ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 111, fax: 234 665 444
posta@uoou.gov.cz, www.uoou.gov.cz

Čj. UOOU-01304/21-20

ROZHODNUTÍ

Úřad pro ochranu osobních údajů, jako příslušný správní orgán podle § 64 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů (dále jen „zákon o zpracování osobních údajů“) a podle čl. 58 odst. 2 písm. i) nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále jen „nařízení (EU) 2016/679“ nebo též „obecné nařízení o ochraně osobních údajů“), v řízení o přestupku vedeném podle zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, ve znění pozdějších předpisů (dále jen „zákon o odpovědnosti za přestupky“), a zákona č. 500/2004 Sb., správní řád, ve znění dalších předpisů (dále jen „správní řád“) rozhodl dne 20. května 2024 takto:

Společnost [redacted] (dále jen „obviněná“ nebo též „správce“):

I. Je vinna tím, že jako správce osobních údajů podle článku 4 odst. 7 nařízení (EU) 2016/679, od blíže nezjištěného data, v období nejméně do 15. dubna 2021, nepřijala dostatečná technická a organizační opatření pro zabezpečení osobních údajů uživatelů aplikace [redacted], neboť jako správce osobních údajů dostatečně nezabezpečila fotografie průkazů totožnosti a řidičských průkazů nahrávaných uživateli do této aplikace proti zneužití vhodným technickým opatřením, a to například alespoň opatřením vodoznaku,

   čímž obviněná ve formě minimálně nedbalosti naplnila skutkovou podstatu přestupku podle ustanovení § 62 odst. 1 písm. a) zákona o zpracování osobních údajů, neboť porušila povinnost stanovenou v článku 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, provede správce vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku.

II. Za tento přestupek se obviněné ukládá v souladu s článkem § 83 odst. 4 písm. a) obecného nařízení ochraně o osobních údajů

pokuta ve výši 106.000 Kč
(slovy sto šest tisíc korun českých)

a dále podle § 95 odst. 1 zákona č. 250/2016 Sb. a ustanovením § 6 odst. 1 vyhlášky 520/2005 Sb., o rozsahu hotových výdajů a ušlého výdělku, které správní orgán hradí jiným osobám, a o výši paušální částky nákladů řízení, ve znění vyhlášky č. 112/2017 Sb., povinnost nahradit náklady řízení ve výši 1.000 Kč.

Obě tyto částky jsou 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 obviněné, konstantní symbol 1148.

Odůvodnění:

Shrnutí průběhu řízení:

[1] Dne 11. března 2021 obdržel dozorový úřad od obviněné oznámení porušení zabezpečení osobních údajů podle článku 34 nařízení (EU) 2016/679. V tomto oznámení obviněná uvedla, že ji kontaktoval její klient [redacted] s tím, že se kdosi pokusil zneužít jeho osobní údaje (prostřednictvím společnosti [redacted] a tyto údaje mohly být získány z databáze obviněné, která provozuje službu aplikaci [redacted] Obviněná dále uvedla, že nemá dostatek informací, aby mohla potvrdit nebo vyloučit, že únik osobních údajů byl z její strany ani jestli se tento únik týká více klientů. Panu [redacted] obviněná doporučila, aby danou věc ohlásil Policii ČR.

[2] Dozorový úřad vydal dne 4. května 2021 písemnost „žádost o doplnění ohlášení porušení zabezpečení osobních údajů“ pod čj. UOOU-01304/21-2, kterou požádal obviněnou o doplnění, zda se v mezidobí objevily jakékoliv nové skutečnosti potvrzující či vyvracující domněnku neoprávněného zneužití osobních údajů klienta [redacted] z databáze obviněné. Dále dozorový úřad v této žádosti uvedl, že pokud se domněnka o zneužití osobních údajů obviněné potvrdila, požádal o popis konkrétních opatření, které obviněná přijala s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

[3] Dne 11. května 2021 obdržel dozorový úřad odpověď obviněné (evidována pod čj. UOOU -01304/21-3). V této písemnosti obviněná uvedla, že v dané věci poskytla součinnost Policii ČR při vyšetřování možného spáchání trestného činu. Obviněná uvedla, že stále nemá najisto potvrzeno, že k úniku osobních dat došlo z její databáze. K přijatým opatřením obviněná uvedla, že u ní proběhl interní audit všech PC zařízení a povolených přístupů do systému, jehož součástí bylo také zrušení přístupových práv všem uživatelům aplikace a jejich obnova při nastavení nových přístupových pravidel. Byla rovněž zahájena interní kontrola v rámci mateřské společnosti obviněné. Obviněná dále uvedla, že byla provedena interní kontrola u jejích dodavatelů, kteří mají do jejího systému přístup [redacted], kde žádné narušení nebylo zajištěno. Obviněná rovněž v této písemnosti uvedla, že pro případ obdobných možných útoků do systému byl zaveden další prvek ochrany těchto údajů – vodoznak, který je vkládán na veškeré ukládané informace/fotografie v systému (okamžitá realizace u nových klientů aplikace a postupné zavádění pro již existující klienty).

[4] Dne 3. června 2021 vydal dozorový úřad sdělení pod čj. UOOU-01304/21-4, kde uvedl, že posoudil povahu porušení zabezpečení, rizika pro subjekty údajů i přijatá opatření směřující ke zmírnění rizikovosti předmětného porušení zabezpečení pro subjekty údajů a neshledal systémové porušení správce při zpracování osobních údajů spočívající v nedodržení článku 32 obecného nařízení o ochraně osobních údajů, které by odůvodňovalo využití dozorových či nápravných opatření

[5] Dne 19. července 2021 zaslala obviněná dozorovému úřadu písemnost „porušení zabezpečení osobních údajů – oznámení“ ve kterém uvedla, že po vyhodnocení získaných informací dospěla k závěru, že došlo k porušení zabezpečení osobních údajů u 13 jejích klientů. Podle informací od klientů bylo zjištěno, že se jedná o totožný případ jako v případě [redacted], neboť tito klienti si měli údajně zřídit účet u společnosti [redacted] a uskutečnit nákup nebo pokus o něj mimo území České republiky. Klienti sami kontaktovali společnost [redacted], kterou jim bylo sděleno, že založené účtu byly založeny na základě zcizených osobních údajů (ve všech případech se jednalo o fotografii občanského průkazu – přední i zadní strany a selfie foto klienta). Společnost [redacted] měla klientům sdělit, že případnou vzniklou škodu nebude po nich požadovat k úhradě.

[6] Obviněná dále uvedla, že kontaktovala předmětné klienty a dospěla k závěru, že ke zneužití osobních údajů došlo pravděpodobně prostřednictvím její databáze někdy v prvním čtvrtletí roku 2021. Obviněná dále uvedla, že vzhledem k závažnému podezření získala od klientů souhlas k tomu, aby mohla kontaktovat společnost [redacted] a mohla porovnat fotografie ze své databáze s fotografiemi, na základě nichž byl zřízen účet u společnosti [redacted] Obviněná dále uvedla, že zahájila šetření v systému vlastní aplikace [redacted] s cílem zjistit, kdy a kde došlo k předpokládanému úniku údajů jejích klientů.

[7] Dne 8. září 2021 vydal dozorový úřad písemnost „ohlášení porušení zabezpečení osobních údajů – žádost o doplnění“ pod čj. UOOU-01304/21-6, ve které dozorový úřad požádal obviněnou o doplnění výsledků předmětného šetření, až je bude mít obviněná k dispozici. Dále dozorový úřad uvedl, že zjistí-li obviněná způsob, jakým došlo k zabezpečení osobních údajů, žádá o popis konkrétních opatření, které obviněná přijala s cílem vyřešit dané porušení zabezpečení osobních údajů včetně případných dalších opatření ke zmírnění možných nepříznivých dopadů.

[8] Dne 23. listopadu 2021 obviněná sdělila, že případ spočívající v možném trestném činu neoprávněný přístup k počítačovému systému a nosiči informací na základě jejího ohlášení prošetřuje Policie ČR pod čj. [redacted]

[9] Dne 4. května 2022 vydal dozorový úřad písemnost pod čj. UOOU-01304/21-8 nazvanou „výzva k doplnění ohlášení porušení zabezpečení osobních údajů“, kterou se dotázal obviněné, zda je jí znám výsledek vyšetřování orgánů činných v trestním řízení v dané věci.

[10] Dne 26. května 2022 obdržel dozorový úřad odpověď obviněné, v jejíž příloze bylo přiloženo usnesení Policie ČR čj. [redacted] Dále obviněná uvedla, že v rámci vnitřních kontrolních mechanismů prověřila přijatá opatření, o kterých informovala dozorový úřad dne 11. května 2021, které měly zabránit možnému neoprávněnému průniku. Opětovnou prověrkou bylo zjištěno, že po zavedení vnitřních kontrolních mechanismů a používaní prvků pasivní ochrany na všech zaslaných

dokumentech od klientů obviněná nezaznamenala žádný nový případ zneužití osobních dokladů svých klientů evidovaných v jejím systému.

[11] Z usnesení Policie ČR vedeného pod čj. [redacted] předně vyplývá, že se v dané věci jedná o trestných čin úvěrový podvod (podezření ze spáchání trestných činů podvod, neoprávněný přístup k počítačovému systému a nosiči informací a poškození cizích práv bylo odloženo). Vyšetřováním bylo zjištěno, že neznámý pachatel pronikl dosud nezjištěným způsobem do počítačového systému nebo jeho části obviněné (aplikace [redacted], kde získal osobní údaje klientů těchto služeb, konkrétně fotografie občanských průkazů, které následně použil ve 197 případech ke sjednání revolvingových úvěrů přes internet u společnosti [redacted], které mu byly ve 186 případech poskytnuty v celkové výši 2.998.540,28 Kč. V 11 případech mu úvěry poskytnuty nebyly. Získané prostředky použil pachatel k nákupům zboží v ČR, následně od 12. prosince 2020 pak v zahraničí, především v Ruské federaci. Z usnesení dále vyplynulo, že majetková újma vznikla pouze společnosti [redacted], která uvedla že po osobách, na které byly úvěry u ní sjednány, nebude škodu vymáhat. U 144 osob se fotografie klientů obviněné shodovaly s fotografiemi, na základě nichž byly založeny účty u společnosti [redacted] V dalších případech byly osobní údaje subjektů údajů získány jiným způsobem.

[12] Co se týče prošetření bezpečnostního incidentu, dozorový úřad ještě vyžádal od obviněné další vyjádření a sdělení dne 12. dubna 2023 (písemnost čj. UOOU -01304/21-11), přičemž uvedl následující:

1. Uveďte, zda jste v mezidobí od posledního incidentu dosud zaznamenali nové případy zneužití osobních údajů klientů.
2. Sdělte a doložte výsledky interního šetření, provedení testů a auditů vztahující se k bezpečnostnímu incidentu, a také výsledky zmiňovaných vnitřních kontrol u dodavatelů společnosti [redacted].
3. Uveďte a důkazně prokažte přesný rozsah osobních údajů klientů jakožto subjektů údajů, které v současnosti zpracováváte v rámci aplikace [redacted], a zároveň důkazně prokažte rozsah osobních údajů dotčených bezpečnostním incidentem.
4. Sdělte přesný počet subjektů údajů dotčených bezpečnostním incidentem a přesný počet subjektů údajů, kteří se na Vás obrátili s podezřením na zneužití osobních údajů, příp. ohledně jiných nepříznivých důsledků spojených s bezpečnostním incidentem.
5. Identifikujte zdroj vzniku bezpečnostního incidentu, resp. co mělo vliv na jeho vznik.
6. Objasněte Úřadu, jestli některý z dodavatelů služeb, zejména Vámi zmiňovaná společnost [redacted] (dále jen [redacted] poskytující společnosti [redacted], cloud pro ukládání elektronických dat, měla nebo mohla mít vliv na vznik bezpečnostního incidentu.
7. Předložte příslušnou smluvní dokumentaci upravující právní vztahy se společností [redacted]. („hlavní smlouva“), a související smlouvu o zpracování osobních údajů (není-li součástí hlavní smlouvy).
8. Uveďte a důkazně prokažte, jakým způsobem byla splněna ohlašovací povinnost ohlašovací povinnost o vzniku bezpečnostního incidentu vůči subjektům údajů ve smyslu čl. 34 nařízení (EU) 2016/679. V případě, že jste v době vzniku bezpečnostního incidentu neinformovali dotčené subjekty údajů o porušení ochrany osobních údajů, uveďte důvody, pro které nebyly informovány.
9. Doložte vnitřní předpisy vztahující se k bezpečnosti zpracování osobních údajů v době vzniku bezpečnostního incidentu a sdělte konkrétní bezpečnostní opatření, které mohli

danému incidentu zabránit. Zároveň uveďte a důkazně prokažte, zdali je už ukončena fáze postupného zavádění prvku ochrany v podobě vodoznaku na ukládaných informacích
/fotografiích, pro již existující klienty.

10. Sdělte, zdali jste v mezidobí přijali jakákoli nová bezpečnostní opatření ke zmírnění možného rizika vzniku bezpečnostního incidentu majícího za následek narušení integrity
a důvěrnosti dat a doložte vnitřní předpisy vztahující se k bezpečnosti zpracování osobních údajů v současnosti.
11. Uveďte případné další informace vztahující se k bezpečnostnímu incidentu, které považujete za relevantní pro objasnění příčin vzniku incidentu.

[13] Obviněná na výše uvedenou žádost reagovala písemností, jež byla dozorovému úřadu doručena dne 27. dubna 2023. V této písemnosti (stručně shrnuto) uvedla k výše uvedeným otázkám následující:

1. Obviněná uvedla, že nezaznamenala žádný nový incident zneužití osobních údajů.
2. Obviněná uvedla, že provedla kontrolu všech zařízení, ze kterých mohli či mohou zaměstnanci vstoupit do databáze klientů a nebyla zjištěna žádná podezřelá aktivita.
3. Obviněná uvedla, že zpracovává tyto osobní údaje klientů: Jméno, příjmení, datum narození, adresu bydliště, rodné číslo (je-li přiděleno), číslo mobilního telefonu, e-mailovou adresu, kopii dokladu totožnosti, kopii řidičského průkazu, fotografii/selfie, vízum (u cizinců), povolení k pobytu (u cizinců).
4. Obviněná uvedla, že z celkového počtu 197 osob zjištěných Policií ČR, jejichž osobní údaje byly zneužity, bylo 148 klientů obviněné; z nichž 12 bylo s různými odchylkami oproti údajům anebo podkladům v databázi.
5. Obviněné se nepodařilo určit zdroj bezpečnostního incidentu.
6. Nebylo prokázáno, že by některý z dodavatelů obviněné mohl mít vliv na vznik bezpečnostního incidentu.
7. Obviněná doložila smlouvu se společností  , která ji poskytuje cloudové úložiště, nemá však přístup do databáze.
8. Obviněná uvedla, že o bezpečnostním incidentu subjekty údajů neinformovala, neboť neměla informace, kterých subjektů údajů se bezpečnostní incident týká, to zjistila teprve ze seznamu od Policie ČR dne 9. listopadu 2021.
9. Obviněná uvedla, že měla v době bezpečnostního incidentu zavedenou směrnici o zpracování osobních údajů. Obviněná uvedla, že bezpečnostnímu incidentu mohlo zabránit označení fotografií dokladů tak, aby se nedaly použít k jinému účely, např. vodoznakem. Dále uvedla, že vodoznak je na nově dodané fotografie umísťován od 15. dubna 2021 a od konce dubna 2021 je umístěn i na fotografie dodané před tímto datem.
10. Obviněná uvedla, že krom uvedených kontrol a zavedení vodoznaku začala provádět kontroly oprávněnosti přístupů k údajům jednotlivých klientů pravidelně a jmenovala manažera pro ochranu osobních údajů.

[14] Dne 7. března 2024 vydal dozorový úřad písemnost „oznámení o zahájení řízení“ vedenou pod čj. UOOU-01304/21-15, kterou zahájil s obviněnou řízení o přestupku podle ustanovení § 62 odst. 1 písm. a) zákona č. 110/2019 Sb. v návaznosti na porušení povinnosti stanovené v článku 32 odst. 1 nařízení (EU) 2016/679.

[15] Dne 4. dubna 2024 obdržel od obviněné dozorový úřad vyjádření. V tomto vyjádření obviněná (stručně shrnuto) uvedla, že v období před 1. dubnem 2021 měla zavedena technická a organizační opatření k zamezení neoprávněného přístupu k osobním údajům svých klientů. Obviněná uvedla, že porušení zabezpečení dozorovému úřadu sama dne 11. března 2021 ohlásila. Po prvotním podezření z porušení zabezpečení začala obviněná zavádět změny a byla zavedena dodatečná opatření zvyšující zabezpečení fotografií subjektů údajů. Obviněná dále uvedla, že způsob úniku ani pachatele se nepodařilo zjistit a únik se týkal 148 subjektů údajů. Obviněná dále uvedla, že spolupracovala na vyšetřování s Policií ČR a od zavedení dodatečných opatření nedošlo k dalšímu porušení zabezpečení osobních údajů. Obviněná uvedla, že provedla další interní audit, který potvrdil, že dodatečná opatření k zabezpečení osobních údajů jsou dostatečná. S ohledem na vše výše uvedené obviněná navrhla, aby bylo řízení o přestupku zastaveno.

Právní rámec posuzovaných skutečností

[16] 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.

[17] 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.

[18] Dle čl. 4 odst. 7 je správcem fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.

[19] Zpracování osobních údajů musí být vždy v souladu se základními zásadami, které jsou zakotveny v čl. 5 nařízení (EU) 2016/679. Tyto zásady představují základní pravidla, od nichž se odvíjejí všechny procesy zpracování, a zároveň jsou též nejdůležitějšími principy, které správci určují, jak má s osobními údajů nakládat. Jednou z těchto zásad je zásada integrity a důvěrnosti stanovená v čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679, která stanoví, že osobní údaje musí být zpracovány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

[20] V článku 32 nařízení (EU) 2016/679 jsou stanoveny konkrétní požadavky na zabezpečení osobních údajů. Dle článku 32 odst. 1 nařízení (EU) 2016/679 správce, popř. zpracovatel musí s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu,

kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob provést vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku, případně včetně opatření uvedených pod písm. a) až d) tohoto článku.

Posouzení věci ze strany dozorového úřadu

[21] Obviněná je ve vztahu ke svým klientům – uživatelům aplikace [redacted] správcem osobních údajů ve smyslu článku 4 odst. 7 nařízení (EU) 2016/679. Osobní údaje ve smyslu článku 4 odst. 1 nařízení (EU) 2016/679, které obviněná zpracovávala, byly jméno, příjmení, datum narození, adresa bydliště, rodné číslo, mobilní telefon, e-mailová adresa, kopie (fotografie) dokladu totožnosti (obě strany), kopie (fotografie) řidičského průkazu (obě strany) a fotografie/selfie (s dokladem totožnosti); u cizinců pak kopii víza, povolení k pobytu uložené ke každému osobnímu účtu.

[22] Jak vyplynulo z šetření Policie ČR v dané věci, v době mezi 23. listopadem 2020 a 25. únorem 2020 se neznámý pachatel nezjištěným způsobem zmocnil osobních údajů nejméně 197 osob, jejichž prostřednictvím žádal o sjednání revolvingových úvěrů u společnosti [redacted], které mu byly ve 186 případech poskytnuty. Z tohoto počtu 197 osob bylo přibližně 144 osob klientů obviněné, neboť při registraci u společnosti [redacted]. byly použity fotografie dokladů, jejichž původ byl v databázi obviněné.

[23] Jak vyplynulo ze všeho výše uvedeného, fotografie/kopie dokladů subjektů údajů, které byly uloženy v databázi obviněné, nebyly nejméně do 15. dubna 2021 chráněny dostatečně proti zneužití k jinému účelu, např. prostřednictvím vodoznaku, což koneckonců připustila i obviněná mj. ve svém vyjádření ze dne 27. dubna 2023. Tento ochranný prvek obviněná zavedla dne 15. dubna 2021 u nových klientů a do konce měsíce dubna 2021 tímto prvkem opatřila fotografie svých stávajících klientů.

[24] Jak již bylo zmíněno výše, jednou ze základních zásad zpracování osobních údajů je zásada integrity a důvěrnosti definovaná v článku 5 odst. 1 písm. f) nařízení (EU) 2016/679, tedy 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. Tato zásada je dále rozvinuta v článku 32 odst. 1 nařízení (EU), kde je uvedeno, že 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, případně včetně: a) pseudonymizace a šifrování osobních údajů; b) schopnosti zajistit neustálou důvěrnost a integritu, dostupnost a odolnost systémů a služeb zpracování; c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů; d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování. V odst. 2 předmětného článku je pak uvedeno, že při posuzování vhodné úrovni bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

[25] Lze tedy konstatovat, že obviněná neměla v rozhodném období (od blíže nezjištěného data nejméně do 15. dubna 2021, kdy tato opatření dle svého vyjádření začala zavádět), dostatečně zabezpečeny proti zneužití fotokopie dokladů totožnosti a řidičských průkazů proti zneužití vhodným technickým prostředkem, ačkoliv riziko při zpracování takovýchto osobních údajů je vysoké, což se koneckonců ukázalo při následném narušení bezpečnosti, kdy tyto fotografie neznámý pachatel zneužil ke sjednání revolvingových úvěrů.

[26] S ohledem na výše uvedené má tedy dozorový úřad nade vši pochybnost za prokázané, že obviněná jako správce osobních údajů svých klientů porušila povinnost stanovenou v článku 32 odst. 1 nařízení (EU) 2016/679 a v návaznosti na to se dopustila přestupku podle ustanovení § 62 odst. 1 písm. a) zákona č. 110/2019 Sb.

K vyjádření obviněné

[27] K vyjádření obviněné, jež přijal dozorový úřad dne 4. dubna 2024, je nutno uvést, že co se zabezpečení osobních údajů pomocí technických a organizačních opatření týče, nejméně před 15. dubnem 2021 nebyly osobní údaje klientů obviněné zabezpečeny dostatečně (k tomuto se dozorový úřad vyjádřil výše). Pokud jde o to, že obviněná sama aktivně upozornila dozorový úřad na porušení zabezpečení a informovala 13 subjektů údajů, u kterých k němu mohlo dojít, je nutno uvést, že toto jsou zákonné povinnosti obviněné uvedené v článku 33 a 34 nařízení (EU) 2016/679 (a případně polehčující nebo přitěžující okolnosti ve smyslu článku 83 odst. 2 nařízení). Daným bezpečnostním incidentem vznikla škoda necelé 3.000.000 Kč (byť tato škoda nevznikla subjektům údajů, ale společnosti poskytující revolvingové úvěry, tj. společnosti [redacted] Vyšetřování Policie ČR prokázalo, že přibližně ¾ osobních údajů, které byly zneužity, pocházelo právě z databáze obviněné. Dozorový úřad tedy neshledal důvod pro zastavení řízení, jak navrhovala obviněná ve svém vyjádření. K ostatním okolnostem, zejména přijatým opatřením, se dozorový úřad vyjádřil níže (posouzení polehčujících a přitěžujících okolností).

Posouzení polehčujících a přitěžujících okolností

[28] V ustanovení článku 83 odst. 4 písm. a) nařízení (EU) 679/2016 je uvedeno, že za porušení článků 8, 11, 25 až 39, 42 a 43 lze uložit správní pokutu až do výše 10.000.000 EUR, nebo jedná-li se o podnik, až do výše 2 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší.

[29] V článku 83 nařízení (EU) 2016/679 je uvedeno, že každý dozorový úřad zajistí, aby ukládání správních pokut v souladu s tímto článkem ohledně porušení tohoto nařízení podle odstavců 4, 5 a 6 bylo v každém jednotlivém případě účinné, přiměřené a odrazující.
Správní pokuty se ukládají podle okolností každého jednotlivého případu kromě či namísto opatření uvedených v čl. 58 odst. 2 písm. a) až h) a j). Při rozhodování o tom, zda uložit správní pokutu, a rozhodování o výši správní pokuty v jednotlivých případech se řádně zohlední tyto okolnosti:

a) povaha, závažnost a délka trvání porušení s přihlédnutím k povaze, rozsahu či účelu dotčeného zpracování, jakož i k počtu dotčených subjektů údajů a míře škody, jež jim byla způsobena;

b) zda k porušení došlo úmyslně nebo z nedbalosti;

c) kroky podniknuté správcem či zpracovatelem ke zmírnění škod způsobených subjektům údajů;

d) míra odpovědnosti správce či zpracovatele s přihlédnutím k technickým a organizačním opatřením jimi zavedeným podle článků 25 a 32;

e) veškerá relevantní předchozí porušení správcem či zpracovatelem;

f) míra spolupráce s dozorovým úřadem za účelem nápravy daného porušení a zmírnění jeho možných nežádoucích účinků;

g) kategorie osobních údajů dotčené daným porušením;

h) způsob, jakým se dozorový úřad dozvěděl o porušení, zejména zda správce či zpracovatel porušení oznámil, a pokud ano, v jaké míře;

i) v případě, že vůči danému správci nebo zpracovateli byla v souvislosti s týmž předmětem dříve nařízena opatření uvedená v čl. 58 odst. 2, splnění těchto opatření;

j) dodržování schválených kodexů chování podle článku 40 nebo schváleného mechanismu pro vydávání osvědčení podle článku 42 a

k) jakoukoliv jinou přitěžující nebo polehčující okolnost vztahující se na okolnosti daného případu, jako jsou získaný finanční prospěch či zamezení ztrátám, přímo či nepřímo vyplývající z porušení.

[30] Povaha jednání obviněné spočívala v nedostatečném zabezpečení zpracování osobních údajů – v tomto případě fotografií průkazů totožnosti a řidičských průkazů. Vzhledem k tomu, že zneužití těchto osobních údajů bylo způsobilé vyvolat značný poruchový následek (zde spočívající v získání revolvingových úvěrů prostřednictvím úvěrového podvodu), považuje dozorový úřad toto porušení za velmi závažné. Trvání porušení bylo po dobu fungování aplikace obviněné až do dubna roku 2021; neznámý pachatel osobní údaje zneužíval k úvěrovému podvodu, jak bylo zjištěno Policií ČR, již někdy od podzimu roku 2020. Počet (zjištěných) dotčených subjektů byl 148. Výše způsobené škody byla vysoká, společnosti [redacted] vznikla škoda ve výši 2.998.540,28 Kč. Okolnost podle článku 83 odst. 2 písm. a) nařízení (EU) 2016/679 hodnotí dozorový úřad jako přitěžující.

[31] Jako polehčující okolnost hodnotí dozorový úřad okolnost podle článku 83 odst. 2 písm. b) nařízení (EU) 2016/679, neboť obviněná se daného jednání nedopustila úmyslně, ale ve formě nedbalosti. V daném případě se podle názoru dozorového úřadu jednalo o nedbalost vědomou.

[32] Subjektům údajů v daném případě nevznikla škoda, okolnost podle článku 83 odst. 2 písm. c) nařízení (EU) 2016/679 tedy dozorový úřad nehodnotil.

[33] Co se týče míry odpovědnosti správce s přihlédnutím k technickým a organizačním opatřením, je nutno uvést, že technická opatření byla v daném případě nedostatečná. Jak již zmínil dozorový úřad výše, zabezpečení fotografií pomocí vodoznaku není nijak nákladné ani technicky složité opatření. Tuto okolnost hodnotil dozorový úřad jako přitěžující (článek 83 odst. 2 písm. d) nařízení (EU) 2016/679).

[34] Obviněná doposud nebyla uznána vinnou z přestupku proti nařízení (EU) 2016/679, okolnost podle článku 83 odst. 2 písm. e) hodnotí dozorový úřad jako polehčující.

[35] Dále jako polehčující okolnost dozorový úřad hodnotil okolnost podle článku 83 odst. 2 písm. f) nařízení (EU) 2016/679, neboť obviněná s dozorovým úřadem spolupracovala a na písemnosti zaslané dozorovým úřadem včas a v dostatečném rozsahu reagovala.

[36] V daném případě nebyly dotčeny osobní údaje zvláštní kategorie ve smyslu článku 9 nařízení (EU) 2016/679, avšak osobní údaje, které daným porušením zabezpečení ohroženy byly, byly mimořádně citlivé (veškeré údaje z průkazů totožnosti a řidičských průkazů, na základě nichž si neznámý pachatel mohl sjednat revolvingový úvěr). Okolnost podle článku 83 odst. 2 písm. g) nařízení (EU) 2016/679 hodnotí dozorový úřad jako přitěžující.

[37] Jako polehčující okolnost dozorový úřad dále hodnotí okolnost podle článku 83 odst. 2 písm. h) nařízení (EU) 2016/679, neboť obviněná dozorovému úřadu ohlásila porušení zabezpečení, jakmile se o něm dozvěděla.

[38] Okolnosti podle článku 83 odst. 2 písm. i) a j) nařízení (EU) 2016/679 dozorový úřad nehodnotil, neboť obviněné nebylo uloženo dozorovým úřadem opatření ani není dozorovému úřadu známo, že by měla obviněná schváleny kodexy chování a schválené mechanismy pro vydávání osvědčení.

[39] K okolnostem podle článku 83 odst. 2 písm. k) nařízení (EU) 2016/679 dozorový úřad uvádí, že bylo vzato v úvahu, že k porušení zabezpečení došlo trestným činem neznámého pachatele, přičemž jak vyplynulo z šetření Policie ČR (viz usnesení Policie ČR založené ve spisovém materiálu), stalo se tak poměrně důmyslným a sofistikovaným způsobem a doposud není známo, jakým způsobem neznámý pachatel prolomil zabezpečení (nejen) obviněné. Tuto okolnost hodnotí dozorový úřad jako polehčující.

Stanovení sankce

[40] Za porušení povinnosti správce podle článků 8, 11, 25 až 39, 42 a 43 lze uložit správní trest pokuty až do výše 10.000.000 EUR, nebo jedná-li se o podnik, až do výše 2 % celkového celosvětového ročního obratu za předchozí rok, podle toho, která hodnota je vyšší. Čistý obrat obviněné za předchozí finanční rok byl  Kč, 2 % z této částky odpovídá částce nižší, než hodnota 10.000.000 EUR je tedy vyšší. Při určení výchozí částky pokuty tedy dozorový úřad vycházel z částky 10.000.000 EUR.

[41] K samotnému stanovení konkrétní výše pokuty dozorový úřad uvádí, že v jeho rámci byla zvažována řada výše uvedených kritérií podle článku 83 odst. 1, 2 nařízení (EU) 2016/679, přičemž současně byl zohledňován doporučený postup podle Pokynů Evropského sboru pro ochranu údajů 04/2022 o výpočtu správních pokut podle nařízení 2016/679 (dále jen „pokyny 4/2022“), a to zejména ve vztahu ke klasifikaci podle závažnosti porušení nařízení (EU) 2016/679 a k doporučenému postupu při určování výchozí částky pro výpočet pokuty.

[42] Podle výše zmíněných pokynů 04/2022 dozorový úřad vyhodnocoval, zda se v daném případě jednalo o porušení nízké, střední nebo vysoké úrovně závažnosti. Při posouzení míry závažnosti dozorový úřad posuzoval okolnosti podle článku 83 odst. 2 písm. a), b) a g). Vzhledem k tomu, že okolnosti podle zmíněného článku posoudil dozorový úřad v písm. a) jako přitěžující a v písm. b) jako polehčující a g) jako přitěžující, bylo dané porušení posouzeno jako střední úrovně závažnosti zejména s ohledem na okolnost pod písm. a) a též písm. g). U střední úrovně závažnosti dozorový úřad stanoví výchozí částku pro další výpočet pokuty ve výši 10 % až 20 % maximální zákonné sazby. S ohledem na zmíněné okolnosti stanovil dozorový úřad výchozí částku ve výši 17 % platné maximální sazby, tedy při spodní hranici určeného rozmezí, tedy ve výši 1.700.000 EUR.

[43] Dále dozorový úřad podle pokynů 04/2022 zvažoval další úpravu výchozí částky s ohledem na čistý roční obrat obviněné. U podniků s ročním obratem ≤ 10 milionů EUR může dozorový úřad zvážit úpravu od 0,2 % až do výše 0,4 % určené výchozí částky. Dozorový úřad s ohledem na výši obratu obviněné upravil výchozí částku pro výpočet pokuty na 0,3 % z již výše upravené výchozí částky, tedy konečnou výchozí částku pro výpočet pokuty stanovil dozorový úřad ve výši 5.100 EUR.

[44] Dozorový úřad následně hodnotil ostatní okolnosti podle článku 83 odst. 2 nařízení (EU) 2016/679. Okolnost podle písm. d) hodnotil dozorový úřad jako přitěžující a přikládá ji vyšší váhu, takže výchozí částku pokuty navýšil o 10 % (na 5.610 EUR). Okolnost podle písm. e) hodnotil dozorový úřad jako polehčující, přičemž ji přikládá nižší důležitost a výchozí částku snížil o 5 % (na 5.329,50 EUR). Okolnost podle písm. f) hodnotil dozorový úřad jako polehčující s tím, že ji přikládá nižší důležitost a výchozí částku snížil o 5 % (zaokr. na 5.063 EUR). Okolnost podle písm. h) hodnotil dozorový úřad jako polehčující s nižší důležitostí a částku dále snížil o 5 % (na 4.809,85 EUR). Okolnost podle písm. k) hodnotil dozorový úřad jako polehčující s vyšší důležitostí a částku dále snížil o 10 % (zaokr. na 4.328,87 EUR). Tato částka odpovídá podle kurzu ČNB (ke dni 15. května 2024) 24,710 Kč za 1 EUR, tedy 106.966 Kč, zaokrouhleno na celé tis. Kč dolů stanovil dozorový úřad výši peněžité pokuty na 106.000 Kč.

[45] Při rozhodnutí o uložení povinnosti uhradit náklady řízení správní orgán vycházel z § 95 odst. 1 zákona č. 250/2016 Sb., který správnímu orgánu ukládá uložit obviněné, která byla uznána vinnou, náklady řízení paušální částkou, 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, podle kterého paušální částka nákladů správního řízení, které obviněná vyvolala porušením své právní povinnosti, činí 1.000 Kč.

[46] Vzhledem ke všem výše uvedeným skutečnostem dozorový úřad rozhodl tak, jak je uvedeno ve výroku tohoto rozhodnutí.

Poučení:

V souladu s § 152 odst. 1 správního řádu lze u Úřadu pro ochranu osobních údajů proti tomuto rozhodnutí podat ve lhůtě 15 dnů ode dne doručení rozhodnutí rozklad předsedovi 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, 20. května 2024

Mgr. Eva Cupáková
vedoucí oddělení kontroly soukromého sektoru
(podepsáno elektronicky)