ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 555, fax: 234 665 444
e-mail: posta@uoou.cz, www.uoou.cz

Č.j. UOOU-08428/17-31
Praha 21. března 2018

Protokol o kontrole

Kontrolní orgán
Úřad pro ochranu osobních údajů, se sídlem 170 00 Praha 7 – Holešovice, Pplk. Sochora 727/27, IČ: 708 37 627 (dále jen „Úřad“)

Pravomoc kontrolního orgánu k výkonu kontroly vyplývá z § 2 odst. 2 a 3, § 29 odst. 1 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů;

Kontrolující
inspektor Úřadu MVDr. František Bartoš, držitel průkazu č. [redacted]
pověřený zaměstnanec Úřadu JUDr. Michal Jelínek, držitel průkazu č. [redacted]
pověřený zaměstnanec Úřadu Ing. Max Gůt, držitel průkazu č. [redacted]
pověřený zaměstnanec Úřadu Ing. Radek Loub, držitel průkazu č. [redacted]

Kontrolovaná osoba
[redacted] (dále jen „[redacted]“ nebo „Společnost“)

zastoupená
[redacted],

Místo provedení kontroly
sídlo kontrolované společnosti [redacted]
sídlo Úřadu, Pplk. Sochora 27, 170 00 Praha 7

Předmět kontroly
Předmětem kontroly je dodržování povinností správce osobních údajů stanovených zákonem č. 101/2000 Sb., při zpracování osobních údajů zákazníků kontrolované Společnosti, se zaměřením na dodržování povinností dle § 13 zákona č. 101/2000 Sb., v souvislosti s podezřením na neoprávněné zpřístupnění osobních údajů zákazníků Společnosti.

Zahájení kontroly

Kontrola byla zahájena dne 2. října 2017 doručením písemného Oznámení o zahájení kontroly, č.j. UOOU-08428/17-9, do datové schránky [redacted].

Posledním kontrolním úkonem předcházejícím vyhotovení protokolu o kontrole bylo písemné sdělení Policie ČR ze dne 27. února 2018.

Přehled podkladů

Protokol o kontrole se opírá o následující podklady, které byly pořízeny v průběhu kontroly a podklady, které byly kontrolnímu orgánu známy z jeho úřední činnosti:

1. Přípis společnosti [redacted] Oznámení o narušení bezpečnosti při správě osobních údajů ze dne 27. srpna 2017, č.j. UOOU-08428/17-1
2. Podnět na podezření z porušení povinností správce osobních údajů, e-mail stěžovatele ze dne 29. srpna 2017, č.j. UOOU-08428/17-4
3. Podnět na podezření z porušení povinností správce osobních údajů, e-mail stěžovatele ze dne 29. srpna 2017, č.j. UOOU-08428/17-6
4. Úřední záznam o vložení dokumentů ze dne 26. září 2017, č.j. UOOU-08428/17-8

[redacted]

5. Přípis Oznámení o zahájení kontroly ze dne 2. října 2017, č.j. UOOU-08428/17-9
6. Úřední záznam o podkladech analýzy podnětu ze dne 27. září 2017, č.j. UOOU-08428/17-10
7. Žádost právního zástupce [redacted] o změnu termínu ústního jednání a místního šetření, e-mail ze dne 13. října 2017, č.j. UOOU-08428/17-11 a kopie Plné moci, kterou [redacted] zmocňuje [redacted]
8. Potvrzení přijetí žádosti o změnu termínu ústního jednání a místního šetření ze dne 13. října 2017, e-mail č.j. UOOU-08428/17-12
9. Přípis – vyrozumění o změně termínu ústního jednání a místního šetření ze dne 16. října 2017, č.j. UOOU-08428/17-13
10. Úřední záznam o provedení kontrolního úkonu ze dne 26. října 2017, č.j. UOOU-08428/17-14, + přílohy:
    a) záznam o bezpečnostní události a výsledcích šetření ze dne 8. 9. 2017

b) interní předpis [redacted]
c) interní předpis [redacted]
d) interní předpis [redacted]

11. Zaslání Úředního záznamu právnímu zástupci společnosti [redacted] ze dne 31. října 2017, č.j. UOOU-08428/17-15
12. Přípis – sdělení o změně kontrolní skupiny ze dne 21. listopadu 2017, č.j. UOOU-08428/17-16
13. Pověření ke kontrole, IS ze dne 21. listopadu 2017, č.j. UOOU-08428/17-17
14. Přípis - Žádost o součinnost ze dne 18. prosince 2017, č.j. UOOU-08428/17-19
15. Přípis - Žádost o součinnost společnost Ulož.to cloud, a.s., ze dne 18. prosince 2017, č.j. UOOU-09428/17-20
16. Přípis - žádost právního zástupce společnosti [redacted] o prodloužení lhůty k poskytnutí součinnosti ze dne 20. prosince 2017, č.j. UOOU-08428/17-21
17. Přípis – Prodloužení lhůty k poskytnutí součinnosti ze dne 22. prosince 2017, č.j. UOOU-08428/17-22
18. Přípis - poskytnutí součinnosti společnosti [redacted] ze dne 8. ledna 2018
    a) plná moc právního zástupce společnosti [redacted] ze dne 25. srpna 2016, udělaná [redacted] i
    b) substituční plná moc, udělená advokátem [redacted], ze dne 19. září 2016

19. Žádost Obvodního soudu pro Prahu 7 ze dne 8. ledna 2018, č.j. 4C 13/2017 o informace o výsledcích kontroly společnosti [redacted]
20. Přípis – odpověď Obvodnímu soudu pro Prahu 7 ze dne 15. ledna 2018, č.j. UOOU-08428/17-25
21. Odpověď právního zástupce společnosti [redacted] na žádost o poskytnutí součinnosti ze dne 15. ledna 2018, č.j. UOOU-08428/17-26
22. Přípis – žádost o poskytnutí součinnosti společnost [redacted] ze dne 25. ledna 2018, č.j. UOOU-08428/17-27
23. Odpověď společnosti [redacted], na žádost o součinnosti ze dne 1. února 2018, č.j. UOOU-08428/17-28
24. Žádost o informaci zaslaná KŘ PČR ze dne 23. února 2018, č.j. UOOU-08428/17-29
25. Zpráva k žádosti o informaci KŘ PČR ze dne 27. února 2018, č.j. UOOU-08428/17-30

I. Kontrolní zjištění kontrolujících

A. Zjištěný skutkový stav

1. Dne 27. srpna 2017 obdržel Úřad od společnosti [redacted] písemnou informaci Oznámení o narušení bezpečnosti při správě osobních údajů. Obsahem sdělení je informace, že společnost [redacted] která v rámci svého předmětu podnikání provozuje internetovou nákupní galerii [redacted] oznamuje, že dne 25. srpna 2017 zaznamenala narušení bezpečnosti při správě osobních údajů. Dále sděluje,

že narušení se týká starší databáze uživatelských účtů z období před rokem 2015, konkrétně jde o databázi čítající [redacted] záznamů o zákaznících Společnosti v rozsahu e-mail, heslo, jméno, příjmení, telefonní číslo. Dále, že se jedná o uživatelské účty, které obsahovaly jednoduchá hesla, která neodpovídají bezpečnostním zásadám. V systémech užívaných Společností dochází k tzv. „hashování hesel“, kdy jsou hesla uložena v zakódované podobě. Dotčená databáze byla zakódována starším a dnes již nepoužívaným způsobem, který umožnil narušiteli jednodušší hesla rozkódovat. Od roku 2012 do roku 2016 Společnost zajišťovala bezpečnost hesel metodou [redacted] Od října roku 2016 jsou přístupové údaje chráněny [redacted] Používaná metoda byla v době jejího použití vždy obvyklým bezpečnostním standardem.

Společnost [redacted] dále sdělila, že k minimalizování následků narušení bezpečnosti, již podnikla následující kroky:

- reset hesel všech potenciálně ohrožených uživatelských účtů založených před [redacted]
- písemné informování dotčených subjektů osobních údajů prostřednictvím e-mailu o vzniklé situaci
- posílení centra zákaznické péče za účelem zodpovídání dotazů zákazníků

2. Kontrolovaná společnost [redacted] dne 27. srpna 2017 odeslala z e-mailové adresy [redacted] dvě elektronické zprávy, které byly adresovány cca [redacted] vlastním zákazníkům, a to:

První sdělení „Overeni vasi e-mailove adresy“. Text sdělení: „Dobrý den, je nám líto, ale musíme potvrdit, že došlo k narušení bezpečnosti Vašeho účtu a proto jsme Vám resetovali heslo. Váš účet na [redacted] to ale nijak nepoškodilo a všechny údaje s ním spojené zůstaly zachovány. Zároveň Vás tímto vyzýváme, pokud jste tak zatím neučinili, abyste si ke svému účtu nastavili nové heslo – jednoduše to můžete udělat [redacted]. Pro zvýšení bezpečnosti doporučujeme změnit heslo i na jiných webových stránkách, na kterých jste používali stejné heslo (jako jsou sociální sítě, jiné e-shopy a další weby). Více informací najdete v článku [redacted] a pokud máte další dotazy, neváhejte nás prosím kontaktovat – naši kolegové na zákaznické lince jsou připraveni Vám pomoct. Tým [redacted].“

V zápatí obsahuje tato zpráva sdělení „Tento e-mail byl odeslán na základě žádosti o ověření uživatelského účtu, odeslané z [redacted]

Druhé sdělení, označené „Důležité bezpečnostní upozornění: Zvolte prosím nové heslo do [redacted]“ Text sdělení: „Dobrý den, píšeme vám protože Vaše původní heslo k [redacted] už nefunguje. Pro jistotu jsme se rozhodli ho z bezpečnostních důvodů zrušit, zaznamenali jsme totiž pokus o narušení bezpečnosti, který se dotkl starší databáze uživatelských účtů, jež neměly dostatečné silné heslo. Aby Vás účet nikdo nezneužil, neváhali jsme a neprodleně jej zablokovali. Nastavit nové bezpečné heslo je jednoduché. Při přihlášení do Vašeho uživatelského účtu na [redacted] zvolte možnosti „Zapomněl jsem heslo“, zadejte Vás e-mail, na který Vám obratem přijde výzva k zadání nového hesla, čímž svůj účet opět aktivujete. Případně také můžete kliknout na odkaz [redacted]

a postupovat již podle instrukcí. Prosíme, abyste situaci věnovali pozornost, i pokud svůj [redacted] účet moc často nepoužíváte. Pokud se heslo k Vašemu účtu shoduje

například s hesly na sociálních sítích, v e-mailu nebo v dalších e-shopech, radši na nic nečekejte a co nejdřív tato hesla všude změňte. Náš bezpečnostní tým složený ze zákaznické podpory, odborníků na IT bezpečnost a právníků problém urgentně řeší a zkoumá všechny potenciální možnosti zneužití přístupů. Ochrana osobních údajů zákazníků je pro nás prioritou, takže připravujeme právní kroky vůči pachatelům. Teď jste pro nás ale na prvním místě vy, naši zákazníci. Proto jsme posílili zákaznickou linku, na kterou se můžete obrátit mezi 9. a 18. hodinou včetně víkendů. Dále jsme pro Vás sepsali nejčastější otázky a odpovědi – najdete je. Velmi se omlouváme a děkujeme Vám za podporu i pochopení. Tým."

3. Článek který je expertem na IT bezpečnost, který byl uveřejněn na webových stránkách ze dne 29. srpna 2017 obsahuje informaci, že systém zabezpečení hesel v nebyl vhodný už v době zavedení, stále je ale rozšířený. Dále, že e-mail s upozorněním na nutnost změny hesla dostal více než milion zákazníků. Dále článek obsahuje informaci, že společnost na základě studia získaných dokumentů soudí, že jde o data z roku 2014, v současné době není známo, jakým způsobem data unikla a dále, že vzhledem k stáří dat to nevypadá na aktuální průnik, spíše, že utekla data z nějaké zálohy nebo dumpu, který se válel někde, kde neměl.
   Článek dále obsahuje informace, že v současnosti podle svého tvrzení ukládá hesla způsobem, který lze pokládat pro současnou dobu za bezpečný – To znamená, že pokud by hesla unikla nyní, útočníkovi k ničemu nebudou. Tuto metodu ale zavedla poměrně pozdě, až v říjnu roku 2016. Dále, že od roku 2012 používala metodu kterou nelze již pokládat za bezpečnou (a nebyla bezpečná ani v době zavedení), a ještě předtím používala prosté (které není bezpečné v žádném případě). Pokud jste tedy měli na v roce 2015 účet, předpokládejte, že je vaše heslo v otevřené podobě (v kombinaci s e-mailovou adresou, jménem, příjmením a možná telefonem) volně k dispozici, a pokud jej používáte ještě někde jinde, změňte si ho.

4. Článek autora ze dne 29. srpna 2017, který byl zveřejněn v internetovém serveru o českém internetu (...) je uvedeno, že celkem hesel v čitelné podobě, unikátních e-mailových adres a obdobný počet telefonních čísel, je obsah souboru s uniklými přihlašovacími údaji z internetového obchodu který neznámí autoři uložili dočasně na úložiště V článku je dále uvedeno, že redakci databázi poskytl člověk, který si nepřál být jmenován. Dále se v článku uvádí, že přihlašovací údaje jsou v databázi uvedené v plně čitelné podobě. To neznamená, že by hesla neměl vůbec chráněna. Jde pravděpodobně o výsledek cracknutí slabšího zabezpečení starších účtů v jeho systémech. Firma ve svém oficiálním prohlášení přiznala, že do podzimu při šifrování hesel používala k hashování prolomitelný algoritmus poté přešla na a teprve v říjnu začala používat bezpečnější . Dále, že jména, hesla a telefonní čísla stovek tisíc uživatelů každopádně jsou v plně čitelné podobě už minimálně měsíc dostupná na internetu než server kopii databáze

smazal ( ), mohl si soubor stáhnout kdokoli.
Dále článek obsahuje informace, že uniklé údaje se v souboru nacházejí ve formátu EMAIL:PASSWORD:NAME:SURNAME:PHONE. Autor v článku uvádí: „Pravost údajů v souboru jsme ověřovali dotazem u několika uživatelů. Většina z nich potvrdila, že údaje spojené v úniku s jejich e-mailovou adresou jsou skutečně jejich hesla z .“

5. V rámci zahájení kontroly byla kontrolovaná společnost požádána o poskytnutí nezbytné součinnosti, a to aby v rámci stanoveného úvodního ústního jednání byly předloženy:
   a) Přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů ve smyslu ustanovení § 13 zákona č. 101/2000 Sb.
   b) Písemná informace o narušení bezpečnosti při správě osobních údajů, včetně informace o přesném rozsahu, době a počtu osobních údajů zákazníků, který se narušení týká, dále informace o tom, kdy a jakým způsobem bylo narušení zjištěno.
   c) Písemná informace o průběhu, resp. výsledcích vlastního šetření narušení bezpečnosti.

6. V rámci úvodního jednání zástupci kontrolované Společnosti kontrolujícím předali:
   záznam o bezpečnostní události a výsledcích šetření ze dne 8. 9. 2017
   interní předpis
   Interní předpis
   interní předpis
   Dále zástupci sdělili, že Společnost v letošním roce získala informace o tom, že na webovém portálu je vložen soubor, který obsahoval indicie, že by se mohlo jednat o zákazníky . Proto provedli základní porovnání této databáze s vlastními informacemi a zjistili, že se databáze shoduje s jejich vlastní databází zákazníků z roku 2014. Proto zahájili nejen vlastní šetření, ale ve spolupráci s provozovatelem portálu zajistili okamžité stažení zveřejněné databáze a dále postupovali tak, že upozornili prostřednictvím e-mailu všechny zákazníky, jejichž osobní údaje mohli být napadeny, na nebezpečí prolomení jejich přístupových dat s doporučením, aby si je změnili. Zástupci sdělili, že společnost podala ve věci trestní oznámení, a to u KŘ Policie ČR HMP.

7. Záznam o bezpečnostní události a výsledcích šetření (data breach inventory), vypracovaný pro interní potřeby společností ze dne 8. září 2019 obsahuje informace:

   Datum uskutečnění bezpečností události
   Zveřejnění databáze
   Potvrzení o přijetí informace o zveřejnění databáze
   Pachatel
   Žádost o odstranění databáze

Reset hesel zákazníků [redacted]
Příprava externí komunikace [redacted]
Oznámení dozorové autoritě v oblasti ochrany osobních údajů [redacted]
Oznámení orgánům činným v trestním řízení [redacted]

Interní zpráva označená jako „Záznam o bezpečnostní události a výsledcích šetření“, ze dne 8. září 2017, obsahuje informace o popisu incidentu:

[redacted]

Kontrolovaná společnost [redacted] na základě zjištěného a popsaného incidentu rozhodla o podání trestního oznámení orgánům činným v trestním řízení a dále rozhodla o podání oznámení o narušení bezpečnosti při správě osobních údajů.

8. Kontrolovaná společnost [redacted] má zpracované vnitřní předpisy, kterými dokumentovala přijatá technicko-organizační opatření v oblasti ochrany osobních údajů, platná v době zahájení kontroly.

Interní předpis Pravidla pro využívání ICT, č. [redacted]

[redacted]

Interní předpis č. 2013-1-1, Bezpečnostní politika upravuje postupy při zjištění bezpečnostní události či bezpečnostního incidentu a jejich navazujícího řešení. Deklarovaným předmětem směrnice, jako bezpečnostní politiky je reakce na potenciální rizika v případech bezpečnostních událostí a bezpečnostních incidentů s cílem zamezit nežádoucím dopadům do oblasti ochrany osobních údajů zákazníků [redacted] Za tímto účelem upravuje standardizované kroky následující po detekování bezpečnostní události či bezpečnostního incidentu, rozhodnutí týkající se jejich řešení, shromáždění informací o události či incidentu a jejich prevenci do budoucna.
Směrnice upravuje definice pojmů (např. co to je bezpečnostní událost, bezpečnostní incident, bezpečnostní tým, odpovědná osoba a další).

[redacted]

[redacted]

[redacted]

b) [redacted]

h) [redacted]

Směrnice dále upravuje způsob a odpovědnost za zřizování uživatelských účtů, včetně povinností uživatelů za jejich ochranu (ochrana uživatelských účtů, oprávnění a hesel), včetně požadavků na tvorbu a náležitostí hesla.

Kontrolovaná společnost [redacted] dokumentovala interní předpis 2013-1-2, Směrnice o ochraně osobních údajů zákazníků společnosti [redacted] Směrnice upravuje zpracování osobních údajů zákazníků [redacted] a to fyzických osob nebo fyzických podnikajících. Upravuje postavení společnosti [redacted], jako správce osobních údajů, účel zpracování osobních údajů, předmět evidence a povinnosti při zpracování osobních údajů, rozsah zpracovávaných osobních údajů (, [redacted]

[redacted]

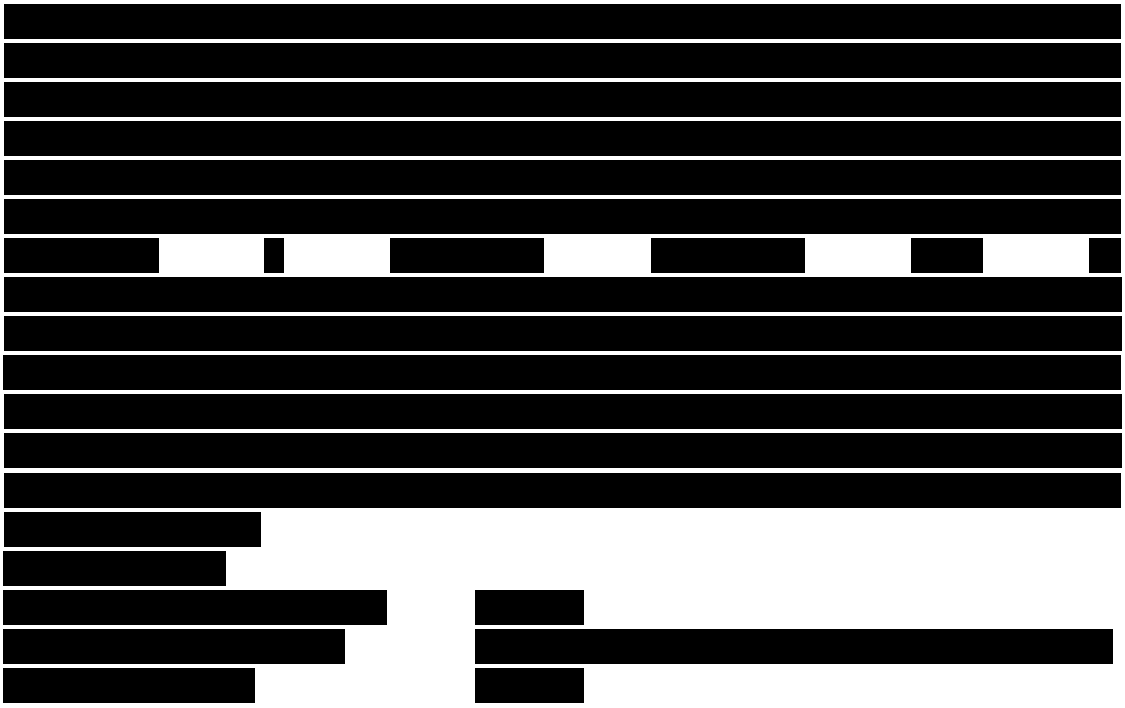
[redacted]

[redacted]

9. K žádosti, aby společnost [redacted] předložila kopii záznamu o bezpečnostní události a bezpečnostním incidentu – viz kapitola 5. Interního předpisu 2013-1-1 k datu incidentu, tedy ke dni, který uvádí Společnost 31. 12. 2014, zejména potom informace z provedené analýzy – viz kapitola 5.2 uvedeného Interního předpisu, dále aby předložila kopii Zápisu z postupu řešení incidentu ze dne 31. 12. 2014, se zaměřením na postup Odpovědné osoby (viz kapitola 2.5 Interního předpisu 2013-1-1) včetně záznamu Bezpečnostního týmu, dle postupu uvedeného v kapitole 3.1 uvedeného Interního předpisu a dále, aby sdělila přesnou informaci, kolik záznamů celkem

obsahovala napadená databáze Společnosti k datu incidentu, společnost upřesnila, že některé skutečnosti vyplývají z interního šetření, které provedl [redacted] v souvislosti s bezpečnostní událostí. Dále, že společnost [redacted] zaznamenala dne 25. 08. 2017 dopad v oblasti ochrany osobních údajů zákazníků, vzniklý jako následek bezpečnostní události z roku 2014 a dále, že o uvedeném mimo jiné informovala Úřad pro ochranu osobních údajů (dále jen „Úřad“) prostřednictvím oznámení ze dne 27. 08. 2017 a dále prostřednictvím „Záznamu o bezpečnostní události a výsledcích šetření (viz výše). Dále společnost [redacted] sdělila, že v záznamu je kromě dalšího specifikována i geneze bezpečnostní události, z níž vyplývá, že se [redacted] dozvěděl o odcizení databáze v srpnu 2017. Teprve až následně po prověření všech okolností, včetně zveřejněné databáze, bylo zjištěno, že se bezpečnostní událost uskutečnila v roce 2014 a dále, že jak plyne ze Záznamu o bezpečnostní události a výsledcích šetření, [redacted] měl jako správce osobních údajů v dané době zavedena odpovídající technická a organizační opatření, která byla použita u osobních údajů dotčených narušením zabezpečení, a to zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup a dále, že veškerá opatření činící data nečitelná pro jakékoli třetí strany odpovídala standardům toho času běžným v daném odvětví (tj. v roce 2014). Společnost dále sdělila, že při prověřování okolností vzniku události a jejího časového zařazení pověření zástupci IT oddělení dospěli k závěru, že daný případ nebylo možné v tehdejší době zaznamenat s přihlédnutím ke všem dostupným technickým řešením a prevenčním mechanismům.

Společnost [redacted] dále sdělila, že [redacted]



Společnost dále sdělila, že s ohledem na objektivní nemožnost zjistit vznik bezpečnostní události v roce 2014, nezávisle na přijatých opatřeních ze strany , byl ztížen způsob obstarání důkazů. S přihlédnutím ke stáří incidentu (kdy od jeho uskutečnění uplynuly minimálně tři roky) je související evidence důkazního materiálu složitá, ne-li vyloučená vzhledem k proběhlým personálním a technickým změnám. I přes tuto skutečnost přistoupil k řešení celé záležitosti s maximální otevřeností a respektováním principů ochrany osobních údajů svých zákazníků. Při řešení bezpečnostní události aplikoval standardní postup stanovený vnitřními předpisy při zjištění povahy incidentu, jeho rozsahu, charakteru a souvisejících znaků. Z pohledu tak došlo k zajištění minimalizace dopadů na dotčené subjekty údajů a shromáždění maxima podkladů pro navazující šetření jak orgánů činných v trestním řízení, tak Úřadu.

10. Společnost , v rámci šetření, kdo a kdy uložil na úložiště soubor dat (hesla a kontakty z databáze společnosti a to zejména IP adresu, datum a čas, po kdy byla uvedená data zpřístupněna, dále, jaký tvar v podobě „název souboru.přípona“ měl zpřístupněný soubor (databáze), kdy (přesné datum a čas) obdržela tato společnost od společnosti podnět ke stažení uvedeného soboru a kdy přesně k jeho stažení došlo, sdělila, že není schopna na tyto otázky odpovědět, neboť není schopna dle popisu identifikovat předmětný soubor. S ohledem na množství souborů v současnosti uložených na webovém úložišti a s ohledem na množství souborů každý den mazaných je pro společnost , prakticky nemožné dohledat informace o předmětném nijak blíže nekonkretizovaném souboru. Dále společnost uvedla, že údaje o smazání souboru (a žádosti tomuto smazání předcházející) by teoreticky měla být schopna poskytnout, ale v tomto případě nejsou schopni zúžit období, kdy měla být žádost o smazání soubru doručena. I kdyby Společnost vycházela z časového rozmezí 25. 8. 2017 – 1. 9. 2017 (v tomto rozmezí došlo k medializaci úniku

dat u Kontrolované osoby), tak jen za takto vymezený týden eviduje přes [redacted] žádostí o smazání různých souborů. V situaci, kdy není známo, kdy mělo k nahlášení dojít, považuje společnost za téměř nemožné najít konkrétní žádost týkající se navíc blíže neidentifikovaného souboru. Rovněž ani v samotné žádosti o smazání nemusel být uveden údaj o tom, že se jedná o soubor s daty obsahující osobní údaje zpracovávané Kontrolovanou osobou. Společnost dále upozorňuje na to, že pokud soubor smazal sám uživatel, který jej nahrál (např. v reakci na medializaci úniku dat u Kontrolované osoby), nebyla by společnost vůbec schopna dohledat informace o tomto souboru.
K žádosti o sdělení, zda má společnost [redacted], stažený (odstraněný soubor) stále k dispozici, zda je archivován, resp. likvidován, společnost sdělila, že smazané soubory nijak nearchivuje.

11. Společnost [redacted], která je provozovatelem webového portálu [redacted], na žádost Úřadu sdělila, že informace zveřejněné prostřednictvím serveru [redacted], v článku [redacted] dne 28. 8. 2017 použila databázi klientů [redacted], zveřejněnou na [redacted] použila jako podklad pro článek, po té ji několik měsíců měla v držení, zejména s ohledem na možnou žádost Policie ČR o její vydání, ale po třech měsících ji smazali, protože nebyl důvod si ji ponechávat. Dále společnost [redacted] potvrdila údaje o počtu hesel, počtu unikátních e-mailových adres, telefonních čísel, které byly ve výše uvedeném článku zveřejněny.

12. Z šetření policejního orgánu vyplývá, že v blíže nezjištěné době od 31.12.2014 do 23.7.2017 nezjištěným způsobem odcizil neznámý pachatel elektronickou databázi uživatelských účtů z období do 31.12.2014 v rozsahu email, heslo (v zašifrované podobě), jméno, příjmení, telefonní číslo, přičemž se jedná o celkem [redacted] záznamů zákazníků společnosti internetového portálu [redacted] a [redacted] které byly ze strany spol. [redacted] převzaty a následně provozovány, neznámý pachatel následně nezjištěným způsobem překonal hesla jednotlivých účtů, přičemž tento nejméně ve dnech 23.7.2017 a 27.7.2017 uploadoval danou databázi na server [redacted] pod názvem [redacted].
Policie ČR zjistila, že dne 1. září 2017 bylo na Policii ČR podáno trestní oznámení zaslané společností [redacted] týkající se výše popsaného jednání neznámého pachatele. Tento v přesně nezjištěném období od konce měsíce prosince roku 2014 do 23.7.2017 odcizil elektronickou databázi uživatelských účtů z období založení do 31.12.2014 v rozsahu e-mail, heslo (v zašifrované podobě), jméno, příjmení, telefonní číslo, přičemž se jedná o celkem [redacted] záznamů zákazníků společnosti internetového portálu [redacted] které byly ze strany spol. [redacted] převzaty a následně provozovány. Dle sdělení poškozené společnosti neznámý pachatel dne 27.7.2017 uploadoval danou databázi na server [redacted] pod názvem [redacted]. Po doručení daného oznámení byla neprodleně kontaktována společnost [redacted] se sídlem [redacted], a to z důvodu

žádosti o zjištění veškerých identifikačních údajů k uživateli, který na server [redacted] umístil předmětný soubor. Na základě vypracované zprávy poskytnuté společností [redacted], bylo zjištěno, že obdobný soubor byl již na daný server uploadován dne 23.7.2017, přičemž tento byl na základě upozornění společnosti [redacted] odstraněn. K uživateli, který dané soubory na daný server umístil, bylo sděleno, že se jedná o nepřihlášeného uživatele a daná společnost nemá k dispozici žádné údaje. [redacted]
Na základě sdělených skutečností nebylo tedy možné získat žádné konkrétní informace k osobě, která danou databázi na daný server umístila. Policie ČR sdělila, že další šetření bylo zaměřeno na server [redacted] který byl rovněž uveden v oznámení poškozené společnosti. Na uvedeném serveru mělo dne 29.8.2017 v 09:00 hodin dojít ke zveřejnění článku obsahujícího části odcizené databáze v čitelné podobě. V rámci daného prověřování byl vyslechnut redaktor serveru [redacted] a zároveň autor článku pan [redacted]. Výslech byl zaměřen převážně na zjištění způsobu získání zveřejněných souborů obsahujících uniklé uživatelské účty. Jmenovaný při výslechu uvedl, že tento danou galerii získal od anonymního zdroje jako námět na článek. Zveřejněná databáze byla dle sdělení získána z výše uvedeného serveru [redacted] kde byla volně dostupná ke stažení. Ani tímto šetřením se nepodařilo získat žádné skutečnosti vedoucí ke zjištění možného pachatele daného jednání. V rámci prověřování uvedeného skutku byl rovněž ztotožněn a následně vyslechnut [redacted] prostřednictvím e-mailové adresy S[redacted], jako první upozornil poškozenou společnost na možný únik dat, které jsou volně ke stažení na serveru [redacted]. Jmenovaný byl vyslechnut za účelem získání skutečností vedoucích k možnému pachateli daného skutku. Při výslechu jmenované osoby bylo zjištěno, že tento v přesně nezjištěném období cca v srpnu roku 2017 prostřednictvím torrentových vyhledávačů shromažďoval pro svůj projekt volně dostupná hesla. Při následném vyhodnocení získaného obsahu jmenovaný dle svého sdělení narazil na výše popsanou databázi, která obsahovala v čitelné podobě jména osob, telefonní čísla a hesla klientských účtů poškozené společnosti. [redacted] Policii dále sdělil, že ihned po zjištění popsaného obsahu tento prostřednictvím e-mailové zprávy kontaktoval společnosti [redacted], aby ji o úniku jejich dat informoval. Žádné další konkrétní skutečnosti se provedeným výslechem zjistit nepodařilo. K danému skutku byl také vyslechnut zástupce společnosti [redacted], a to za účelem upřesnění podaného oznámení. Výslech osoby byl zaměřen na získání upřesňujících údajů k úniku databáze. Konkrétně na zjištění doby možného úniku a způsob provedení. Z výslechu zástupce společnosti však bylo zjištěno, že analýza bezpečnostní události je složitá, a to vzhledem k obměně většiny kategorií, jak v rovině personální, tak v rovině technické. Ohledně konkrétního přístupu osob k uživatelským účtům, se rovněž nepodařilo od zástupce společnosti získat žádné konkrétní údaje, kdy ve vyjádření je uvedeno, že z důvodu stáří dat, jakož i bezpečnostní události je určení jednotlivých zaměstnanců složité, a to vzhledem k obměně většiny personálu, nákupu a slučování společností a s tím spojené slučování jednotlivých databází. Ze strany poškozené společnosti se tedy nepodařilo získat žádné konkrétní skutečnosti, které by napomohly k řádnému objasnění daného jednání.

13. Shrnutí

V blíže neupřesněné době od 31. prosince 2014 do 23. července 2017 neznámá osoba nebo neznámé osoby odcizily ze serverů společnosti [redacted] elektronickou databázi uživatelských účtů vzniklou za období nejpozději do 31. prosince 2014. Elektronická databáze uživatelských účtů, tj. klientů společnosti [redacted], obsahovala osobní údaje klientů v rozsahu e-mailový kontakt, přístupové heslo (v šifrované podobě), jméno, příjmení, telefonní kontakt.
Celkem bylo odcizeno [redacted] elektronických záznamů, z nichž [redacted] obsahovalo unikátní e-mailové adresy. Celkem bylo odcizeno cca [redacted] záznamů z celkové zákaznické databáze a cca [redacted] záznamů bylo aktivních i v roce 2017, kdy bylo odcizení zjištěno.

Nejméně v době od 23. července 2017 do 27. srpna 2017 byla odcizená databáze uložena (uploadovaná) nezjištěnou osobou nebo osobami na server [redacted], a to pod názvem [redacted] Uložením databáze na toto úložiště došlo ke zpřístupnění celé databáze nezjištěnému počtu příjemců, nezjištěnému počtu stažení – nahrání uložené databáze.

Společnost [redacted] byla na zpřístupnění její databáze klientů (uživatelských účtů) upozorněna fyzickou osobou [redacted] prostřednictvím elektronické zprávy odeslané z e-mailové adresy [redacted].
Vlastním šetřením a porovnáním zpřístupněných údajů, byla zveřejněná databáze ztotožněna s databází vlastních klientů z roku 2014 [redacted] (internetové servery provozované v roce 2014 společností [redacted]).
Po obdržení zprávy požádala společnost [redacted] dne 25. srpna 2017 provozovatele webového portálu [redacted] společnost [redacted], o odstranění zpřístupněné databáze. Téhož dne společnost [redacted] zajistila smazání výše uvedené databáze.

Společnost [redacted] v období od 25. do 27. srpna 2017, resetovala hesla zákazníků registrovaných před 1. lednem 2015 (cca [redacted] klientů), dále připravila a realizovala opatření spočívající v informování klientů prostřednictvím e-mailů a prostřednictvím blogu [redacted] a prostřednictvím sdělovacích prostředků o bezpečnostní události, včetně nutnosti změny přihlašovacích údajů, resp. vygenerování nového přihlašovacího hesla a výzvy ke kontrole použití přihlašovacích údajů na jiných serverech, včetně vytvoření ověřovacího nástroje za účelem kontroly, zda konkrétní uživatelský účet nebyl předmětem zveřejněné databáze.
Společnost [redacted] dne 27. srpna 2017 oznámila Úřadu pro ochranu osobních údajů informaci o narušení bezpečnosti při správě osobních údajů.
Společnost [redacted] dne 1. září 2017 podala trestní oznámení na neznámého pachatele Policii ČR.

Společnost [redacted] v rámci kontroly předložila a dokumentovala jimi přijatá technicko-organizační opatření v oblasti ochrany osobních údajů, stanovení pravidel pro využívání ICT, má vypracovanou bezpečnostní politiku upravující postupy při zjištění bezpečnostní události.
Společnost [redacted] dokumentovala, že v době, kdy došlo k odcizení databáze klientů, využívala standardní zabezpečení ICT. Tvrzení, že k prolomení jednotlivých hesel uživatelů (klientů), mohlo dojít až v roce 2017 postupem technologického vývoje nebylo doloženo.

Společnost [redacted] vlastním šetřením nezjistila, kdo a jakým způsobem databázi odcizil. Nebylo zjištěno přesné datum odcizení, resp. přístupu do IT systémů, nebylo zjištěno, zda k neoprávněnému přístupu a odcizení databáze klientů došlo zvnějšku nebo zevnitř společnosti, tedy zda se jednalo o hackerský útok zvnějšku nebo zda k odcizení došlo plně nebo z části prostřednictvím vlastních zaměstnanců, a to buď úmyslně, nebo nedbalostním jednán resp. zda došlo ze strany zaměstnance nebo konkrétních zaměstnanců k porušení pracovních povinností. Odcizení databáze uživatelů v roce 2014 společnost [redacted] sama nezjistila. Na zpřístupnění databáze klientů byla upozorněna zvnějšku, třetí osobou. Do dnešního dne není zjištěno, kolika osobám byla databáze klientů v období od 31. 12. 2014 do 23. 7. 2017 zpřístupněna. Do dnešního dne není zjištěno, kolika osobám byla databáze uložená v období od 23. července 2017 do 27. srpna 2017 na [redacted] zpřístupněna a kolik osob si zde uloženou databázi nahrálo, resp. pořídilo její kopii.

B. Porovnání zjištěného stavu věci s relevantním ustanovením právního předpisu

Kontrolní zjištění č. 1
Společnost [redacted], v rámci své podnikatelské činnosti shromažďuje od svých zákazníků informace v rozsahu jméno, příjmení, adresa, korespondenční adresa, číslo telefonu a elektronický kontakt (e-mailovou adresu) a dále informace, které se týkají realizace obchodu (zboží, dodání, platba). Na základě těchto informací lze nepochybně přímo identifikovat konkrétní fyzickou osobu. Společnost [redacted] zpracovává ve smyslu § 4 písm. a) zákona č. 101/2000 Sb., osobní údaje svých zákazníků.
Prostřednictvím internetového obchodu jsou osobní údaje zákazníků [redacted] automatizovaně a systematicky shromažďovány, tříděny, používány, vyhledávány a ukládány na nosiče a jsou s nimi prováděny soustavy operací. Společnost [redacted] ve smyslu § 4 písm. e) zákona č. 101/2000 Sb. zpracovává osobní údaje.
Společnost [redacted] rozhodla o účelu a prostředcích zpracování osobních údajů prostřednictvím E-shopu v rámci své podnikatelské činnosti a je tedy ve smyslu § 4 písm. j) zákona č. 101/2000 Sb., správcem osobních údajů, zpracování provádí a odpovídá za ně.

Kontrolní zjištění č. 2

Tím, že v období od 31. prosince 2014 do 23. června 2017 došlo nezjištěným způsobem a nezjištěnou osobou, resp. osobami k odcizení databáze [redacted] záznamů o zákaznících společnosti [redacted] obsahujících [redacted] unikátních adres zákazníků v rozsahu jméno příjmení, uživatelské heslo, e-mailová adresa, a číslo telefonu, které měla uloženy

v ICT systémech, přičemž společnost [redacted] jako správce osobních údajů neoprávněnému přístupu a odcizení databáze uživatelů, nejen nezabránila, ale ani jej nezaznamenala a nezjistila, porušila povinnost správce osobních údajů uloženou ji § 13 odst. 1 zákona č. 101/2000 Sb., neboť jako správce nepřijala taková opatření, aby nedošlo k neoprávněnému odcizení výše uvedené databáze záznamů vlastních zákazníků, přičemž následkem porušení této povinnosti bylo zveřejnění databáze [redacted] záznamů o zákaznících společnosti [redacted] obsahujících [redacted] unikátních adres zákazníků v rozsahu jméno příjmení, uživatelské heslo, e-mailová adresa, a číslo telefonu na veřejně přístupném webovém portálu [redacted] po dobu 23. července 2017 – 27. srpna 2017.

III.

Poučení o opravném prostředku:
Proti kontrolnímu zjištění uvedenému v protokolu o kontrole může Kontrolovaná osoba podat kontrolnímu orgánu ve lhůtě 15 dnů ode dne doručení protokolu o kontrole námitky. Námitky se podávají písemně, musí z nich být zřejmé, proti jakému kontrolnímu zjištění směřují, a musí obsahovat odůvodnění nesouhlasu s tímto kontrolním zjištěním.
Pokud kontrolující inspektor nevyhoví námitkám ve lhůtě 7 dnů ode dne jejich doručení, vyřídí je předsedkyně Úřadu ve lhůtě 30 dnů ode dne jejich doručení.

Protokol o kontrole je vypracován ve dvou vyhotoveních. Jedno vyhotovení bude doručeno Kontrolované osobě formou stejnopisu, druhé vyhotovení bude založeno jako originál s podpisem kontrolujících v kontrolním spisu čj. UOOU-08428/17. V tomto spisu jsou rovněž založeny všechny podklady (dokumenty, úřední záznamy apod.) uvedené ve sběrném archu kontrolního spisu pod pořadovým číslem 1-31.
V rámci této kontroly bylo kontrolujícími kontrolováno a prověřováno výhradně zpracování osobních údajů v čase provedení kontroly uvedeném v tomto Protokolu o kontrole a v rozsahu stanoveném předmětem kontroly.

Podpisová doložka:

Kontrolující:

otisk
úředního
razítka

MVDr. František Bartoš inspektor *(dokument podepsán elektronicky)*

…… ……..
jméno podpis

Ing. Radek Loub	pověřený zaměstnanec Úřadu	*(dokument podepsán elektronicky)*
…….		……..
jméno		podpis
JUDr. Michal Jelínek	pověřený zaměstnanec Úřadu	*(dokument podepsán elektronicky)*
…….		……..
jméno		podpis
Ing. Max Gůt	pověřený zaměstnanec Úřadu	*(dokument podepsán elektronicky)*
…….		……..
jméno		podpis