



## ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ

Pplk. Sochora 27, 170 00 Praha 7  
tel.: 234 665 111, fax: 234 665 444  
posta@uouu.cz, www.uouu.cz



Čj. UOUU-07567/18-22  
Praha 12. října 2018

### Protokol o kontrole

#### Kontrolní orgán:

Úřad pro ochranu osobních údajů, se sídlem Pplk. Sochora 727/27, 170 00 Praha 7

Pravomoc kontrolního orgánu k výkonu kontroly vyplývá z čl. 58 odst. 1 písm. b) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), ve spojení s ustanovením § 2 odst. 2 a odst. 3, ustanovením § 29 odst. 1 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, dále ze zákona č. 255/2012 Sb., o kontrole (kontrolní řád) a ze zákona č. 500/2004 Sb., správní řád.

#### Kontrolující:

PhDr. Petr Krejčí – inspektor Úřadu pro ochranu osobních údajů  
JUDr. Jana Kosobudová – pověřená zaměstnankyně Úřadu pro ochranu osobních údajů

#### Kontrolovaná osoba:

██████████, ██████████, ██████████, ██████████, ██████████

Osoba jednající za kontrolovanou osobu:

██████████, ██████████

#### Místo provedení kontroly:

██████████, ██████████, ██████████ a ██████████, ██████████

#### Předmět kontroly:

Předmětem kontroly je dodržování povinností stanovených Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) ve spojení se zákonem č. 101/2000 Sb. v souvislosti se zpracováním osobních údajů shromážděných ve smlouvách o poskytování veřejně dostupných služeb elektronických komunikací a rámcových smlouvách o poskytování veřejně dostupných služeb elektronických komunikací, které byly zpřístupněny u obchodního domu ██████████, ██████████ dne ██████████ ve ██████████ ██████████ nalezeném usb flash disku, obsahujícím několik set souborů s osobními údaji v těchto na usb flash disk ██████████ naskenovaných smlouvách uzavřených kontrolovanou osobou s fyzickými osobami v době ██████████

### **Zahájení kontroly:**

Kontrola byla zahájena Oznámením o zahájení kontroly ze dne 19. září 2018, čj. UOOU-07567/18-13, doručené kontrolované osobě dne 21. září 2018.

### **Poslední kontrolní úkon:**

Vyhodnocení kontrolovanou osobou doplněných podkladů doručených datovou schránkou ze dne 4. října 2018 a ze dne 5. října 2018 k protokolu z ústního jednání a místního šetření ze dne 27. září 2018.

### **1) Přehled podkladů:**

Protokol o kontrole se opírá o následující podklady a dokumenty, které byly pořízeny před zahájením kontroly a v jejím průběhu, popř. o dokumenty a skutečnosti, které jsou kontrolnímu orgánu známy z jeho úřední činnosti:

1. *Podnět ze dne [redacted] o zpřístupnění osobních údajů několika set souborů s citlivými údaji v naskenovaných smlouvách místního poskytovatele internetu [redacted], na nalezeném usb flash disku [redacted] u obchodního domu [redacted] 07567/18-1. 1 list + 6 příloh:*
  - 1.1. *Smlouva o poskytování veřejně dostupných služeb elektronických komunikací uzavřená kontrolovanou osobou s [redacted]. 1 list;*
  - 1.2. *Smlouva o poskytování veřejně dostupných služeb elektronických komunikací uzavřená kontrolovanou osobou se [redacted]. 1 list;*
  - 1.3. *Smlouva o poskytování veřejně dostupných služeb elektronických komunikací uzavřená kontrolovanou osobou s [redacted]. 1 list;*
  - 1.4. *Smlouva o poskytování veřejně dostupných služeb elektronických komunikací uzavřená kontrolovanou osobou s [redacted]. 1 list;*
  - 1.5. *Smlouva o poskytování veřejně dostupných služeb elektronických komunikací uzavřená kontrolovanou osobou s [redacted]. 1 list;*
  - 1.6. *Smlouva o poskytování veřejně dostupných služeb elektronických komunikací uzavřená kontrolovanou osobou s [redacted]. 1 list.*
2. *Interní sdělení o postoupení podnětu obsahujícího podezření z porušení nařízení Evropského parlamentu a Rady (EU) 2016/679 odborem konzultačních agend odboru kontrolnímu, ze dne 7. srpna 2018, čj. UOOU-07567/18-2. 1 list.*
3. *Vyrozumění ze dne 13. srpna 2018 doručené v e-mailové zprávě oznamovateli téhož dne, čj. UOOU-07567/18-3 s žádostí o poskytnutí usb flash disku. 1 list.*
4. *Interní sdělení o postoupení podnětu odborem kontrolním inspektorem inspektorátu 3 k dalšímu postupu, ze dne 13. srpna 2018, čj. UOOU-07567/18-4. 1 list.*
5. *E-mailovou zprávou zasláná informace od oznamovatele ze dne 20. srpna 2018, čj. UOOU-07567/18-5. 1 list.*
6. *Příprava kontroly – návrh řešení, ze dne 10. září 2018, čj. UOOU-07567/18-6. 1 list.*
7. *Výzva oznamovateli k předložení podkladů k podnětu ze [redacted] s možností osobně se účastnit jednání k doplnění podnětu, čj. UOOU-07567/18-7. 1 list.*



18. Vyjádření a doplnění informací ke kontrole od kontrolované osoby ze dne 4. října 2018 k protokolu z ústního jednání a místního šetření ze dne čj. UOOU-07567/18-18. 2 listy + 5 příloh:
- 18.1. Usnesení o odložení trestní věci – podezření ze spáchání přečinu krádeže, týkající se vloupání do budovy [REDACTED] ve [REDACTED] v době [REDACTED], kde nezjištěný pachatel odcizil věci v celkové hodnotě [REDACTED]. 1 list;
- 18.2. Prezenční listina zaměstnanců o absolvování školení na práci s osobními údaji podle GDPR v době od [REDACTED].
- 18.3. Potvrzení o přijatém oznámení Policií ČR ze dne [REDACTED], ve věci „Neoprávněný přístup k počítačovému systému a nosiči informací“. 1 list;
- 18.4. Úřední záznam ze dne [REDACTED] o podaném vysvětlení na Policii ČR. 2 listy;
- 18.5. GDPR Analýza pro potřeby [REDACTED]. 1 list.
19. Doplnění informací ke kontrole kontrolovanou osobou ze dne 5. 10. 2018 o nový vnitřní předpis „GDPR Analýza pro potřeby [REDACTED]“. 1 list.

## 2) Kontrolní zjištění:

### A. Zjištěný stav věci

1. Úřadu pro ochranu osobních údajů byl dne [REDACTED] doručen podnět, ve kterém mj. oznamovatel vyzval Úřad pro ochranu osobních údajů k zahájení šetření společnosti [REDACTED] z důvodu podezření na porušení zákona o ochraně osobních údajů a GDPR nařízení proto, že dne [REDACTED] našel u obchodního domu [REDACTED] usb flash disk, který měl obsahovat několik set souborů s citlivými osobními údaji, včetně souboru s rodným číslem stěžovatele (pozn.: podle několika jmen užívaných oznamovatelem v rámci komunikace s kontrolujícími, nebylo takové jméno v seznamu smluv dohledáno). Jako důkaz, že se jedná o smlouvy uvedeného místního poskytovatele internetu, předložil oznamovatel v příloze podnětu v listinné podobě 6 souborů, o nichž tvrdil, že jsou pořízeny z nalezeného usb flash disku, obsahujícího naskenované smlouvy o poskytování veřejně dostupných služeb elektronických komunikací, uzavřené uvedenou společností se zákazníky/uživateli, obsahující:

Ve smlouvě [REDACTED] uzavřené dne [REDACTED] s [REDACTED] adresu, telefon, číslo OP, rodné číslo;

Ve smlouvě [REDACTED] uzavřené dne [REDACTED] se [REDACTED] adresu, telefon a rodné číslo;

Ve smlouvě [REDACTED] uzavřené dne [REDACTED] s [REDACTED] adresu, telefon, email, datum narození a rodné číslo;

Ve smlouvě [REDACTED] uzavřené dne [REDACTED] s [REDACTED] adresu, telefon, email a rodné číslo;

Ve smlouvě [REDACTED] uzavřené dne [REDACTED] s [REDACTED] adresu, telefon, číslo OP a rodné číslo;

Ve smlouvě [REDACTED] uzavřené dne [REDACTED] s Robertem Krausem, adresu, telefon, email, datum narození, číslo OP a IČ.

Na vyžádání podkladů kontrolujícím stěžovatel doručil usb flash disk, z něhož bylo pořízeno kontrolujícím v listinné podobě 7 souborů a seznam všech smluv, které byly zaslány kontrolované osobě v příloze Oznámení o zahájení kontroly čj. UOOU-07567/18-13 tak, aby

měla kontrolovaná osoba dostatek času, aby se k nim mohla vyjádřit na ústním jednání a místním šetření konaném dne [REDACTED].

Jednalo se tedy o předložení těchto 7 souborů z usb flash disku obsahující tyto osobní údaje:

Ve smlouvě [REDACTED] uzavřené dne [REDACTED] s [REDACTED], adresu, telefon, datum narození, rodné číslo;

Ve smlouvě [REDACTED] uzavřené dne [REDACTED] s [REDACTED], adresu, telefon, email, datum narození, číslo OP;

Ve smlouvě [REDACTED] uzavřené dne [REDACTED] s [REDACTED], adresu, telefon, email, rodné číslo;

Ve smlouvě [REDACTED] uzavřené dne [REDACTED] s [REDACTED], adresu, telefon, email, rodné číslo, adresa místa odběru služby;

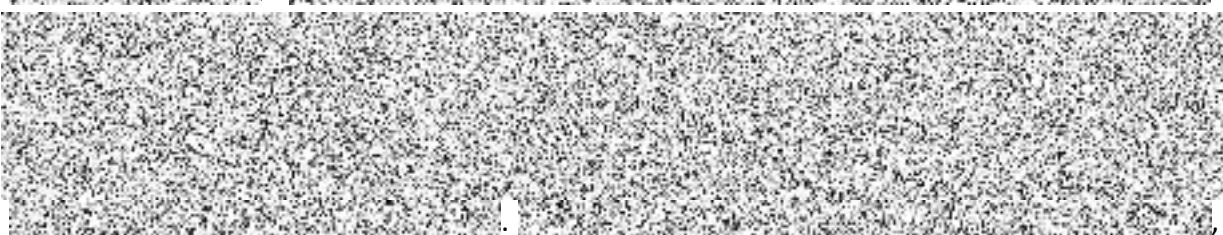
Ve smlouvě [REDACTED] uzavřené dne [REDACTED] s [REDACTED], adresu, telefon, email, datum narození, číslo OP;

Ve smlouvě [REDACTED] uzavřené dne [REDACTED] s [REDACTED], adresu, email, datum narození, rodné číslo, IČ;

Ve smlouvě [REDACTED] uzavřené dne [REDACTED] s [REDACTED], adresu, telefon, email, datum narození, číslo OP;

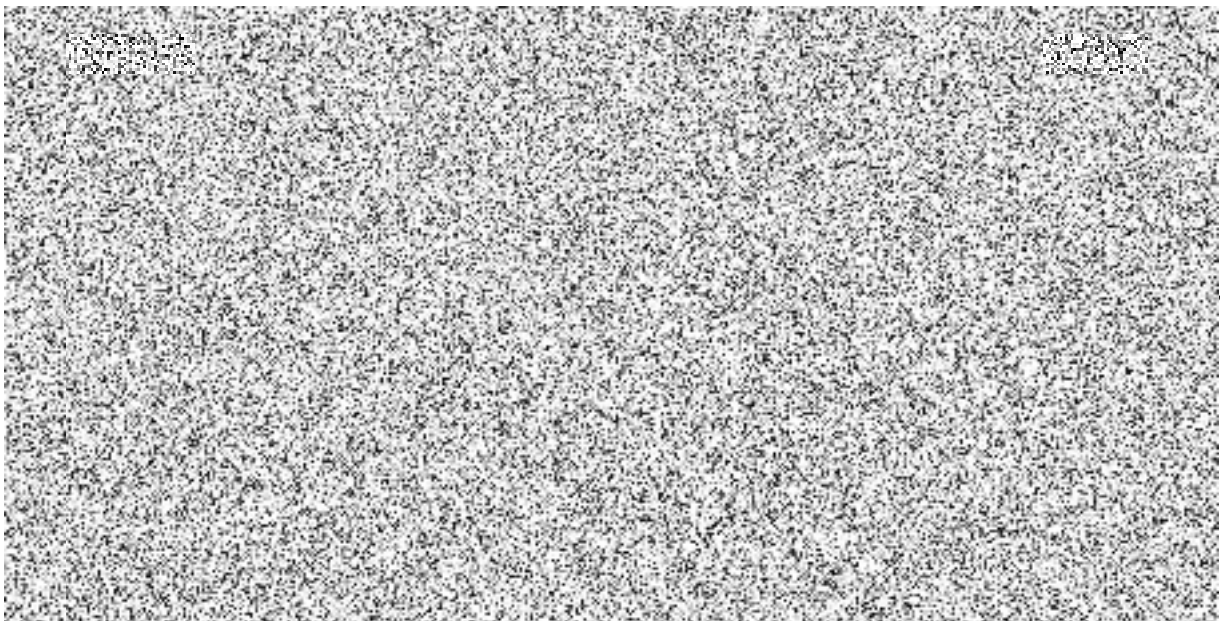
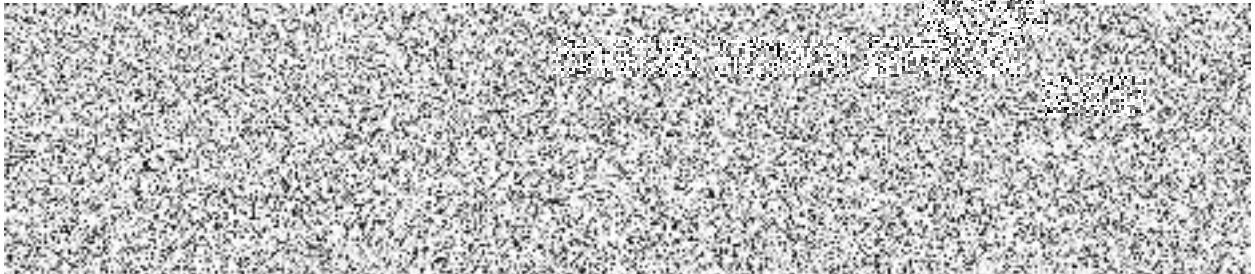
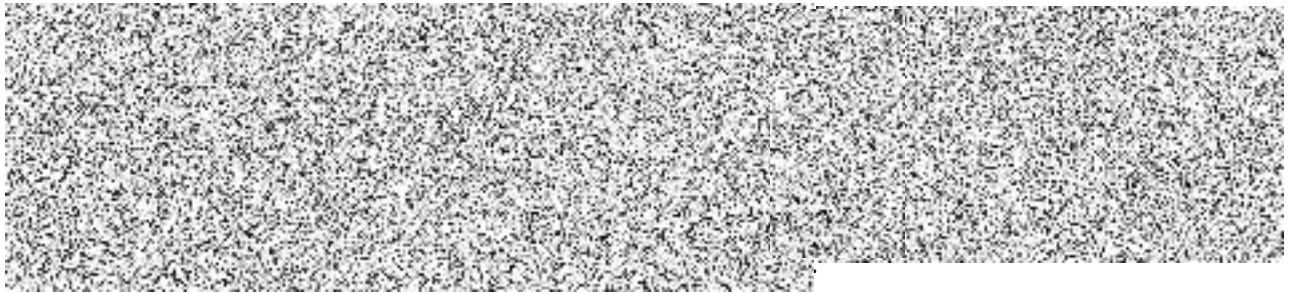
2. Kontrolovaná osoba je zapsána v obchodním rejstříku, vedeném Městským soudem v Praze, oddíl [REDACTED], vložka [REDACTED] od [REDACTED], jejímž předmětem podnikání je Výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona, Poskytování služeb elektronických komunikací, Zajišťování veřejných komunikačních sítí. Jménem společnosti je oprávněn jednat samostatně jednatel, [REDACTED], který je současně i jediným společníkem, od data vzniku a zápisu společnosti do obchodního rejstříku, přičemž druhým jednatelem byl [REDACTED]. Kontrolovaná osoba nemá jmenovaného pověřence.







3. Kontrolovaná osoba se zabývá poskytováním telekomunikačních služeb, zejména Internetu a projekty budování datové komunikační infrastruktury, tj. WAN sítí, serverů pro internetové služby (www.mail apod.), software atd. Od svého vzniku [REDACTED] buduje vlastní telekomunikační síť [REDACTED].



Hlavní činnost společnosti se [REDACTED] přesunula do kancelářských prostor ve [REDACTED] (sídlo kontrolované osoby), pro lepší dostupnost ze strany zákazníků pro doplňkové služby – konzultace, správa pc apod. Vzhledem k častým výpadkům elektrické energie v regionu v [REDACTED], vyvíjí vlastní dlouhodobé záložní zdroje elektrické energie umožňující překlenout plánované, leč celodenní výpadky elektrické energie. [REDACTED]





6. V souvislosti se zajištěním péče o zákazníky má kontrolovaná osoba tým , kteří plní vůči zákazníkům informační povinnost přímo při vyplňování smluv s nimi uzavíranými, včetně kontrolovanou osobou na webových stránkách zveřejněných všeobecných podmínek platných , obchodních podmínek přenesení čísla platných , , včetně ceníku služeb platný , . Kontrolovaná osoba nemá obchodní zástupce, kteří by nebyly zaměstnanci kontrolované osoby a jsou na smlouvách podepsaní. Kontrolovaná osoba při vyplňování smlouvy údaje získanými osobně od subjektů údajů při uzavírání smluvního vztahu dává na výběr, zda kontrolovaná osoba poskytne rodné číslo nebo číslo občanského průkazu. Rodné číslo tak, jak je uvedeno v předmětných smlouvách vyžadovala v daném období proto, že jako povinný údaj bylo vyžadováno v případě soudního vymáhání dlužné částky ve smyslu ustanovení § 320c zákona č. 99/1963 Sb, občanský soudní řád, podle něhož „k návrhu oprávněného, který musí kromě obecných náležitostí obsahovat i rodné číslo povinného....“, tj. dle zákonné úpravy do 31. 12. 2012, přičemž v dalších právních úpravách pro přetrvávající různorodost právních výkladů došlo k několika novým právním úpravám ustanovení § 261 odst. 1, podle něhož „uvede oprávněný v návrhu na výkon rozhodnutí rodné číslo povinného, je-li mu známo“. Rovněž ve věci obsahových náležitostí žalobního návrhu z důvodů různých právních názorů, kdy soudy



požadovaly pro správnou identifikaci osoby žalovaného, dle ustanovení § 79 podle právní úpravy stavu k 13. 5. 2008 kromě obecných náležitostí, jména, příjmení a bydliště také „další údaje potřebné k identifikaci účastníků řízení“. Dalšími upřesňujícími novelami rozpor v právním výkladu odstraněn nebyl, pokud byl do § 79 dále implementován do obsahových náležitostí žalobního návrhu současný text: „Návrh musí kromě obecných náležitostí § 42 odst. 4 obsahovat jméno, příjmení bydliště, popřípadě rodná čísla účastníků...“. Nadto se kontrolovaná osoba odvolává na zákon č. 127/2005 Sb., podle jehož ustanovení § 63 odst. 3 písm. b) bod 3 je vyžadováno rodné číslo u smluv o poskytování veřejně dostupné služby elektronických komunikací. Proto se kontrolovaná osoba domnívá, že by nemělo jít k její tíži, pokud rodné číslo sděloval do smlouvy sám subjekt údajů v souvislosti s uzavřením smluvního vztahu s kontrolovanou osobou, resp. se souhlasem a současně v souvislosti s možností do budoucna vymáhaných částek bylo toto rodné číslo ve smlouvě ponecháno pro případné soudní řízení a jakýkoliv pozdější jednostranný zásah kontrolované osoby do smlouvy, tj. vymazání rodného čísla, by nebyl možné, jestliže nikdo ze subjektů údajů vymazání rodného čísla ze smlouvy nepožadoval a kontrolovaná osoba vzhledem k zákonné úpravě v občanském soudním řízení (v případě nezaplacení antény) a v řízení o sporech, které řeší Český telekomunikační úřad (ČTÚ), tj. o službě, resp. připojení, nepovažovala tento údaj za nadbytečný. Z jednání, tj. řešení sporů s ČTÚ, kdy došlo k prvním rozhodnutím, bylo teprve z těchto rozhodnutí potvrzeno, jaké údaje jsou skutečně nutné, provedla kontrolovaná osoba vlastní rozhodnutí o tom, že již rodná čísla v současné době do smluv nezapisuje. Na základě doporučení Úřadu pro ochranu osobních údajů si kontrolovaná osoba provedla změnu obsahu smlouvy i na vzoru umístěného na webové stránce kontrolované osoby, přičemž tímto způsobem vyhověla nové přísnější úpravě v Obecném nařízení o ochraně osobních údajů, než byl původní výklad jak Úřadu pro ochranu osobních údajů podle zákona č. 101/2000 Sb., tak i Českého telekomunikačního úřadu podle zákona č. 127/2005 Sb.

7. Kontrolovaná osoba zpracovává smlouvy obsahující osobní údaje v listinné a elektronické podobě, a to v jedné evidenci, přičemž nevyužívá služeb zpracovatelů osobních údajů. Smlouvy uzavírá prostřednictvím vlastních zaměstnanců, přičemž v rozhodné době se jednalo o tyto zaměstnance: [redacted] a [redacted]

8. Kontrolovaná osoba zpracovává pouze osobní údaje, které získala přímo od subjektu údajů, který je tak přímo informován v celém rozsahu o zpracovávání jeho osobních údajů, a v rozsahu předmětu kontroly i informacemi na webové stránce kontrolované osoby, která tuto informační povinnost plní v souvislosti s uzavíráním smlouvy, jejíž úplné znění včetně příloh je zveřejněno na webové stránce kontrolované osoby. Kontrolovaná osoba tak zpracovává pouze přesné osobní údaje a nepřesné osobní údaje, resp. změny, aktualizuje podle doplňujících údajů přímo od subjektů údajů a tyto dále nepředává jiné třetí osobě, kromě firmy, která zpracovává účetnictví pro kontrolovanou osobu, resp. jsou jí předávány pouze faktury v požadovaném rozsahu zpracovávaných údajů podle zákona o účetnictví, nikoliv smlouvy. Jedná se o fyzickou osobou podnikající podle živnostenského zákona [redacted], s níž má kontrolovaná osoba uzavřenou smlouvu o vedení účetnictví.

9. Osobní údaje se likvidují jejich výmazem, jakmile pomine účel jejich zpracování. V listinné podobě jsou osobní údaje v listinách skartovány ve skartovacím stroji. O likvidaci, resp. skartaci trvalým vyřazením klienta z evidence, bude dle tvrzení kontrolované osoby vždy sepsán protokol. Zatím kontrolovaná osoba k likvidaci faktur a smluv nepřistoupila, vzhledem ke kontrole uskutečněné v roce [redacted] z finančního úřadu a k rozsahu požadovaných listin

i z dob minulých. Obecně musí kontrolovaná osoba uchovávat minimálně tyto údaje po dobu 10 let, a pokud do nejstaršího roku po uplynutí této lhůty zasahuje úvěr, leasing či jiná finanční záležitost, tak finanční úřad může požadovat podklady za dobu trvání tohoto úvěru, leasingu a celého účetnictví. Proto jsou tyto finančním úřadem požadované údaje, vždy po provedené účetní závěrce, v listinné podobě uloženy v archivu kontrolované osoby. K likvidaci osobních údajů nedošlo také proto, aby byly k dispozici jako důkaz při případném uplatnění nároků v občanskoprávním řízení, včetně plnění povinností vyplývajících i ze zvláštních zákonů pro uchovávání dokumentů, zejména podle zákona 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, zákona č. 127/2005 Sb. v souvislosti s rozhodování ve sporech Českého telekomunikačního úřadu, a pro účely případné daňové kontroly apod. Lhůta pro uplatnění nároku se nepočítá ve smyslu zákona č. 127/2005 Sb. jen ode dne ukončení smluvního vztahu, ale i ode dne přerušení nebo ode dne odepření poskytované služby, vždy podle konkrétního případu.

10. Kontrolovaná osoba stanovila účel, k němuž mají být osobní údaje zpracovány, jímž je zpracování osobních údajů v souvislosti s poskytováním služby, resp. poskytování internetu a k tomuto účelu je shromažďuje pouze otevřeně a nebylo zjištěno, že by je zpracovávala pod záminkou jiného účelu nebo jiné činnosti, než k němuž byly shromážděny. Kontrolovaná osoba nesdružuje osobní údaje, které by měly být získány k rozdílným účelům. Z jiných zdrojů než od samotných zájemců o internet kontrolovaná osoba osobní údaje subjektů údajů nezískává. Kontrolovaná osoba uvedla, že svým zákazníkům žádné reklamní e-maily nezasílá.

11. Kontrolovaná osoba neviduje zejména podle ustanovení § 12 zákona č. 101/2000 Sb. žádnou žádost o informaci, jež by byla zpoplatněna, jejímž obsahem by mělo být sdělení o účelu zpracování osobních údajů, o osobních údajích, případně kategoriích osobních údajů, které jsou předmětem zpracování, včetně veškerých dostupných informací o jejich zdroji, o povaze automatizovaného zpracování v souvislosti s jeho využitím pro rozhodování, jestliže jsou na základě tohoto zpracování činěny úkony nebo rozhodnutí, jejichž obsahem je zásah do práva a oprávněných zájmů subjektu údajů, o příjemci, případně kategoriích příjemců a podle ustanovení § 21 tohoto zákona žádost o podání informace, případně nápravě subjektem údajů vytykávaném stavu, resp., že by subjekt údajů, včetně oznamovatele, využil svého práva podle čl. 12 odst. 3 nařízení a požádal kontrolovanou osobu o informaci ke zpracování svých osobních údajů.

12. Dokumentovaná přijatá a provedená technická a organizační opatření k zajištění ochrany osobních údajů v souladu s obecně platnými právními předpisy má kontrolovaná osoba zpracované v novém vnitřním předpisu „GDPR Analýza pro potřeby [redacted] z něhož dle původního rozsahu požadovaných údajů bylo vypuštěno rodné číslo, podle něhož kontrolovaná osoba posuzuje rizika týkající se plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům. Přístup do aplikace (systému) je možný [redacted]. Pokud se zaměstnanec přihlašuje do systému mimo pracoviště, [redacted]. Neoprávněné dotazy jsou webovou aplikací zamítnuty. Zobrazení smluv se dá dohledat [redacted]. Kontrolovaná osoba prohlašuje, že má dostatečně chráněn elektronický systém tak, aby bylo zabráněno neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování, resp. zabráněno neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje. Má opatření, která umožní určit a ověřit, komu byly osobní údaje předány. [redacted].



[REDACTED]. Kontrolovaná osoba prokázala logování vzorkem zaznamenaných přihlášení obsahující číslo přihlášení, jedinečný klíč přihlášení - [REDACTED], a k tomu vzorkem akcí v systému, [REDACTED], včetně účelu, resp. jakou operaci kdo prováděl, obsahující IP adresu, odkud přišel požadavek (přihlášení podle klíče), čas, systémová akce s klíčem přihlášení. Ke všem elektronickým datům mají přístup jednatel a ze zaměstnanců [REDACTED] a [REDACTED], které, se k předmětu kontroly vyjádřili v písemných vyjádřeních založených ve spise. Se souhlasem jednatele mohli/mohou k datům přistupovat administrátoři sítě, kteří mají přístup na servery v souvislosti s plněním jejich pracovních povinností.

13. Kontrolovaná osoba umožnila provést kontrolu, tj. místní šetření na třech místech, a to v sídle kontrolované osoby ve [REDACTED], [REDACTED], [REDACTED] do [REDACTED]. Listiny jsou do doby převozu do archivu uloženy [REDACTED]. Zákazník telefonicky nebo osobně v sídle kontrolované osoby, si objedná instalaci internetu s tím, že v dohodnuté době se dostaví technik či obchodní zástupce, resp. zaměstnanec kontrolované osoby na místo instalace a po potvrzení možnosti připojení jsou do formulářového znění smlouvy doplněny během instalace osobní údaje zákazníka. Smlouvu následně odveze do kanceláře, pokud není při osobní účasti zákazníka uzavřena přímo v kanceláři. Následně dojde k dozapsání údajů do systému v elektronické podobě, resp. k jejich oskenování.

14. [REDACTED] - [REDACTED] - [REDACTED]. V systému je vedena osoba pouze podle jména, zákaznického čísla, telefonního čísla, pokud jej uvedla.

15. Budova archivu a kanceláři [REDACTED], [REDACTED], [REDACTED]

16. [REDACTED]

17.

18. Zaměstnanci v provozovně pracují na terminálech. Podle své pracovní pozice mají přístup do části administračního systému, obsahující osobních údaje v rozsahu jméno, příjmení, adresa, telefonní číslo, vystavení faktury a stav úhrady, IP adresa. Nemají však přístup ke smlouvám, resp. k naskenovaným smlouvám. Zaměstnanci jsou oprávněni k používání elektronického systému tak, aby měli přístup pouze k osobním údajům, které potřebují k výkonu své pracovní činnosti a k tomu mají zřízená zvláštní uživatelská přístupová oprávnění, tj.

Kontrolovaná osoba pořizuje elektronické záznamy, tj. logy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány. Vzorky logů zakládá kontrolovaná osoba do přílohy k tomuto protokolu. Kontrolovaná osoba tak garantuje, že ochrana osobních údajů je dostatečně zabezpečena tak, aby nemohlo dojít k neoprávněnému zpřístupnění osobních údajů, a to zejména s ohledem na nová pravidla pro správce osobních údajů stanovená v Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), s účinností od 25. 5. 2018, jehož ustanoveními implementovanými do právního řádu České republiky se kontrolovaná osoba řídí, a k tomu přizpůsobila svojí činnost, zejména při zpracování osobních údajů v elektronické podobě, kdy musí být vždy dohledatelné kdo, kdy a z jakého důvodu se s nimi mohl seznámit, resp. je měl v dispozici (tj. zabezpečila logování na neomezeně dlouhou dobu tak, aby bylo dohledatelné nakládání s osobními údaji konkrétními zaměstnanci) a rovněž zajistila řádnou likvidaci, pomine-li účel jejich zpracování, a aby tak byla snadněji zjistitelná konkrétní osoba, která případně neoprávněně zpřístupnila osobní údaje. Přitom zejména dbá na ochranu soukromí zpracovávaných osobních údajů, což má zdokumentováno ve vnitřním předpisu k zajištění ochrany osobních údajů, včetně návodu či postupu při informování o rozsahu zpracování jejich osobních údajů, včetně jejich zpřístupnění.

19. Kontrolovaná osoba dodatečně předložila kontrolujícím předpis, který obsahuje popis a postup při zpracování osobních údajů, včetně prezenční listiny zaměstnanců o seznámení se s postupy a ochranou osobních údajů subjektů údajů, jejichž osobní údaje kontrolovaná osoba zpracovává a že je tak závazný pro všechny zaměstnance kontrolované osoby. Vzhledem k většímu časovému odstupu již kontrolovaná osoba nedisponuje obdobným předpisem, kterým se v době pořízení či uložení smluv na usb flash disk měli zaměstnanci kontrolované osoby řídit. Kontrolovaná osoba zcela vylučuje, že by zaměstnanci mohli bez souhlasu zaměstnavatele kopírovat či ukládat na usb disk pro vlastní potřebu jakékoliv smlouvy či osobní údaje subjektů údajů zpracovávané kontrolovanou osobou v souvislosti s uzavřenými smlouvami, a pokud by tak někdo učinil, dopustil by se porušení pracovních povinností.

20. U kontrolované osoby nedošlo, resp. jí není známo, že by za její existence, tedy kdy zpracovává osobní údaje subjektů údajů, k jakékoliv mimořádné události související se ztrátou dat, tedy k neoprávněnému vstupu do databáze, resp. do informačního systému vedeného v elektronické podobě, k žádné ztrátě listin obsahujících osobní údaje subjektů údajů, ani jí není známo, že by doklady určené ke skartaci nebyly někdy v minulosti řádně



hodin formátován, tedy nemohla být pravdivá informace podaná oznamovatelem Úřadu pro ochranu osobních údajů, že usb flash disk s předmětnými údaji, který byl Úřadu doručen až na výzvu dodatečně poštou [REDACTED] byl nalezen [REDACTED] před obchodním domem [REDACTED]. S diskem nemohl pracovat amatér, pokud je celý disk důkladně vyplněn jen 0 a nelze zjistit, co na něm bylo předtím. V rozděleném disku se kontrolované osobě podařilo najít jen zbyteček skrytých informací o předchozím formátování [REDACTED]. K tomu kontrolovaná osoba předložila ilustraci analýzy, která byla provedena programem [REDACTED], s příložením screenshoty z bitové analýzy disku, včetně přístupu k souborům [REDACTED] v ilustraci 2, které odpovídá přístupu kontrolujících k údajům v usb flash disku. Taktéž pojmenování souborů neodpovídá tomu, co používá kontrolovaná osoba. Číslo XXX je na disku náhodné. Kontrolovaná osoba používá pojmenování smluv před nahráním do databáze jen ve tvaru XXXX, kde XXXX je číslo zákazníka, což neodpovídá u smluv na „nalezeném nosiči dat“.

25. Na základě zjištěného kontrolovaná osoba nabyla přesvědčení; i s ohledem na to, že usb flash disk byl formátován několikrát opakovaně, aby nebylo nic prozrazeno o jeho původu, obálka s usb flash diskem byla silně parfémovaná, usb flash disk byl pojmenován MAKR, což má evokovat, že patří jednateli [REDACTED]; že data nebyla získána legálně, ale trestnou činností se snahou poškodit dobré jméno kontrolované osoby či přímo jednatele, a proto podala kontrolovaná osoba [REDACTED] trestní oznámení na Policii České republiky k šetření orgánům činným v trestním řízení tak, aby byl pachatel vypátrán a oprávněně potrestán a očištěno tak dobré jméno kontrolované osoby. Přitom v souvislosti s podaným vysvětlením navrhla, aby byla orgány činnými v trestním řízení zajištěním stop provedena analýza e-mailu s vyžádáním si uživatelských přístupů se zjištěním IP adresy se ztotožněním uživatele a provedena důkladná rekonstrukce usb disku, včetně případné obnovy vymazaných údajů z disku a tak zjištěn skutečný majitel a jeho pravá motivace k vymyšlení celé záležitosti, včetně zjištění, jakým způsobem si opatřil osobní údaje (došlo ke zcizení dat) poskytnutých na usb flash disku, případně tak mohla být zjištěna osoba, která zřejmě disponuje dalším souborem smluv, resp. ve dvou případech i smluv, které nebyly v elektronické podobě uloženy do systému, resp. šesti smlouvami příloženými k podnětu, avšak tyto nejsou obsahem poskytnutého usb flash disku, a tak na základě těchto si přisvojených cizích dat neoprávněně nakládá s osobními údaji subjektů údajů, tj. klientů kontrolované osoby, které tak mohly být získané některou z trestných činností podle ustanovení trestního zákona.

26. Kontrolovaná osoba upřesnila dodatečně po vyhodnocení všech dostupných informací, resp. důkladnější analýze usb flash disku tak, jak uvedla do úředního záznamu o podaném vysvětlení ze [REDACTED] na Policii ČR ve [REDACTED] možné varianty úniku dat, resp. jejich zcizení, které jsou nyní v šetření orgánů činných v trestním řízení. Za nejpravděpodobnější variantu považuje kontrolovaná osoba, že zcizení dat došlo z počítače, kde byly pořízeny skeny, či z přenosného media. V obou případech, ale po přesunu na koncový počítač, odkud byly nahrány do systému, byla data smazána, mohlo tak dojít k jejich obnovení pomocí specializovaného programu. Mohlo se tak stát např. [REDACTED], kdy bylo rozhodnuto z důvodu zvýšené ochrany dat o naskenování všech dokumentů v listinné podobě, které byly do té doby uzamčené v kanceláři. Poté byly listiny uloženy v uzamčeném archivu a v elektronické verzi nahrány do administračního systému, kde jsou zpřístupněny jen některým zaměstnancům. Vše je tedy předmětem šetření orgánů činných v trestním řízení.

27. V rámci součinnosti kontrolující potvrdili kontrolované osobě, že pokud budou orgány činnými v trestním řízení vyzváni v souvislosti se šetřením případné trestné činnosti oznamovatele, usb flash disk těmto orgánům k dalšímu šetření, včetně další důkazů, tj. e-mailové adresy, od tohoto oznamovatele, poskytnou k jeho případné identifikaci a získání od něho pravdivých informací, o důvodu jejich pořízení a nakládání s nimi, resp. jakým způsobem si opatřil soubory smluv s velkým množstvím osobních údajů klientů kontrolované osoby, které nemohli být pořízeny z elektronické databáze, nepatří na souboru označeném zkratkou [REDACTED], který jej ani nemohl ztratit, pokud takový typ disku neužívá, v rozhodné době u obchodního domu [REDACTED] nebyl a na usb flash disk byl soubor pořízen až po jeho formátování, tj. [REDACTED].

28. Po této zkušenosti kontrolované osoby, kdy dosud nečelila jinému zpřístupnění či zveřejnění údajů týkajících se jejich klientů/zákazníků ani se na ní nikdo ve smyslu žádosti o informace nebo vysvětlení či odstranění vzniklého stavu neobrátil, provedla další technická opatření a místo rychlého formátu tak, aby usb disk byl po přesunutí oskenovaných souborů prázdný, nově bude opakovaně disk zaplňovat jiným souborem pro maximální možnou ochranu, resp. nenávratnou likvidaci osobních údajů v souboru tak, aby mohl čelit případnému zneužití údajů svými zaměstnanci, resp. IT specialisty.

**B. Porovnání zjištěného stavu věci s relevantním ustanovením Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) ve spojení se zákonem č. 101/2000 Sb.**

29. K článku 2 a článku 3 Obecného nařízení o ochraně osobních údajů:

Podle věcné a místní působnosti uvedené v článku 2 a článku 3 Obecného nařízení o ochraně osobních údajů, podle nichž se nařízení vztahuje v daném případě zejména na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těchto osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny a nevztahují se na ně v čl. 2 odst. 2 vyjmenované výjimky a takového zpracování osobních údajů souvisí zejména s činností provozovny správce nebo zpracovatele v Unii, resp. v České republice, spadá kontrolovaná osoba pod působnost Obecného nařízení o ochraně osobních údajů.

30. K článku 4 odst. 1) Obecného nařízení o ochraně osobních údajů:

Podle odst. 1) tohoto článku se pro účely tohoto nařízení rozumí „osobními údaji“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.


Ze shromažďovaných informací kontrolovanou osobou v rozsahu předmětu kontroly uvedených ve smlouvách o poskytování veřejně dostupných služeb elektronických komunikací a rámcových smlouvách o poskytování veřejně dostupných služeb elektronických komunikací, které byly obsahem nalezeného usb flash disku, lze zjistit identitu fyzických osob, které smlouvu podepsaly, a proto informace o těchto nositelích takto shromážděných

informací, které se jich týkají, jsou osobními údaji podle článku 4 Obecného nařízení o ochraně osobních údajů.

Za osobní údaje subjektů údajů lze kromě jména, příjmení, adresy bydliště, telefonu, emailové adresy, data narození, rodného čísla, čísla OP/pasu, IČ a DIČ považovat i dle obsahu smlouvy určitá sdělení o poskytované službě, pokud zasahují do osobnostní integrity jejího nositele a tudíž požívají rovněž ochrany osobních údajů.

### 31. K článku 4 odst. 2) Obecného nařízení o ochraně osobních údajů:

Pro účely tohoto nařízení se rozumí „zpracováním“ jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Kontrolovaná osoba jako provozovatel telekomunikační sítě  s osobními údaji fyzických osob, resp. subjektů údajů, kterými jsou jeho zákazníci/uživatelé poskytnuté služby na základě uzavřené smlouvy, shromážděnými za účelem, k němuž mají být osobní údaje zpracovány, jímž je zpracování osobních údajů v souvislosti s poskytováním internetu a služeb s tím souvisejících, provádí operace, a to i s pomocí automatizovaných postupů jako je zejména shromáždění osobních údajů ve smlouvách, jejich uspořádání, použití, uložení, zpřístupnění určeným zaměstnancům za účelem plnění pracovních povinností, a to v listinné podobě s uložením do archivu po převedení smlouvy do elektronické podoby. Proto v daném případě jde o zpracování osobních údajů předmětných fyzických osob, resp. subjektů údajů, kontrolovanou osobou.

### 32. K článku 4 odst. 7) Obecného nařízení o ochraně osobních údajů:

Pro účely tohoto nařízení se rozumí „správcem“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů, jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho jmenování.

Kontrolovaná osoba jako právnická osoba určila účel, k němuž mají být osobní údaje zpracovány, jímž je zpracování osobních údajů zákazníků/uživatelů z uzavřených smluv na poskytování dohodnutých služeb v souvislosti s provozováním telekomunikační sítě skvelý.net., což je v souladu se zákonem č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, (zákon o elektronických komunikacích).

Kontrolovaná osoba určila prostředky zpracování osobních údajů, jimiž jsou automatizované i neautomatizované, resp. uložené smlouvy v listinné podobě po jejich převedení do elektronické podoby naskenováním do archivu.

Tím, že si kontrolovaná osoba sama určila účel i prostředky zpracování osobních údajů, které získala osobně od zákazníků jejich vyplněním do smlouvy, je správcem osobních údajů podle Obecného nařízení o ochraně osobních údajů.



### 33. K článku 5 Obecného nařízení o ochraně osobních údajů:

V souladu se zásadami zpracování osobních údajů uvedenými v článku 5 tohoto nařízení tak, jak bylo jejich dodržování kontrolovanou osobou ve smyslu odst. 2. tohoto článku doloženo, nebylo zjištěno, že by ve smyslu odst. 1. písm. a) až f) tohoto článku kontrolovaná osoba v rozsahu předmětu kontroly ve vztahu k subjektu údajů nezpracovávala osobní údaje korektně a zákonným a transparentním způsobem; neshromažďovala je pro určité, výslovně vyjádřené a legitimní účely; nebyly by přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovány; nebyly by přesné a v případě potřeby aktualizované, a pokud by byly nepřesné s přihlédnutím k účelu, pro které se zpracovávají, nebyly by bezodkladně vymazány nebo opraveny; nebyly by uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovány; nebo zpracovány způsobem, který nezajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

### 34. K článku 6 odst. 1. Obecného nařízení o ochraně osobních údajů:

V souladu s článkem 6 odst. 1. tohoto nařízení je zpracování zákonné pouze, pokud je splněna nejméně jedna z podmínek uvedených pod písm. a) až f) tohoto odstavce a pouze v odpovídajícím rozsahu, přičemž podmínkou podle písm. a), b) a c) tohoto odstavce je, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů; zpracování je nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů; a zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje.

Kontrolovaná osoba provádí zpracování osobních údajů zákazníků v rozsahu předmětu kontroly v souvislosti s uzavíráním smluvních vztahů a plnění povinností s tím souvisejících, včetně vymáhaného plnění za poskytnutou službu. Pokud zpracovávala osobní údaje v rozsahu tak, jak je prezentován ve smlouvě, jejíž formulářové znění určené k vyplnění osobních údajů je zveřejněno na webové stránce kontrolované osoby, tj. v rozsahu jméno, příjmení, adresa, telefon, e-mail, datum narození, číslo OP/pasu, IČ, DIČ, korespondenční adresa, a podpis, jedná se o zpracování osobních údajů nezbytné pro plnění smlouvy ve smyslu článku 6 odst. 1 písm. b) nařízení. Pokud zpracovávala rodná čísla zákazníků jako alternativu k číslu občanského průkazu, jednalo se o zpracovávání takovýchto osobních údajů ve smlouvách uzavřených do roku 2013 v souladu zejména s ustanovením § 261 a § 320c zákona č. 99/1963 Sb., v tehdy platném znění, podle nichž bylo nutné v případě soudního sporu disponovat rodným číslem zákazníka, dále v souladu s ustanovením §63 odst. 1 písm. b) bod 3. zákona č. 127/2005 Sb., resp. tehdy platných právních výkladů zákona autoritami, tedy v souladu s ustanovením § 13 odst. 9 ve spojení s ustanovením § 13c zákona č. 133/2000 Sb. Pokud jsou ve starších smlouvách rodná čísla ponechána, je to tak proto, že je nelze bez dodržení určitých právních postupů jednostranně pozměnit, a rovněž pro velké množství v té době uzavřených smluv by bylo nevhodné a možná i neproveditelné, takovéto rodné číslo ze smluv oboustranně vyškrtnout bez možnosti obnovy. Nemůže jít k tíži kontrolované osoby, pokud rodná čísla ve smlouvách ponechala, pokud je má řádně zabezpečené, resp. uložené na bezpečném místě. Tak jako v minulosti, tak i v současnosti zpracovává kontrolovaná osoba osobní údaje subjektů údajů zákonně, resp. v souladu s článkem 6 odst.

1. písm. b), podle něhož je zpracování nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů.

### 36. K článku 12 odst. 1. a odst. 3. Obecného nařízení o ochraně osobních údajů:

Správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v článcích 13 a 14 a učinil veškerá sdělení podle článku 15 až 22 a 34 o zpracování, zejména pokud se jedná o informace určené konkrétně dítěti. Informace poskytne písemně nebo jinými prostředky, včetně ve vhodných případech v elektronické formě. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně, a to za předpokladu, že identita subjektu údajů je prokázána jinými způsoby.

Správce poskytne subjektu údajů na žádost podle článků 15 až 22 informace o přijatých opatřeních, a to bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Tuto lhůtu je možné v případě potřeby a s ohledem na složitost a počet žádostí prodloužit o další dva měsíce. Správce informuje subjekt údajů o jakémkoliv takovém prodloužení do jednoho měsíce od obdržení žádosti spolu s důvody pro tento odklad. Jestliže subjekt údajů podává žádost v elektronické formě, poskytne se informace v elektronické formě, je-li to možné, pokud subjekt údajů nepožádal o jiný způsob.

I když oznamovatel tvrdil, že jsou jeho osobní údaje uvedené mezi zákazníky v souboru na jím nalezeném usb flash disku tak, buď nebyla pravdivá jím užívaná jména, kterými podepisoval e-mailové zprávy, nebo není pravdivé tvrzení, že jsou na usb flash disku uvedené jeho osobní údaje. Nebylo zjištěno, že by oznamovatel či jiná osoba/zákazník využili svého práva podle článku 12 a požádali kontrolovanou osobu o informaci ke zpracování svých osobních údajů.

### 35. K článku 24 odst. 1. a článku 25 odst. 2. Obecného nařízení o ochraně osobních údajů:

S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována.

Správce zavede vhodná technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnost. Tato opatření zejména zajistí, aby osobní údaje nebyly standardně bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob.

Kontrolovaná osoba garantovala a při místním šetření demonstrovala tak, jak bylo podrobně popsáno do protokolu z ústního jednání a místního šetření, včetně jeho doplnění, že má provedená dostatečná technická a organizační opatření jak v případě zpracování smluv v listinné, tak i v elektronické podobě, aby nemohly být zpřístupněny neomezenému počtu fyzických osob.

Pokud však existuje nezjištěný počet souborů smluv v bezdůvodném držení nezjištěné osoby, která si je zřejmě opatřila nedovoleným způsobem a z nezjištěných pohnutek, jedná se o nezákonný/nestandardní zásah neznámého člověka, který by měl být v trestní věci zjištěn/ztotožněn a celá událost předmětem šetření orgánů činných v trestním řízení. Až tedy

podle oznámeného výsledku tohoto šetření bude rozhodnuto o případném dalším řízení, resp. by až poté mohlo být posouzeno, zda je zjištění úplné a tvrzení kontrolované osoby o tom, že jsou technická a organizační opatření dostatečná, pravdivé.

### 36. K článku 32 odst. 1. a odst. 2. Obecného nařízení o ochraně osobních údajů:

S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu a účelům zpracování i k různě pravděpodobným a různě závazným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně: pseudonymizace a šifrování osobních údajů; schopností zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování; schopnost obnovit dostupnost údajů a přístup k nim včas v případě fyzických či technických incidentů; procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Dokud nebude v trestní věci Policií České republiky, resp. orgány činnými v trestním řízení zjištěna osoba, resp. oznamovatel, který disponuje větším množstvím dat, k nimž se dostal dosud nezjištěným způsobem, když byla zjištěna jeho rozporná či nepravdivá tvrzení uvedená v podnětu, nelze než uvěřit kontrolované osobě, která je navíc specialista přes IT tak, jak i demonstrovala při místním šetření, že má dostatečná vhodná technická a organizační opatření, aby zajistila úroveň zabezpečení odpovídající danému riziku, a aby zabránila neoprávněnému přístupu jak do archivu, kde má uložené smlouvy v listinné podobě, tak i do databáze uložené v elektronické podobě.

### 37. K článku 33 odst. 1., odst. 3., odst. 4. a odst. 5. Obecného nařízení o ochraně osobních údajů:

Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu příslušnému podle článku 55 (v daném případě Úřad pro ochranu osobních údajů), ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

Ohlášení musí přinejmenším obsahovat: popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorii a přibližného počtu dotčených subjektů údajů a kategorii a přibližného množství dotčených záznamů osobních údajů; jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace; popis pravděpodobných důsledků porušení zabezpečení osobních údajů; popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Není-li možné poskytnout informace současně, mohou být poskytnuty bez dalšího zbytečného odkladu.

Správce dokumentuje veškeré případy porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Tato dokumentace musí dozorovému úřadu umožnit ověření souladu s tímto článkem.

V rámci nestandardního řešení a zjišťování způsobu úniku osobních údajů Policií České republiky se zjištěním pachatele mimořádné události, který disponuje nezjištěným větším množstvím souborů/uzavřených smluv kontrolované osoby, obsahující osobní údaje zákazníků kontrolované osoby, a současně není znám skutečný motiv, resp. jakým způsobem nakládá či hodlá nakládat tato osoba se zpracovávanými osobními údaji, směřovala kontrolovaná osoba svůj dotaz na Úřad pro ochranu osobních údajů.

### 38. K článku 34 odst. 1., odst. 2, odst. 3 a odst. 4. Obecného nařízení o ochraně osobních údajů:

Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů.

V oznámení určeném subjektu údajů podle předchozího odstavce se za použití jasných a jednoduchých jazykových prostředků popíše povaha porušení zabezpečení osobních údajů a uvedou se v něm přinejmenším informace a doporučení, a to: jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace; popis pravděpodobných důsledků porušení zabezpečení osobních údajů; popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Oznámení subjektu údajů se nevyžaduje, je-li splněna kterákoli z těchto podmínek: správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování; správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví; vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

Jestliže správce dotčenému subjektu údajů porušení zabezpečení osobních údajů ještě neoznámil, může dozorový úřad po posouzení pravděpodobnosti toho, že dané porušení bude mít za následek vysoké riziko, požadovat, aby tak učinil, nebo může rozhodnout, že je splněna některá z podmínek uvedených v předchozím odstavci.

Až na základě šetření orgánů činných v trestním řízení, resp. až bude zjištěno, k jakému porušení zabezpečení osobních údajů došlo, kdo za něj zodpovídá (pokud by došlo ke krádeži osobních údajů) a jednalo by se o nezákonné jednání sledující poškození zájmů kontrolované osoby, a bylo by zjištěno, že měla dostatečné zabezpečení, které lze po ní spravedlivě požadovat v souvislosti s předmětem kontroly, nebyla by kontrolovaná osoba odpovědná za takovéto porušení, i když by jí to nezbavovalo povinnosti informovat subjekty údajů podle tohoto článku nařízení. Pokud by informování jednotlivých subjektů vyžadovalo nepřiměřené úsilí tak, jako v daném případě, lze subjekty údajů informovat veřejným oznámením nebo podobným opatřením. Je však na zvážení, zda v tomto případě by zveřejněním nedošlo ke zmaření vyšetřování orgánů činných v trestním řízení v souvislosti se zjišťování osoby, která

disponuje větším množstvím dat, případně, zda naopak by mohl být cíleným způsobem a textem oznámení osoba vypátrána. Tuto záležitost, pokud je veřejný zájem na vypátrání pachatele incidentu s ohledem na větší množství souborů, kterým disponuje, musí kontrolovaná osoba danou věc konzultovat s Policií České republiky.

### 39. K článku 37 odst. 1. Obecného nařízení o ochraně osobních údajů:

Správce nebo zpracovatel jmenují pověřence pro ochranu osobních údajů, kdy: zpracování provádí orgán veřejné moci či veřejný subjekt s výjimkou soudů jednajících v rámci svých soudních pravomocí; hlavní činností správce nebo zpracovatele spočívající v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů; nebo hlavní činností správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9. nařízení nebo osobní údajů týkajících se rozsudků v trestních věcech a trestních činů uvedených v článku 10. nařízení.

Kontrolovaná osoba nejmenovala pověřence pro ochranu osobních údajů, neboť jí taková povinnost za daných podmínek nevznikla, a proto byl kontaktní osobou jednatel, který je statutárním orgánem kontrolované osoby.

### Závěr:

V souvislosti s kontrolním zjištěním, pokud bylo kontrolovanou osobou potvrzeno, že má zavedena dostatečná opatření, která lze po ní spravedlivě požadovat k ochraně osobních údajů zákazníků/klientů uvedených ve smlouvách a zjištěno, že oznamovatel (anonym) má/měl v dispozici větší množství smluv na usb flash disku a nejméně 6 dalších smluv přiložených k podnětu doručeného [REDACTED], a pokud byly smlouvy na předmětný usb flash disk umístěny až po jeho zformátování, [REDACTED], nemohla být pravdivá informace, že usb flash disk obsahující v souboru 760 smluv našel oznamovatel [REDACTED] před obchodním domem [REDACTED], [REDACTED]. Rozpor v podané informaci oznamovatele je i v tom, že 6 smluv přiložených k podnětu ze [REDACTED] není obsahem usb flash disku doručeného [REDACTED] kontrolujícím a žádné oznamovatelem uvedené jméno neodpovídá jménu zákazníka v souboru smluv na usb flash disku. Podezření o neoprávněném nakládání s osobními údaji nezjištěného většího počtu smluv uzavřených kontrolovanou osobou a na nedovolený způsob jejich pořízení vyvolává i skutečnost, že usb flash disk byl označen [REDACTED], což je jednatelům obdobně užívaná zkratka [REDACTED] u podpisu, nikoliv však u označování jeho usb flash disku, který ani typově neodpovídá usb flash disku jím užívaného a má navíc jiné formátování. Daný typ disku není užíván ani žádným zaměstnancem kontrolované osoby. Taktéž pojmenování souborů, kdy číslo zákazníka neodpovídá číslu v databázi, neodpovídá tomu, co používá kontrolovaná osoba, tedy číslo zákazníka s číslem v databázi musí být shodné. Pro zakrývání manipulaci s usb flash diskem svědčí i jeho přeformátování tak, aby nemohl být vyvolán případný původní text, včetně přenastavení času v počítači nebo pozdější úpravou dokumentu jinde a jeho manipulací s časovým záznamem s vyvoláním dojmu, že soubory byly zkopírovány postupně v [REDACTED]. O snaze, aby nebyl oznamovatel odhalen, svědčí i odmítnutí se identifikovat, používání různých jmen pod e-mailové zprávy a zaslání usb flash disku po urgenci kontrolujících až dne [REDACTED] v silně parfémované obálce se samolepící známkou a razítkem [REDACTED] a se strojově napsaným adresátem na obálce nalepeném samostatným kusu papíru.

Vzhledem ke zjištění porušení také Listiny základních práv Evropské unie; v níž v článku 8 upravuje ochranu osobních údajů tak, že každý má právo na ochranu osobních údajů, které se ho týkají a tyto údaje musí být řádně zpracovány pro určené účely na základě souhlasu dotčené osoby nebo dle jiného oprávněného důvodu stanoveného zákonem, přičemž každý má právo na přístup k shromážděným údajům, které se ho týkají, a právo na jejich opravu; je rovněž důležité pokud neznámá osoba může disponovat osobními údaji neurčeného většího množství souborů, resp. 760 smluv z usb flash disku a dalším nezjištěným množstvím smluv, resp. nejméně dalšími 6 smlouvami přiloženými k podnětu, které v rozporu s tvrzením oznamovatele nejsou obsahem usb flash disku, je rovněž i ve veřejném zájmu, aby taková osoba, která disponuje/disponovala větším množstvím smluv kontrolované osoby, vysvětlila skutečný původ souborů poskytnutých smluv Úřadu pro ochranu osobních údajů a tudíž byla v trestním řízení vypátrána, pokud se na výzvu odmítla Úřadu pro ochranu osobních údajů identifikovat a Úřad pro ochranu osobních údajů jako správní orgán nedisponuje možností takovou osobu vypátrat. Za tohoto stavu; kdy je zde důvodné podezření na neoprávněné nakládání s osobními údaji nezjištěného množství zákazníků kontrolované osoby neznámou osobou, která si je opatřila a může s nimi nakládat nedovoleným způsobem, resp. došlo nezjištěným způsobem k neoprávněnému přístupu k počítačovému systému či nosiči informací s největší pravděpodobností samotným oznamovatelem či jiným způsobem si přisvojení cizích dat a k nedovolené manipulaci/nakládání s větším množstvím osobních údajů subjektů údajů, s podezřením na některý z trestných činů podle ustanovení § 120, §180, § 182, § 205, § 230 § 231 a § 232 trestního zákona; došlo k ukončení kontroly s kontrolovanou osobou s tím, že je připravena v trestní věc poskytnout vyžádané podklady Policii České republiky.

Až podle výsledku tohoto probíhajícího trestního řízení pod bude určeno, zda bude a případně s jakým správcem či zpracovatelem zahájena, ať už z podnětu nebo úřední povinnosti, nová kontrola v případě zjištěného porušení obecně platných právních předpisů, zejména Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). V rámci daného šetření může být tak kontrolovaná osoba, resp. správce osobních údajů, zproštěna odpovědnosti za případnou újmu, která může být způsobena subjektu/ům údajů, pokud bude prokázáno ve smyslu článku 82 odst. 3. nařízení, že kontrolovaná osoba nenesla žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla.

Ze strany kontrolované osoby byla učiněna dostatečná opatření k ochraně osobních údajů subjektů údajů, která lze po ní spravedlivě požadovat a navíc provedla/provede další opatření, aby se daná věc neopakovala, případně učiní ještě další opatření, budou-li potřebná s ohledem na výsledek trestního řízení.

Lze než doporučit kontrolované osobě nad rámec předmětu kontroly, aby se zaměřila zejména na plnění informační povinnosti dle článku 13. nařízení, které je povinna vždy prokázat, a to nejlépe ve smlouvě, pokud tak neučinila v jiném samostatném dokumentu, včetně poučení ve smyslu článků 15 až 20, který by mohl být součástí smlouvy, resp. prezentovaném na webové stránce.



### 3) Poučení o opravném prostředku:

Proti kontrolnímu zjištění uvedenému v tomto protokolu o kontrole může kontrolovaná osoba podat námitky Úřadu pro ochranu osobních údajů ve lhůtě 15 dnů ode dne doručení protokolu o kontrole. 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 pro ochranu osobních údajů ve lhůtě 30 dnů ode dne jejich doručení.

#### Podpisová doložka:

##### Kontrolující:

otisk  
úředního  
razítka

PhDr. Petr Krejčí

inspektor

.....

.....

.....

titul, jméno, příjmení

funkce

podpis  
(podepsáno elektronicky)

JUDr. Jana Kosobudová

pověřená zaměstnankyně

.....

.....

.....

titul, jméno, příjmení

funkce

podpis  
(podepsáno elektronicky)