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-11289/17-16
Praha 21. května 2018

Protokol o kontrole

Kontrolní orgán:

Úřad pro ochranu osobních údajů, se sídlem 170 00 Praha - Holešovice, Pplk. Sochora 727/27 (dále také „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.

Kontrolující:

Mgr. Daniel Rovan – inspektor Úřadu, číslo průkazu
Ing. Zdenka Filová – pověřená zaměstnankyně Úřadu, číslo průkazu
Mgr. Marta Lásiková – pověřená zaměstnankyně Úřadu, číslo průkazu
Ing. Radek Loub - pověřený zaměstnanec Úřadu, číslo průkazu

Kontrolovaná osoba:

Generální finanční ředitelství, se sídlem Praha, Nové Město, Lazarská 15/7, PSČ 110 00, IČO: 72080043 (dále také „kontrolovaný“)

Osoba jednající za kontrolovanou osobu:
Ing. Martin Janeček, generální ředitel
Ing. Jarmila Vocetková, ředitelka odboru a zástupce ředitele sekce

Místo provedení kontroly:

Úřad pro ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7

Odbor daňových informačních systémů Žitná 563/12, Praha 2
Státní pokladna Centrum sdílených služeb s. p. se sídlem Na Vápence 915/14, Praha 3
Finanční úřad pro hlavní město Prahu, Štěpánská 619/28, 111 21 Praha 1

Předmět kontroly:

Předmětem kontroly je dodržování povinností správce/zpracovatele osobních údajů stanovených zákonem č. 101/2000 Sb. v souvislosti se zpracováním osobních údajů Finanční správou České republiky se zaměřením na zpracování údajů podle zákona č. 112/2016 Sb., o evidenci tržeb. Kontrola byla zahájena na základě kontrolního plánu Úřadu na rok 2017 a podnětu, který Úřad obdržel v době přípravy zahájení kontroly.

Zahájení kontroly: kontrola byla zahájena *Oznámením o zahájení kontroly* ze dne 20. listopadu 2017, Č.j. UOOU-04507/17-6, doručené kontrolovanému dne 21. listopadu 2017.

Poslední kontrolní úkon: posledním kontrolním úkonem předcházejícím vyhotovení protokolu o kontrole byl *Úřední záznam o telefonickém rozhovoru* ze dne 16. května 2018 Čj. UOOU-11289/17-17.

Přehled podkladů:

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

1. Stížnost ze dne 25. dubna 2017. Doručeno 25. dubna 2017. Čj. UOOU-11289/17-1. 1 s. 2 přílohy.

2. Oznámení o zahájení kontroly ze dne 20. listopadu 2017 . Doručeno dne 21. listopadu 2017. Čj. UOOU-11289/17-5. 2 s. 1 příloha.

3. Vyjádření kontrolovaného k otázkám v rámci zahájené kontroly ze dne 12. prosince 2017. Doručeno 12. prosince 2017. Čj. UOOU-11289/17-7. 17 s.

4. Předání příloh k odpovědím na otázky v rámci zahájené kontroly. Doručeno dne 11. prosince 2017. Čj. UOOU-11289/17-6. 2 s. 1 příloha (CD).

4.1. Přehled útvarů ke dni 28.11.2017- příloha k bodu 2- č.1.

4.2. Rámcová smlouva na služby související s přípravou a provozem elektronické evidence tržeb (ev.č. Dodavatele 36/2016/UOM) mezi kontrolovaným a Státní pokladnou Centrem sdílených služeb, s.p.)ze dne 26.5.2016. 18 s.- příloha k bodu 4 č.1.

Příloha č. 1 Rámcové smlouvy na služby související s přípravou a provozem EET. Rozsah služeb EET. 5 s.

Příloha č. 2 Rámcové smlouvy na služby související s přípravou a provozem EET. Řízení přípravy a provozu. 2 s.

Příloha č. 3 Rámcové smlouvy na služby související s přípravou a provozem EET. Vzor Akceptačního protokolu služby EET typu S1. 1 s.

Příloha č. 4 Rámcové smlouvy na služby související s přípravou a provozem EET. Vzor záznamu o poskytnutí služby EET. 1 s.

Příloha č. 5 Rámcové smlouvy na služby související s přípravou a provozem EET. Základní osnova Zprávy o úrovni a provozu poskytované služby EET. 9 s.

Příloha č. 6 Rámcové smlouvy na služby související s přípravou a provozem EET. Vzor Zadávajícího a pověřujícího listu pro služby EET typu S4.1 s.

Příloha č. 7 Rámcové smlouvy na služby související s přípravou a provozem EET. Vzor Akceptačního protokolu pro Služby EET typu S4. 1 s.

4.3. Požadavky na zajištění funkčních procesů elektronické evidence tržeb. 4 s.

4.4. Uživatelské zadání. Požadavky na zjištění funkčních procesů elektronické evidence tržeb. 4 s.

4.5. Příručka  *ze dne 28.4.2016.*

4.6. Směrnice  *generálního ředitele. Bezpečnost informací ze dne 14. června 2017. 10 s.*

4.7. Směrnice  *generálního ředitele. Zabezpečení informačních systémů ze dne 17.12.2013. Stav ke dni 25.5.2016. 9 s.*

4.8. Směrnice  *generálního ředitele. Zásady přístupových práv v Automatizovaném daňovém informačním systému ze dne 19.12.2012. Stav k 18.9.2017. 11 s.*

4.9. Směrnice  *generálního ředitele. Zásady ochrany dat a přístupu do osobních počítačů ze dne 30. července 2013. Stav k 1.1. 2016. 14 s.*

4.10. Směrnice  *generálního ředitele. Subjekty informačních systémů, jejich práva a povinnosti ze dne 19.12.2012. Stav k 1.1.2016. 7 s.*

4.11. Metodický pokyn k přidělování autentizačních údajů, účinný ode dne 1.9.2016. 18 s.

4.12. Přidělená přístupová práva do aplikací ADIS v databázích FU- Příloha k bodu 7 č. 1-ADIS.

4.13. Seznam pracovníků pro přidělení přístupu na Daňový portál- Příloha k bodu 7 č. 2 – DPR.

4.14. Celní správa – tabulka- Příloha k bodu 7 č. 3.

4.15. Útvary – tabulka- Příloha k bodu 7 č. 4.

4.16. Popis pracovní náplně podle jednotlivých útvarů- Příloha k bodu 7 č. 5.

4.17. Logy FU- Příloha k bodu 8 č. 1.

4.18. Logy EET- Příloha k bodu 8 č. 2.

4.19. Logy CEK- Příloha k bodu 8 č. 3.

4.20. Logy WS- Příloha k bodu 8 č. 4.

4.21. Logy WS- Příloha k bodu 8 č. 4.

4.22. Příloha k bodu 11.

4.23. Příloha ke stížnosti 1.

4.24. Příloha ke stížnosti 2.

4.25. Příloha ke stížnosti 3.

5. Sdělení kontrolujícího o změně kontrolní skupiny ze dne 1. března 2018. Doručeno 1. března 2017. Čj. UOOU-11289/17-8. 1 s.

6. Žádost o součinnost kontrolovaného ze dne 15. března 2018. Doručeno dne 15. března 2017. Čj. UOOU-11289/17-9. 1 s.

7. Úřední záznam z ústního jednání a místního šetření konaného dne 5. dubna 2018 ve věci kontroly dodržování povinností stanovených zákonem č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů a zákona č. 255/2012 Sb., o kontrole (kontrolní řád). Čj. UOOU-11289/17-10. Čj. UOOU-11289/17-10. 2 s. 2 přílohy.

7.1. Zápůjční protokol karty hosta - Státní pokladna Centrum sdílených služeb. 1 s.

7.2. Prohlášení návštěvníka/zaměstnance zákazníka/smluvního dodavatele - Státní pokladna Centrum sdílených služeb. 2 s.

8. Žádost o součinnost kontrolovaného ze dne 6. dubna 2018. Doručeno dne 6. dubna 2018. Čj. UOOU-11289/17-11. 1 s.

9. Odpověď na žádost o součinnost kontrolovaného ze dne 13. dubna 2018. Doručeno dne 6. dubna 2018. Čj. UOOU-11289/17-12. 3 s. 1 příloha.

10. Úřední záznam z ústního jednání a místního šetření konaného dne 18. dubna 2018 ve věci kontroly dodržování povinností stanovených zákonem č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů a zákona č. 255/2012 Sb., o kontrole (kontrolní řád). Čj. UOOU-11289/17-10. Čj. UOOU-11289/17-13. 1 s.

11. Doplnění odpovědi na žádost o součinnost kontrolovaným ze dne 2.5.2018. Čj. UOOU-11289/17-14. 1 s.

12. Úřední záznam – pořízení dokumentace ze dne 11. května 2018. Čj. UOOU-11289/17-15. 1 s. 5 příloh.

12.1 Údaje o subjektech DPH - [redacted]

12.2 Údaje o subjektech DPH- [redacted]

12.3 Přihlášení uživatele ke službám aplikace EET. Otisk webové stránky [redacted]

12.4 Přihlášení uživatele ke službám aplikace EET. Otisk webové stránky [redacted]

12.5. Ověření účtenky. Zadání údajů z účtenky. Otisk webové stránky [redacted]

13. Úřední záznam o telefonickém rozhovoru ze dne 16.5.2018. Čj. UOOU-11289/17-17.

I. <u>Kontrolní zjištění</u>

Skutečnosti zjištěné z vlastní činnosti Úřadu

1. Podle vyjádření Ministerstva financí České republiky, se sídlem Letenská 525/15, 118 00 Praha 1 - Malá Strana, IČO: 00006947, ze dne 15. listopadu 2017 (*Čj. UOOU-04507/17-7)* a ustanovení § 2 zákona o evidenci tržeb, je působnost podle tohoto zákona vykonávána orgány Finanční správy České republiky. Orgány Finanční správy České republiky jsou stanoveny zákonem č. 456/2011 Sb., o Finanční správě České republiky, ve znění pozdějších

předpisů (dále jen „zákon o Finanční správě“), resp. ustanovením § 1 tohoto zákona a jsou jimi Generální finanční ředitelství, Odvolací finanční ředitelství a finanční úřady, které jsou správními úřady a organizačními složkami státu.

Správce daně zveřejní způsobem umožňujícím dálkový přístup podmínky a postup pro přístup na společné technické zařízení správce daně umožňující poplatníkovi správu certifikátu pro evidenci tržeb a údajů pro správu evidence tržeb. Komunikace probíhá přes daňový portál, viz. http://adisspr.mfcr.cz/adist/idpr_pub/dpr/uvod.faces. Daňový portál obecně slouží pro komunikaci s Finanční správou České republiky a k získávání informací v rámci správy daní, přičemž provozovatelem daňového portálu je Generální finanční ředitelství (*Čj. UOOU-04507/17-7).* Kontrola byla zahájena na základě kontrolního plánu Úřadu na rok 2017 a podnětu, který Úřad obdržel v době přípravy zahájení kontroly.

2. Dne 6. listopadu 2017 byla v rámci předkontrolní činnosti na internetové stránce kontrolovaného https://adiseet.mfcr.cz/adistc/adis/idpr_pub/auth/LoginPage.faces *přihlášení uživatele ke službám aplikace EET* při vyplnění *název uživatele, heslo*, nalezena tabulka označená *nejsem robot, reCAPTCHA, ochrana soukromí – smluvní podmínky.* Po vyplnění je přihlášení umožněno.
Tatáž internetová stránka dne 20. dubna 2018 obsahovala *přihlášení uživatele ke službám aplikace EET* při vyplnění *název uživatele, heslo a pětici čísel, přehrát kód, opište kód z obrázku.* Jedná se o vlastní software řešení kontrolovaného, který je ochranou proti robotickým přístupům (l.12.3 a l.12.4).

3. Dne 20. dubna 2018 bylo na internetové stránce kontrolovaného https://adisspr.mfcr.cz/adistc/adis/idpr_pub/eet/uct/overeni.faces *pro veřejnost, ověření účtenky, zadání údajů z účtenky*, po zadání technických údajů k ověřované účtence požadováno opsání pětice čísel *(přehrát kód, opište kód z obrázku).* Jedná se o vlastní software řešení kontrolovaného, které je ochranou proti robotickým přístupům (l.12.5).

4. Účtenka [redacted] obsahovala informaci o uskutečněné transakci (nákupu), přičemž na účtence bylo uvedeno rodné číslo subjektu DPH, a to jako součást DIČ. Dále obsahovala informaci [redacted]

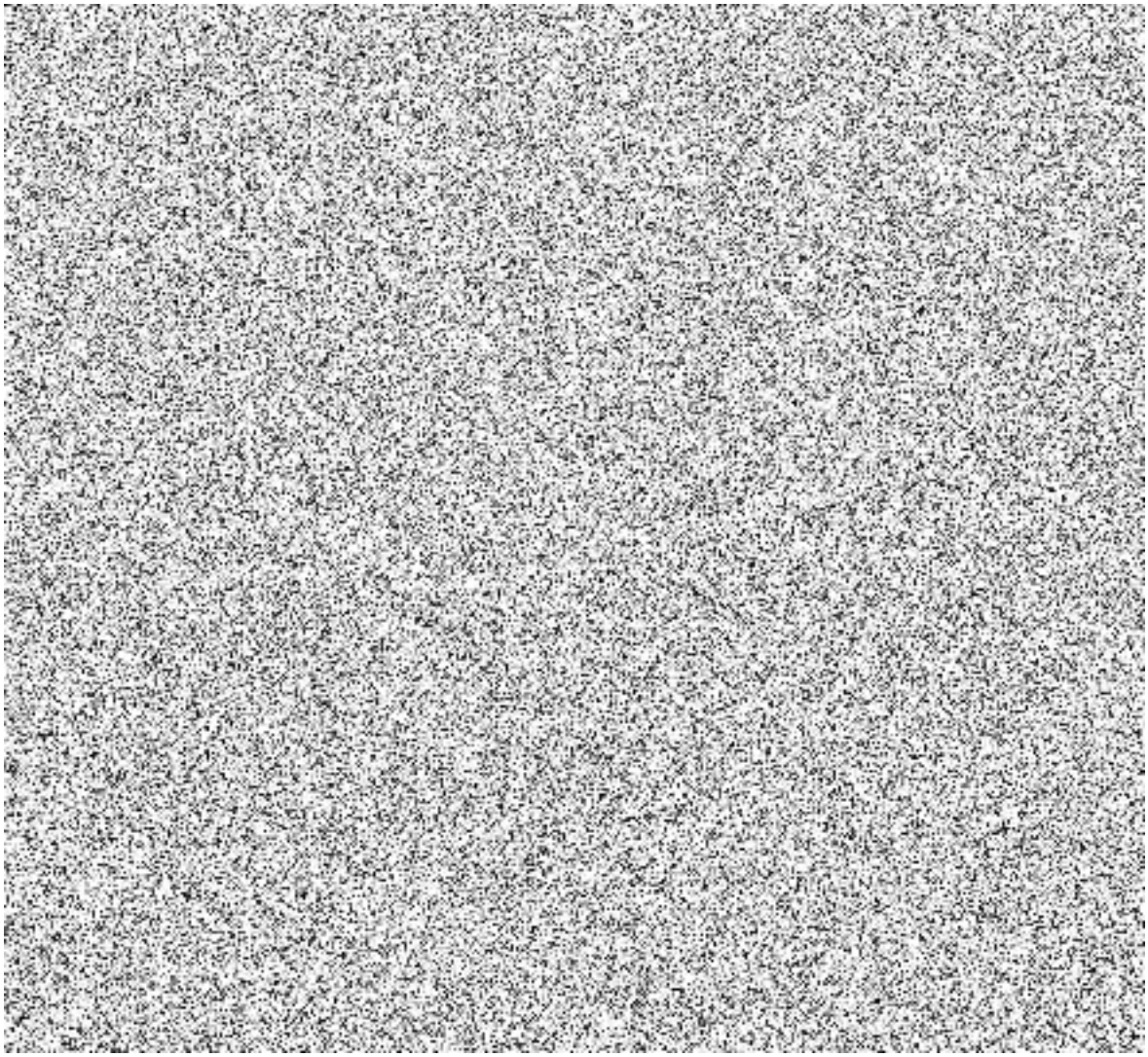
Účtenka/doklad č. 102805, vydaná dne [redacted] právnickou osobou [redacted] obsahovala informaci o uskutečněné transakci (nákupu) [redacted].

Skutečnosti zjištěné u kontrolovaného

5. Kontrolovaný dne 12. prosince 2017 písemně uvedl, že provozuje:
Automatizovaný daňový informační systém (ADIS), Státní pokladnou Centrum sdílených služeb, s. p. (SPCSS) je provozována Transakční část a krátkodobé úložiště elektronické evidence tržeb.

Analytický prostor, který není v pravém slova smyslu aplikací, jsou data uložená na databázovém serveru. Pro práci s daty slouží analytický nástroj [redacted].

Výše uvedené schematicky popisuje následující obrázek z Rámcové smlouvy, popsané v kontrolním zjištění č. 21.



K tomu kontrolovaný dne 13. dubna 2018 písemně uvedl, že *automatizovaný daňový informační systém ADIS byl určen jako IS kritické informační infrastruktury podle Zákona č. 181/ 2014 Sb. o kybernetické bezpečnosti a navazující Vyhlášky č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti.*
Požadavky výše zmiňovaných dokumentů hovoří o bezpečnostních opatřeních, mezi které patří i technická opatření, mimo jiná i opatření uživatelského rozhraní systému ADIS a jeho bezprostředního systémového okolí (operační systémy, databáze, webové služby):
- *ochrana integrity komunikačních sítí*
- *ověřování identity uživatelů*
- *řízení přístupových oprávnění*
- *ochrana před škodlivým kódem*
- *zaznamenávání činností kritické informační infrastruktury a významných informačních*

systémů, jejich uživatelů a administrátorů
• detekci kybernetických bezpečnostních událostí
• sběr a vyhodnocení kybernetických bezpečnostních událostí
• aplikační bezpečnost
• kryptografické prostředky
Ochrana proti robotickým útokům je jedním, nikoliv však jediným technickým opatřením, které jsou určeny ke snížení hranice zranitelnosti provozovaného IS.

Komunikace mezi GFŘ a [redacted] probíhá formou [redacted], tj. hlášení o chybách nebo požadavcích na úpravy aplikace ADIS, případně na realizaci legislativních nebo metodických změn, a to v aplikaci [redacted]. Pro přístup do [redacted] je zaměstnanci GFŘ přiděleno přístupové jméno a heslo a jeho id. Vkládat a číst [redacted] může pouze uživatel, kterému jsou přidělena přístupová práva do aplikace [redacted]. Zadavatel [redacted] vyplní nejprve povinné údaje, tj. název aplikační oblasti, režim aplikace, závažnost podle zadavatele, verze ADIS, Id obrazovky nebo sestavy, cesta v nabídce/dokumentace a stručný popis (na 60 znaků). Na základě jeho přihlášení se předvyplní jeho jméno – zodpovědná osoba uzlu a uzel [redacted]. Následně upřesní chybu nebo popíše požadavek na úpravu nebo novou aplikaci v části „Upřesnění chyby – Základní popis“, případně vloží Přílohu, ve které nejsou uvedeny osobní údaje subjektu. [redacted] ukončí odsouhlasením a potvrzením, že [redacted] neobsahuje osobní údaje a je uložena ve stavu = 0 Nově pořízená [redacted]. [redacted] vývojového pracoviště [redacted] převzata [redacted] a podle povahy je nadále zpracovávána.
Pokud se jedná o nahlášenou chybu, je v části „Vyjádření řešitele“ popsán způsob nápravy, případně požadavek na dopřesnění zadavatelem nebo odsouhlasení úpravy garantem příslušné aplikační oblasti. Po vyřešení je oprava chyby nahlášená v [redacted] zařazena do verze ADIS. Jedná-li se o námět, tj. úpravu stávající aplikace nebo požadavek na novou aplikaci, je v části „Vyjádření řešitele“ popsán návrh řešení, případně požadavek na upřesnění garantem nebo na projednání v rámci garanční skupiny dané aplikační oblasti.
To kontrolovaný doložil příklady [redacted] *(l.3 a l.9).*

k Automatizovanému daňovému informačnímu systému (ADIS):

6. Kontrolovaný předložil úplný přehled adres (míst), kde jsou zpracovávány osobní údaje v souvislosti s evidencí v ADISu. Jedná se o [redacted] míst zpracování *(l.3 a l.4.1).*

7. Kontrolovaný dne 12. prosince 2017 uvedl, že e*xterním zpracovatelem dat z ADIS je Celní správa. Výkon činnosti CS týkající se prověřování plnění povinností při evidence tržeb je dle § 2 odst. 2 zák. č. 112/2016 Sb., o evidenci tržeb, ve znění pozdějších předpisů. Dle § 30 odst. 1 zák. č. 112/2016 Sb., o evidenci tržeb, ve znění pozdějších předpisů je celní úřad příslušný k řízení o přestupcích dle tohoto zákona (l.3).*

8. Kontrolovaný předložil projektovou a provozní dokumentaci:
Příloha č. 2 – Uživatelské zadání, nedatováno, která popisuje požadavky na zajištění funkčních procesů elektronické evidence tržeb a [redacted].

9. Kontrolovaný dále uvedl, že v*zhledem k tomu, že Aplikace evidence tržeb a Centrální evidence kontrol jsou součástí ADISu, nebyly pro nakládání s osobními údaji vydány speciální předpisy, platí pro ně stejné předpisy jako pro zpracovávání dat a osobních údajů v ADISu.*

10. Kontrolovaný předložil interní předpisy, upravující nakládání s osobními údaji, a to: *Směrnice*  *generálního ředitele, Bezpečnost informací, ze dne* 14. června 2017, jejímž účelem *je zajistit soulad se zákonem o kybernetické bezpečnosti1), a se zvláštním právním předpisem2) v oblasti systému řízení bezpečnosti informací ve Finanční správě České republiky.*  (*l.4.6)*.

Dále uvedl, že *SPCSS nemá v současné chvíli speciální právní předpis pro ochranu zpracovávaných osobních údajů pro externí subjekty (l.3 a l.4.6).*

Směrnice  *generálního ředitele, Zabezpečení informačních systémů, Stav ke dni 25.5.2016 ze dne 17. prosince 2013,* stanovuje povinnosti a zásady spolupráce subjektů informačních systémů a bezpečnostního managementu při vytváření, kontrole a hodnocení bezpečnosti jednotlivých informačních systémů. Stanovuje zásady vytváření dokumentů pro bezpečnost informačních systémů *a zavádění prostředků bezpečnosti IS s ohledem na vynaložené náklady a s důrazem na prevenci a vytváření záznamů o bezpečnostních incidentech. S*měrnice je závazná pro všechny fyzické osoby ve služebním, nebo pracovním poměru k České republice – Generálnímu finančnímu ředitelství a fyzické osoby činné pro Českou republiku – Generální finanční ředitelství na základě dohod o pracích konaných mimo pracovní poměr *(l.4.7).*

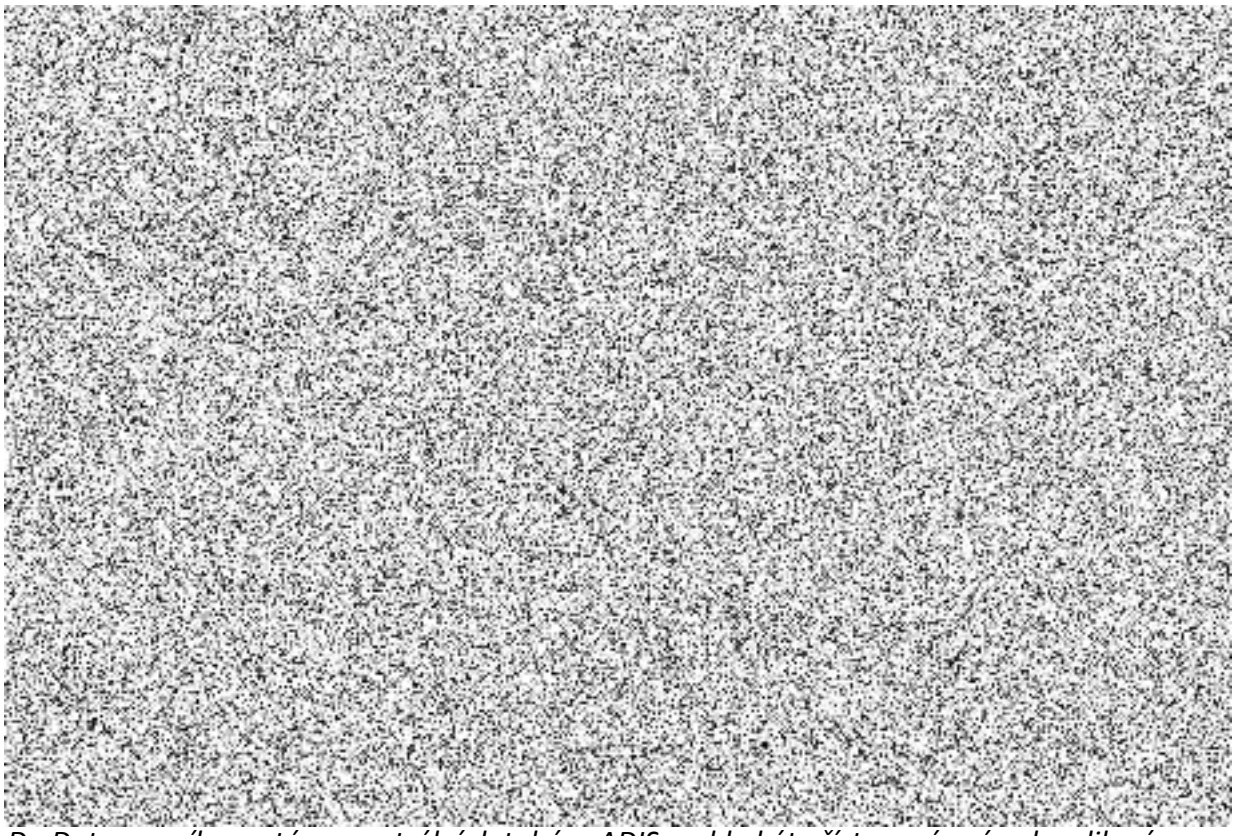
Směrnice  *generálního ředitele, Zásady přístupových práv v Automatizovaném daňovém informačním systému ze dne 19.12.2012, stav k 18.9.2017,* stanovuje způsob a rozsah přidělování přístupových práv do jednotlivých databází Automatizovaného daňového informačního systému, přihlašování do aplikace, práci s aplikací včetně odebírání přístupových práv, bezpečnostní pravidla a odpovědnost představených za bezpečnost informačního systému. Směrnice je závazná pro všechny představené a vedoucí zaměstnance, fyzické osoby ve služebním, nebo pracovním poměru k České republice – Generálnímu finančnímu ředitelství a fyzické osoby činné pro Českou republiku – GFŘ na základě dohod o pracích konaných mimo pracovní poměr, kteří se v rámci svých služebních, resp. pracovních úkolů podílejí na činnosti upravené touto směrnicí *(l.4.8).*

Směrnice  *generálního ředitele, Zásady ochrany dat a přístupu do osobních počítačů ze dne 30. července 2013, stav k 1.1. 2016,* stanovuje *zásady ochrany dat a přístupu do nepřenosných (stabilně umístěných) a přenosných osobních počítačů* ve všech útvarech orgánů Finanční správy České republiky. Směrnice je závazná *pro všechny fyzické osoby ve služebním nebo pracovním poměru k České republice – Generálnímu finančnímu ředitelství a fyzické osoby činné pro Českou republiku – Generální finanční ředitelství na základě dohod o pracích konaných mimo pracovní poměr (l.4.9).*

Směrnice  *generálního ředitele, Subjekty informačních systémů, jejich práva a povinnosti ze dne 19.12.2012, stav k 1.1.2016* stanovuje subjekty informačních systémů v rámci orgánů Finanční správy České republiky, tj. Generálního finančního ředitelství , Odvolacího

finančního ředitelství a finančních úřadů, a určuje vztahy mezi nimi, definuje jejich práva a povinnosti v celém životním cyklu informačního systému. Směrnice je závazná pro všechny fyzické osoby ve služebním2) nebo pracovním3) poměru k České republice – GFŘ a fyzické osoby činné pro Českou republiku – GFŘ na základě dohod o pracích konaných mimo pracovní poměr *(I.4.10).*

11. Kontrolovaný předložil přehled přístupů zaměstnanců na jednotlivých FÚ, rozčleněných podle jednotlivých krajů *do aplikací ADIS FÚ evidence tržeb a do Dotazovacího systému centrální databáze ADIS do aplikace Centrální evidence kontrol EET a Aplikace evidence tržeb na GFŘ :*
K tomu dále uvedl, že z*aměstnancům na FÚ mohla být přidělena přístupová práva do aplikací ADIS:*



Do Dotazovacího systému centrální databáze ADIS mohla být přístupová práva k aplikacím Centrální evidence kontrol EET a Aplikace evidence tržeb přidělována od 1. prosince 2016 (I.4.12).

Kontrolovaný dále předložil *seznam pracovníků pro přidělení přístupu na Daňový portál, které byly zřízeny k 1. září 2016 s uvedením změn*, tříděno podle jednotlivých krajů *(I.4.13).*

Dále předložil seznam osob *přistupujících k údajům evidence tržeb v aplikacích Centrální evidence kontrol EET a Aplikace evidence tržeb na GFŘ z celní správy, přístupy bylo možné přidělovat od 1. prosince 2016*. Evidence obsahuje pořadové číslo, osobní číslo, jméno a příjmení zaměstnance, datum založení, popř. změn, datum zřízení oprávnění a popis pracovní činnosti *(I.4.14).*

Kontrolovaný dále předložil popis pracovní náplně zaměstnanců (*I.4.15 a I.4.16).*

12. Kontrolovaný dne 12. prosince 2017 předložil *logy z jednotlivých databází ADIS za období od 10. – 15. října 2017. Jedná se o logy přístupů k osobním údajům v databázích, a to:*
Logy z FU – Záznam obsahuje: *ID záznamu, datum záznamu, kód pracovníka, DIČ subjektu*, rodné číslo, aplikační oblast, aplikační podoblast, název programu *(l.4.17).*

Logy EET – logy přístupů k údajům evidence tržeb v Aplikaci evidence tržeb v Dotazovacím systému centrální databáze ADIS na GFŘ. Záznam obsahuje: *ID záznamu, kód pracovníka, číslo FÚ, číslo odboru, číslo oddělení, čas nahlížení, datum a čas události, subjekt, DIČ (rodné číslo), kód důvodu, důvod přístupu k údajům, aplikační oblast,* aplikační podoblast, název programu, typ údaje a doplňující poznámka *(l.4.18).*

Logy CEK - logy přístupů k údajům evidence tržeb do aplikace Centrální evidence kontrol EET na GFŘ. Záznam obsahuje: *ID záznamu, kód pracovníka, číslo FÚ, číslo odboru, číslo oddělení, čas nahlížení, subjekt, DIČ (*rodné číslo), *kód důvodu, důvod přístupu k údajům,* aplikační oblast, název programu, typ údaje, ID kontroly, č. kontroly FS, č. kontroly CS, typ provozovny a datum zahájení a ukončení kontroly *(l.4.19).*

Logy WS – logy s předávanými údaji webovou službou celní správě. Záznam obsahuje: *ID záznamu, kód pracovníka, název webové služby, čas přenosu dat, doba události, id požadavku, subjekt (l.4.20-21).*

13. Kontrolovaný dne 12. prosince 2017 předložil *oprávnění přístupů k údajům evidence tržeb pro jednotlivé útvary GFŘ a FÚ s upřesněním jejich pracovní náplně za útvary Generálního finančního ředitelství ke dni 1.12.2017 a popis pracovních náplní jednotlivých útvarů (l.4.15 a l.4.16).*

14. Kontrolovaný dne 12. prosince 2017 písemně uvedl, že *doba uchovávání záznamů zatím nebyla stanovena, záznamy zůstávají uchovávány v databázi (l.3).*

15. Kontrolovaný dne 12. prosince 2017 písemně uvedl, že d*okumentace k analýze rizik jednotlivým zpracovávaným osobním údajům, které jsou předmětem kontroly, nebyla samostatně zpracovávána. Tato data jsou chápána jako jiná daňová data. (l.3).*

16. Kontrolovaný dne 12. prosince 2017 písemně uvedl, že n*a žádném orgánu finanční správy neevidujeme žádost či stížnost podle zákona č. 101/2000 Sb., o ochraně osobních údajů. Pouze na Finanční úřad v Českých Budějovicích byl doručen dotaz, zda evidence tržeb neporušuje uvedený zákon, obdobný dotaz eviduje i GFŘ. (l.4.22).*

17. Kontrolovaný dále dne 12. prosince 2017 písemně uvedl, že *Systém ADIS je napojen na Transakční část elektronické evidence tržeb SPCSS, kde dochází k příjmu účtenek (l.3).*

18. Kontrolovaný dne 12. prosince 2017 písemně uvedl, že *celkový počet podnikatelů, jejichž DIČ obsahuje rodné číslo a jsou subjekty elektronické evidence dle zákona č. 112/2016 Sb., o evidenci tržeb je k 27. listopadu 2017 celkem 111 507 (l.3).*

k Transakční části a krátkodobému úložišti EET

19. Kontrolovaný dne 12. prosince 2017 písemně uvedl, že *využívá datové centrum –* [redacted] *(I.3).*

Kontrolující dne 5. dubna 2018 provedli de visu fyzickou kontrolu datového úložiště a aplikační serverovny v [redacted] a to za přítomnosti zástupce kontrolovaného a ředitele úseku ICT bezpečnosti, [redacted]

Zabezpečení přístupu:
Každá návštěva autorizovaného pracovníka s hostem (osobou neevidovanou v Autorizačních seznamech) musí být ohlášena [redacted]. Přístup samostatného autorizovaného pracovníka stačí ohlásit ostraze [redacted], [redacted] a ou u n á t *a*

20. Kontrolovaný dále uvedl, že *SPCSS nevyužívá žádné externí zpracovatele osobních údajů. Pokud by tyto údaje zpracovával, případně je zpracovává, pak by tak činil či činí sám. V obecné rovině pak externí dodavatelé přímo nepracují s daty aplikace Elektronické evidence tržeb, podílejí se pouze na technické podpoře systémů (I.3).*

21. Kontrolovaný dne 12. prosince 2017 předložil *Rámcovou smlouvu na služby související s přípravou a provozem elektronické evidence tržeb (ev.č. Dodavatele 36/2016/UOM) mezi kontrolovaným a Státní pokladnou Centrem sdílených služeb, s.p.) ze dne 26.5.2016.* Předmětem smlouvy je závazek dodavatele poskytovat objednateli služby související s přípravou a provozem EET na základě prováděcích smluv uzavřených mezi smluvními stranami postupem smlouvou upraveným *(I.3).*

22. Kontrolovaný dne 12. prosince 2017 písemně uvedl, že *SPCSS nebyly ze strany GFŘ nikdy specifikovány konkrétní osobní údaje, které by měly být ze strany SPCSS zpracovávány.* SPCSS má jako dodavatel provozních služeb povinnost v souladu s odst. 16.9 specifikované rámcové smlouvy*, chránit osobní údaje a nakládat s nimi v souladu s příslušnými právními předpisy. Ve smyslu uvedeného ustanovení smlouvy je povinností GFŘ upozornit SPCSS na možný kontakt s osobními údaji a následně povinností obou smluvních stran uzavřít dodatek ke smlouvě spočívající v dohodě smluvních stran o zpracování osobních údajů. K tomu však nikdy nedošlo. Technologické řešení aplikace je GFŘ známé (I.3).*

23. Kontrolovaný dále dne 12. prosince 2017 písemně uvedl, že *Provozní a bezpečnostní dokumentace včetně analýzy rizik části EET provozované formou služeb SPCSS je zpracována ve standardním rozsahu podle požadavků smlouvy s GFŘ a interních směrnic SPCSS.*

Dále uvedl, že *příjem tržeb - záznamy o tržbách jsou přijímány komponentou*

a prostřednictvím aplikačních serverů

a) Logy -

b) Provozní monitoring -

c) Bezpečnostní monitoring -

24. Kontrolovaný předložil přehled skupin *pracovníků SPCSS*, majících přístup k datům EET*:*

Přístup k některým z uvedených komponent mají rovněž pracovníci .

, zajištěné smluvně s externími společnostmi. Smlouvy s externími společnostmi obsahují standardní klauzule SPCSS upravující problematiku mlčenlivosti a ochrany osobních údajů.

25. Kontrolovaný dne 12. prosince 2017 písemně uvedl, že e*lektronické auditní záznamy* k transakční části a krátkodobému úložišti EET *nejsou prováděny. Dle smlouvy nejsou požadovány (l.3).*

26. Kontrolovaný dne 12. prosince 2017 dále písemně uvedl, že a*nalýza rizik k jednotlivým zpracovávaným osobním údajům nebyla provedena, jelikož SPCSS nebyla obeznámena s tím, že zpracovávané údaje jsou považovány za osobní. Správce tyto údaje žádným způsobem nespecifikoval (l.3).*

k Analytickému prostoru

27. Kontrolovaný předložil úplný přehled adres (míst), kde jsou zpracovávány osobní údaje v souvislosti s Analytickým prostorem, a [redacted] *(l.3).*

28. Kontrolovaný dne 12. prosince 2017 písemně uvedl, že *ve spojitosti s Analytickým prostorem nevyužívá žádné externí zpracovatele osobních údajů (l.3).*

29. K rozsahu zpracovávaných osobních údajů kontrolovaný dne 12. prosince 2017 písemně uvedl, že je *stejný jako u ostatních komponent EET. Vzorky dat pro zpracování jsou po použití smazány(l.3).*

30. Kontrolovaný dále dne 12. prosince 2017 písemně uvedl, že provozní a projektovou dokumentaci ve vztahu k analytickému prostoru v současné době tvoří.
Základní prvky současného stavu:

[redacted]

Dále uvedl, že *pro Analytický prostor EET není k dispozici konkrétní interní předpis, vztahují se na něj interní předpisy GFŘ obecnějšího charakteru (l.3).*

31. Kontrolovaný dále uvedl výčet jednorázově zřízených uživatelských oprávnění pro zkušební provoz *na základě § 78 zákona č. 280/2009 Sb., daňový řád, v účinném znění, a to :*

[redacted]

32. Kontrolovaný dne 12. prosince 2017 písemně uvedl, že e*lektronické auditní záznamy z období* 10. – 15. října 2017 *nejsou k dispozici. Důvodem je charakter zpracování dat ve zkušebním provozu Analytického prostoru EET (l.3).*

Ve zkušebním provozu jsou data po ověřovacím zpracování analytickým nástrojem smazána.
Dále uvedl, že *analýza rizik pro Analytický prostor EET není v tuto chvíli k dispozici.*

33. Kontrolovaný dále uvedl, že *data v Analytickém prostoru EET pocházejí ze systému ADIS. Po spuštění produkčního prostředí budou výsledky analýz (podněty) předávány ke kontrole zpět do systému ADIS. Ve zkušebním provozu se tak neděje, potřebná funkcionalita není k dispozici (l.3).*

Rozsah osobních údajů

34. Kontrolovaný zpracovává osobní údaje v souvislosti s předmětem kontroly v rozsahu:

V Centrální evidenci kontrol

Daňové identifikační číslo poplatníka (RČ poplatníka), datum založení poplatníka v EET, jméno a příjmení, datum narození, bydliště – ulice, obec, PSČ, údaj, zda je poplatník plátcem daně z přidané hodnoty, místně příslušný správce daně poplatníka dle § 13 zákona č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů, RČ pověřujícího poplatníka (v případě, že kontrolovaný poplatník eviduje tržby na základě pověření dle § 9 odst. 1 zákona o evidenci tržeb).

Dále kontrolovaný zpracovává: *údaje o provozovně poplatníka, které poplatník uvedl v procesu oznámení údajů o provozovnách v aplikaci Elektronická evidence tržeb umístěné na Daňovém portálu,* a to např. *označení provozovny (příslušná číselná identifikace provozovny přidělena poplatníkovi správcem daně v aplikaci Elektronická evidence tržeb umístněné na Daňovém portále v procesu oznámení údajů o provozovnách), název provozovny – slovní popis, který uvedl poplatník v aplikaci Elektronická evidence tržeb umístněné na Daňovém portále v procesu oznámení údajů, stav provozovny (aktivní, přerušená, zrušená). U virtuální provozovny se jedná dále o údaj o webových stránkách, jejichž prostřednictvím poplatník přijímá evidované tržby (l.3).*

V Aplikaci evidence tržeb

Daňové identifikační číslo poplatníka (RČ poplatníka), datum založení poplatníka v EET, jméno a příjmení, datum narození, bydliště – ulice, obec, PSČ, údaj, zda je poplatník plátcem daně z přidané hodnoty, místně příslušný správce daně poplatníka dle § 13 zákona č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů, RČ pověřujícího poplatníka (v případě, že kontrolovaný poplatník eviduje tržby na základě pověření dle § 9 odst. 1 zákona o evidenci tržeb) a údaje o provozovně poplatníka a další údaje administrativního charakteru.

Údaje o tržbách dle § 19 zákona o evidenci tržeb, které je poplatník povinen nejpozději při uskutečnění evidované tržby zaslat na společné technické zařízení správce daně a dále dle dokumentu „Formát a struktura údajů o evidované tržbě a popis datového rozhraní pro příjem datových zpráv evidovaných tržeb (verze 3.1.1).
Osobní údaje v rozsahu: daňové identifikační číslo poplatníka (RČ poplatníka), označení provozovny, ve které je tržba uskutečněna, označení pokladního zařízení, na kterém je tržba evidována, pořadové číslo účtenky, datum a čas přijetí tržby nebo vystavení účtenky, pokud je vystavena dříve, celková částka tržby, bezpečnostní kód poplatníka, podpisový kód poplatníka, údaj, zda je tržba evidována v běžném nebo zjednodušeném režimu, celková částka plateb určených k následnému čerpání, celková částka plateb, které jsou následným čerpáním nebo zúčtováním platby, daňové identifikační číslo (RČ) poplatníka, který pověřil evidováním

této tržby poplatníka, který tržbu eviduje, základ daně z přidané hodnoty a daň podle sazeb daně z přidané hodnoty, celková částka v režimu daně z přidané hodnoty pro cestovní službu, celková částka v režimu daně z přidané hodnoty pro prodej použitého zboží, datum započtení tržby, UUID zprávy, datum a čas odeslání zprávy, údaj, zda se jedná o první zaslání údajů o tržbě, datum a čas přijetí zprávy, fiskální identifikační kód, jednoznačná identifikace tržby, daňové identifikační číslo poplatníka uvedené v certifikátu (RČ poplatníka), identifikátor certifikátu certifikační autority, sériové číslo certifikátu poplatníka(l.3).

Dále kontrolovaný dne 12. prosince 2017 písemně uvedl, že *dle ust. § 27 zákona o evidenci tržeb správce daně umožní způsobem umožňujícím dálkový přístup každému ověřit, zda byly údaje o dané tržbě zaslány správci daně. Ověření účtenky je umožněno prostřednictvím aplikace „Ověření účtenky" na Daňovém portále (l.3).*

Údaje z ověření účtenky: daňové identifikační číslo poplatníka (RČ) poplatníka, datum a čas tržby, celková částka tržby, fiskální identifikační kód, bezpečnostní kód poplatníka, režim tržby, IP adresa, identifikace prohlížeče (l.3).

V žádosti o autentizací údaje

Kontrolovaný dále dne 12. prosince 2017 písemně uvedl, že *dle § 13 zákona o evidenci tržeb je poplatník povinen před přijetím první evidované tržby podat žádost o autentizační údaje. Autentizační údaje slouží k přístupu na společné technické zařízení správce daně umožňující poplatníkovi správu certifikátů pro evidenci tržeb a údajů pro správu evidence tržeb. Žádost může podat poplatník nebo jeho zástupce oprávněný současně k převzetí autentizačních údajů pouze:*

a) prostřednictvím společného technického zařízení správce daně datovou zprávou s ověřenou identitou této osoby způsobem, kterým se lze přihlásit do její datové schránky, a to ve formátu a struktuře zveřejněné správcem daně, nebo

b) ústně do protokolu, a to u kteréhokoliv věcně příslušného správce daně. Požádal-li poplatník o autentizační údaje způsobem, kterým se lze přihlásit do jeho datové schránky, správce daně je dle § 14 odst. 1 zákona o evidenci tržeb poplatníkovi přidělí prostřednictvím této datové schránky bez zbytečného odkladu. Podal-li poplatník žádost o autentizační údaje ústně do protokolu, správce daně je dle § 14 odst. 2 zákona o evidenci tržeb poplatníkovi přidělí v rámci tohoto jednání.

Žádost obsahuje osobní a jiné údaje v rozsahu: *identifikace Finančního úřadu (včetně územního pracoviště), u kterého je o autentizací údaje žádáno, informace pro správce daně, zda se jedná o reakci na výzvu k odstranění vad podání dle § 74 daňového řádu a číslo jednací předmětné výzvy, místo a datum vyhotovení žádosti, identifikace poplatníka, daňové identifikační číslo poplatníka (RČ), typ poplatníka (fyzická nebo právnická osoba), jméno a příjmení, datum narození,* a další údaje týkající se sídla a kontaktních údajů *právnické osoby/adresa místa pobytu fyzické osoby podle § 13 odst. 1 daňového řádu.*

Kontrolovaný dále uvedl, že *autentizační údaje jsou primárně tvořeny názvem uživatele a heslem. Heslo slouží pouze pro prvotní přihlášení. Z důvodu zabezpečení je poplatník při prvním přihlášení k účtu do aplikace Elektronická evidence tržeb vyzván ke změně hesla. Platnost prvotního hesla je maximálně 90 dní.*

Standardním způsobem dochází v Automatizovaném daňovém systému ke zpracování údajů v souvislosti s vyřizováním žádosti dle § 11 a § 32 zákona o evidenci tržeb (l.3).

V aplikaci Elektronická evidence tržeb na Daňovém portálu

Kontrolovaný dne 12. prosince 2017 písemně uvedl, že *dle ust. § 26 zákona o evidenci tržeb je správce daně povinen umožnit poplatníkovi nahlédnout do informací shromažďovaných na technickém zařízení správce daně, tedy údajů, které byly předmětem evidenční povinnosti podle § 18 odst. 1 písm. a) a § 19 zákona o evidenci tržeb. Tato povinnost je plněna prostřednictvím aplikace Elektronická evidence tržeb. Dle ust. § 17 zákona o evidenci tržeb je poplatník povinen prostřednictvím společného technického zařízení správce daně před získáním certifikátu pro evidenci tržeb, oznámit údaje o provozovnách, prostřednictvím kterých provádí činnosti, z nichž plynou evidované tržby, nebo v nichž přijímá evidované tržby. Dojde-li ke změně údajů o provozovnách, je poplatník povinen tuto změnu oznámit správci daně do 15 dnů ode dne, kdy změna nastala, nejpozději však před uskutečněním první evidované tržby v provozovně, které se změna týká. Tato oznamovací povinnost může být splněna pouze prostřednictvím aplikace Elektronická evidence tržeb.*

Osobní údaje poplatníka v rozsahu: *daňové identifikační číslo poplatníka (RČ poplatníka), jméno a příjmení, datum narození, bydliště poplatníka – ulice, obec, PSČ, údaje o provozovně poplatníka, které uvedl v procesu oznámení údajů o provozovnách v aplikaci Elektronická evidence tržeb.*
Dále údaje o uživatelích majících přístup k účtu poplatníka v aplikaci v rozsahu: *název uživatele – číselná identifikace uživatele přidělena na základě žádosti o autentizační údaje nebo založením uživatele v aplikaci, jméno a příjmení, mobilní telefon, E-mail, způsob ověření přístupu k účtu (heslo, SMS), rozsah oprávnění uživatele ke správě účtu (tj. oprávnění ke správě provozoven, certifikátů nebo pouze k prohlížení tržeb, administrátor.)*

Prvotní přístup do aplikace získává poplatník na základě žádosti o přidělení autentizačních údajů podané u správce daně (§ 13 a § 14 zákona o evidenci tržeb). Další uživatele s přístupem k účtu již může zadávat poplatník v aplikaci samostatně. Je tedy pouze na uvážení poplatníka, zda umožní dalším osobám přístup k účtu. Dále jsou v *aplikaci k dispozici údaje o tržbách ve formě součtů tržeb za určité časové období (denní, měsíční, čtvrtletní a roční).*

Poplatník má možnost získat údaje o činnostech všech uživatelů, které byly na účtu poplatníka zaznamenány (l.3).

35. Kontrolovaný dne 12. prosince 2017 písemně uvedl, že *doba uchovávání údajů obsažených v aplikacích evidence tržeb Údaje v aplikacích jsou jedním z podkladů při správě daní, která je dle ust. § 1 odst. 2 daňového řádu postupem, jehož cílem je správné zjištění a stanovení daní a zabezpečení jejich úhrady. Lhůta, po kterou může být daň stanovena, končí nejpozději uplynutím 10 let od jejího počátku (§ 148 odst. 5 daňového řádu). Tato lhůta je obsažena též ve Spisovém řádu Finanční správy České republiky č.j. 47448/12-1910.*
Doba uchovávání údajů je 10 let (l.3).

36. Kontrolovaný dne 12. prosince 2017 předložil *Metodický pokyn k přidělování autentizačních údajů, účinný ode dne 1.9.2016,* stanovující postup orgánů Finanční správy České republiky při zpracování žádosti o autentizační údaje v souladu se zákonem č. 112/2016 Sb., o evidenci tržeb *(l.4.11).*

Ke stížnosti

37. Kontrolovaný dne 12. prosince 2017 písemně uvedl, že k *obdobnému obsahu již GFŘ panu* [redacted] *odpovídalo v rámci zákona č. 106/1999 Sb., o svobodném přístupu k informacím, což kontrolovaný doložil (l.4.23-4.25).*

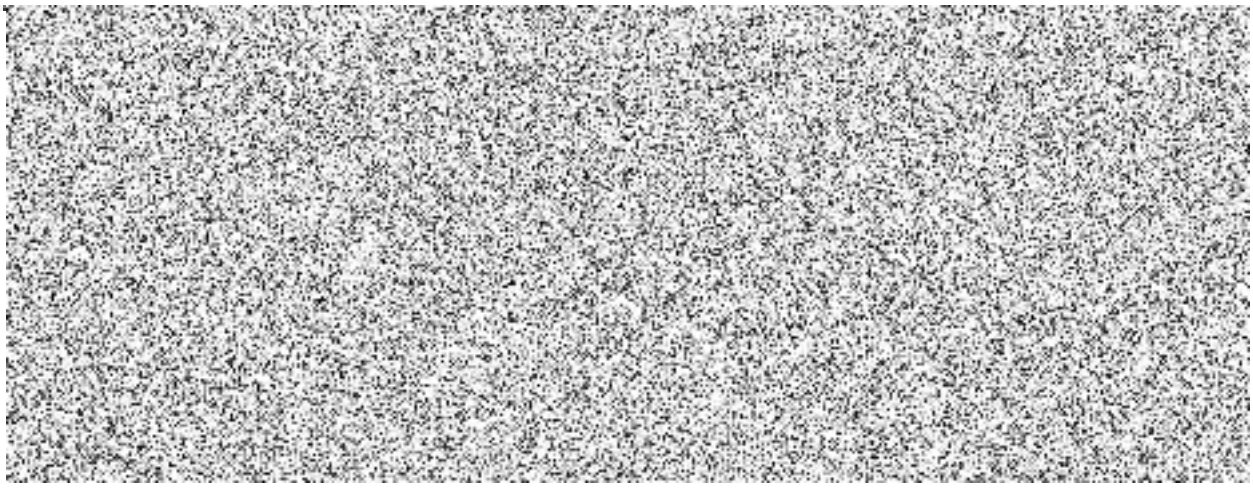
Dále uvedl, že *Komerční produkt reCAPTCHA společnosti Google Inc., jsme na Daňový portál, do přihlašovací stránky SPRÁVA ÚDAJŮ EVIDENCE TRŽEB implementovali, v souvislosti se zapracováním aplikací elektronické evidence tržeb (EET) do finanční správou provozovaného Automatizovaného daňového informačního systému (ADIS), jehož součástí jsou i elektronické služby finanční správy. Z hlediska bezpečnosti a ochrany proti robotickým útokům byla vybrána reCAPTCHA, která je sofistikovanějším systémem zabezpečení, než CAPTCHA, případně systém, který je použit u datových schránek. Prosté alfanumerické znaky jsou roboty snadno rozpoznatelné a nezabezpečují dostatečnou ochranu. Zabezpečení informačního systému před robotickými útoky vnímáme jako zajištění bezpečnosti informací v IT systému a zajištění dostupnosti a spolehlivosti služeb. ADIS, jehož součástí jsou i data EET je informační systém kritické informační infrastruktury, kde oblast kybernetické bezpečnosti vyplývá ze zákona č.181/2014 Sb., o kybernetické bezpečnosti. Jsme si vědomi, možných negativ, které mohou plynout s vazby na komerční produkt společnosti Google Inc., které jsou svázány s obecnými vlastnostmi veřejné internetové komunikace (cookies, footprinting, …), ty jsou však spojeny se zásadami zabezpečení uživatelské stanice (PC, Tablet, Notebook, …). V žádném případě Finanční správa ČR nepředává žádná data uživatelů našich webových aplikací. Nemáme žádnou smlouvu se společností Google Inc. Služba je provozována na základě registrace účtu. Smluvní podmínky a informace o ochraně soukromí jsou k dispozici prostřednictvím odkazů přímo v grafickém poli reCAPTCHA. Jelikož se snažíme našim klientům maximálně zjednodušit práci ve webových aplikacích provozovaných na Daňovém portálu a současně chránit jejich data a soukromí, kontaktovali jsme Ministerstvo vnitra, jako gestora aktivity „Akčního plánu pro Společnost 4.0“, jejímž cílem je kromě jiného zajistit a hlavně pomoci úřadům vytvářet elektronické služby. Naším cílem je jednodušší, bezpečná a pokud možno jednotná práce na Daňovém portálu i ostatních portálech orgánů veřejné moci a věříme, že se podaří najít řešení a tím tak společně postupně naplňovat jednotlivé aktivity Akčního plánu pro Společnost 4.0. (l.3 a l.4.25).*

38. To kontrolovaný dne 13. dubna 2018 písemně doplnil; v žádosti *o pomoc, adresované* Ministerstvu vnitra, jako gestorovi *aktivity „Akčního plánu pro Společnost 4.0“, jejímž cílem je kromě jiného zajistit a hlavně pomoci úřadům vytvářet elektronické služby* [redacted], požadoval *najít jednotné řešení v rámci veřejné správy, které by současně umožnilo nahradit komerční reCAPTCHA. Bohužel jsme v odpovědích* [redacted] *a* [redacted] *nedostali kladné vyjádření. Ve vlastní režii jsme, na bázi již implementované aplikace přihlašování se do Datových schránek, připravili vlastní řešení, které nahradí reCAPTCHA, tedy i jakoukoliv vazbu na Google. Aktuálně je tento produkt nasazen ve veřejném testovacím prostředí a ve velmi krátkém čase bude v prostředí produkčním (l.9).*

Ostatní zjištění

39. Kontrolující dne 5. dubna 2018 provedli de visu kontrolu jednoho z pracovišť kontrolovaného, a to Odboru daňových informačních systémů Žitná 563/12, Praha 2.

40. Kontrolující dne 18. dubna 2018 provedli de visu kontrolu pracoviště kontrolovaného, a to Finančního úřadu pro hlavní město Prahu, Štěpánská 619/28, 111 21, Praha 1.



41. Dne 2. května 2018 obdržel Úřad od kontrolovaného sdělení, že *vlastní řešení, které nahradilo komerční produkt* re CAPTCHA společnosti Google Inc., bylo úspěšně aktivováno do produkčního prostředí dne 17. dubna 2018 *(l.11).*

Porovnání zjištěného stavu věci s relevantním ustanovením zákona č. 101/2000 Sb.

42. <u>k § 4 písm. a)</u>

Podle ustanovení § 4 písm. a) zákona č. 101/2000 Sb. je *osobním údajem 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.*

Údaj se stává osobním údajem ve smyslu zákona č. 101/2000 Sb. na základě obecných zákonných kritérií ztotožnitelnosti spojením s údaji identifikačními. K tomu, aby informace představovala osobní údaj, nemusí obsahovat označení osoby přesným identifikátorem či několika jinými údaji, které jednoznačnou identifikaci tvoří (přímá identifikace), ale postačuje, má-li správce souboru, který neobsahuje identifikátory subjektů údajů umožňující přímou identifikaci, v držení.

Z kontrolního zjištění 34. je zřejmé, že v souvislosti s výkonem působnosti podle zákona č. 112/2016 Sb., jsou kontrolovaným zpracovány osobní údaje ve smyslu § 4 písm. a) zákona č. 101/2000 Sb. [zejména: *jméno a příjmení, datum narození, bydliště – ulice, obec, PSČ, údaj, zda je poplatník plátcem daně z přidané hodnoty, místně příslušný správce daně poplatníka, RČ pověřujícího poplatníka, Daňové identifikační číslo poplatníka (RČ poplatníka), datum založení poplatníka v EET, označení provozovny, označení pokladního zařízení, na kterém je tržba evidována, pořadové číslo účtenky, datum a čas přijetí tržby nebo vystavení účtenky, celková částka tržby, bezpečnostní kód poplatníka, podpisový kód poplatníka, základ daně z přidané hodnoty a daň podle sazeb daně z přidané hodnoty, IP adresa, identifikace prohlížeče, název uživatele - číselná identifikace uživatele přidělena na základě žádosti o autentizační údaje nebo založením uživatele v aplikaci, mobilní telefon, E-mail, způsob ověření přístupu k účtu (heslo, SMS), rozsah oprávnění uživatele ke správě účtu a další technické údaje (např. datum započtení tržby, UUID zprávy, datum a čas odeslání zprávy, údaj, zda se jedná o první zaslání údajů o tržbě, datum a čas přijetí zprávy, fiskální identifikační kód, jednoznačná identifikace tržby)* a další údaje týkající se sídla a kontaktních údajů *právnické osoby/adresa místa pobytu fyzické osob].*

43. <u>k § 4 písm. e)</u>

Podle ustanovení § 4 písm. e) zákona č. 101/2000 Sb. je *zpracováním osobních údajů jakákoliv informace 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.*

Z kontrolního zjištění 5. a 6. je zřejmé, že kontrolovaným je provozován Automatizovaný daňový informační systém (ADIS), v rámci něhož dochází k systematickému shromažďování, ukládání na nosiče informací, uchovávání, tedy ke zpracovávání osobních údajů ve smyslu § 4 písm. e) zákona č. 101/2000 Sb.

44. <u>k § 4 písm. j)</u>

Podle ustanovení § 4 písm. j) zákona č. 101/2000 Sb. *je 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.*

Ze znění § 2 zákona č. 112/2016 Sb. vyplývá účel zpracování osobních údajů a z téhož ustanovení je působnost podle tohoto zákona vykonávána orgány Finanční správy České republiky, resp. GFŘ, které v rámci této působnosti provozuje Automatizovaný daňový informační systém (ADIS).

Kontrolovaný je v pozici správce ve smyslu § 4 písm. j) zák. č. 101/2000 Sb.

45. k § 4 písm. k)

Podle § 4 písm. k) zákona č. 101/2000 Sb. je *zpracovatelem každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona*.

Z kontrolního zjištění 7. je patrné, že zpracovatelem dat z Automatizovaného daňového informačního systému (ADIS) je Celní správa České republiky.

46. k § 5 odst. 1 písm. b)

Podle ustanovení § 5 odst. 1 písm. b) zákona č. 101/2000 Sb. je správce povinen stanovit prostředky a způsob zpracování osobních údajů.

Z kontrolního zjištění 5. je zřejmé, že kontrolovaný provozuje Automatizovaný daňový informační systém (ADIS), a že Státní pokladnou Centrem sdílených služeb, s.p. (SPCSS) je, na základě Rámcové smlouvy na služby související s přípravou a provozem elektronické evidence tržeb, provozována Transakční část a krátkodobé úložiště elektronické evidence tržeb.

Z kontrolního zjištění 8. je zřejmé, že kontrolovaný předložil projektovou a provozní dokumentaci, která popisuje požadavky na zajištění funkčních procesů elektronické evidence tržeb, tedy stanovil prostředky a způsob zpracování osobních údajů.

Kontrolou nebylo zjištěno porušení § 5 odst. 1 písm. b) zákona č. 101/2000 Sb.

47. k § 5 odst. 1 písm. d)

Podle ustanovení § 5 odst. 1 písm. d) zákona č. 101/2000 Sb. je *správce povinen shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu.* Povinnost uvedená v citovaném ustanovení se týká přiměřenosti zpracovávaných osobních údajů.

Přiměřenost rozsahu zpracovávaných osobních údajů je nezbytné posuzovat vždy ve vztahu ke stanovenému účelu zpracování.

Evidenci tržeb upravuje zákon č. 112/2016 Sb. v ustanovení § 19 zákona č. 112/2016 Sb. je stanoven rozsah zasílaných údajů, stejně jako v ustanovení § 20 zákona č. 112/2016 Sb. jsou stanoveny údaje na účtence, které je poplatník povinen na účtence uvádět.

Na základě nálezu Ústavního soudu ze dne 12. prosince 2017, sp. zn. Pl. ÚS 26/16, došlo ke změně § 20 odst. 1 písm. b) zákona č. 112/2016 Sb. DIČ od 1. března 2018 není údajem povinně uváděným na účtence.

Provedenou kontrolou bylo zjištěno, že kontrolovaným je provozován Automatizovaný daňový informační systém (ADIS) v rámci něhož dochází k systematickému shromažďování osobních údajů za účelem a v rozsahu nezbytném pro správu daní.

Kontrolou nebylo zjištěno porušení § 5 odst. 1 písm. d) zákona č. 101/2000 Sb.

48. k § 5 odst. 1 písm. e)

Podle ustanovení § 5 odst. 1 písm. e) zákona č. 101/2000 Sb. *je správce povinen uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely státní statistické služby, pro účely vědecké a pro účely archivnictví. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů a osobní údaje anonymizovat, jakmile je to možné.*

Z kontrolního zjištění 35. je zřejmé, že správce uchovává osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování, tedy 10 let (vyplývající z § 148 odst. 5 zákona č. 280/2009 Sb., daňový řád).

Kontrolou nebylo zjištěno porušení § 5 odst. 1 písm. e) zákona č. 101/2000 Sb.

49. k § 5 odst. 2

Podle § 5 odst. 2 zákona č. 101/2000 Sb. *může správce zpracovávat osobní údaje pouze se souhlasem subjektu údajů.* Bez tohoto souhlasu je může zpracovávat v případě, že je splněn některý z právních titulů uvedených v ustanovení § 5 odst. 2 písm. a) až g) citovaného zákona.

Evidenci tržeb upravuje zákon č. 112/2016 Sb. V ustanovení § 2 zákona č. 112/2016 Sb. je stanovena působnost podle tohoto zákona.

Lze tedy konstatovat, že vést osobní údaje ukládá kontrolovanému zákon č. 112/2016 Sb. Jedná se tedy o právní povinnost stanovenou zákonem. Z hlediska zákona č. 101/2000 Sb. se v takovém případě jedná o zpracování osobních údajů, které je nezbytné pro dodržení právní povinnosti správce dle ustanovení § 5 odst. 2 písm. a) zákona č. 101/2000 Sb., jež správce může provádět bez souhlasu subjektu údajů.

Kontrolou nebylo zjištěno porušení § 5 odst. 2 zákona č. 101/2000 Sb.

50. k § 6

Podle § 6 zákona č. 101/2000 Sb. *pokud zmocnění nevyplývá z právního předpisu, musí správce se zpracovatelem uzavřít smlouvu o zpracování osobních údajů. Smlouva musí mít písemnou formu. Musí v ní být zejména výslovně uvedeno, v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá a musí obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů.*

Provedenou kontrolou bylo zjištěno, že zmocnění Celní správy České republiky k prověřování plnění povinností při evidenci tržeb vyplývá z právního předpisu (zákona č. 112/2016 Sb.).

V § 2 odst. 2 zákona č. 112/2006 Sb. je uvedeno, že působnost k prověřování plnění povinností při evidenci tržeb mají také orgány Celní správy České republiky. Podle § 30 odst. 1 zákona č. 112/2016 Sb. je k řízení o přestupcích podle tohoto zákona příslušný celní úřad.

Kontrolou nebylo zjištěno porušení § 6 zákona č. 101/2000 Sb.

51. k § 13

Kontrolující dále posuzoval, zda kontrolovaná osoba postupovala při zpracování osobních údajů v souladu k ustanovení § 13 zákona č. 101/2000 Sb.

Podle ustanovení § 13 odst. 1 zákona č. 101/2000 Sb. je správce i zpracovatel osobních údajů povinen 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 nebo jinému zneužití.

Tímto ustanovením je stanovena obecná povinnost údaje chránit, a to jak před úmyslným jednáním osob nebo jednáním z nedbalosti, ale i před živelními událostmi anebo selháním techniky, v jejichž důsledku by mohlo dojít ke ztrátě, poškození, zničení či zneužití údajů. Zákonodárce tak stanovil před čím vším je třeba osobní údaje chránit, konkrétní podobu ochrany osobních údajů však ponechal na správci či zpracovateli. Přijatá opatření však musí vykazovat náležitou odbornou úroveň odrážející rizika spojená s konkrétními operacemi s osobními údaji a s povahou zpracovávaných údajů. Součástí této povinnosti je také důsledná kontrola plnění přijatých opatření a povinností odpovědných osob. Povinnost uvedené v citovaném ustanovení je formulována tak, že správce či zpracovatel osobních údajů odpovídají za následek, protiprávní stav, nikoli za zavinění.

Z kontrolních zjištění bodu 19., 39. a 40. je zřejmé, že kontrolovaný přijal 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 nebo jinému zneužití.

Podle ustanovení § 13 odst. 2 zákona č. 101/2000 Sb. je správce nebo zpracovatel povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.

Správci a zpracovatelé tak mají povinnost popsat opatření přijatá při plnění povinností stanovených v ostatních odstavcích § 13 zákona č. 101/2000 Sb.
Kontrolovaný v rámci kontroly předložil dokumenty, které obsahují přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů. Jedná se především o dokument Směrnice  generálního ředitele, Bezpečnost informací (viz kontrolní zjištění č. 9), Směrnice  generálního ředitele, Zabezpečení informačních systémů (viz kontrolní zjištění č. 9), Směrnice  generálního ředitele, Subjekty informačních systémů, jejich práva a povinnosti (viz kontrolní zjištění č. 9), IS kritické informační infrastruktury podle zákona č. 181/ 2014 Sb. o kybernetické bezpečnosti a navazující Vyhlášky č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (viz kontrolní zjištění č. 4).

Podle ustanovení § 13 odst. 3 zákona č. 101/2000 Sb. 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.

Kontrolovaný v rámci kontroly předložil dokumenty, které prokazují, že kontrolovaný posuzuje rizika plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup, a to: Směrnici č. 38/2013 generálního ředitele, Zásady přístupových práv v Automatizovaném daňovém informačním systému, Směrnici č. 39/2013 generálního ředitele, Zásady ochrany dat a přístupu do osobních počítačů (viz kontrolní zjištění č. 10). Kontrolovaný dále předložil přehled přístupů zaměstnanců na jednotlivých FÚ (viz kontrolní zjištění č. 11). Kontrolovaný dále předložil logy z jednotlivých databází ADIS za období 10. -15. října 2017 (viz kontrolní zjištění č. 12).

Z kontrolních zjištění 19., 39. a 40. je zřejmé, že kontrolující provedl de visu fyzické kontroly na pracovištích, kde bylo ověřeno zabezpečení přístupu, a že vstup do prostředí odpovídá dokumentaci zaslané kontrolovaným.

Automatizovaný daňový IS ADIS byl určen jako informační systém kritické informační infrastruktury podle Zákona č. 181/2014 Sb. o kybernetické bezpečnosti a navazující Vyhlášky č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti. Tato skutečnost automaticky nastavuje standardy jeho zabezpečení.

Ke stížnosti

Z kontrolních zjištění 37. a 38. je zřejmé, že kontrolovaný komerční produkt reCAPTCHA společnosti Google Inc. implementoval v souvislosti se zpracováním aplikací elektronické evidence tržeb (EET) do finanční správou provozovaného Automatizovaného daňového informačního systému (ADIS). Dle vyjádření kontrolovaného Finanční správa ČR nepředává žádné nadbytečné údaje uživatelů jeho webových aplikací do Google. Služba je provozována na základě registrace účtu.
Z kontrolních zjištění 2., 3. , 40. a 41. je zřejmé, že kontrolovaný si byl v průběhu kontroly vědom možných negativ, které mohou plynout s vazby na komerční produkt společnosti Google Inc., a proto připravil vlastní řešení. Tím nahradil dne 17. dubna 2018 *komerční produkt* reCAPTCHA.
S ohledem na výše uvedené nebylo konstatováno porušení zákona č. 101/2000 Sb., a to s přihlédnutím ke skutečnosti, že v době provádění kontroly byla problematika produktu reCAPTCHA již vyřešena.

Kontrolou nebylo zjištěno porušení § 13 zákona č. 101/2000 Sb.

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

Kontrolující: otisk úředního razítka

Mgr. Daniel Rovan	inspektor	*(dokument podepsán elektronicky)*
……	……..	
titul jméno příjmení	funkce	podpis
Ing. Zdenka Filová	pověřená zaměstnankyně	*(dokument podepsán elektronicky)*
…….	……	
titul jméno a příjmení	funkce	podpis
Mgr. Marta Lásiková	pověřená zaměstnankyně	*(dokument podepsán elektronicky)*
……..	……..	
titul jméno a příjmení	funkce	podpis
Ing. Radek Loub	pověřený zaměstnanec	*(dokument podepsán elektronicky)*
……..	……..	
titul jméno a příjmení	funkce	podpis

(služební poměr ukončen před vyhotovením kontrolního protokolu)