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-02463/19-3

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 15. července 2019 v souladu s § 150 odst. 1 zákona č. 500/2004 Sb., správní řád, tento příkaz:

I. Je prokázáno, že účastník řízení: [redacted] fyzická osoba podnikající dle živnostenského zákona, se sídlem [redacted], jako správce osobních údajů osob zaregistrovaných na internetové adrese [redacted] podle čl. 4 bodu 7 nařízení (EU) 2016/679,

1. tím, že neuzavřel od 28. prosince 2018 do přesně nezjištěné doby smlouvu o zpracování osobních údajů se společností [redacted] se sídlem [redacted] a s [redacted] jako zpracovateli osobních údajů podle čl. 4 bodu 8 nařízení (EU) 2016/679,

   porušil čl. 28 odst. 3 nařízení (EU) 2016/679, tedy povinnost, že zpracování zpracovatelem se řídí smlouvou nebo jiným právním aktem podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce,

2. a dále tím, že nejméně od 28. prosince 2018 do 30. prosince 2018 nezajistil osobní údaje cca [redacted] subjektů údajů, hráčů internetové online hry provozované na internetové adrese [redacted] a to v rozsahu uživatelské jméno, heslo v zašifrované podobě, telefonní číslo, e-mailová adresa, IP adresa a informace uvedené v databázi pro platby (aktuální stav platby, počet zakoupené virtuální měny, jméno účtu, ze kterého byla platba vytvořena, čas a způsob platby), v důsledku čehož

mimo jiné došlo ke zveřejnění těchto údajů na internetové adrese [redacted] a to dne 30. prosince 2018 po dobu cca 1 h 30 minut,

porušil zásadu zpracování osobních údajů 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 („integrita a důvěrnost“),

II. za což se mu podle čl. 83 odst. 5 písm. a) nařízení (EU) 2016/679 ukládá

pokuta ve výši 25.000 Kč
(slovy dvacet pět 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 účastníka řízení, konstantní symbol 1148.

Odůvodnění

Podkladem pro vydání tohoto příkazu je protokol o kontrole čj. UOOU-00011/19-20 ze dne 23. dubna 2019 pořízený podle nařízení (EU) 2016/679 Úřadem pro ochranu osobních údajů (dále jen „Úřad“) a spisový materiál shromážděný v rámci kontroly vedené u účastníka řízení od 30. ledna 2019 do 14. května 2019.

Ze shromážděného spisového materiálu vyplývá, že dne 31. prosince 2018 Úřad obdržel ohlášení porušení zabezpečení osobních údajů, které bylo doplněno dne 1. a 25. ledna 2019 a 4. února 2019, od [redacted] jako provozovatele online hry dostupné na [redacted] (dále jen jako [redacted]).

Následně na to dne 3. ledna 2019 Úřad obdržel podnět [redacted] který uvedl, že nahlašuje únik dat ze serveru [redacted] K tomu uvedl, že na tomto serveru měl účet a spolu s databází uniklo např. jeho telefonní číslo, e-mailová adresa, ID a heslo včetně podrobností o jeho platbách. [redacted] uvedl, že majitelem serveru je podle jeho názoru [redacted] a provozovatelem je [redacted] Dále uvedl, že mu nepřijde dostatečné, jak byli hráči o úniku informováni, jelikož byli jen upozorněni, že si mají změnit heslo. Následky, jako například ztracené e-mailové adresy, zneužití informací o platbách a jejich osobních údajích, nebyly nikde uvedeny. Na závěr uvedl, že ho obtěžují telefonáty z neznámých telefonních čísel, které jsou důsledkem úniku dat.

Ze spisového materiálu, zejména z ohlášení zabezpečení osobních údajů, jeho doplnění a z protokolu z ústního jednání a místního šetření ze dne 19. března 2019 vyplývá, že účastník řízení je provozovatelem herního serveru [redacted], který provozoval se svým společníkem [redacted]. [redacted] vystupuje ve vztahu k [redacted] jako společník ve vedení projektu, a to jako osoba samostatně výdělečně činná. [redacted]. Zpracovatelská smlouva

nebyla uzavřena, neboť jiné zpracovatele nikdy nepoužívali a veškeré osobní údaje zpracovávají pouze oni. Herní server [redacted] poskytuje hráčům možnost si zahrát hru, kde si zaregistrovaný uživatel vytvoří virtuální postavu, kterou postupem času zdokonaluje.

Účastník řízení uvedl, že hra [redacted] byla účastníkem řízení a jeho společníkem [redacted] provozována od 28. srpna do 31. prosince 2017. Následně byl celý projekt přerušen, hra byla zastavena, server byl vypnutý a databáze smazána, neboť oba společníci začali pracovat na nové verzi hry, která měla být spuštěna dne 28. prosince 2018. Účastník řízení uvedl, že první útoky neznámého útočníka (vystupujícího pod přezdívkou [redacted]) začaly dne 28. prosince 2018 ve večerních hodinách v podobě DDoS útoků, nikoliv útoků na databázový server. Účastník řízení uvedl, že hned večer po útoku se pokusili vylepšit své zabezpečení proti útokům v podobě lepšího filtrování na své stránce za pomoci služeb CloudFlare a dále byl na webový server nainstalován packet filter. Následně na to dne 29. prosince 2018 proběhl další DDoS útok, při kterém se útočníkovi podařilo opět vyřadit jejich služby. Po zahájení útoku se přihlásil útočník (prostřednictvím komunikační platformy Discord), který účastníka řízení vyzval k zaplacení částky 300 euro prostřednictvím služby PayPal. Tato platba měla sloužit jako výkupné, po jehož zaplacení útočník přislíbil účastníku řízení zastavení DDoS útoků a zajištění ochrany hracího serveru. Účastník řízení uvedl, že po tomto nátlaku souhlasili se zaplacením požadované částky, aby útoky ustály. Podle doloženého záznamu z platformy Discord byla částka 300 euro účastníkem řízení zaplacena ve dvou splátkách.

Následující den, tj. 30. prosince 2018, probíhala další komunikace mezi účastníkem řízení a útočníkem, opět prostřednictvím platformy Discord, neboť proběhl další útok, který hru [redacted] zpomalil, a v tomto případě už zaútočil na jejich databázový server a zveřejnil jejich databázi. Ze spisového materiálu vyplývá, že není vyloučeno, že se jednalo o stejného útočníka, ale pod jiným pseudonymem, pravděpodobně [redacted] Účastník řízení se tak obrátil na prvního útočníka [redacted], neboť mu předchozího dne zaplatil požadovanou částku a součástí dohody byla dohoda o poskytnutí firewallu, a vyzval ho, aby pomohl ochránit herní web [redacted]. [redacted] poskytl účastníku řízení soubory, které měly být nahrány do zdrojového kódu na herním webu [redacted]. Účastník řízení uvedl, že tyto soubory nejdříve prověřil a následně nahrál do zdrojového kódu stránek. Takto upravený zdrojový kód byl skutečně odolnější vůči DDoS útokům, avšak zároveň obsahoval tzv. backdoor, který byl skrytě umístěn v obrazovém souboru (soubor typu shell). V tomto zakódovaném souboru byl umístěn skript, který byl nahrán na jejich web, a tím bylo možné zaútočit na databázový server, který byl v tu dobu s webovým serverem propojený. Tento skript nebyl při prověření souboru účastníkem řízení odhalen. Pomocí tohoto skriptu útočník [redacted] vyslal přes herní web [redacted] příkaz, s jehož pomocí získal databázi účastníka řízení, neboť kvůli správnému fungování musí být herní web [redacted] propojen s databází hráčů. Do databázového serveru mohl přistupovat samotný herní server (localhost), který odtud čerpal veškerá data ke správnému fungování hry, dále webový server (IP), který zde získával data pro funkcionalitu služeb poskytovaných na webové stránce (registrace, přihlášení, změna údajů), a nakonec samotný správce serveru pouze ze své domácí IP adresy. Z poslední komunikace mezi účastníkem řízení a [redacted] prostřednictvím platformy Discord vyplývá, že [redacted] byl s největší pravděpodobností zároveň útočníkem pod pseudonymem [redacted].

Účastník řízení dále uvedl, že v databázi pro platby byl uveden pouze aktuální stav platby, počet zakoupené virtuální měny, jméno účtu (UserID), ze kterého byla platba vytvořena, čas a způsob platby. Nenacházely se zde žádné informace o peněžních transakcích, bankovních

účtech či jiných platebních metodách, které bylo možné na jejich stránce využívat. K tomu uvedl, že veškeré údaje o platbách zpracovává společnost [redacted] Pro správný průběh zakoupení virtuálních předmětů použije uvedená společnost údaje pouze v rozsahu User-ID a e-mailová adresa. Žádné jiné přístupy k datům společnosti neposkytují. V příloze zaslal část smlouvy s touto společností, kdy podpisem této smlouvy souhlasili s pravidly a podmínkami uvedenými na internetové adrese [redacted] O úniku databáze se účastník řízení dozvěděl tak, že útočník přesměroval herní web [redacted] na svůj web ([redacted]), na kterém bylo uvedeno, že na [redacted] byl proveden útok. Zveřejněná databáze byla dostupná cca 1,5 hodiny.

K počtu účtů účastník řízení uvedl, že do doby úniku databáze měl účastník řízení [redacted] účtů, každý účet však není individuální osoba. První hráči se registrovali dne 28. prosince 2018 (předchozí databáze první verze hry byla smazána). [redacted] K tomu účastník řízení uvedl, že praxe je taková, že každý hráč má většinou dva účty a není proto možné přesně říct, kolika konkrétních osob se únik týkal, zároveň ale platí, že za 24 hod. se protočilo cca [redacted] lidí. [redacted] Veškeré tyto údaje jsou nezbytné pro funkcionalitu jejich služeb. Účastník řízení uvedl, že je možné založit i více účtů pro stejnou e-mailovou adresu a uživatelé toho využívali pro lepší přístup ke svým účtům a jednodušší správě. Z tohoto důvodu je číslo unikátních uživatelů o něco nižší než odhadované číslo. Účastník řízení dále uvedl, že přímý přístup k databázovému serveru měl pouze hlavní technik [redacted] a automatický systém (webové stránky) pro správnou funkcionalitu služeb. Tento přístup nebyl povolen žádné třetí straně. Byl zde nastaven IP firewall, který pouštěl pouze IP adresu [redacted] a IP adresu webu (hostingu). Z tohoto důvodu útočníkovi stačilo se nabourat do webu, který měl automaticky přístup do databáze, jiným způsobem totiž není možné, aby hra fungovala. Logování přístupu bylo, ale logy odpovídaly pouze IP adrese [redacted] a webu.

Je možné, že uživatelé používali podobné nebo stejné údaje i u jiných herních portálů nebo e-mailových adres, i přesto, že každý uživatel byl při registraci upozorněn, aby použil unikátní údaje, a to upozorněním při registraci nového účtu *„Použijte jiné přihlašovací údaje, pokud hrajete i na dalších serverech.“* Účastník řízení uvedl, že veškeré informace o hráčích byly uloženy v databázi, která se nacházela na serveru v [redacted] u poskytovatele [redacted], tedy u společnosti [redacted] se sídlem [redacted], [redacted] se kterou žádná smlouva o pronajímání serverů neexistuje, neboť byla uzavřena registrací a odsouhlasením obchodních podmínek, ve kterých uživatel pouze souhlasí s podmínkami při registraci svého účtu (viz [redacted]). Dle účastníka řízení se server v [redacted] nacházel z důvodu ceny a jeho nájemcem byl on sám.

K informování hráčů o úniku databáze účastník řízení uvedl, že komunikace s hráči probíhá ve většině případů na facebookové stránce, kde ihned po útoku vydali prohlášení o úniku jejich dat. Podle názoru účastníka řízení dle dosahu příspěvků s oznámením o úniku dat lze usoudit, že se tato zpráva dostala ke všem uživatelům, neboť je zde větší dosah než jen vůči hráčům. Hráče upozornili, že je žádají, aby si změnili některá hesla, že byli cílem útoku a následného zveřejnění databáze. Dále tuto událost oznámili ve své místnosti na komunikační platformě Discord. Informace byla hráčům poskytnuta během pár minut, neboť útočník se účastníkovi řízení „pochlubil“.

Účastník řízení dále uvedl, že jejich herní i databázový server je od doby útoku vypnutý, přerušilo se napojení webu k databázi, stránky byly vypnuty a hrací server byl též vypnut. Od hostingu účastník řízení odešel, ale předtím si stáhl databázi. Šifrovaná databáze, kterou nelze bez hracího serveru rozšifrovat, je uložena u [redacted] K tomu účastník řízení dodal, že jejich prioritou je vyřešit veškeré vzniklé problémy se samotným útokem, proto zatím žádné přímé opatření neprováděli. Tato opatření budou řešit při případném opětovném spuštění serveru. Aktuálně tak veškeré své služby pozastavili, tj. web odpojili a ihned po zjištění upozornili jejich uživatele o úniku dat, kontaktovali Úřad a Policii České republiky. Kontaktovali také [redacted] majitele konkurenčního herního serveru, který má v tomto odvětví lepší zkušenosti než oni, který jim byl nápomocen při řešení problémů a při zjišťování způsobů, které útočník využil k útoku na jejich databázový server, a poskytl jim další doporučení včetně některých částí zabezpečení. Počet registrovaných uživatelů od doby, kdy je server vypnutý, neroste. Toto opatření bylo učiněno, aby nebylo možné zneužívat údaje, útočník s nimi nemohl nadále manipulovat a aby nedošlo k dalšímu poškození či útokům na tyto stránky. Účastník řízení uvedl, že mezi jejich návrhy na opatření po této události patří úplné odstranění nebo zašifrování telefonních čísel a taktéž šifrování e-mailových adres. Dále pracují na účinnějším zabezpečením webového serveru, jako je například přesunutí serverů k novému poskytovateli, který nabízí účinnější ochranu proti DDoS útokům, a samozřejmě kompletní přeinstalování a nastavení webových stránek a webového serveru. Účastník řízení uvedl, že veškerá svá data mají zálohovaná a v případě obnovení projektu jsou schopni je obnovit v plném rozsahu.

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. Účastník řízení tak nepochybně zpracovával při provozování své online hry osobní údaje jednotlivých hráčů v rozsahu uvedeném ve výroku tohoto příkazu, neboť tyto informace je možné zcela zjevně vztáhnout ke konkrétním subjektům údajů.

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 podnikatelské činnosti v souvislosti

s provozováním online hry dostupné na [redacted] nepochybně zpracovával osobní údaje registrovaných hráčů, neboť je shromažďoval, ukládal a používal.

Dále je nezbytné uvést, že účastník řízení je správcem osobních údajů hráčů smyslu čl. 4 bodu 7 nařízení (EU) 2016/679, neboť v rámci své podnikatelské činnosti určil účel a prostředky zpracování osobních údajů, tedy provozování online hry.

K výroku 1 tohoto příkazu správní orgán uvádí, že společnost [redacted] byla ve vztahu k účastníku řízení na základě výše uvedených skutečností v postavení zpracovatele osobních údajů ve smyslu čl. 4 bodu 8 nařízení (EU) 2016/679, neboť databáze s osobními údaji hráčů byla uložena na serveru, který si od této společnosti účastník řízení pronajímal. Ze spisového materiálu vyplývá, že smlouva o pronájmu serveru byla uzavřena registrací a přistoupením k obchodním podmínkám. Účastník řízení zpracovatelskou smlouvu mezi ním a uvedenou společností nedoložil.

Dále ze spisového materiálu vyplývá, že [redacted] je společníkem účastníka řízení, který byl v celém projektu [redacted] technikem a z povahy této činnosti musel mít v době úniku osobních údajů přístup k databázi obsahující osobní údaje hráčů, neboť IP firewall pro přístup do databáze byl nastaven tak, aby do ní mohl přistoupit pouze [redacted] (jeho IP adresa) a IP adresa hracího webu. Dále je nutné uvést, že [redacted] měl v držení databázi hráčů i v průběhu kontroly. Též [redacted] byl tedy na základě výše uvedených skutečností v postavení zpracovatele osobních údajů ve smyslu čl. 4 bodu 8 nařízení (EU) 2016/679.

K tomu správní orgán uvádí, že zpracovatelská smlouva podle č. 28 odst. 3 nařízení (EU) 2016/679 musí mít dle čl. 28 odst. 9 uvedeného nařízení písemnou formu, za kterou se považuje i forma elektronická. Čl. 28 odst. 3 nařízení (EU) 2016/679 dále stanoví povinné náležitosti tohoto typu smlouvy. Zpracovatelská smlouva tak musí obsahovat předmět a dobu zpracování osobních údajů, povahu a účel zpracování, vázanost doloženými pokyny správce, mlčenlivost, možnost/nemožnost řetězení zpracovatelů a další ustanovení, která jsou v čl. 28 odst. 3 nařízení (EU) 2016/679 specifikována.

Ze spisového materiálu vyplývá, že smlouva s požadovanými náležitostmi s [redacted] uzavřena nebyla a vše se dělo na základě ústní dohody.

Na základě výše uvedeného lze shrnout, že účastník řízení jako správce osobních údajů v rámci své podnikatelské činnosti využíval zpracovatele osobních údajů ve smyslu čl. 4 bodu 8 nařízení (EU) 2016/679. Těmito zpracovateli byli společnost [redacted] a [redacted] Správní orgán má přitom za prokázané, že smlouva o zpracování osobních údajů ve smyslu čl. 28 odst. 3 nařízení (EU) 2016/679 mezi správcem a zpracovateli osobních údajů uzavřena nebyla, čímž došlo k porušení tohoto ustanovení.

K výroku 2 tohoto příkazu správní orgán uvádí, že účastník řízení je jako správce osobních údajů zaregistrovaných hráčů ve smyslu čl. 4 bodu 7 nařízení (EU) 2016/679 povinen dodržovat veškeré relevantní povinnosti stanovené tímto nařízením pro zpracování osobních údajů. Jedna z těchto povinností je vyjádřena v zásadě integrity a důvěrnosti stanovené v čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679, podle které musí být osobní údaje 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. Na tuto zásadu pak navazuje čl. 32 odst. 1 nařízení (EU) 2016/679, dle kterého 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, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku.

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.

V tomto případě účastník řízení zpracovával osobní údaje registrovaných hráčů, které ukládal na serveru v [redacted] který si pronajímal od společnosti [redacted]. Z vyjádření účastníka řízení vyplývá, že přímý přístup k databázovému serveru měl pouze hlavní technik v postavení zpracovatele osobních údajů [redacted] a automatický systém (webové stránky) pro správnou funkcionalitu služeb. Dále ze spisového materiálu vyplývá, že ihned po prvním útoku dne 28. prosince 2018 se účastník řízení pokusil vylepšit zabezpečení proti útokům v podobě lepšího filtrování na své stránce za pomoci služeb Cloudflare a dále byl na webový server nainstalován packet filter. To však nezabránilo dalšímu DDoS útoku, který proběhl dne 29. prosince 2018 a který opět vyřadit služby účastníka řízení. Následně účastník řízení přistoupil na přislib útočníka na zajištění ochrany hracího serveru. Útočník proto poskytl účastníku řízení soubory, které měly být nahrány do zdrojového kódu na herním webu. Tyto soubory účastník řízení, dle svého vyjádření, nejdříve prověřil a následně nahrál do zdrojového kódu stránek. Takto upravený zdrojový kód byl odolnější vůči DDoS útokům, avšak zároveň obsahoval tzv. backdoor; v zakódovaném souboru byl umístěn skript, který byl nahrán na jejich web a tím bylo možné zaútočit na databázový server, který byl s webovým serverem propojený. Pomocí tohoto skriptu útočník vyslal skrz herní web [redacted] příkaz, s jehož pomocí získal databázi účastníka řízení.

Správní orgán k výše uvedenému uvádí, že tím, že účastník řízení přijal nabízené řešení ochrany od osoby, která DDoS útoky provedla, celou situaci z hlediska ochrany osobních údajů nepřijatelně podcenil. Svým jednáním zásadním způsobem přispěl ke vzniku bezpečnostního incidentu, tj. ke krádeži databáze, neboť útočník, který DDoS útoky provedl, se k hráčské databázi účastníka řízení dostal pomocí ukrytého souboru v řešení, které od něj účastník řízení převzal.

Účastník řízení tedy porušil čl. 32 odst. 1 písm. b) nařízení (EU) 2016/679, podle kterého správce provede vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku, včetně schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování; neboť nezajistil odolnost systémů, a toto pochybení následně vedlo k porušení zabezpečení osobních údajů a zveřejnění hráčské databáze prostřednictvím internetu.

Nad rámec shora uvedeného správní orgán k přijatým bezpečnostním opatřením uvádí, že po útoku dne 30. prosince 2018 přerušil účastník řízení spojení mezi herním webem a databází, vypnul hrací server a webové stránky [redacted]. Následně na to účastník řízení stáhl svoji

databázi od zpracovatele osobních údajů, společnosti [redacted], a uložil ji u zpracovatele osobních údajů [redacted]

K porušení zabezpečení osobních údajů tedy správní orgán uvádí, že účastník řízení nepřijal taková opatření, která by dokázala zabránit porušení důvěrnosti u jím zpracovávaných údajů. V souvislosti s tím je nutné odkázat i na čl. 24 nařízení (EU) 2016/679, který zakládá odpovědnost správce osobních údajů za veškeré zpracování osobních údajů a ukládá mu povinnost zavést vhodná technická a organizační zabezpečení, jejichž cílem je provádět zpracování osobních údajů v souladu s celým nařízením (EU) 2016/679.

Na základě výše uvedeného má správní orgán za prokázané, že účastník řízení, jako správce osobních údajů, porušil zásadu zpracování osobních údajů stanovenou v čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679, neboť nezajistil náležité zabezpečení jím zpracovávaných osobních údajů.

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.

Podle čl. 83 odst. 3 nařízení (EU) 2016/679 pokud správce nebo zpracovatel úmyslně či z nedbalosti u stejných nebo souvisejících operací poruší více ustanovení tohoto nařízení, nesmí celková výše správní pokuty překročit výši stanovenou pro nejzávažnější porušení. Správní orgán tak aplikuje tzv. absorpční zásadu, v jejímž rámci musel posoudit porušení kterého ustanovení je nejzávažnější. Dospěl přitom k závěru, že je jím v tomto konkrétním případě porušení čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679, neboť se jedná o jednu ze základních zásad pro zpracování osobních údajů, které je nutno vnímat jako nejdůležitější principy určující, jak může správce s osobními údaji nakládat. Za porušení této základní zásady dle čl. 83 odst. 5 nařízení (EU) 2016/679 lze uložit správní pokutu až do výše 20 000 000 EUR, jedná-li se o podnik, až do výše 4 % z celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, které hodnota je vyšší.

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 počtu dotčených subjektů údajů. Okolností zvyšující závažnost je pak nepochybně postup účastníka řízení po prvních útocích, jehož součástí bylo zaplacení neznámé osobě za ukončení jejích útoků a (a to zejména) za údajné zvýšení zabezpečení online hry. Tento postup přitom přímo vedl k porušení zabezpečení, které spočívalo v odcizení osobních údajů hráčů a jejich zveřejnění prostřednictvím internetu. Dále správní orgán přihlédl, jako k okolnosti zvyšující závažnost jednání, že došlo k porušení více povinností. Současně však správní orgán při rozhodování o uložení sankce a její výši, jako k okolnosti snižující závažnost jednání, přihlédl k tomu, že účastník řízení učinil kroky směřující k následnému zabezpečení zpracování osobních údajů a současně činil kroky, jejichž cílem bylo informovat dotčené subjekty údajů a poučit je, jak mají dále postupovat. Po souhrnném zhodnocení všech okolností byla pokuta

uložena při samé dolní hranici sazby, kterou nařízení (EU) 2016/679 stanoví a která 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 účastník řízení porušil povinnosti specifikované ve výroku tohoto příkazu, 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 15. července 2019

otisk
úředního
razítka

Vanda Foldová
ředitelka odboru dozoru