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-00163/19-3

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

I. Je prokázáno, že účastník řízení: , ,

IČO: jako správce osobních údajů osob zaregistrovaných na internetové adrese podle čl. 4 bodu 7 nařízení (EU) 2016/679,

1. tím, že neuzavřel s (od přesně nezjištěné doby nejméně do 11. června 2018) a (od 20. dubna 2018 nejdéle do 25. května 2018) jako zpracovateli osobních údajů podle čl. 4 bodu 8 nařízení (EU) 2016/679 smlouvu o zpracování osobních údajů,

   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 21. dubna 2018 do 25. května 2018 nezajistil osobní údaje nejméně subjektů údajů, hráčů internetové online hry provozované na internetové adrese , a to v rozsahu hráčské jméno, heslo k hernímu účtu, ID herního účtu, e-mailová adresa a IP adresa, v důsledku čehož mimo jiné došlo ke zveřejnění těchto údajů na internetové adrese , a to pravděpodobně 24. nebo 25. května 2018 po dobu cca 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 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 účastníka řízení, konstantní symbol 1148.

Odůvodnění

Podkladem pro vydání tohoto příkazu je protokol o kontrole čj. UOOU-06122/18-24 ze dne 16. listopadu 2018 pořízený podle nařízení (EU) 2016/679 inspektorem Úřadu pro ochranu osobních údajů (dále jen „Úřad“) Ing. Josefem Vaculou a spisový materiál shromážděný v rámci kontroly vedené u účastníka řízení od 8. srpna 2018 do 14. listopadu 2018.

Ze shromážděného spisového materiálu vyplývá, že dne 26. května 2018 Úřad obdržel od účastníka řízení , jako provozovatele online hry dostupné na ohlášení porušení zabezpečení osobních údajů. Tuto hru je možné popsat jako tzv. RPG hru (role-playing game), kdy každý hráč ovládá svou postavu, vylepšuje její vlastnosti, nakupuje, vyměňuje či vylepšuje vybavení své postavy, obchoduje a střetává se s jinými hráči, resp. jejich postavami.

Ve svém ohlášení účastník řízení uvedl, že se jedná o internetovou online hru, kde lidé mají veřejné ID, dále mají své heslo a e-mailovou adresu, které jsou neveřejné, a to za účelem potvrzování úkonů na svém uživatelském účtu. K tomu dodal, že databáze je více než měsíc stará a kroky, které vedly k tomu, aby se nic podobného neopakovalo, byly zavedeny. Podle jeho názoru šlo o zneužití pravomoci programátora. Účastník řízení uvedl, že k úniku databáze na veřejnost došlo v pátek dne 25. května 2018 ve večerních hodinách a podle jeho názoru jsou důsledky porušení zabezpečení osobních údajů dost možná nulové a o nic závažnějšího se nejedná, ale i tak nechtěl nic ponechat náhodě, neboť je možné například využití e-mailů pro spam, reklamu apod. K heslům uvedl, že i když byl každý uživatel při registraci srozuměn s tím, že má používat heslo, které nikde jinde nepoužívá a má mít určitou úroveň, tak nepochybně někdo použil stejné heslo, které má i na jiných účtech. Dále popsal opatření, která jako správce osobních údajů přijal nebo navrhl k přijetí s cílem vyřešit porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů, a to, že

K tomu dodal, že v budoucnosti po případném najímání programátorů již budou opatření, kde budou mít všichni značně omezené přístupy. Na závěr účastník řízení uvedl, že zabezpečení bylo již předtím na vysoké úrovni,

neboť byly ošetřeny přístupy pouze z povolených IP adres, avšak nepředpokládal zneužití přímo ze strany programátora, což byla chyba.

Téhož dne Úřad obdržel podnět doplněný dne 6. června 2018, který uvedl, že z webového portálu unikla databáze, jejímž provozovatelem je K tomu uvedl, že databázi viděl a nachází se v ní údaje uživatelů jako je e-mailová a IP adresa a z tohoto důvodu provozovatele kontaktoval. V doplnění svého podnětu uvedl, že tento případ nechce řešit a dodal, že databáze již není nikde dostupná, na odkazu, kde se nacházela, byla pouze několik hodin a dle statistik je tam pouze pár zobrazení, což zmenšuje počet osob, které to mohly vidět. K tomu upřesnil, že by se mělo jednat okolo neunikátních a unikátních účtů. Na závěr uvedl, že provozuje obdobnou hru a ze zkušenosti ví, že si hráči jako uživatelé vytváří více účtů.

Dne 10. srpna 2018 bylo Úřadu doručeno vyjádření účastníka řízení, ve kterém mimo jiné uvedl, že v souvislosti se zabezpečením osobních údajů byly dodrženy všechny ustanovení nařízení (EU) 2016/679 a podle jeho názoru nedošlo k žádnému porušení, neboť osobní údaje svých hráčů chrání a o všem je vždy informují. K tomu dodal, že v tomto případě šlo o trestný čin programátora který zneužil svých pravomocí a stáhl si data, které pak poslal konkurenci, kdy v současné době celý případ řeší policie. K uvedl, že měli mezi sebou uzavřenou smlouvu o dílo (smlouvu o zhotovení webových stránek). K dané věci dodal, že oznámení o úniku databáze bylo učiněno na facebookové stránce ve formě příspěvku, kde mají jejich hráči největší dosah, a dále po přihlášení na samotný portál kde byl uživatel seznámen s tím, co se stalo, a to formou odkazu k videu s doporučením změny uživatelského hesla. Každý, kdo se od té doby přihlásil, byl tedy s tímto únikem obeznámen, to je přibližně uživatelských účtů. Dále uvedl, že je nutné brát v potaz i to, že lidé porušují pravidla hry, se kterými souhlasí při registraci, a vytváří v některých extrémních případech i padesát účtů na osobu a tím jsou ve hře určitým způsobem zvýhodněni vůči ostatním. K tomu dodal, že i když na serveru v době úniku bylo až účtů, reálně unikátních uživatelů nebyla ani polovina, tj. až účtů. K rozsahu osobních údajů uvedl, že únik se týkal pouze e-mailové adresy, hesla k uživatelskému účtu a IP adresy. Dále uvedl, že nemá žádné zaměstnance a opatření k zajištění ochrany byly provedeny ve formě kdy se ke svým údajům na stránkách dostane pouze jejich majitel a člověk s daty z uniklé databáze by se k více osobním údajům nedostal. Pokud jde o to, kde a jak došlo k tomuto incidentu, účastník řízení uvedl, že den, kdy programátor získal údaje, neznají a ani znát nemohou, neboť pracoval na stránkách více jak dva týdny, a mohlo se to stát kdykoliv, protože v rámci jeho pracovní činnosti byl nutný přístup přímo do databáze. Na závěr účastník řízení uvedl, že na konkurenční server databáze unikla prostřednictvím neznámého pachatele dne 25. června 2018 a dostalo se k ní jen omezené množství lidí (asi 5 lidí k ní mohlo mít přístup). Byla zveřejněna přibližně po dobu třiceti minut. Ke svému vyjádření přiložil smlouvu o dílo (smlouvu o zhotovení webových stránek) uzavřenou mezi ním a dne 20. dubna 2018, která se týkala zhotovení webových stránek, a dále Oznámení o skutečnostech nasvědčujících tomu, že byl spáchán trestný čin ze dne 9. srpna 2018, ze kterého vyplývá, že podal trestní oznámení na programátora , u kterého vzniklo podezření na odcizení databáze, kterou potřeboval pro zhotovení webových stránek.

Z úředního záznamu o úkonech v rámci kontroly ze dne 14. srpna 2018 vyplývá, že Úřad provedl ve smyslu § 3 zákona č. 255/2012 Sb., o kontrole (kontrolní řád), zkušební registraci

na herním portálu ze dne 13. srpna 2018. V rámci provedené zkušební registrace bylo zjištěno, že se nelze zaregistrovat bez odsouhlasení *„Zpracování dat a osobních údajů“*. Dále při odsouhlasení všech podmínek byl na zkušební e-mailovou adresu zaslán potvrzující e-mail pro dokončení registrace, tedy ověření e-mailu. Políčka: *„Souhlasím s VOP a Pravidly hry“*, *„Souhlasím se Zpracováním dat a osobních údajů“* a *„Jsem starší 16 let“* nebyla dopředu zaškrtnuta.

Účastníkovi řízení byla zaslána žádost o součinnost ze dne 15. srpna 2018, na kterou odpověděl dopisem doručeným Úřadu dne 28. srpna 2018. Na dotaz, zda může sdělit podrobnou informaci týkající se herního portálu jak ke dni úniku databáze, tak ke stávajícímu stavu ve vztahu ke společnosti se sídlem , IČO: především pak vysvětlením, jakou roli měla tato společnost v době úniku dat, účastník řízení uvedl, že v době úniku dat nehrála společnost , žádnou roli, neboť byla založena až dne 11. června 2018 a herní portál na tuto společnost přepsali o několik dní později. Na dotaz, kdo byl správcem osobních údajů ke dni úniku databáze a proč bylo související trestní oznámení učiněno i přesto, že je účastník řízení jednatelem, účastník řízení uvedl, že trestní oznámení podal , jelikož je spolumajitelem, vznikla daným jednáním škoda a bylo jedno, kdo podává trestní oznámení. K tomu účastník řízení dodal, že bylo lepší, když trestní oznámení podal neboť mu neznámý pachatel smazal jeho osobní záložní disk, který byl připojen k serveru. K trestnímu oznámení účastník řízení uvedl, že jej nebylo možné podat přímo na , protože neměli žádné přímé důkazy, a z tohoto důvodu ho podal s podezřením na . Dále byl účastník řízení dotázán, jaká byla přijata opatření ve smyslu čl. 32 nařízení (EU) 2016/679 ve vztahu ke zhotoviteli, programátorovi . Účastník řízení uvedl, že před únikem databáze byl zamezen přístup, avšak pravděpodobně si údaje stáhl, dále přešli na nové počítače, do kterých již neměl absolutně žádný přístup, byla K dotazu, zda může sdělit přesné datum úniku databáze, vzhledem k tomu, že ve svém vyjádření účastník řízení uvedl datum úniku databáze 25. června 2018, které je zjevně nesprávné, neboť ohlášení případu porušení zabezpečení osobních údajů bylo učiněno dne 26. května 2018, účastník řízení uvedl, že si spletl měsíc, kdy byla data zveřejněna, nezná však přesný čas, ale ví jistě, že to bylo mezi 24. a 25. květnem 2018. Domnívá se však, že to bylo těsně před půlnocí z 24. na 25. květen 2018, jelikož neznámý pachatel to podle jeho názoru udělal schválně těsně před platností nového nařízení (EU) 2016/679. K dotazu, kdy byla programátorovi udělena přístupová práva a v jakém rozsahu, účastník řízení uvedl, že byla přístupová práva udělena dne 21. dubna 2018 bohužel v plném rozsahu, jelikož potřeboval tvořit nové tabulky apod. Účastník řízení byl vyzván k doložením e-mailové komunikace s uživatelem e-mailové adresy která měla být přílohou trestního oznámení, dále k doložení dokumentů týkajících se pravidel hry, obchodních podmínek, reklamačního řádu a zpracování dat a osobních údajů, případně dalších dokumentů vztahujících se k zabezpečení osobních údajů, ve znění účinném ke dni 26. května 2018. Účastník řízení přiložil požadované dokumenty ke svému vyjádření s tím, že bohužel ke dni 26. května 2018 jejich zálohy nemá, ale byly téměř stejné s rozdílem vlastníka.

Dle protokolu z ústního jednání a místního šetření ze dne 25. října 2018 účastník řízení uvedl, že mají společně s online hru, a to původně pouze na identifikační číslo účastníka řízení. V průběhu dubna 2018 najali programátora , který pro ně

měl zhotovit webovou aplikaci, jako doplněk ke hře. V rámci jeho pracovní náplně mu zpřístupnili celou svou databázi, a to na plný přístup k serveru ve kde jsou uloženy soubory ke hře a databáze hráčů, která obsahuje hráčské jméno, heslo, e-mail (slouží pro ověření registrace herního účtu) a IP adresu. Z tohoto serveru podle názoru účastníka řízení získal údaje, které mu umožnily přístup k osobnímu cloudovému úložišti , které mu poskytuje společnost k čemuž došlo v květnu 2018. K tomu účastník řízení dodal, že než byla databáze zpřístupněna na internetu zjistili, že se asi tak od dubna jednotlivým hráčům

) a zároveň provedli změny v administraci přístupu k úložišti ve a to tak, že toto úložiště bylo přístupno pouze jemu a Účastník řízení dále uvedl, že poté, co byl takto zamezen přístup k úložišti ve neznámý pachatel odcizil zálohu databáze hráčských účtů ze soukromého cloudového úložiště a tato databáze byla následně zveřejněna na internetu. O tomto byli informováni prostřednictvím konkurenčních herních serverů s tím, že dne 24. května 2018 byla databáze nahrána na server Herním serverům byla databáze zpřístupněna přes anonymní účet, a tak se mohla dále šířit. Proto účastník řízení provedl nahlášení data breach.

V další fázi ústního jednání byly účastníku řízení položeny konkrétní dotazy, kdy na dotaz, jaký je jeho vztah ke společnosti , kdy byla tato společnost založena, zda provozuje online hru dostupnou na , kdy se stal herní portál majetkem společnosti a jakou roli hraje v této společnosti, účastník řízení odpověděl, že společnost založili společně (s pozn. správního orgánu) v červnu roku 2018 a oba jsou zde jednatelé. Online hra dostupná na je od července roku 2018 ve vlastnictví společnosti , Na dotaz, zda mají přesně zjištěno, kdy došlo ke ztrátě dat jejich zákazníků (hráčů), účastník řízení odpověděl, že přesné datum odcizení dat neví. Je možné že se tak stalo v průběhu cca jednoho měsíce, kdy měl jimi najatý programátor přístup k jejich datům. Dne 24. května 2018 byla data nahrána na sever

úniku dat se dozvěděli prostřednictvím konkurenčních serverů, kterým byla data zpřístupněna přes anonymní účet, a tyto o úniku dále informovaly. Na dotaz, jakým způsobem, kdy a kde informovali hráče o úniku dat, účastník řízení uvedl, že vložili na facebookovou stránku hry video s oznámením o tom, co se stalo, a také s doporučením, jakým způsobem zabezpečit své údaje i vůči jiným serverům, kde využívají stejné přihlašovací údaje. Dále únik dat oznámili každému jednotlivému hráči při jeho přihlášení do hry. Taktéž přijali protiopatření, (

). Na dotaz, jakým způsobem a kde uchovávali osobní údaje jednotlivých hráčů, kdo a za jakých podmínek měl k těmto údajům přístup, zda prováděli logování přístupu k těmto osobním údajům, zda mají doložené IP adresy přístupů do odcizené databáze a zda ví, komu dané IP adresy patří, účastník řízení odpověděl, že

). Přístup k údajům měli pouze oni dva s tím, že se mohl přihlásit pouze ze svého počítače a toto povolení dále udělil programátorovi . Logování přístupu do serveru a databáze neprováděli. Na dotaz, že na základě jejich vyjádření, že před samotným únikem dat, za který je dle jejich názoru odpovědný , již byl zamezen přístup do jejich databáze a pravděpodobně, ještě v době neomezeného přístupu tato data získal, zda mají o takovém přístupu a získání dat nějaké záznamy (logy apod.), a proč mu zamezili v přístupu, účastník řízení odpověděl, že k omezení přístupu došlo z toho důvodu, že hráčům začaly mizet věci ze hry. Cílem bylo, aby administrátorský přístup k serveru získali pouze oni dva. Hráčská hesla byla v otevřené formě, toto však již teď není. Na dotaz, v jakém rozsahu měl přístup do jejich databáze, účastník řízení uvedl, že měl plný přístup, protože ho potřeboval pro svoji práci a potřeboval zjistit, jaké ID hráče má na sebe napsané, jaké věci ve hře a toto potřeboval pro webovou aplikaci, kterou vytvářel jako doplněk ke hře. K tomu dodal, že je však pravdou, že heslo k jednotlivým hráčským účtům nepotřeboval. Na dotaz, zda provedli po zjištění úniku dat nějaká nápravná opatření, popřípadě jaká, jaký měla tato opatření dopad a jak mají provedeno nastavení zabezpečení v současné době, účastník řízení uvedl, že v současné době je

K tomu dodal, že ve chvíli, kdy jeho práci odstranili, tak přestalo docházet . Na dotaz, zda zjistili od doby prvního úniku dat nějaké další pokusy o odcizení dat, účastník řízení uvedl, že již ne a od té doby je klid. Na dotaz, jaké soubory přesně se nacházely na jejich záložním disku, zda obsahovaly osobní údaje a pokud ano, zda mají uzavřenou smlouvu se zpracovatelem osobních údajů (tedy se společností u které byly data z jejich záložního disku uložena), účastník řízení odpověděl, že se jednalo o celou databázi a serverové soubory hry a šlo o zálohy. K tomu uvedl, že se společností byla uzavřena smlouva souhlasem s podmínkami a zaplacením pronájmu úložiště a totožně taktéž ve . Na dotaz, komu byl a komu je nyní poskytován dedikovaný server ve , a kdo platí za pronájem tohoto serveru, účastník řízení uvedl, že za pronájem platil ale v současné době je server placen společností . Na dotaz, zda účastník řízení měl s uzavřenou zpracovatelskou smlouvu, účastník řízení uvedl, že zpracovatelská smlouva nebyla uzavřena s tím, že v současné době je záložní server u společnosti který jen stále v osobním vlastnictví a společnost nemá s uzavřenou zpracovatelskou smlouvu.

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 hráčské jméno, heslo k hernímu účtu, ID herního

účtu, e-mailová adresa a IP adresa, neboť tyto informace je možné zcela zjevně vztáhnout ke konkrétnímu subjektu 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 vytvářel databázi registrovaných hráčů obsahující jejich osobní údaje a nepochybně je tak zpracovával, neboť je shromažďoval, zaznamenal, uložil a taktéž zpřístupnil třetím subjektům, tj. programátorovi za účelem vytvoření doplňující aplikace ke hře.

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

K výroku 1 tohoto příkazu správní orgán uvádí, že byl od přesně nezjištěné doby na základě výše uvedených skutečností v postavení zpracovatele osobních údajů ve smyslu čl. 4 bodu 8 nařízení (EU) 2016/679, neboť pro účastníka řízení osobní údaje hráčů ukládal na dedikovaný server ve a následně, za účelem zajištění souladu s čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679, prováděl zálohu tohoto serveru na cloudové úložiště u společnosti ; tyto společnosti tak byly dalšími zpracovateli. Z hlediska nařízení (EU) 2016/679 se tak jedná o tzv. řetězení zpracovatelů ve smyslu čl. 28 odst. 2. K tomu správní orgán uvádí, že řetězení zpracovatelů osobních údajů není nařízením (EU) 2016/679 obecně zakázáno, je však vyžadováno, aby k tomu dal správce osobních údajů souhlas. Vzhledem k výše popsaným vztahům jednotlivých zainteresovaných subjektů na tvorbě online hry dostupné na má správní orgán za prokázané, že použití dedikovaného serveru ve a cloudového úložiště od společnosti a. s., se dělo s plným vědomím účastníka řízení jako správce osobních údajů. Zároveň je však třeba upozornit na skutečnost, že využití dalšího zpracovatele osobních údajů je dle čl. 28 odst. 2 nařízení (EU) 2016/679 podmíněno „předchozím konkrétním nebo obecným písemným povolením správce“.

Dále 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.

Vzhledem ke skutečnosti, že byl nejméně do 10. června 2018, kdy vznikla společnost , v postavení zpracovatele osobních údajů ve smyslu čl. 4 bodu 8 nařízení (EU) 2016/679, neboť byl fyzickou osobu, která zpracovávala osobní údaje pro správce osobních údajů, měla mezi ním a účastníkem řízení být uzavřena smlouva o zpracování

osobních údajů ve smyslu čl. 28 odst. 3 nařízení (EU) 2016/679. Ze spisového materiálu však vyplývá, že výše uvedená smlouva s požadovanými náležitostmi uzavřena nebyla.

Pokud se jedná o vztah účastníka řízení a programátora , ten se v rámci své činnosti smluvně zavázal pro správce osobních údajů vykonat činnost, jejíž součástí bylo též zpracovávat osobní údaje, které mu byly účastníkem řízení zpřístupněny. S těmito osobními údaji provedl sérii operací, jejichž cílem bylo provázat online hru dostupnou na s doplňkovou aplikací. Byl tak též v postavení zpracovatele osobních údajů ve smyslu čl. 4 bodu 8 nařízení (EU) 2016/679. Na základě výše uvedeného správní orgán konstatuje, že měla být s jako zpracovatelem osobních údajů uzavřena zpracovatelská smlouva ve smyslu čl. 28 odst. 3 nařízení (EU) 2016/679. V této souvislosti je nutné odkázat na smlouvu o dílo uzavřenou dne 20. dubna 2018 mezi účastníkem řízení a , která však postrádá ustanovení, která by bylo možné považovat za zpracovatelskou smlouvu; jinou smluvní dokumentaci účastník řízení nepředložil.

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 a , se kterými měla být uzavřena zpracovatelská smlouva. Správní orgán má 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, jak je uvedeno výše, účastník řízení byl (od přesně nezjištěné doby nejméně do 10. června 2018, kdy vznikla společnost , která začala následně online hru provozovat) správcem osobních údajů hráčů zaregistrovaných na internetové adrese ve smyslu čl. 4 bodu 7 nařízení (EU) 2016/679 a jako takový byl 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 (ukládal) osobní údaje na dedikovaném serveru ve který byl v pronájmu zpracovatele osobních údajů . Z vyjádření účastníka řízení vyplývá, že byl přístup na tento dedikovaný server umožněn pouze účastníku řízení a jeho společníkovi a zároveň zpracovateli osobních údajů . Data včetně

osobních údajů byla za účelem zajištění bezpečnosti a obnovitelnosti osobních údajů z tohoto dedikovaného serveru ukládána na soukromé cloudové úložiště , které si tento zpracovatel osobních údajů pronajímal od společnosti Dále je nutné uvést, že za účelem vytvoření webové aplikace, která měla být doplňkem k online hře dostupné na , byla uzavřena smlouva o dílo mezi správcem osobních údajů a programátorem Za účelem vytvoření aplikace byla databáze na dedikovaném serveru ve zpřístupněna i tomuto programátorovi v plném rozsahu, neboť bez přístupu k této databázi nemohla být webová aplikace vyhotovena a s online hrou dostupnou na provázána. Sám účastník řízení však uvedl, že programátor ke své činnosti nepotřeboval hesla k jednotlivým hráčským účtům, která mu však byla též zpřístupněna a která byla uchovávána v otevřené formě.

Po provedení výše uvedených bezpečnostních opatření, která účastník řízení přijal po prvních bezpečnostních incidentech, přestalo docházet
online hry dostupné na a přístup na dedikovaný server ve byl obnoven pouze pro účastníka řízení a Následně na to se neznámý pachatel „naboural“ do soukromého cloudového úložiště zpracovatele osobních údajů . Účastník řízení uvedl, že: „

“. Jak již bylo uvedeno výše, na tomto soukromém úložišti se zálohovala data, včetně osobních údajů hráčů online hry dostupné na Následně na to byla neznámou osobou databáze získaná na soukromém úložišti zpracovatele zveřejněna na

Správní orgán dále doplňuje, že po prvním bezpečnostním incidentu, u kterého není prokázáno, že se dotýkal zpracovávaných osobních údajů hráčů online hry dostupné na přijal účastník řízení bezpečnostní opatření, která zabránila dalším škodám na majetku hráčů online hry dostupné na Osobní údaje však nebyly odcizeny a získány ze serveru ve ke kterému měly přístup celkem tři osoby (účastník řízení, a), ale došlo k jejich ztrátě, resp. odcizení a následnému neoprávněnému zveřejnění ze soukromého cloudového úložiště zpracovatele osobních údajů K tomuto úložišti měl přístup pouze a na základě vyjádření účastníka řízení nejspíše i programátor na základě přístupu do dedikovaného serveru ve Je však nutné uvést, že konkrétní osoba, která neoprávněně vnikla do cloudového úložiště je v současné době v šetření orgánů činných

v trestním řízení a není pro účel správního řízení relevantní, neboť se jednalo o chybu, která mohla být zneužita jakýmkoli jiným vývojářem (zpracovatelem), kterému by účastník řízení umožnil neomezený přístup na server.

Z výše uvedeného vyplývá, že účastník řízení nepřijal taková opatření, která by byla dostatečně účinná, aby nemohlo dojít k nahodilému či neoprávněnému přístupu k osobním údajům, neboť na dedikovaném serveru ve ukládal takové údaje (taková data) s jejichž pomocí bylo možné přistoupit do soukromého úložiště zpracovatele osobních údajů a v důsledku toho tak zálohované osobní údaje neoprávněně zpřístupnit na

K porušení zabezpečení osobních údajů dále správní orgán uvádí, že účastník řízení po uzavření smlouvy s programátorem nepřijal taková bezpečnostní opatření, která by dokázala zabránit nahodilé ztrátě osobních 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 tomu, že došlo k úniku osobních údajů nejméně hráčů, dotčených subjektů údajů. Dále správní orgán přihlédl, jako k okolnosti zvyšující závažnost jednání, že došlo k porušení více povinností. Dále 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 28. února 2019

otisk
úředního
razítka

Vanda Foldová
ředitelka odboru kontrolního