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

Čj. UOOU-13260/16-22
Praha 17. května 2018

Protokol o kontrole

Kontrolní orgán:

Úřad pro ochranu osobních údajů, se sídlem Pplk. Sochora 27, 170 00 Praha 7 (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, dále pravomoc kontrolního orgánu k výkonu kontroly vyplývá z § 10 odst. 1 písm. a) zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti).

Kontrolující:

- inspektor Úřadu, **Ing. Josef Vacula,** průkaz inspektora č. [redacted];
- pověřená zaměstnankyně Úřadu, **Mgr. Martina Šnajderová, DiS.**, číslo průkazu [redacted];
- pověřený zaměstnanec Úřadu, **Josef Polák,** číslo průkazu [redacted];
- pověřený zaměstnanec Úřadu, **Michal Choutka,** číslo průkazu [redacted];
- pověřený zaměstnanec Úřadu, **Mgr. Vojtěch Dlouhý,** číslo průkazu [redacted];
- pověřený zaměstnanec Úřadu, **Ing. Radek Loub,** číslo průkazu [redacted], služební poměr ukončen k 9. květnu 2018.

Kontrolovaná osoba:

[redacted]

Zastoupená:

[redacted] Manažerem Data Privacy & Processing
na základě „Pověření„ člena představenstva [redacted]
[redacted] a místopředsedy představenstva [redacted],
[redacted].

Místo provedení kontroly:

- **sídlo kontrolovaného**
- **sídlo Úřadu**

Předmět kontroly:
Předmětem kontroly je dodržování povinností správce osobních údajů stanovených zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, v souvislosti se zpracováním osobních údajů při používání cloudových služeb v souvislosti s plněním povinností správce osobních údajů, zejména s ohledem na podmínky zabezpečení osobních údajů.

Zahájení kontroly: kontrola byla zahájena doručením *oznámení o zahájení kontroly* ze dne 5. prosince 2016 Čj. UOOU-13260/16-1, doručené kontrolované osobě dne 7. prosince 2016.

Poslední kontrolní úkon: posledním kontrolním úkonem předcházejícím vyhotovení protokolu o kontrole bylo doplnění podkladů ke kontrole ze dne 22. února 2018 Čj. UOOU-13260/16-21.

I. **Přehled podkladů:**
Protokol o kontrole se opírá o následující podklady (údaje, dokumenty a věci vztahující se k předmětu kontroly, nebo k činnosti kontrolované osoby, které byly pořízeny v průběhu kontroly) a o podklady a skutečnosti, které jsou kontrolnímu orgánu známy z jeho úřední činnosti:

1. Oznámení o zahájení kontroly, pod Čj. UOOU-13260/16-1 ze dne 5. prosince 2016, doručeno do datové schránky dne 7. prosince 2016, počet listů: 1
2. Vyjádření k oznámení o zahájení kontroly – [redacted], pod Čj. UOOU-13260/16-2 doručeno Úřadu dne 9. ledna 2017, počet listů: 2, přílohy:
   - 2.1. [redacted]
   - 2.2. [redacted]
   - 2.3. [redacted]
   - 2.4. [redacted]
   - 2.5. [redacted]
   - 2.6. [redacted]
   - 2.7. [redacted]
   - 2.8. [redacted]
   - 2.9. [redacted]

2.10.

2.11.

2.12.

2.13.

2.14.

2.15.

2.16.

2.17.

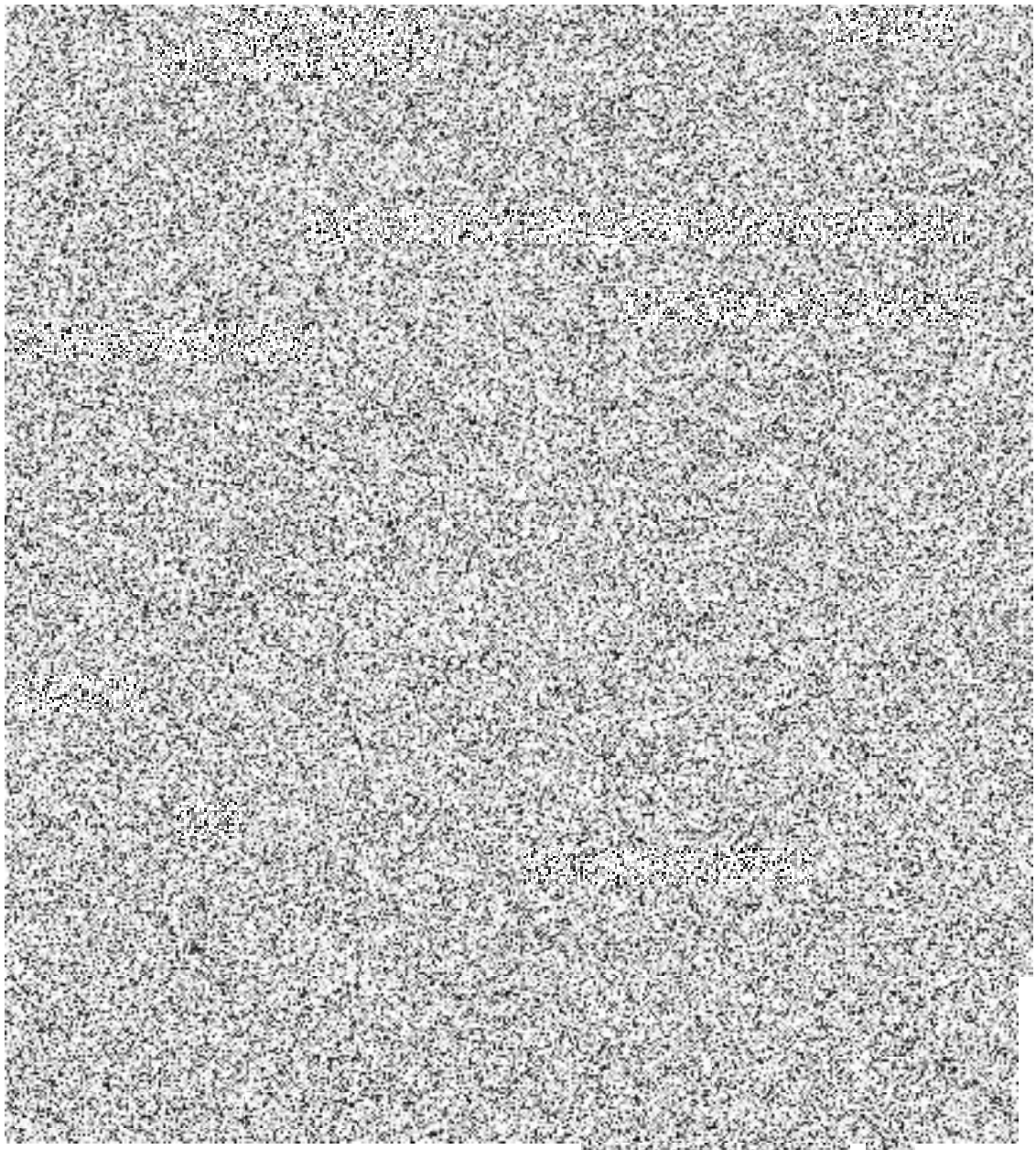
2.18.

2.19.

2.20.

2.21.

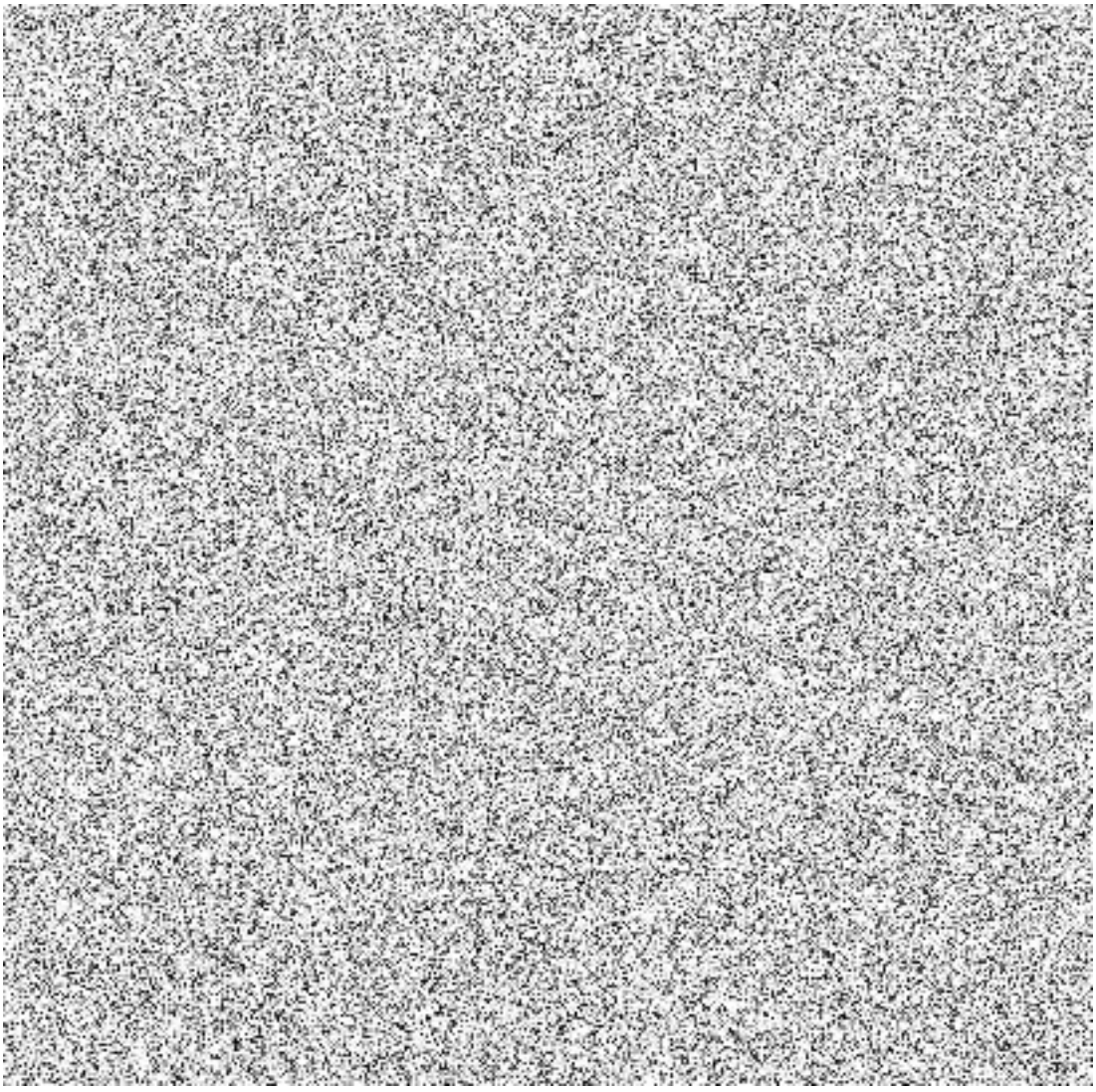
2.22.



3. Analýza rizik pro využití služeb společnosti Microsoft – [redacted], [redacted], pod Čj. UOOU-13260/16-3, doručená Úřadu dne 9. ledna 2017, počet listů: 1;
4. Žádost o dodání překladu dokumentů předložených ke kontrole v angličtině - [redacted], pod Čj. UOOU-13260/16-4 ze dne 26. ledna 2017, doručena do datové schránky dne 27. ledna 2017, počet listů: 1;
5. Reakce na „žádost o dodání překladu dokumentů předložených ke kontrole v angličtině“ - [redacted], pod Čj. UOOU-13260/16-5 doručena Úřadu dne 6. února 2017, počet listů: 2;
6. Žádost o součinnost - [redacted], pod Čj. UOOU-13260/16-6 ze dne 21. února 2017, doručena do datové schránky dne 23. února 2017, počet listů: 2;

7. Vyjádření k žádosti o součinnost - [redacted], pod Čj. UOOU-13260/16-7 doručeno Úřadu dne 3. března 2017, počet listů: 2;
8. Interní sdělení – postoupení stížnosti podle § 175 SŘ k vyřízení, pod Čj.UOOU-13260/16-8 ze dne 9. března 2017, počet listů: 1; příloha:
   8.1. Vyjádření ke stížnosti [redacted]. – Ing. Vacula, inspektor, počet listů: 1
9. Vyřízení stížnosti podle § 175 SŘ - [redacted], pod Čj. UOOU-02837/17-5 (Čj. UOOU-13260/16-11) ze dne 27. března 2017, počet listů: 1;
10. Výzva ke splnění povinnosti - [redacted], pod Čj. UOOU-13260/16-13 ze dne 11. dubna 2017, doručena do datové schránky dne 12. dubna 2017, počet listů: 1;
11. Dopis předsedkyně Úřadu ke splnění povinnosti - [redacted], pod Čj. UOOU-02837/17-9 (Čj. UOOU-13260/16-14) ze dne 4. května 2017, doručen do datové schránky dne 9. května 2017, počet listů: 2;
12. Výzva ke splnění povinnosti - [redacted], pod Čj. UOOU-13260/16-15 ze dne 23. května 2017, doručena do datové schránky dne 24. května 2017, počet listů: 1;
13. Zaslání překladu smluvní dokumentace - [redacted], pod Čj. UOOU-13260/16-16 doručeno Úřadu dne 9. června 2017, počet listů: 1; přílohy:

13.1.
13.2.
13.3.
13.4.
13.5.
13.6.
13.7.
13.8.
13.9.
13.10.
13.11.



13.12. [redacted]

13.13. [redacted]

13.14. [redacted]

14. Úřední záznam - § 12 odst. 2 zákona č. 255/2012 Sb., o kontrole (kontrolní řád), pod Čj. UOOU-13260/16-17 ze dne 9. srpna 2017, počet listů: 1;

15. Žádost o součinnost - oznámení ústního jednání a místního šetření - [redacted], pod Čj. UOOU-13260/16-18 ze dne 24. ledna 2018, doručena do datové schránky dne 25. ledna 2018, počet listů: 1;

16. Sdělení o změně (rozšíření kontrolní skupiny) - [redacted], pod Čj. UOOU-13260/16-19 ze dne 24. ledna 2018, doručeno do datové schránky téhož dne, počet listů: 1;

17. Protokol z ústního jednání a místního šetření pod Čj. UOOU- 13260/16-20 ze dne 8. února 2018, počet listů: 3;

18. Doplnění podkladů ke kontrole - [redacted], pod Čj. UOOU-13260/16-21 doručeno Úřadu dne 22. února 2018, počet listů: 1, přílohy:

    18.1. Penetration Test [redacted] (Záznam z penetračního testu [redacted], počet listů: 13;

    18.2. Rozhodnutí [redacted] Chief Information Officeer [redacted] zabezpečení informací [redacted]: 6;

    18.3. Rozhodnutí [redacted] Chief Executive Officer [redacted], Zásady informační bezpečnosti [redacted], počet listů: 9;

    18.4. Rozhodnutí [redacted] Chief Information Officer [redacted], Správa uživatelských účtů, ze dne [redacted], počet listů: 7;

    18.5. [redacted]

    18.6. Rozhodnutí [redacted] Chief Executive Officer [redacted], Zásady užívání informačních zdrojů [redacted], počet listů: 6;

    18.7. Analýza rizik pro využití nástroje [redacted], počet listů: 1;

    18.8. Rozhodnutí [redacted] Chief Compliance Officer [redacted], ze dne [redacted], počet listů: 7;

    18.9. [redacted]

18.10. Rozhodnutí Chief Compliance Officer [redacted], Pravidla vzdělávání v oblasti [redacted], počet listů: 3;

18.11. Rozhodnutí Chief Informatioon Officer [redacted], Klasifikace informací [redacted], počet listů: 2;

18.12. Koncernové rozhodnutí představenstva [redacted], Pravidla pro správu IT Zařízení a Softwaru, [redacted], počet listů: 4;

18.13. Záznam logu z nástroje [redacted], počet listů: 1;

18.14. Příklady alertů z nástroje [redacted], počet listů: 2;

18.15. Rozhodnutí č. [redacted], Řízení případů ztráty a úniku informací, [redacted], počet listů: 3;

18.16. [redacted]

18.17. Popis procesu kontroly a správy uživatelských účtů [redacted] e -mail ze dne 21. února 2018, počet listů: 2;

18.18. Schvalovací [redacted] pro připojitelná zařízení, platné [redacted], počet listů: 1;

18.19. [redacted], počet listů: 1;

18.20. Příloha podezřelého Alertu [redacted], počet listů: 8;

18.21. Podezřelý Alert [redacted], počet listů: 1,

18.22. Pověření zaměstnance banky k zastupování v rámci kontroly, počet listů: 1.

II. Kontrolní zjištění kontrolujícího:

1. Obecně k předmětu kontroly:

Předmětem kontroly je zjištění stavu zabezpečení cloudových služeb, které kontrolovaná osoba využívá ve vztahu k ochraně osobních údajů.

Kontrolující z doložených dokumentů, které jsou uvedeny v rámci přehledu podkladů pod body 13 a 18 a také na základě výsledků ústního jednání a místního šetření (viz přehled podkladů bod 17) zjistil, že kontrolovaná osoba využívá tři typy níže uvedených cloudových služeb.

V prvním případě využívá kontrolovaná cloudovou službu [redacted], která slouží jako úložiště dokumentů, které jsou podstatné pro jednání orgánů a výborů kontrolované osoby. [redacted]

[redacted]

Další cloudovou službou, která je kontrolovanou osobou využívána, je služba společnosti Microsoft. Od této společnosti kontrolovaná osoba odebírá produkt [redacted]

[redacted]

Ze závěrů ústního jednání a místního šetření (viz bod 17 přehledu podkladů) vyplývá, že osobní údaje se nacházejí pouze ve třetí využívané cloudové službě – službě společnosti [redacted]

[redacted]

Z vyjádření kontrolované osoby na tomto jednání dále vyplývá, že osobní údaje fyzických osob nejsou v [redacted]. Osobní údaje fyzických osob se nacházejí pouze v úložištích kontrolované osoby s tím, že pro přístup k těmto datům má kontrolovaná osoby vypracován vnitřní předpis.

2. Kontrolující jako první posuzoval, zda kontrolovaná osoba při své činnosti zpracovává osobní údaje. K tomu kontrolující cituje zákon č. 101/2000 Sb.:

> *„Osobním údajem* (se rozumí) *jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“*

Z předložených dokumentů pod bodem č. 13 přehledu podkladů a z vyjádření kontrolované osoby (viz bod č. 17 přehledu podkladů) vyplývá, že v případě využití cloudového řešení [redacted]

Kontrolovaná osoba tak v rámci využití služeb zpracovatele, svého smluvního partnera, výše uvedené společnosti, nakládá se širokým spektrem informací, které je možné označit za osobní údaje, neboť na základě takových informací, jako je např.: číslo bankovního účtu, či číslo smlouvy, má kontrolovaná osoba možnost přímo identifikovat konkrétní fyzickou osobu. K tomu je možné odkázat na odbornou literaturu, která uvádí: *„...nicméně osobním údajem mohou být i informace odlišného charakteru, nezávislé na osobnosti jedince, např. rodné číslo nebo číslo bankovního účtu.“*[1] V této otázce se kontrolující rovněž odkazuje na Přílohu 1: Kategorie údajů a subjekty údajů Dodatku o zpracování údajů a zabezpečení

[1] Kučerová, A., Nováková, L., Foldová, V., Nonneman, F., Pospíšil, D. Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012 s. 51.

(Čj. UOOU-13259/16-8). V tomto dokumentu je jednoznačně uvedeno, že *„osobní údaje předložené, uložené, zaslané, ... prostřednictvím Služeb mohou zahrnovat ID uživatele, email, dokumenty, prezentace,...“.*

Dle vyjádření zástupce kontrolované osoby (viz bod č. 17 přehledu podkladů) se v systému [redacted] nacházejí údaje o právnických a o fyzických osobách podnikajících. K fyzickým osobám podnikajícím kontrolující konstatuje, že jde o osoby, které podnikají na základě zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon). Údaje vztahující se k osobám podnikajícím dle živnostenského zákona (a rovněž údaje vztahující se k příslušníkům svobodných povolání) jsou sice převážně vázány na jejich profesní (ekonomickou) sféru, což by naznačovalo vyloučení aplikace zákona č. 101/2000 Sb., o ochraně osobních údajů, na druhou stranu jsou tyto údaje zveřejňovány a mají jednoznačně dopad i na jejich soukromý život a zároveň je v některých případech těžko oddělitelné, které údaje se vztahují ke které části jejich života – zda k jejich profesní části, či k části soukromé.

Na základě toho je možné konstatovat, že kontrolovaná osoba je schopna identifikovat konkrétní fyzickou osobu (respektive fyzickou osobu podnikající), tedy subjekt údajů ve smyslu § 4 písm. d) zákona č. 101/2000 Sb., a kontrolovaná osoba tak při své činnosti pracuje s osobními údaji ve smyslu § 4 písm. a) zákona č. 101/2000 Sb.

3. Dle § 4 písm. e) zákona č. 101/2000 Sb. se zpracováním osobních údajů rozumí:

   „...jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.“

   K tomu kontrolující uvádí, že k naplnění shora uvedeného definičního znaku zpracování není nutné, aby došlo k naplnění všech uvedených činností, ale postačuje, aby byla vykonávána alespoň jedna z nich.

   K tomu kontrolující dodává, že zaměstnanci kontrolované osoby při své činnosti využívají mj. právě shora uvedený systém [redacted], tedy aplikaci, ve které jsou ukládány osobní údaje o fyzických osobách podnikajících, které jsou zákazníky kontrolované osoby.

   Dle shora popsaného, využíváním systému [redacted], ukládáním informací do něj a dalšími operacemi s osobními údaji jako například vyhledáváním, shromažďováním, úpravou či jejich používáním, tak kontrolovaná osoba zpracovává osobní údaje, nacházející se v tomto systému, ve smyslu zákona č. 101/2000 Sb.

4. Pojem správce osobních údajů je zákonem č. 101/2000 Sb. definován následovně:

   „Správcem každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak.“

   K tomu kontrolující konstatuje, že kontrolovaná osoba zpracovává v rámci systému [redacted] osobní údaje svých klientů – fyzických osob podnikajících, a to za účelem poskytování bankovních služeb těmto osobám.

   Jako prostředek pro správu portfolia svých klientů – fyzických osob podnikajících – si kontrolované osoba vybrala nástroj svého smluvního partnera, aplikaci [redacted], která je poskytována jako cloudová služba.

   Kontrolovaná osoba **je správcem osobních údajů** ve smyslu § 4 písm. j) zákona č. 101/2000 Sb., neboť stanovila účel a prostředky zpracování osobních údajů, jak je uvedeno výše.

5. V návaznosti na předmět kontroly se kontrolující zabýval posouzením celého § 13 zákona č. 101/2000 Sb., a to jak obecně, tak ve vztahu k systému [redacted]. Kontrolující níže cituje ustanovení § 13 zákona č. 101/2000 Sb.:

   „§ 13
   (1) Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k 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. Tato povinnost platí i po ukončení zpracování osobních údajů.

   (2) Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.

   (3) V rámci opatření podle odstavce 1 správce nebo zpracovatel posuzuje rizika týkající se

   a) plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům,
   b) zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování,
   c) zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje a
   d) opatření, která umožní určit a ověřit, komu byly osobní údaje předány.

(4) V oblasti automatizovaného zpracování osobních údajů je správce nebo zpracovatel v rámci opatření podle odstavce 1 povinen také

a) zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby,

b) zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,

c) pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, a

d) zabránit neoprávněnému přístupu k datovým nosičům.“

Obecně k předmětu kontroly kontrolující konstatuje, že si od kontrolované osoby vyžádal materiály, které se k předmětu kontroly vztahují. Jedná se především o vnitřní technicko-organizační opatření a také o dokumenty vztahující se k využívání cloudových služeb. Tyto jsou uvedeny pod body 13 a 18 přehledu podkladů a kontrolující z nich uvádí relevantní:

- Zabezpečení informací, [redacted], viz bod 18.2. přehledu podkladů, upravující pravidla a zásady v oblasti prevence a ochrany před únikem dat,
- Zásady informační bezpečnosti, [redacted], viz bod 18.3. přehledu podkladů, definující zásady v oblasti informační bezpečnosti a upravující dodržování bezpečnostních zásad, vychází z norem ISO 27001 a 27002,
- Správa uživatelských účtů, [redacted], viz bod 18.4. přehledu podkladů, upravující procesy v oblasti uživatelských účtů v rámci kontrolované osoby,
- Klasifikace informací, [redacted], viz bod 18.11. přehledu podkladů,
- Řízení případů ztráty a úniku informací, [redacted], viz bod 18.15. přehledu podkladů, upravující postup v případě ztráty nebo úniku informací.

Za tím účelem kontrolující vyhodnotil dokumenty dodané kontrolovanou osobou. Jako první se kontrolující zabýval dokumentem „Zabezpečení informací“ (viz bod č. 18.2. přehledu podkladů). V úvodu tohoto dokumentu vymezila kontrolovaná osoba pojem „nakládání s informacemi“ jako *„jakoukoli práci s informacemi, zejména pak jejich vytváření, úprava, ukládání, odesílání, tisk a jiné formy zpracování“*. Ze smyslu celého dokumentu pak vyplývá, že pojmem „informace“ se rozumí jak informace obecné (vztahující se např. k vnitřním záležitostem kontrolované osoby), tak i osobní údaje.

Kontrolovaná osoba rozděluje informace do čtyř stupňů (bod 3.1. Zabezpečení informací), kdy podrobný popis těchto stupňů je obsažen v [redacted] upravující klasifikaci informací (viz bod 18.11. přehledu podkladů). V rámci tohoto rozlišení se mohou osobní údaje nacházet [redacted]. Dokumenty podle příslušného klasifikačního stupně musí být ukládány v souladu s bodem 4.4.4. shora uvedeného dokumentu, tedy pouze do úložišť, která jsou schválená a jejichž seznam se nachází na intranetu kontrolované osoby. [redacted]

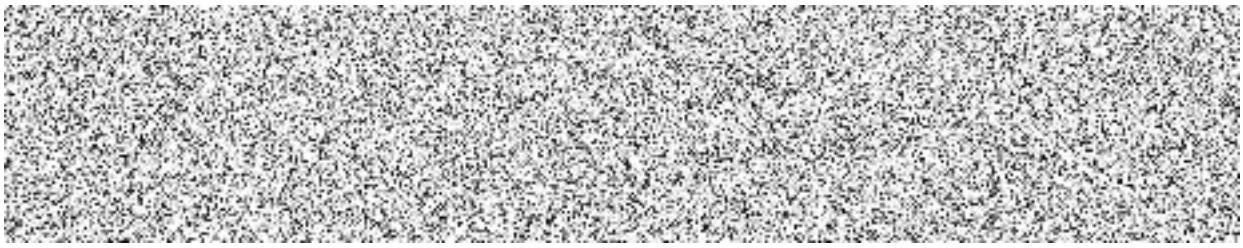
Kontrolovaná osoba rovněž upravila povinnosti týkající se pracování s informacemi ve spojitosti s mobilními telefony a tablety, které je možné připojovat k majetku kontrolované osoby jak pomocí kabelu, tak bezdrátově, vždy však pouze v případě, že jsou splněny podmínky pro toto připojování, které jsou popsány v tabulce (bod 4.5.2.). [redacted]. Kontrolovaná osoba rovněž upravila otázky týkající se připojování zařízení typu počítače, notebooky a jiná paměťová zařízení. Způsob, jakým lze tato zařízení připojovat a kdy je možné z těch zařízení číst, či kdy je možné na tato zařízení ukládat informace, je upraven bodem 8.2. [redacted].

Kontrolovaná osoba rovněž provádí školení informační bezpečnosti a také další školení, která jsou uvedena v dokumentu „Pravidla vzdělávání“ viz bod 18.10. přehledu podkladů. Školení mají tři různé charaktery – vstupní školení, periodické školení a nadstavbové školení. Vstupní školení mají povinnost absolvovat všichni zaměstnanci, [redacted]. Periodická školení jsou rozdělena dle zařazení zaměstnanců na pracovní pozice s tím, že každý zaměstnanec má povinnost toto školení opakovaně absolvovat [redacted]. Nadstavbová školení se týkají pouze vybraných zaměstnanců a jsou zaměřena na aktuální problematiku vztahující se k pozici (pracovnímu zařazení) daného zaměstnance.

Dále k odstavci 1 kontrolující uvádí, že kontrolovaná osoba v dokumentu „Zásady informační bezpečnosti“ (viz bod 18.3. přehledu podkladů) zakotvuje za účelem předejití ztráty informací povinnost pravidelného zálohování a též testování obnovy pořízených záloh (bod 7.6. Zásad informační bezpečnosti). [redacted]

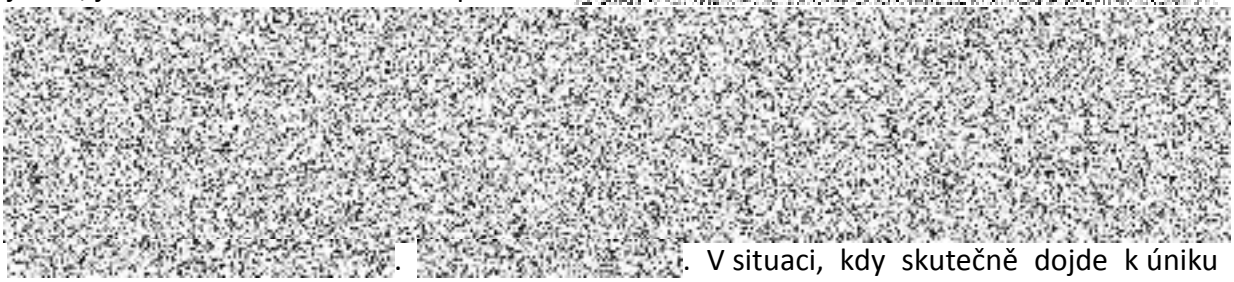
Elektronická pošta prochází, v případě, že je odesílána mimo síť kontrolované osoby, „skenováním“, [redacted].

Aby nedocházelo k neoprávněnému přístupu k informacím, přijala kontrolovaná osoba potřebná opatření, která jsou definována v dokumentu „Správa uživatelských účtů“ (viz bod 18.4. přehledu podkladů).



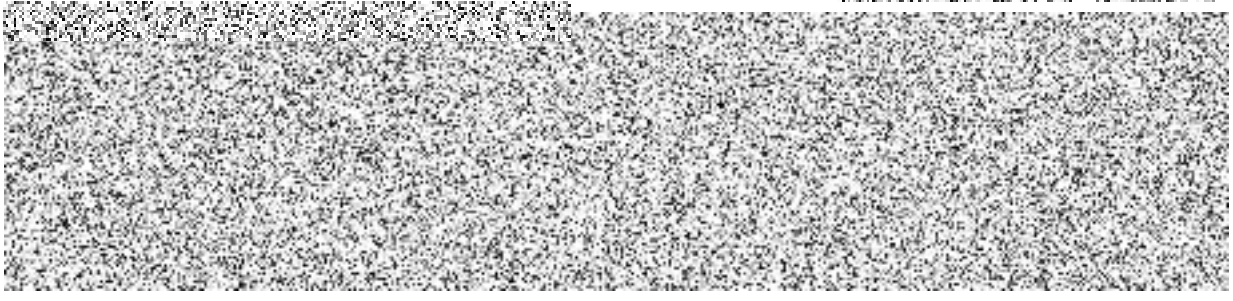
Kontrolovaná osoba rovněž přijala opatření, která se týkají ukončení přístupu a ukončení účtu celého.

V případě neadekvátní činnosti uživatele každého účtu má kontrolovaná osoba nastaveny alerty, které jsou následně řešeny. V záznamu z alertu je možné seznat, o kterého uživatele se jedná, jakou nestandardní činnost provedl.



. . V situaci, kdy skutečně dojde k úniku informací, má kontrolovaná osoba přijatá opatření, která tento únik mají řešit. Jedná se o dokument „Řízení případů ztráty a úniku informací“, bod 18.15. přehledu podkladů. V tomto dokumentu jsou stanoveni zaměstnanci, kteří se podílejí na řešení úniku informací a jsou také zakotveny postupy vnitřního šetření úniku informací a přijetí následných nápravných opatření.

Obecně k odstavci 1 ve vztahu k zabezpečení ukládaných dat do prostředí svého smluvního partnera kontrolující dodává, že této problematice se věnuje .



V rámci odstavce 2 poskytla kontrolované osoba dokumenty, které jsou uvedeny v přehledu podkladů pod body 13 a 18. Tyto dokumenty obsahují technicko-organizační opatření a také smluvní dokumentaci mezi správcem a zpracovatelem osobních údajů.

K odstavci 3 kontrolující sděluje, že kontrolovanou osobou byla rovněž doložena analýza rizik (příloha č. 7 k Čj. UOOU-13260/16-21). V rámci této analýzy rizik kontrolovaná osoba vyhodnotila vliv osob, které pracují s osobními údaji (např. bankéři) na potenciální rizika, která jsou s touto činností spjata, dále též přístup neoprávněných osob k osobním údajům zákazníků kontrolované osoby jakož i neoprávněné nakládání s osobními údaji a také vyhodnotila rizika spjatá s předáním osobních údajů. V návaznosti na tuto analýzu rizik a z ní vyplývající závěry, přijala kontrolovaná osoba předmětná technicko-organizační opatření, která obsahují i úpravu problematiky ochrany osobních údajů s tím, že jednotlivé ustanovení z těchto technicko-organizačních opatření, která se vztahují k předmětu kontroly, jsou součástí tohoto protokolu o kontrole.

Dále k tomuto odstavci kontrolující sděluje, že v rámci analýzy rizik si kontrolovaná osoba podstoupila tzv. penetrační test, jehož výsledek je obsažen v dokumentu pod bodem 18.1. přehledu podkladů.

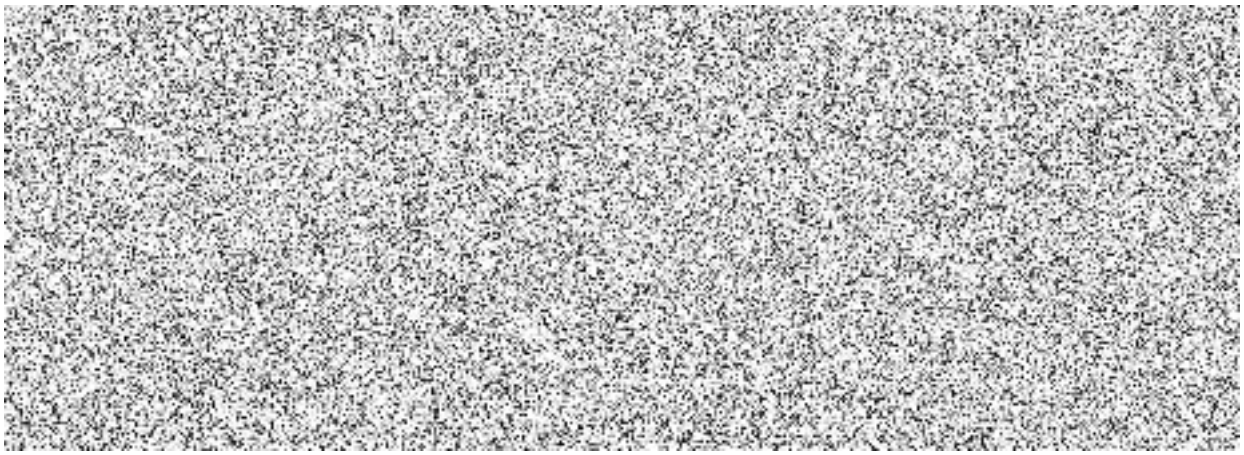
K odstavci 4 písm. a) kontrolující konstatuje, že tím, že kontrolovaná osoba přijala [redacted], jasným způsobem stanovila oprávnění jednotlivých uživatelů k přístupu do vnitřních informačních systémů kontrolované osoby, a tím i stanovila oprávnění přístupu každého zaměstnance k osobním údajům.

K odstavci 4 písm. b) kontrolující konstatuje, že tato problematika je obsažena v dokumentu Zabezpečení informací (viz bod 18.2. přehledu podkladů). V tomto dokumentu kontrolovaná osoba zakotvuje povinnost každého uživatele nakládat pouze s těmi informacemi, které potřebuje k výkonu svých pracovních povinností (bod 4.1. Zabezpečení informací) a rovněž s těmito informacemi provádět pouze takové operace, ke kterým mají uživatelé přidělena oprávnění (bod 4.2. cit. dokumentu). Dále se kontrolující odkazuje na dokument „Zásady informační bezpečnosti“, viz bod 18.3. přehledu podkladů. V tomto dokumentu pod bodem 5.4. je zakotvena povinnost jednotlivých přímých nadřízených zajistit, aby každý jejich podřízený měl zajištěn takový rozsah přístupových práv, který je nezbytný k výkonu jim přidělené práce. Zároveň mají tito vedoucí pracovníci povinnost dodržovat postupy při ukončení přístupových práv.

K písm. c) odst. 4 se vztahuje čl. V. shora uvedeného dokumentu (Zabezpečení informací). Za tím účelem kontrolovaná osoba rozlišuje přenos informací v rámci struktur kontrolované osoby a přenos informací mimo tyto struktury. Přenosem uvnitř struktur kontrolované osoby se rozumí takový přenos dle bodu 5.2.1. písm. a) a b) čl. V. V rámci těchto přenosů musí být informace zabezpečeny, a to dle toho, jaké informace jsou přenášeny [redacted]

, doložila tedy výpis logů z přístupů do systému . Z tohoto záznamu je patrné, že kontrolovaná osoba zaznamenává uživatele, čas, IP adresu a území, ze kterého bylo do systému přistupováno.

K písm. d) odst. 4 kontrolující konstatuje, že se jedná o problematiku, která se rozprostírá jak od fyzického zabezpečení, tak po zabezpečení, které se dotýká IT oblasti a softwaru. V rámci tohoto ustanovení kontrolovaná osoba doložila vnitřní směrnici (příloha č. 3 k Čj. UOOU-13260/16-21), ve které je upraven vstup osob do chráněných prostor,



Na základě vyhodnocení veškerého shora uvedeného má kontrolující za prokázané, že kontrolovaná osoba v době prováděné kontroly postupovala v oblasti zabezpečení v souladu s § 13 zákona č. 101/2000 Sb., kdy kontrolovaná osoba přijala dostatečná opatření, která by měla minimalizovat rizika úniku informací a tato opatření kontrolovaná osoba řádně dokumentovala. Dále pak kontrolovaná osoba vyhodnotila rizika, která pro osobní údaje vyplývají z její činnosti a z činnosti a počtu svých zaměstnanců a dále přijala kontrolovaná osoba v oblasti automatizovaného zpracování dostatečná opatření, jejichž cílem je minimalizovat riziko nezákonného nakládání s osobními údaji, se kterými se kontrolovaná osoba při výkonu své činnosti dostává do kontaktu.

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.

Podpisová doložka:

otisk
úředního
razítka

	inspektor	
…….	……	…….
Ing. Josef Vacula	funkce	podpis
		(dokument podepsán elektronicky)

	pověřený zaměstnanec Úřadu	
…….	……..	…….
Josef Polák	funkce	podpis
		(dokument podepsán elektronicky)

	pověřený zaměstnanec Úřadu	
…….	…….	…….
Michal Choutka	funkce	podpis
		(dokument podepsán elektronicky)

	pověřený zaměstnanec Úřadu	
…….	…….	…….
Mgr. Vojtěch Dlouhý	funkce	podpis
		(dokument podepsán elektronicky)

	pověřená zaměstnankyně Úřadu	
…….	…….	…….
Mgr. Martina Šnajderová, DiS.	funkce	podpis
		(dokument podepsán elektronicky)