní orgán nevyhodnotil jako přitěžující ani polehčující okolnost. Správní orgán má za to, že kvalifikovaná skutková podstata správního deliktu obsažená v § 45 odst. 2 písm. a) zákona č. 101/2000 Sb. je naplněna v případě, že jsou protiprávním jednáním dotčeny řádově statisíce subjektů údajů. V případě účastníka řízení se jedná více než o jeden milion osob; takový počet v rámci uvedené skutkové podstaty nelze považovat za dostatečný na to, aby byl posouzen jako přitěžující okolnost, ale současně přesahuje množství, které by bylo možno považovat za okolnost polehčující.

Způsob protiprávního jednání účastníka řízení správní orgán nevyhodnotil jako přitěžující ani polehčující okolnost. Účastník řízení se správního deliktu dopustil jednáním, které je popsáno ve výroku tohoto rozhodnutí, tj. nepřijetím dostatečných opatření k zabezpečení osobních údajů, což je v zásadě obvyklý způsob, kterým je zákon č. 101/2000 Sb. porušován.

Stejně tak nehodnotil správní orgán jako přitěžující ani jako polehčující okolnost dobu, po kterou nepřijal účastník řízení účinná opatření k zabezpečení osobních údajů obsažených v databázi zákazníků, a to z toho důvodu, že ji není možné přesně určit. Doba protiprávního jednání se totiž v zásadě shoduje s dobou, po kterou měl účastník řízení nastavena bezpečnostní opatření právě takovým způsobem, který následně umožnil, aby došlo k předmětnému bezpečnostnímu incidentu. Vymezení uvedené ve výroku tohoto rozhodnutí je proto vymezení minimální, které se s reálnou dobou protiprávního jednání ani nemůže shodovat.

K okolnostem protiprávního jednání usoudil správní orgán následovně. Jako polehčující okolnost posoudil správní orgán to, že účastník řízení přijal opatření, aby se daná situace již neopakovala, když provedl kontrolu systému a nastavených procesů a přijal opatření k zajištění dodatečné nápravy závadného stavu, tj. omezení zápisu zákaznických dat na externí média zaměstnanci, opětovné proškolení zaměstnanců. Jako významnou polehčující okolnost pak hodnotil správní orgán množství a charakter přijatých opatření k zabezpečení zpracovávaných osobních údajů, která však, jak bylo opakovaně uvedeno, nebyla dostatečná a ve svém důsledku nezabránila odcizení osobních údajů. Za polehčující okolnost je třeba z hlediska okolností protiprávního jednání považovat i to, že ztráta dispozice nad předmětnými údaji byla přímým následkem trestné činnosti zaměstnance účastníka řízení.

Vzhledem k uvedenému byla stanovena sankce v dolní polovině zákonné sazby, která činí 10.000.000 Kč.

Při rozhodnutí o uložení povinnosti uhradit náklady řízení správní orgán vycházel z ustanovení § 79 odst. 5 správního řádu, který správnímu orgánu ukládá povinnost uložit paušální částkou náhradu nákladů řízení účastníkovi, který řízení vyvolal porušením své právní povinnosti, a z § 6 odst. 1 vyhlášky č. 520/2005 Sb., o rozsahu hotových výdajů a ušlého výdělku, které správní orgán hradí jiným osobám, a o výši paušální částky nákladů řízení, kterou se stanoví paušální částka nákladů správního řízení ve výši 1.000 Kč.

S ohledem na výše uvedené, bylo rozhodnuto, jak je uvedeno ve výroku tohoto rozhodnutí.

Poučení: V souladu s § 152 odst. 1 správního řádu lze u oddělení správních činností Úřadu pro ochranu osobních údajů proti tomuto rozhodnutí podat ve lhůtě 15 dnů ode dne doručení rozhodnutí rozklad předsedkyni Úřadu pro ochranu osobních údajů.

Rozhodnutí je doručeno 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 rozhodnutí do datové schránky.

Praha, 10. srpna 2016

otisk
úředního
razítka

Vanda Foldová
vedoucí oddělení správních činností