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 XXXXX
pověřený zaměstnanec Úřadu JUDr. Michal Jelínek, držitel průkazu č. XXXXX
pověřený zaměstnanec Úřadu Ing. Max Gůt, držitel průkazu č. XXXXX
pověřený zaměstnanec Úřadu Ing. Radek Loub, držitel průkazu č. XXXXX

**Kontrolovaná osoba**
XXXXXXXX (dále jen „XXXXX“ nebo „Společnost“)

zastoupená
XXXXXXXXXXXXX,

**Místo provedení kontroly**
sídlo kontrolované společnosti XXXXXXXX

**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 XXXXXX.

**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 XXXXXX 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

   *XXXXXXXXXXXXX*
   *XXXXXXXXXXXX*
   *XXXXXXXXXXXXX*

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. UOOU08428/17-10
7. Žádost právního zástupce XXXXX 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 XXXXXX zmocňuje XXXXXX, advokáta k zastupování
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. UOOU08428/17-14, + přílohy:
    a) záznam o bezpečnostní události a výsledcích šetření ze dne 8. 9. 2017
    b) interní předpis IT 2011-1-1, Pravidla pro využívání ICT
    c) interní předpis 2013-1-1, Bezpečnostní politika společnosti XXXXXXXX, a.s., či jejích dceřiných společností na území České republiky
    d) interní předpis 2013-1-2, Směrnice o ochraně osobních údajů zákazníků společnosti XXXXXXX, či jejich dceřiných společností na území České republiky

11. Zaslání Úředního záznamu právnímu zástupci společnosti XXXXXX 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. UOOU08428/17-16
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 XXXXX, ze dne 18. prosince 2017, č.j. UOOU-09428/17-20
16. Přípis - žádost právního zástupce společnosti XXXXXX 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 XXXXXX, a.s. ze dne 8. ledna 2018
    a) plná moc právního zástupce společnosti XXXXXX, a.s. ze dne 25. srpna 2016, udělaná XXXXX, advokátovi
    b) substituční plná moc, udělená advokátem XXXXXX XXXXXX, advokátovi, 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 XXXXX
20. Přípis – odpověď Obvodnímu soudu pro Prahu 7 ze dne 15. ledna 2018, č.j. UOOU08428/17-25
21. Odpověď právního zástupce společnosti XXXXX na žádost o poskytnutí součinnosti ze dne 15. ledna 2018, č.j. UOOU-08428/17-26
22. Přípis – žádost o poskytnutí součinnosti společnost XXXXX ze dne 25. ledna 2018, č.j. UOOU-08428/17-27
23. Odpověď společnosti XXXXXX., 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 XXXXX písemnou informaci Oznámení o narušení bezpečnosti při správě osobních údajů. Obsahem sdělení je informace, že společnost XXXXXX, která v rámci svého předmětu podnikání provozuje XXXXXX nákupní XXXXXX 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 766 421 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 XXXXXX 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 XXXXXX. Od října roku 2016 jsou přístupové údaje chráněny XXXXXXXX. Používaná metoda byla v době jejího použití vždy obvyklým bezpečnostním standardem.

Společnost XXXXXXX dále sdělila, že k minimalizování následků narušení bezpečnosti, již podnikla následující kroky:

- reset hesel všech potenciálně ohrožených uživatelských účtů založených před rokem 2015
- písemné informování dotčených subjektů osobních údajů prostřednictvím e-mailu o vzniklé situaci
- posílení centra zákaznické péče za účelem zodpovídání dotazů zákazníků

2. Kontrolovaná společnost XXXX, dne 27. srpna 2017 odeslala z e-mailové adresy XXXXXXX dvě elektronické zprávy, které byly adresovány cca 1,3 mil. 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 XXXXX 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 na tomto odkazu. 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 u nás na blogu, a pokud máte další dotazy, neváhejte nás prosím kontaktovat – naši kolegové na zákaznické lince jsou připraveni Vám pomoct. Tým XXXXX.“

   V zápatí obsahuje tato zpráva sdělení „Tento e-mail byl odeslán na základě žádosti o ověření uživatelského účtu, odeslané z http://www.XXXXXX.cz/bezpecnost.

   Druhé sdělení, označené „Důležité bezpečnostní upozornění: Zvolte prosím nové heslo do XXXXX“ Text sdělení: „Dobrý den, píšeme vám, protože Vaše původní heslo k XXXX 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 XXXX 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 xxxx a postupovat již podle instrukcí. Prosíme, abyste situaci věnovali pozornost, i pokud svůj XXXXXX.cz 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 u nás na blogu. Velmi se omlouváme a děkujeme Vám za podporu i pochopení. Tým XXXX."

3. Článek Michala Valáška, který je expertem na IT bezpečnost, který byl uveřejněn na webových stránkách XXXXXXXXXXXXXXX Hospodářské noviny ze dne 29. srpna 2017 obsahuje informaci, že systém zabezpečení hesel v XXXXXX 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 XXXXXX.cz podle svého tvrzení ukládá hesla způsobem, který lze pokládat pro současnou dobu za bezpečný – hashování pomocí algoritmu XXXXX. 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 XXXXXX, kterou nelze již pokládat za bezpečnou (a nebyla bezpečná ani v době zavedení), a ještě předtím používala prosté MD5 (které není bezpečné v žádném případě). Pokud jste tedy měli na XXXXXX.cz 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 XXXXXXX ze dne 29. srpna 2017, který byl zveřejněn v XXXXXX serveru o českém XXXXXX XXXXXXXXX je uvedeno, že celkem 766 421 hesel v čitelné podobě, 735 056 unikátních e-mailových adres a obdobný počet telefonních čísel, je obsah souboru s uniklými přihlašovacími údaji z XXXXXX obchodu XXXXXX.cz, který neznámí autoři XXXXXX dočasně na úložiště Uloz.to. V článku je dále uvedeno, že redakci XXXXXX 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 XXXXXX 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 2012 při šifrování hesel používala k hashování prolomitelný XXXXXX, poté přešla na XXXXXX s unikátní XXXX a teprve v říjnu 2016 začala používat bezpečnější XXXXX. Dále, že jména, hesla a telefonní čísla stovek tisíc uživatelů XXXXXXu každopádně jsou v plně čitelné podobě už minimálně měsíc dostupná na XXXXXXu XXXXXXX , než server XXXX kopii databáze smazal (XXXXXX), 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 XXXXXX.cz.“

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 IT 2011-1-1, Pravidla využívání ICT
   Interní předpis 2013-1-1, bezpečnostní politika společnosti XXXXXX XXXXXX, a.s., či jejich dceřiných společností na území České republiky interní předpis 2013-1-2, Směrnice o ochraně osobních údajů zákazníků společnosti XXXXXX XXXXXX, a.s., či jejích dceřiných společností na území České republiky.
   Dále zástupci XXXXXX XXXXXX sdělili, že Společnost v letošním roce získala informace o tom, že na webovém portálu XXXXXX je vložen soubor, který obsahoval indicie, že by se mohlo jednat o zákazníky XXXXXX XXXXXX. 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 XXXX 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 XXXXXX XXXXXX sdělili, že společnost XXXXXX XXXXXX 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 XXXXXX XXXXXX ze dne 8. září 2019 obsahuje informace:

| | |
|---|---|
| Datum uskutečnění bezpečností události | 31. 12. 2014 |
| Zveřejnění databáze | 27. 07. 2017, 10:58:22 |
| Potvrzení o přijetí informace o zveřejnění databáze | 25. 08. 2017 |
| Pachatel | neznámý |
| Žádost o odstranění databáze | 25. 08. 2017 |
| Reset hesel zákazníků | 25. – 27. 08. 2017 |
| Příprava externí komunikace | 25. – 27. 08. 2017 |
| Oznámení dozorové autoritě v oblasti ochrany osobních | |

| | |
|---|---|
| údajů | 27. 08. 2017 |
| Oznámení orgánům činným v trestním řízení | 01. 09. 2017 |

Interní zpráva označená jako „Záznam o bezpečnostní události a výsledcích šetření“, ze dne 8. září 2017, obsahuje informace o popisu incidentu:
Dne 25. 08. 2017 XXXXXX obdržel informace o zveřejnění části databáze obsahující údaje o zákaznících XXXXXXových serverů www.XXXXXX.cz, www.XXXXX.cz, www.XXXXX.cz a www.XXXXXXX.cz (tři poslední zmíněné e-shopy již k dnešnímu dni neexistují) z roku 2014 v souboru .txt na serveru XXXXX neznámým uživatelem. Z informace, kterou kontrolovaná společnost XXXXXX obdržela od provozovatele serveru XXXX, společnosti XXXXX vyplynulo, že daný soubor byl nahrán nepřihlášeným uživatelem dne 27. července 2017 v 10:58:22 hodin. V návaznosti na tuto skutečnost XXXXXX zahájil fázi řešení bezpečnostní události zacílenou primárně na odstranění a snížení dopadů incidentu.
Z interní zprávy vyplývá, že kontrolovaná společnost nezjistila vlastním šetřením kdo a kdy databázi odcizil a kdo a kdy ji umístil na webový portál XXXXXX. Dále ze záznamu vyplývá, incident se týká 766.421 záznamů o zákaznících z roku 2014, z nichž zhruba 735.956 obsahuje unikátní e-mailové kontakty zákazníků, jedná se tak o cca 20% unikátních údajů z celkové zákaznické databáze XXXXXX. Dále z analýzy vyplynulo, že v posledním roce bylo z těchto uživatelských účtů aktivních cca 350.000. Vlastním šetřením bylo zjištěno, že v daném případě došlo ke zveřejnění osobních údajů zákazníků v rozsahu jméno, příjmení, e-mailový kontakt, heslo k uživatelskému účtu, některá telefonní kontakt.
Záznam dále obsahuje zjištění, že v systémech užívaných XXXXXX dochází k tzv. hashování hesel, přičemž hesla jsou XXXXXX v zakódované podobě. Dotčená databáze byla zakódována starším a dnes již nepoužívaným způsobem, který umožnil narušiteli jednodušší hesla rozkódovat. Do roku 2012 byly údaje hashovány metodou XXXXXX, která dnes již není považována za bezpečnou. Od roku 2012 do roku 2016 společnost zajišťovala bezpečnost XXXXXXX. Dále záznam uvádí, že používaná metoda byla v době jejího použití vždy obvyklým bezpečnostním standardem.
Záznam obsahuje dále informaci o opatřeních, které společnost XXXXXX po zjištění incidentu přijala a realizovala. XXXXXX přistoupil preventivně k resetování hesel uživatelských účtů zákazníků registrovaných před datem 1. 1. 2015 (cca 1,3 mil. zákazníků), dále XXXXXX informoval prostřednictvím e-mailů a prostřednictvím blogu XXXXXX, dotčené subjekty údajů (zákazníky) o bezpečnostní události, včetně nutnosti změny přihlašovacích údajů, resp. vygenerování nového přihlašovacího hesla. Dále XXXXXX vyzval dotčené subjekty údajů ke kontrole použití přihlašovacích údajů na jiných serverech a současně zákazníky instruoval ohledně bezpečnostních standardů při správě hesla zejména ohledně programů typu „správce hesel“, obecné politiky tvorby hesel. XXXXXX dále vytvořilo pro zákazníky ověřovací nástroj za účelem kontroly, zda jejich konkrétní uživatelský účet byl předmětem zveřejnění databáze. Bezprostředně po zjištění incidentu prezentoval XXXXXX tento nástroj pro zákazníky na adrese https://www.XXXXXX.cz/bezpecnost.

Kontrolovaná společnost XXXXXX 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 XXXXXX 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. IT-2011-1-1, upravuje vnitřní pravidla ve společnosti pro využívání informačních a komunikačních technologií (ICT). Upravena je oblast práva k majetku, pravidla po užívání ICT pro soukromé účely v pracovní době, pravidla pro užívání ICT pro soukromé účely v mimopracovní době, dále část ochrana a zabezpečení prostředků ICT, která upravuje oprávnění zaměstnance nakládat s ICT, např. měnit a zasahovat do konfigurace technických prostředků, připojovat a odpojovat zařízení typu flash disků, externích disků, paměťových karet, reproduktorů mp3 přehrávače, jednotky CD, DVD aj., instalovat žádný software, měnit nastavení operačního systému, aplikačního programového vybavení aj. Dále zákaz připojování do firemní sítě LAN/WIFI, soukromá zařízení (telefon, notebook aj.), stahovat z XXXXXX do prostředků ICT žádný obsah, vkládat do ICT paměťová média, diskety, CD, DVD s obsahem. Směrnice dále obsahuje pokyn, že přístup do systémů je umožněn jen oprávněnému uživateli. Tento přístup je chráněn identifikací uživatele a autorizací (uživatelské jméno a heslo) a dále, že zaměstnanec nesmí své identifikační údaje sdělit žádné třetí osobě. Dále směrnice upravuje omezení přístupu zaměstnance do systémů v závislosti na činnosti, které jsou vymezeny jeho pracovními povinnostmi, včetně deklarace, že zaměstnanec není oprávněn pracovat se systémy a aplikacemi, které se netýkají plnění jeho pracovních povinností s výjimkou jejich využití pro soukromé potřeby v souladu se směrnicí. Dále, že zaměstnanec je povinen vypínat na konci pracovní doby své PC včetně monitoru, notebooku a dále směrnice obecně upravuje obecnou výjimku z této povinnosti. V části směrnice označené Sankce, je v části 6.3 upraveno, že „Zaměstnavatel *si* vyhrazuje právo dodržování těchto pravidel kontrolovat, a to i při využívání prostředků ICT zaměstnancem v mimopracovní době“.

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 XXXXXX. 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).
V části 3. je upraveno složení a činnost bezpečnostního týmu, a to: „bezpečnostní tým je složen minimálně z šesti osob delegovaných dle závažnosti události, přičemž zahrnuje nejméně jednoho člena z následujících oddělení: právní oddělení, IT oddělení,

Management, Compliance, Projektové vedení, Loss Prevention. Dle závažnosti události, resp. incidentu lze zahrnout i další delegované osoby, např. komunikační, tiskové, HR oddělení, případně z externích dodavatelských společností. Směrnice dále upravuje povinnosti hlášení bezpečnostní události a bezpečnostního Incidentu.
Část směrnice označená Hlášení bezpečnostní události a bezpečnostního incidentu upravuje práva a povinnosti v případě zjištění porušení povinnosti vyplývajících z bezpečnostní politiky, a to vždy informovat svého nadřízeného, IT oddělení, osoby, kterou jsou součástí bezpečnostního týmu a dále, že na základě individuálního posouzení závažnosti, míry zavinění a konkrétního rizika, případně míry dopadu a následků bezpečnostní události či bezpečnostního incidentu způsobeného porušením bezpečnostních předpisů, uskuteční zvolené osoby potřebná opatření. Dále předpis upravuje povinnost v případě události nebo incidentu týkajících se narušení technické infrastruktury, včetně databází XXXXXX, IT oddělení v součinnosti s bezpečnostním týmem odpovídá za nastavení procesů řízení bezpečnostních incidentů v rámci systému a volí odpovídající řešení podle závažnosti incidentu v souladu s následujícím plánem
a) detekce události
b) rozhodnutí týkající se jejího řešení
c) příprava řešení
d) řešení bezpečnostního incidentu
e) shromáždění informací o incidentu (data breach inventory)
f) prevence události do budoucna

Směrnice dále deklaruje, že pro účely detekce události je v systémech spravovaných společností zavedeno automatické hlášení nestandardních stavů.
V části záznam o bezpečnostní události a bezpečnostním incidentu upravuje povinnost, že o každé události a bezpečnostním incidentu bude sepsán a vyhotoven záznam obsahující informace o okolnostech jeho vzniku, možných důsledcích, zejména dopadech do oblastí ochrany osobních údajů, vyčíslení náhrady škody (je-li nezbytné), přijatých opatřeních, nutnosti systémových změn či změn technického zabezpečení. Dále předpis upravuje, že na podkladě provedené analýzy a shromážděných materiálů bude evidence bezpečnostní události nebo bezpečnostního incidentu zahrnovat následující informace: a) kdy k incidentu došlo
b) kde k incidentu došlo (přesné určení místa a jeho popis)
c) kdo incident spáchal
d) jak k incidentu došlo (průběh incidentu)
e) co bylo cílem útoku
f) jaký atribut bezpečnosti byl narušen
g) jaký byl charakter narušení (úmyslné nebo neúmyslné)
h) jaké opatření bylo překonáno (opatření na úrovni fyzické, logické, organizační, personální nebo technické bezpečnosti)
i) jaké aktivum bylo narušeno (hardware, software: operační systém, aplikace, databáze, síť, data)
j) pravděpodobnost opakování bezpečnostní události či bezpečnostního incidentu (spíše nízká, střední, vysoká, jistá)
k) seznam opatření zavedených bezprostředně po incidentu

l) popis opatření navržených za účelem zmírnění dopadů
m) popis opatření navržených za účelem prevence do budoucna.

Směrnice dále obsahuje povinnost společnosti XXXXXX zajistit odpovídající externí komunikaci s příslušnými státními orgány, v případech potenciálního ohrožení v oblasti ochrany osobních údajů, jichž je XXXXXX správcem zváží bezpečnostní tým nutnost komunikovat s dozorovou autoritou v oblasti ochrany osobních údajů a dojde-li k ohrožení, ztrátě či přenosu osobních údajů, má povinnost v opodstatněných či zákonem vymezených případech v přiměřené době nahlásit tento incident dohledové autoritě (ÚOOÚ) a jsou-li k tomu dány předpoklady a podmínky také dotčeným subjektům údajům. Směrnice dále upravuje, že dle povahy incidentu bezpečnostní tým v součinnosti s komunikačním/tiskovým oddělením zajistí informování subjektů údajů přímo, případně prostřednictvím mediálního sdělení.

V další části směrnice Bezpečnostní politika je upravena oblast Preventivní opatření – zajištění bezpečnostních systémů s tím, že IT oddělení společnosti odpovídá za chod serveru, jeho výkon, integraci a konfiguraci a nainstalované softwarové nástroje, včetně jejich aktualizace, odstranění chyb, aktualizace uživatelských účtů (přidání, smazání uživatele, reset hesel), zabezpečuje rutinní zálohy systému, integruje nové technologie, zabezpečuje správu sítí a přidaných programů, dále zajišťuje veškeré opravy a změny konfigurace operačního systému v souladu s bezpečnostním provozním módem.
V části 7.2 jsou upravena v oblasti ochrany osobních údajů oddělení IT následující pravidla:

a) zálohování lokální stanice probíhá 1x týdně. Zálohování serverů obsahujícího osobní údaje je prováděno 1x týdně. Zálohování serveru obsahujícího osobní údaje je prováděno na několika úrovních, primárně s frekvencí 24hodinového cyklu, samotná záloha probíhá s využitím integrovaných nástrojů použitého XXXX na externí zabezpečený souborový XXXXX. IT oddělení uchovává klouzavé plné zálohy vždy za poslední 2 dny, přičemž eviduje zálohu z prvního dne aktuálního a předchozího měsíce. Pro rychlou obnovu IT oddělení zajišťuje bitovou kopii databáze přímo na databázových serverech.
b) IT oddělení zabezpečuje existenci individuálních přístupových oprávnění. V případě ukončení pracovního poměru uživatele dochází k okamžité deaktivaci přístupu do všech systémů. V rámci e-mailového účtu je nastaveno okamžité přesměrování a k deaktivaci samotné adresy dochází do 2 týdnů.
c) Pro účely testování bezpečnostních hrozeb či reakcí systému zřizuje IT oddělení testovací účty, které se nacházejí výhradně v jeho správě, a oprávnění přístupu k nim nemohou být přidělena jiným osobám.
d) IT oddělení odpovídá za dostatečnou úroveň ochrany pomocí generovaných hesel jednotlivých uživatelů
e) IT oddělení odpovídá za provedení pravidelných aktualizací využívaných programů (zejména Skype, Outlook, Messenger a jiných).
f) IT oddělení odpovídá za údržbu sdíleného firemního disku

g) IT oddělení zastřešuje ochranu systémů XXXXXX, zejména pak prevenci instalace neautorizovaných aplikací, ohrožení před malware, počítačovými viry, phishingovými útoky, spamem a jinými souvisejícími bezpečnostními riziky.
h) IT oddělení informuje dle potřeby ostatní oddělení o možnostech bezpečnostních hrozeb, které by mohly ovlivnit jejich činnost, dále vyžaduje součinnost jednotlivých oddělení, které by mohly ovlivnit jejich činnost, dále vyžaduje součinnost jednotlivých oddělení v případě instalace bezpečnostních aktualizací, řešení bezpečnostních hrozeb a incidentů a dalších dle potřeby.
i) Pro účely testování zabezpečení systému, IT oddělení realizuje pravidelné penetrační testy.

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 XXXXXX dokumentovala interní předpis 2013-1-2, Směrnice o ochraně osobních údajů zákazníků společnosti XXXXXX XXXXXX, a.s., či jejích dceřiných společností na území České republiky, aktualizace ze dne 1. 4. 2013. Směrnice upravuje zpracování osobních údajů zákazníků XXXXXX, a to fyzických osob nebo fyzických podnikajících. Upravuje postavení společnosti XXXXXX, jako správce osobních údajů, účel zpracování osobních údajů, předmět evidence a povinnosti při zpracování osobních údajů, rozsah zpracovávaných osobních údajů („XXXXXX eviduje osobní údaje zákazníků v následujícím rozsahu: jména a příjmení, titul, adresa trvalého pobytu, korespondenční adresa, identifikační údaj (IČ), v případě OSVČ, daňové identifikační číslo (DIČ) v případě OSVČ plátce z přidané hodnoty, další údaje vyplývající z platných právních předpisů České republiky a vztahující k prodeji zboží zákazníkům. Předpis dále upravuje právní titul zpracování osobních údajů.

Směrnice dále upravuje rozsah pracovních funkcí, které mají přístup k osobním údajům zákazníků v závislosti na rozsahu pracovních rolí.
Dále směrnice upravuje Režim ochrany údajů, zajištění databáze:
Databáze obsahující zákaznické údaje je XXXXXX na vyhrazeném a chráněném serveru v rámci IT sítě XXXXXX. Přístup do této databáze je chráněn systémem přístupových účtů a oprávnění hesel a práv stanovených v rozsahu potřebném pro plnění úkolů pověřených osob dle příslušných oddělení XXXXXX.

Data XXXXXX v databázi jsou dále přímo na serveru chráněna interními bezpečnostními mechanismy zvoleného softwaru. Server je dále chráněn XXXXX. Veškerá komunikace prochází přes firewall s XXXXX.
XXXXXXXXX.
Pověřené osoby jsou povinny zpracovávat osobní údaje výhradně v rámci své pracovní náplně a úkolů, které jim byly stanoveny jejich vedoucími zaměstnanci, ve výše uvedeném rozsahu a účelu a ve shodě s ustanovením Zákona, dalších závazných předpisů a interních předpisů XXXXXX.

Směrnice dále upravuje konkrétní povinnosti pověřených osob (dbát na správnost zpracovávaných osobních údajů, vyvarovat se jakéhokoliv jednání, které by mohlo vést k neoprávněnému přístupu třetí osoby k osobním údajům, bezprostředně hlásit nadřízenému zaměstnanci každou stížnost, kterou subjekt osobních údajů podá ať ústně nebo písemně v souvislosti s ochranou svých osobních údajů, zachovávat mlčenlivost o osobních údajích a bezpečnostních opatřeních, bezodkladně hlásit nadřízenému zaměstnanci jakékoli podezření související s narušením bezpečnosti ochrany osobních údajů na pracovišti).
Dále Směrnice upravuje, že pověřeným osobám není dovoleno sdělovat komukoliv svá přístupová hesla, kódy či jiné identifikátory umožňující přístup do IT sítě XXXXXXu, případně jakéhokoli jiného interního systému XXXXXXu, sdělovat nepovolaným osobám informace o bezpečnostních opatřeních na ochranu databáze, dovolit pohyb nepovolaným osobám v prostoru, kde jsou osobní údaje zpracovávány a ukládány, sdělovat osobní údaje ve veřejných prostorách XXXXXXu, umožnit nahlížet nepovolaným osobám do listin a databáze.

Dále směrnice XXXXXX stanovuje minimální standardy ochrany osobních údajů zákazníků, které musí být na pracovišti dodržovány. „Osobní údaje budou zabezpečeny zejména, nikoliv však výlučně, následujícím způsobem:

a) veškerá data obsahující osobní údaje budou zpracovávána a budou s nimi disponovat pouze určení a pověření zaměstnanci
b) přístup k datům je vyhrazen pouze pověřeným zaměstnancům. XXXXXX zabezpečí určený prostor, kde se nacházejí nosiče dat a listiny obsahující osobní údaje tak, aby XXXXXX osobní údaje nemohly být zneužity nepovolanou osobou.
c) XXXXXX povede evidenci a dokumentaci o všech případech porušení ochrany zpracovávaných dat
d) XXXXXX zřídí individuální uživatelská oprávnění
e) XXXXXX zajistí evidenci přístupových oprávnění prostřednictvím tzv. logů (záznamů umožňujících ověření, kdo, kdy zpracovával osobní údaje zákazníků)
f) XXXXXX zajistí průběžná školení pověřených osob
g) XXXXXX zajistí zavedení opatření bránících neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů, zejména v podobě kopírování, přenosu, úpravě či vymazání dat neoprávněnými osobami
h) XXXXXX zajistí v daném odvětví odpovídající úroveň šifrování / hashování osobních údajů
i) XXXXXX zajistí zavedeni opatření pro obnovení dostupnosti osobních údajů a odpovídající přistup k nim v případě fyzických či technických incidentů
j) XXXXXX zabezpečí postupy pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování
k) XXXXXX zdokumentuje veškerá přijatá opatření
l) K výše uvedeným standardům technických a organizačních opatření je XXXXXX povinen zavázat zpracovatele, případně 3. strany, které zapojí do zpracování.

9. K žádosti, aby společnost XXXXXX 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 2013-11) 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 XXXXXX XXXXXX v souvislosti s bezpečnostní událostí. Dále, že společnost XXXXXX XXXXXX 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 XXXXXX sdělila, že v záznamu je kromě dalšího specifikována i geneze bezpečnostní události, z níž vyplývá, že se XXXXXX XXXXXX 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, XXXXXX XXXXXX 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 XXXXXX dále sdělila, že „z provedeného šetření tedy vyplývá, že narušení bezpečnosti osobních údajů v dané době společnost XXXXXX XXXXXX nebyla schopna identifikovat s ohledem na technickou pokročilost a využité nástroje ze strany původce bezpečnostní události. Veškerá data nicméně byla chráněna odpovídajícím bezpečnostním standardem. V rámci „Záznamu o bezpečnostní události a výsledcích šetření“ společnost definovala tehdejší používané bezpečnostní standardy zabezpečení hesel, přičemž od roku 2012 do roku 2016 šlo o XXXXX *(has*hování unikátní XXXXX). Používaná metoda byla v době jejího použití obvyklým bezpečnostním standardem. V současné době jsou na XXXXXX k nalezení návody na dešifrování starších typů těchto zabezpečovacích metod. Z uvedeného plyne, že databáze zveřejněná na XXXXXX obsahující rozšifrované údaje byla pravděpodobně prolomena až v pozdějším období v souvislosti s nástupem nových výkonnějších technologií. Je tak pravděpodobné, že starší a dnes již nepoužívaný způsob zakódování umožnil narušiteli jednoduchá hesla typu „123456“, „heslo“ apod. rozkódovat. K uvedenému nicméně nedošlo v roce 2014, kdy se událost uskutečnila, ale teprve až *v* roce 2017, kdy s

přihlédnutím k technologickému vývoji mohlo dojít k prolomení starších typů ochranných opatření, jako v tomto případě.

Nelze současně opomenout, že XXXXXX XXXXXX zvolil při řešení dopadů této bezpečnostní události v roce 2017 transparentní přístup zaměřený na minimalizaci jakýchkoli bezpečnostních rizik pro subjekty údajů. Bezprostředně po identifikaci *incident*u přijal odpovídající opatření společně s opatřeními určenými pro zmírnění dopadů (blíže viz Záznam o bezpečnostní události a výsledcích šetření ze dne 8. 9. *2017).*

V dnešní době je běžné, že se útočníci, jejichž cílem je odcizení databáze, zaměřují *prim*árně na technické mezery v systémech, které však nelze přikládat k tíži správce. Uvedené nedostatky nejsou při vývoji software a jiných aplikací neobvyklé, proto jsou k počítačovým aplikacím jejich tvůrci více či méně pravidelně vydávány různé *aktualizace,* typicky zaměřené na „zalepení" bezpečnostních děr (viz např. široce využívaný operační systém Windows). Právě z toho důvodu je kladen důraz na sekundární typ ochrany, tedy nemožnost data rozšifrovat. V daném případě je přitom jasné, že byť data pochází z konce roku 2014, útočník nebyl s to data v té době rozšifrovat, neboť zabezpečení bylo dostatečné. K uvedenému rozšifrování došlo až s dalším postupem technologického vývoje, o čemž svědčí zveřejnění až v roce 2017. Za takových okolností byla přirozeně řada útočníkem zveřejněných údajů již neaktuálních".

XXXXXX sdělila, že incident se týkal 766.421 záznamů o zákaznících z roku 2014, z nichž 735.956 obsahovalo unikátní e-mailové kontakty zákazníků. Jednalo se tak o cca 20 % unikátních údajů z celkové zákaznické databáze XXXXXX. Z analýzy dále vyplynulo, že v posledním roce bylo z těchto uživatelských účtů aktivních pouze cca 350.000, tedy méně než polovina.

Incident se týkal:

| | |
|---|---|
| Počet dotčených subjektů byl | 766.421 |
| Unikátní e-mailové adresy | 735.956 (cca 20% z celkové zákaznické databáze) |
| Aktivní v roce 2017 | 350.000 |

Společnost XXXXXX dále sdělila, že s ohledem na objektivní nemožnost zjistit vznik bezpečnostní události v roce 2014, nezávisle na přijatých opatřeních ze strany XXXXXX XXXXXX, 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 XXXXXX XXXXXX přistoupil k řešení celé záležitosti s maximální otevřeností a respektováním principů ochrany osobních údajů svých zákazníků. Při řešení bezpečnostní události XXXXXX XXXXXX aplikoval standardní postup stanovený vnitřními předpisy při zjištění povahy incidentu, jeho rozsahu, charakteru a souvisejících znaků. Z pohledu XXXXXX XXXXXX 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 XXXXXXX, v rámci šetření, kdo a kdy XXXXXX na úložiště XXXXXX soubor dat (hesla a kontakty z databáze společnosti XXXXXX XXXXXX, 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 XXXXXX 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 XXXXXX na webovém úložišti a s ohledem na množství souborů každý den mazaných je pro společnost Uloz.to cloud, a.s. prakticky nemožné dohledat informace o předmětném nijak blíže nekonkretizovaném souboru. Dále společnost Uloz.to cloud, a.s. 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 souboru doručena. I kdyby Společnost Uloz.to cloud, a.s. 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 500 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 Uloz.to cloud, a.s., stažený (odstraněný soubor) stále k dispozici, zda je archivován, resp. likvidován, společnost sdělila, že smazané soubory nijak nearchivuje.

11. Společnost XXXXXX XXXXX, která je provozovatelem webového portálu XXXX.cz, na žádost Úřadu sdělila, že informace zveřejněné prostřednictvím serveru XXXXX.cz, v článku XXXXXX, dne 28. 8. 2017 použila databázi klientů XXXXXX, zveřejněnou na XXXXX použila jako podklad pro článek, poté 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 XXXXXX. 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 766.421 záznamů zákazníků společnosti XXXXXXového portálu XXXXXX.CZ, XXXXX.cz, XXXXX.cz XXXX.cz, které byly ze strany spol. XXXXXX XXXXXX, a.s. 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 XXXXXX pod názvem XXXXXXX

    Policie ČR zjistila, že dne 1. září 2017 bylo na Policii ČR podáno trestní oznámení zaslané společností XXXX XXXXXX, a.s., XXXXXX, 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 766.421 záznamů zákazníků společnosti XXXXXXového portálu XXXXXX.cz, XXXXXX.cz, XXXXX.cz a XXXX.cz, které byly ze strany spol. XXXXXX XXXXXX, a.s. převzaty a následně provozovány. Dle sdělení poškozené společnosti neznámý pachatel dne 27.7.2017 uploadoval danou databázi na server XXXXX, pod názvem XXXXXXX. Po doručení daného oznámení byla neprodleně kontaktována společnost XXXXXX., se sídlem XXXXXXX, a to z důvodu žádosti o zjištění veškerých identifikačních údajů k uživateli, který na server ulozto.cz umístil předmětný soubor. Na základě vypracované zprávy poskytnuté společností Uloz.to Cloud a.s., bylo zjištěno, že obdobný soubor byl již na daný server uploadován dne 23.7.2017, přičemž tento byl na základě upozornění společnosti XXXXXX XXXXXX, a.s. 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. Vzhledem k tomu, že ze zákona nevyplývá povinnost logování IP adres uživatelů, nejsou IP adresy logovány a společnost tedy nemá informace o tom, z jaké IP adresy došlo k uploadování souborů. 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 XXXXX.cz, 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 Lupa.cz a zároveň autor článku pan XXXXX. 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 uloz.to, 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 XXXXXXX. XXXXXXX prostřednictvím e-mailové adresy XXXXXXXX, jako první upozornil poškozenou společnost na možný únik dat, které jsou volně ke stažení na serveru uloz.to. 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. Petr XXXXXX Policii dále sdělil, že ihned po zjištění popsaného obsahu tento prostřednictvím e-mailové zprávy kontaktoval společnosti XXXXXX XXXXXX, a.s., aby ji o úniku jejich dat informoval. Žádné další konkrétní skutečnosti se provedeným výslechem zjistit nepodařilo. K danému skutku byl také vyslechnut zástupce společnosti XXXXXX XXXXXX, a.s., 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 XXXXXX XXXXXX elektronickou databázi uživatelských účtů vzniklou za období nejpozději do 31. prosince 2014. Elektronická databáze uživatelských účtů, tj. klientů společnosti XXXXXX, obsahovala osobní údaje klientů v rozsahu e-mailový kontakt, přístupové heslo (v šifrované podobě), jméno, příjmení, telefonní kontakt.
Celkem bylo odcizeno 766.421 elektronických záznamů, z nichž 735.956 obsahovalo unikátní e-mailové adresy. Celkem bylo odcizeno cca 20% záznamů z celkové zákaznické databáze a cca 350.000 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 XXXXXXena (uploadovaná) nezjištěnou osobou nebo osobami na server XXXXX, a to pod názvem XXXXXX databáze na toto úložiště došlo ke zpřístupnění celé databáze nezjištěnému počtu příjemců, nezjištěnému počtu stažení – nahrání XXXXXXené databáze.

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

Společnost XXXXXX XXXXXX v období od 25. do 27. srpna 2017, resetovala hesla zákazníků registrovaných před 1. lednem 2015 (cca 1,3 mil. klientů), dále připravila a realizovala opatření spočívající v informování klientů prostřednictvím e-mailů a prostřednictvím blogu XXXXXX 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 XXXXXX XXXXXX dne 27. srpna 2017 oznámila Úřadu pro ochranu osobních údajů informaci o narušení bezpečnosti při správě osobních údajů.
Společnost XXXXXX XXXXXX dne 1. září 2017 podala trestní oznámení na neznámého pachatele Policii ČR.

Společnost XXXXXX XXXXXX 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 XXXXXX XXXXXX 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 XXXXXX XXXXXX 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 jednání, resp. zda došlo ze strany zaměstnance nebo konkrétních zaměstnanců k porušení pracovních povinností. Odcizení databáze uživatelů v roce 2014 společnost XXXXXX XXXXXX 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 XXXXXXená v období od 23. července 2017 do 27. srpna 2017 na www. XXXXXX.cz zpřístupněna a kolik osob si zde XXXXXXenou databázi nahrálo, resp. pořídilo její kopii.

**B. Porovnání zjištěného stavu věci s relevantním ustanovením právního předpisu**

Kontrolní zjištění č. 1
Společnost XXXXXX XXXXXX, 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 XXXXXX XXXXXX zpracovává ve smyslu § 4 písm. a) zákona č. 101/2000 Sb., osobní údaje svých zákazníků.
Prostřednictvím XXXXXXového obchodu jsou osobní údaje zákazníků XXXXXX automatizovaně a systematicky shromažďovány, tříděny, používány, vyhledávány a ukládány na nosiče a jsou s nimi prováděny soustavy operací. Společnost XXXXXX XXXXXX ve smyslu § 4 písm. e) zákona č. 101/2000 Sb. zpracovává osobní údaje.

Společnost XXXXXX XXXXXX 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 766.421 záznamů o zákaznících společnosti XXXXXX XXXXXX obsahujících 735.056 unikátních adres zákazníků v rozsahu jméno příjmení, uživatelské heslo, e-mailová adresa, a číslo telefonu, které měla XXXXXXeny v ICT systémech, přičemž společnost XXXXXX XXXXXX, jako správce osobních údajů neoprávněnému přístupu a odcizení databáze uživatelů, nejen nezabránila, ale ani jej nezaznamenala a nezjistila, porušila povinnost správce osobních údajů XXXXXXenou 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 766.421 záznamů o zákaznících společnosti XXXXXX XXXXXX obsahujících 735.056 unikátních adres zákazníků v rozsahu jméno příjmení, uživatelské heslo, e-mailová adresa, a číslo telefonu na veřejně přístupném webovém portálu www. XXXXX.cz 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<br>zaměstnanec Úřadu | pověřený | (dokument podepsán elektronicky) |
| ……. | | …….. |
| jméno | | podpis |
| JUDr. Michal Jelínek<br>zaměstnanec Úřadu | pověřený | (dokument podepsán elektronicky) |
| ……. | | …….. |
| jméno | | podpis |
| Ing. Max Gůt | pověřený<br>zaměstnanec Úřadu | (dokument podepsán elektron*icky)* |
| ……. | | …….. |
| jméno | | podpis |