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

Čj. UOOU-09654/18-10
Praha 4. března 2019

Protokol o kontrole

Kontrolní orgán:
Úřad pro ochranu osobních údajů, se sídlem Pplk. Sochora 27, 170 00 Praha 7 (dále jen „Úřad“) Pravomoc kontrolního orgánu k výkonu kontroly vyplývá z 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 (dále jen „Nařízení EU“).

Kontrolující:
- MVDr. František Bartoš – inspektor Úřadu, číslo služebního průkazu XXX
- JUDr. Michal Jelínek – pověřený zaměstnanec Úřadu, číslo služebního průkazu XXX
- Ing. Max Gůt – pověřený zaměstnanec Úřadu, číslo služebního průkazu č. XXX

Kontrolovaná osoba
XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX
XXXXXXXXXX
(dále jen „Společnost“)

Místo provedení kontroly
- sídlo Úřadu - Pplk. Sochora 27, 170 00 Praha 7
- sídlo Společnosti – XXXXXXXXXXXXXXXXXXXXXXX

Předmět kontroly:
Předmětem kontroly je dodržování povinností správce osobních údajů v souvislosti s používáním dynamického biometrického podpisu, se zaměřením na zákonnost tohoto zpracování, poskytování informací o tomto zpracování a zabezpečení zpracovávaných osobních údajů.

První kontrolní úkon:
Prvním kontrolním úkonem je písemné Oznámení o zahájení kontroly č.j. UOOU-09654/18-3 ze dne 24. října 2018, které bylo do datové schránky Společnosti dodáno téhož dne.

Poslední kontrolní úkon:
Posledním kontrolním úkonem je sdělení informací a doložení dokumentů Společností, ze dne 30. ledna 2019.

I.Protokol o kontrole se opírá o následující podklady, které byly pořízeny v průběhu kontroly.

1. Kontrolní plán Úřadu pro rok 2018, č.j. UOOU-09654/18-1

2. Analýza před zahájením kontroly, č.j. UOOU-0v.49654/18-2
Přílohy:
- Protokol o kontrole UOOU-02757/17-17, ze dne 14. srpna 2017 (příloha č. 1).
- Informace o Společnosti a dynamickém biometrickém podpisu získané z internetu (příloha č. 3–16).
- Stanovisko Úřadu č. 2/2014 – „Dynamický biometrický podpis z pohledu zákona o ochraně osobních údajů".

3. Oznámení o zahájení kontroly, ze dne 24. října 2018 č.j. UOOU-09654/18-3.

4. Sdělení informací a doložení dokumentů v rámci zahájené kontroly č.j. UOOU-09654/18-4, ze dne 19. listopadu 2018.
Přílohy:
- Znalecký posudek č. 120-1110/10/2017, ze dne 9. dubna 2018
- Memorandum – XXXXXXXXXXXXXXXXXXXXXXX, ze dne 27. dubna 2018
- Fotokopie formuláře – „Základní osobní údaje"
- „Informace o zpracování osobních údajů klientů XXXXX"
- Seznam zpracovatelů
- Smlouva o poskytování služeb XXX, ze dne 26. listopadu 2015
- Žádost Úřadu o součinnost, ze dne 7. ledna 2019

5. Úřední záznam z ústního jednání a místního šetření, ze dne 16. ledna 2019, č.j. UOOU-09654/18-6.

6. Průvodní dopis k zaslání Úředního záznamu, ze dne 18. ledna 2019, č.j. UOOU-09654/18-7.

7. Dopis Společnosti, ze dne 25. ledna 2019 – Zaslání informací a doložení dokumentů v návaznosti na ústní jednání, č.j. UOOU-09654/18-8.
Přílohy:
- Postup při volbě dokončení rámcové smlouvy.
- Vyhodnocení rizik zpracování osobních údajů – Zkrácené vymezení pro rolovací program.
- Dokument „Kontrolní a bezpečnostní opatření pro zpracování dat XXX".
- Dokument „Ochrana osobních údajů XXX"
- Informace zákazníkovi, že do systému XXXXX byla úspěšně zavedena smlouva.
- 3 x PrintScreen – Rámcová smlouva.

8. - Sdělení informací a doložení dokumentů, ze dne 30. ledna 2019, č.j. UOOU-9654/18-6.
Přílohy:
- Úschova soukromého klíče – bezpečnostní politika (XXXXXXXXXXXXXXXXXXXX)
- Protokol o kontrole funkčnosti a čitelnosti soukromého klíče

II. Důvod kontroly:
Kontrola byla zahájena na základě kontrolního plánu Úřadu pro rok 2018, za účelem používání dynamického biometrického podpisu (dále jen „DBP“) klienty Společnosti, se zaměřením na zákonnost a tohoto zpracování, poskytování informací o tomto zpracování a zabezpečení zpracovávaných osobních údajů.

III. Kontrolní zjištění kontrolujících:
Hlavní aktivitou Společnosti je poskytování finančního poradenství a zprostředkování uzavírání životního pojištění, investic a hypoték.
DBP je datová struktura, která vzniká v okamžiku, kdy se klient Společnosti podepisuje perem na podepisovacím zařízení (tzv. signature pad), které kromě výsledné grafické podoby samotného podpisu sleduje a zaznamenává i rychlost, sklon, křivky, posloupnost a přítlak tahů apod., které jsou pro každého člověka charakteristické a jedinečné. DBP obsahuje nejen samotné vyobrazení podpisu, ale současně i jeho skryté, jedinečné dynamické vlastnosti a individuální charakteristiky. Poskytnutím DBP se tedy zpracovávají biometrické (statické a dynamické) charakteristiky vlastnoručního podpisu (dynamický biometrický podpis).

Oznámení o zahájení kontroly č.j. UOOU-09654/18-3, ze dne 24. října 2018, bylo do datové schránky Společnosti dodáno téhož dne. V „Oznámení“ byla Společnost požádána o předložení následujících informací a dokumentů:

1. Předložte informaci – analýzu rizik a posouzení vlivu na ochranu osobních údajů vztahující se ke zpracování osobních údajů v rámci využívání technologie dynamického biometrického podpisu.
2. Popište Vámi používanou technologii dynamického biometrického podpisu.
3. Popište důvod / účel používání systému dynamického biometrického podpisu, zejména ozřejměte otázku, zda dynamický biometrický podpis používáte pouze k podpisu konkrétních dokumentů, nebo dynamický biometrický podpis používáte obecně k autentizaci klienta.
4. Sdělte, zda umožňuje využívaná technologie dynamického biometrického podpisu zaznamenaný, uchovávaný, podpisový vzor připojit i k jiným dokumentům, než pro jaký byl od subjektu údajů získán.
5. Popište přijatá bezpečnostní opatření k zabránění zneužití dynamického biometrického podpisu.
6. Popište postup při využívání dynamického biometrického podpisu a sdělte, jakým způsobem klient uděluje svůj souhlas se zpracováním a jakým způsobem postupujete v případě neudělení souhlasu.
7. Doložte plnění povinnosti správce osobních údajů dle čl. 13 a násl. Nařízení (EU) v oblasti Informace a přístupu k osobním údajům při zpracování osobních údajů prostřednictvím dynamického biometrického podpisu.
8. Jakým způsobem probíhá archivace dokumentů s dynamickým biometrickým podpisem.
9. Jakým způsobem je zabezpečený privátní klíč dynamického biometrického podpisu.

Společnost jako správce a zprostředkovatel finančních služeb shromažďuje osobní údaje za účelem uzavírání smluv v níže uvedených kategoriích a rozsahu osobních údajů. Zpracovávané osobní údaje jsou zveřejněny v dokumentu „Zásady zpracování osobních údajů“ na webových stránkách Společnosti XXXXXXXXXXXXXXXXXXXXXXX.
a) Identifikační údaje (jméno a příjmení, rodné příjmení, rodné číslo, datum narození, místo

a země narození, národnost, informace týkající se průkazu totožnosti).
b) Kontaktní údaje (např. trvalá adresa, korespondenční adresa, telefonní čísla, e-mail).
c) Údaje o stavu, rodině, zaměstnání (např. rodinný stav, děti, jiné závislé osoby, vzdělání, údaje o zaměstnání, PEP).
d) Elektronické údaje (např. IP adresy, časy připojení, vygenerovaná a zaslaná hesla, grafická podoba podpisu, cookies, tj. textové soubory – prohlížeč při používání webových stránek.).
e) Finanční údaje (např. příjmy, hotovost, výdaje, číslo bankovního účtu, údaje o majetku, údaje o jiných smlouvách na finanční produkty, plány do budoucna, aktuální životní situace, investiční dotazník atd.
f) Odvozené údaje (např. jméno poradce, navržené řešení, ID klienta).
g) Zvláštní kategorie osobních údajů (údaje o zdravotním stavu a zašifrovaná biometrická data, tedy DBP).
Výše uvedené údaje zpracovává Společnost podle druhu smluv, případně dalších dokumentů.

Kontrolou bylo zjištěno, že Společnost využívá DBP jako správce osobních údajů ve vztahu k dokumentům Společnosti, v souvislosti se smluvním vztahem k zákazníkům a dále jako zpracovatel ve vztahu k některým dokumentům svých obchodních partnerů, pro které Společnost provádí zprostředkovatelské finanční služby, přičemž podpis dokumentu, jako stvrzení smluvních ujednání.
Účelem zpracování DBP jako biometrického údaje je dle vyjádření Společnosti stvrzení platnosti právního jednání učiněného v písemné formě, a to způsobem, který zejména zjednodušuje proces poskytování finančně-poradenských služeb a zároveň ho i zatraktivňuje pro zákazníky (subjekty údajů). Společnost tedy zpracovává osobní údaje včetně DBP za účelem uzavírání smluv

Kontrolou bylo zjištěno, že Společnost zpracovává DBP za účelem potvrzení a uchování smluv a současně za účelem nepochybného ověření/verifikace podpisu klienta.

Společnost zpracovává DBP pouze u formulářů, které jsou k tomu uzpůsobeny a jako takové jsou naprogramovány v aplikaci XXX. Jedná o formuláře Finanční analýza, Zjištění potřeb a Předávací protokol. Tyto formuláře je možné vyplnit v aplikaci XXX a následně zvolit, zda má být pro účely podpisu konkrétní formulář vytištěn, nebo odeslán do aplikace XXXXX, určené pro připojení DBP. DBP je tedy vždy spojen s konkrétním podepsaným dokumentem a nelze jej použít obecně k autentizaci jinak než ve vztahu k tomuto dokumentu.

Osobní údaje týkající se zprostředkovatelské činnosti zpracovává Společnost po dobu trvání smluvního vztahu navázaného na podpis smlouvy a dalších 10 let po jeho ukončení. Jednotlivé produktové smlouvy jsou Společností zpracovávány po dobu jejich platnosti a dalších 10 let od jejich ukončení. Pokud se však klient Společnosti dohodne na schůzce s poradcem nebo Společnost požádá o kontakt později, zpracovává Společnost osobní údaje bez podpisu smlouvy, nejdéle po dobu 1 roku. Klienti jsou o výše uvedené době zpracování osobních údajů včetně DBP informování v dokumentu „Zásady zpracování osobních údajů“, který je umístěný na webových stránkách Společnosti XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.
Fyzická likvidace nosičů osobních údajů (zejména v listinné podobě) probíhá ve Společnosti v termínech a způsobem stanoveným v Archivačním a skartačním řádu. Stejné archivační lhůty má Společnost i pro anonymizaci osobních údajů v informačních systémech Společnosti.

Metoda anonymizace byla zvolena s ohledem na zachování integrity systémů a možnosti použít anonymizovaná data pro statistické účely. Přesný způsob anonymizace je určován IT oddělením s ohledem na aktuální znalosti technických prostředků, které zajistí nevratnost procesu anonymizace. Vzhledem k tomu, že anonymizace probíhá i v návazných systém zpracovatelů, jsou anonymizovaná data přesunuta do tzv. karantény, a teprve po ověření bezproblémové anonymizace ve všech návazných systémech je přistoupeno k vymazání tohoto souboru.

Kontrolou souhlasu se zpracováním DBP bylo zjištěno, že v návaznosti na „Memorandum" ze dne 27. dubna 2018, které pro Společnost zpracovala advokátní kancelář XXXXXXXXXXXXXXXXXXXXXXX, přistoupila Společnost k názoru, že v případě DBP nedochází ke zpracování zvláštních kategorií osobních údajů resp. k takovému zpracování dochází až ve chvíli, kdy tomu svědčí i zákonný důvod dle čl. 9 odst. 2 písm. f), tedy jako zpracování nezbytné pro určení, výkon nebo obhajobu právních nároků nebo pokud soudy jednají v rámci svých soudních pravomocí. Pro podporu tohoto tvrzení uvádí Společnost následující důvody:

„1) [redacted]

2) Pokud je účelem pořízení dynamického biometrického podpisu pouze akt podpisu samotného a zároveň ostatní znaky (data) vznikající při této činnosti (které ostatně v částečné míře vznikají i při standardním podepisování psacím prostředkem na hmotný nosič – typicky tlak) jsou ihned zabezpečeny takovým způsobem, že k nim nelze standardně přistupovat (a tedy více než při standardním podpisu), nelze na tento proces, který klient vědomě zvolil, použít pravidla, která jeho použití významně ztíží či znemožní, resp. jej významně odliší od standardního podepisování, když se má jednat o ekvivalentní proces, pouze provedený jinou formou.

3) Podle recitálu 15 GDPR „…by ochrana fyzických osob měla být technologicky neutrální a nezávislá na použitých technologiích. Ochrana fyzických osob by se měla vztahovat jak na automatizované zpracování osobních údajů, tak na manuální zpracování…". Ve smyslu tohoto ustanovení je pak neodůvodnitelný rozdíl v ochraně dynamického biometrického podpisu oproti podpisu standardnímu, za předpokladu že jediným účel je stvrzení platnosti právního jednání učiněného v písemné formě tak jak to vyžaduje § 561 z.č. 89/2012 Sb., Občanský zákoník.

4) Uchovávání zašifrovaných biometrických údajů, ke kterým lze získat přístup pouze za velmi specifických situací nelze považovat za zpracování zvláštní kategorie osobních údajů a jedná se nanejvýše o zpracování údajů ekvivalentní běžnému podpisu na písemném dokladu o právním jednání.

5) Z tohoto důvodu by bylo také absurdní vyžadovat ve vztahu k biometrickému podpisu, užitému výlučně k potvrzení písemného právního jednání způsobem popsaným ve znaleckém posudku, souhlas se zpracováním osobních údajů a uvádět tak subjekt údajů v omyl (dosahující intenzity klamání spotřebitele) tím, že se v něm vzbuzuje očekávání ohledně možnosti odvolání souhlasu (jako neomezitelného práva) a následků takového odvolání. Ve skutečnosti však odvolání souhlasu nemůže mít žádný dopad na pořízená data, když takové odvolání nemá vliv na zákonnost zpracování učiněného před jeho odvoláním, tedy na pořízení podpisu včetně biometrických údajů. Pokud by bylo v případě odvolání souhlasu požadavkem vymazat celý

podpis či i jen biometrická data, došlo by tím v podstatě k zneplatnění právního jednání. Vyžadovat souhlas subjektu údajů s takovýmto užitím biometrického podpisu by tak bylo typickým případem nadbytečného využití souhlasového režimu v případě, kdy případné zpracování osobního údaje je kryto jiným právním titulem.“

Kontrolou bylo zjištěno, že na formulářích smluv je dána možnost, aby si klient vybral způsob podpisu smlouvu, a to **v listinné podobě** nebo **biometricky** (příloha č. 1 k č.j. UOOU-09654/18-8).
Výše uvedené možnosti výběru podpisu se Společnosti týkají jako správce i zpracovatele osobních a biometrických údajů. O možnosti vybrat si způsob podpisu je klient informován při podpisu smlouvy. Kontrolou však nebylo prokázáno, zda je klient také informován ústně o tom, že jeho biometrické údaje budou uloženy v zašifrovaných metadatech v uložišti Společnosti.

Společnost informuje klienty o zpracování osobních údajů více způsoby.
a) Informace o zpracování osobních údajů je obsažená ve formuláři Finanční analýza, konkrétně na listu, kde se vyplňují základní osobní údaje. Tento formulář může subjekt údajů společně s finančním poradcem vyplňovat ručně, vyplňovat v aplikaci XXXX a následně vytisknout, nebo vyplňovat v aplikaci XXXX a následně podepsat DBP v aplikaci XXXXX. Informace o zpracování osobních údajů umístěna bezprostředně pod podpisem subjektu údajů a uvozena tučným nadpisem. V uvedené informaci je odkaz na dokument „Zásady zpracování osobních údajů“ zveřejněný na níže uvedených webových stránkách.
b) Podrobnější informace o zpracování osobních údajů a právech subjektů údajů jsou uveřejněny v dokumentu „Zásady zpracování osobních údajů“ na webových stránkách Společnosti v sekci poradenství XXXXXXXXXXXXXXXXXXX, kde je možné tyto informace stáhnout. V bodě 3.5 je uvedeno, že Společnost zpracovává zvláštní kategorie osobních údajů. Dále je v dokumentu uvedeno, že přestože při využití technologie DBP získává zpracováním biometrické údaje, jako tah, tlak, rychlost podpisu a jiné, tyto údaje ihned po získání zašifruje a uchovává v zašifrované podobě, tedy s nimi Společnost nijak nepracuje. [redacted]
Pod bod bodem 4. je v dokumentu uvedeno, že „Společnost zpracovává elektronické údaje (např. IP adresy, časy připojení, vygenerovaná a zaslaná hesla, zašifrovaná biometrická data, grafická podoba podpisu, cookies).“
c) Dále je v dokumentu uveden kontakt na pověřence pro ochranu osobních údajů, spolu s e-mailovou adresou XXXXXXXXXXXXXX.

Společnost informuje o právech subjektů údajů ve smyslu čl. 15 – 23 Nařízení EU na svých webových stránkách XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX v „Zásadách zpracování osobních údajů“. Práva subjektů údajů obsahuje také interní předpis Společnosti „Ochrana osobních údajů XXXX“.

Společnost na svých webových stránkách a ani v předložených podkladech neinformuje o tom, zda je klient DBM povinen pro stanovené účely poskytnout, a o důsledcích jejich případného neposkytnutí.

Společnost má na svých webových stránkách XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX informaci o svých zpracovatelích. Společnost zpracovává osobní údaje zejména prostřednictvím svých poradců, kteří působí jako podřízení pojišťovací zprostředkovatelé, zprostředkovatelé jiných finančních produktů, kteří jsou osoby samostatně výdělečně činné. Ve vztahu ke zpracování osobních údajů se v daném případě jedná o vztah zpracovatele vůči správci, kterým je Společnost. Jednotliví poradci se při kontaktu s klienty identifikují. Aktuální seznam všech spolupracujících poradců naleznou zájemci na stránkách České národní banky (www.cnb.cz) v sekci Seznamy a evidence, podsekci Seznamy regulovaných a registrovaných subjektů.

Mimo poradce, kteří jsou osoby samostatně výdělečně činné má Společnost tyto další zpracovatele:

Název	IČ	Oblast
XXXXXXXXXXXXXXXX	XXXXXXXX	IT služby
XXXXXXXXXXXXXXXX	XXXXXXXX	IT služby
XXXXXXXXXXXXXXXX	XXXXXXXX	IT služby
XXXXXXXXXXXXXXXX	XXXXXXXX	IT služby
XXXXXXXXXXXXXXXX	XXXXXXXX	IT služby
XXXXXXXXXXXXXXXX	XXXXXXXX	IT služby

Kontrolou bylo zjištěno, že má Společnost vyhotovenou analýzu rizik při zpracování osobních údajů, včetně DBP (příloha č. 2 dopisu, ze dne 25. ledna 2019, č.j. UOOU-09654/18-8).
Analýza obsahuje popis rizik a při zpracování osobních údajů včetně DBP, stupně rizik a jejich hodnocení: a) vysoce rizikové, b) zpracování s rizikem, c) ostatní zpracování.

Kontrolou bylo dále zjištěno, že si Společnost dala vyhotovit „Znalecký posudek č. 120-1110/10/2017“, ze dne 9. dubna 2018, ve kterém jsou uvedeny konkrétní technologické postupy při zpracování DBP, včetně PrintScreenu obrazovek jednotlivých postupů aplikace XXXXX, ve vztahu k elektronickému uzavření smlouvy s klientem pomocí zařízení XXXXXX, resp. použití DBP při zmapovaných postupech, včetně zabezpečení DBP proti zneužití.
Společnost byla zadavatelem Znaleckého posudku a závěry vyhotovené znalcem předložila kontrolujícím jako své stanovisko ke zpracování DBP.

Ze „Znaleckého posudku“, bylo zjištěno, že Společnost zpracovává osobní údaje na elektronických dokumentech, jak vlastních, tak dokumentech obchodních partnerů, a to jak v provedení, které nazývá originálem (elektronické dokumenty které obsahují DBP), tak v provedení, které nazývá kopií (elektronické dokumenty, které jsou zbaveny DBP, přičemž dokument obsahuje pouze 2D obrázek „vlastnoručního“ podpisu. Některé elektronické dokumenty vznikají u Společnosti (obsahující osobní údaje fyzických osob) a některé

elektronické dokumenty jsou Společnosti elektronicky předány obchodními partnery k zajištění podpisu. Dokumenty jsou mezi informačními systémy předávány pomocí zabezpečených protokolů, kdy informační systémy jsou připravené omezit seznam uživatelů s přístupem ke konkrétním obchodním případům, tedy k datům obsahujícím osobní údaje konkrétních, identifikovaných fyzických osob. Přístup k osobním údajům je přidělen pouze oprávněným osobám. O schválení přístupu rozhoduje vždy člen představenstva Společnosti. Systém přístupu je pravidelně vyhodnocován a probíhá periodická kontrola autenticity a integrity uchovávaných dat. Jednou za rok probíhá ověření dostupnosti dokumentů a ověření zabezpečení biometrických dat. HW a SW infrastruktura zajišťuje minimální ztrátu dat v případě havárie. [redacted]

Přístup k dokumentům s DBP má:
Uživatel – který je poradce nebo manažer v poradenské struktuře Společnosti.
Klient – má právo na zpřístupnění dokumentů, které sám podepsal DBP.
Obchodní partner vstupuje do systémů Společnosti přes rozhraní XXXXXX nebo za využití jiného rozhraní určeného pro tento účel. Předání biometricky podepsaných dokumentů obchodnímu partnerovi je možné výhradně způsobem k tomu určeným za dodržení bezpečnosti přenášených dat.
Zaměstnanec a spolupracovník Společnosti má přístup do systémů spravujících dokumenty obsahující dynamické biometrické podpisy pouze s uděleným oprávněním.
Zaměstnanci oddělení vývoje IT a SW.

Serverové části infrastruktury jsou ošetřeny v interní, bezpečnostní směrnicí, kdy o hardware a data se stará interní a vymezená obsluha. Elektronické dokumenty jsou uloženy v elektronickém archivu, kde je dokumentovaný přístup. Společnost má plán záloh, který dostatečně zajišťuje možnost obnovy v takovém čase, kdy minimální riziko s dopadem na práva a svobody fyzických osob z hlediska dostupnosti (plnění ze smlouvy apod.).
DBP je zpracován tak, že údaje (biometrika podpisu) jsou připojeny k elektronickému dokumentu takovým způsobem, že je eliminováno riziko neoprávněného zpracování [redacted]). [redacted]

Ze „Znaleckého posudku“ bylo dále zjištěno, že z podepsaného elektronického dokumentu není možné vlastnoruční digitální podpis "duplikovat" na další dokumenty, ani získat data vlastnoručního digitálního podpisu podepisující se osoby. V případě, kdy bude podepisovaný dokument před podpisem zobrazen a budou v něm určena místa, kde se má osoba podepsat a po uskutečnění podpisu bude dokument znovu zobrazen podepsaný, lze mít dle Společnosti za to, že podepisující osoba je dostatečně informována, co podepisuje.

Podle „Znaleckého posudku“ je dynamický biometrický podpis – druhý hash (pomocí XXXXX) vypočítán z původního hashe dokumentu a surových biometrických dat. Tím je docíleno svázání konkrétního podpisu s dokumentem. Jelikož surová biometrická data nejsou nikde uložena, není možné hash 2 podvrhnout. Dynamický biometrický podpis sám o sobě nezaručí (stejně jako klasický podpis), že dokument není po jeho vložení změněn. Technologie dynamického biometrického podpisu ale zajistí, že jakákoliv dodatečná změna po vložení podpisu se projeví jako úprava dokumentu a všechny tyto úpravy jsou v dokumentu vidět i

s vyznačením času. Není tedy možné již podepsaný dokument změnit a následně jej prohlásit za podepsaný originál s platným původním podpisem.

Ze Znaleckého posudku bylo dále zjištěno, že vlastnoruční digitální podpis (grafická podoba DBP) umožňuje identifikaci podepisující osoby použitím dvou kroků:

a) Identifikace osoby podle obsahu podepsaného dokumentu.
b) Autentizace podpisu písmoznalecky (grafologem).

Ve svém Znaleckém posudku vychází znalec XXXXXXXXXX. také ze závěrů Znaleckých posudků č. 2419/2014 a č. 55/2014, vypracovaných znalci XXXXXXXXXXXXXXXXXX a XXXXXXXXXXXXXXXXXXXXXX. Zadáním uvedených Znaleckých posudků byla problematika posouzení řešení systému XXXXXXXXXX (technologie DBP – vypracovaná společností XXXXXXXXXXXXXXXXXX). Znalec se také v posudku odkazuje na odborný článek „Závěry znaleckých posudků určujících pravost podpisu z kopie smlouvy“, autora XXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXX, který se v článku zabývá identifikaci rukou psaného popisu a podpisy na kopiích listin.

Kontrolou bylo zjištěno, že Společnost zabezpečuje databáze aplikace XXXXXX (obsahující osobní a biometrické údaje), tak externí elektronické dokumenty s DBP jsou šifrovány.

[redacted]

K zabezpečení soukromí klientů bylo ze „Znaleckého posudku“ také zjištěno, že viditelnost údajů klienta vůči ostatním uživatelům si může klient nastavit sám v sekci Profil. Pomocí tzv. “Domácnosti” v Profilu může k jeho údajům umožnit přístup i dalším osobám (např. životnímu partnerovi/ partnerce). V sekci “Profil – Moje soukromí – Povolit přístup svému finančnímu poradci, který se bude moci kdykoliv přihlásit za něho a vidět veškerá jeho data v portálu, avšak nebude moci za něj upravovat nebo přidávat obsah.

Kontrolou bylo dále zjištěno, že má Společnost zpracovaný interní předpis „Kontrolní a bezpečnostní opatření pro zpracování dat XXXXX“.
Podle uvedeného předpisu provádí oddělení IT Společnosti pravidelné kontroly základních funkcí technických a programových prostředků, které slouží jako operační infrastruktura pro firemní informační systémy. Zabezpečuje sledování jejich provozuschopnosti a aktualizaci především s ohledem na odstraňování bezpečnostních chyb v operačních systémech. Vedoucí

oddělení IT je povinen zajistit maximální dosažitelnou bezpečnost, v podmínkách Společnosti informačních systémů a chránit je před neoprávněným přístupem, zásahem či útokem, a to jak interním, tak externím. Za tím účelem aplikuje Společnost technologické prostředky ochrany, jako jsou firewally, sledování abnormalit v síťovém provozu, důsledné vyžadování přihlašovacích údajů, implementaci antivirové ochrany apod.

Kontrolou bylo dále zjištěno, že výše uvedený předpis upravuje postupy Společnosti, kterými je zajišťováno elektronické zpracování informací. Jedná se o popis technických a softwarových požadavků na zabezpečení osobních údajů, popis jednotlivých povinností subjektů při práci s technologickým zařízením, včetně popisu přístupů k jednotlivým informačním systémům Společnosti (XXXXXXXXXXx, XXXXX a XXXXXXXXXXX). Poštovní server je hostován u společnosti XXXXXXX. Veškerá správa poštovního serveru, včetně správy hesel je zcela v kompetenci IT Společnosti. Společnost má nastaven systém delegování pravomocí systémových správců serveru tak, aby nebyla všechna práva soustředěna u jedné osoby.
Dále bylo zjištěno, že síťové infrastruktury poradenských sítí jsou nezávislé a zcela mimo přímý vliv centrály Společnosti. Centrála Společnosti ovlivňuje bezpečnostní pravidla využívání technických prostředků sítě stanovením práv a povinností poradců Společnosti a technickým nastavením příslušných oprávnění. Konkrétní pravidla jsou vynucována technickými prostředky ([redacted]
Poradce Společnosti nemá žádná zvláštní přístupová práva k prostředkům sítě Společnosti a připojení k Internetu přes vnitřní síť. Přístup poradce je omezen pouze na datové zdroje, které potřebuje ke své práci. To jsou především služby webových aplikací XXXXXXXXXXX, XXXX, XXXXXXXXXXX, XXXXXXXXXX, XXXXXXXXX, XXXXXXXXXXX a XXXXXXXXXXXX. Tyto aplikace jsou přístupné odkudkoliv z prostředí Internetu. XXXXXXXXX má i režim pro práci off-line, ale v okamžiku, kdy má dostupnou síť, provede synchronizaci dat s databázemi Společnosti.
Každý vedoucí zaměstnanec Společnosti je povinen provádět průběžně kontrolu rozsahu přístupových práv jemu podřízených zaměstnanců. Kontrolu lze provádět dotazem na oddělení IT, které je povinno bezodkladně vyhotovit autorizovaný výpis všech přístupových práv u dané osoby v rámci firemní infrastruktury. Pokud má zaměstnanec přístupová práva i k systémům mimo Společnost, je to na odpovědnosti přímého vedoucího zaměstnance.
Technické prostředky Společnosti jsou zabezpečeny především heslem. Některé mobilní prostředky (notebooky) umožňují i jinou ochranu, kterou mají zabudovánu v podobě kombinace hardwarových a softwarových prostředků. Pokud je zařízení vybaveno prostředky pro biometrické přihlašování, doporučuje se je plně využívat. Je nepřípustné, aby počítače poradců byly přístupné bez úvodního přihlášení do operačního systému.
V příloze interního předpisu „Kontrolní a bezpečnostní opatření pro zpracování dat XXXX“ je dále uvedeno rozdělení a rozsah přístupových práv, povinnosti zaměstnanců v souvislosti s využíváním výpočetní techniky Společnosti.

Kontrolou bylo zjištěno, že má Společnost zpracovaný dokument „Ochrana osobních údajů XXXX“. Dokument obsahuje základní pojmy z Nařízení EU, zásady zpracování osobních údajů, povinnosti odpovědných osob při zpracování osobních údajů, práva subjektů údajů podle Nařízení EU, organizační a technická zabezpečení s odkazem na interní dokument „Kontrolní a bezpečnostní opatření pro zpracování dat XXXX“, dále povinnosti zaměstnanců a poradců Společnosti, odkaz na pověřence pro ochranu osobních údajů.

Společnost má uzavřenou Smlouvu o poskytování služeb XXXXXX se společností XXXXXXXXXXXXXXXXX, ze dne 26. listopadu 2015, jejímž předmětem je poskytování služby „Úschova soukromého klíče“ pro Společnost a definování vzájemných povinností při poskytování této služby. V dokumentu zpracovaného společností XXXXXXXXXXXXXXXXXXx. „Úschova soukromého klíče“, jsou uvedeny zásady a postupy při vytvoření a úschově soukromého klíče, bezpečnostní politika úschovy soukromého klíče určeného k dešifrování. Úschova soukromého klíče musí zohlednit tyto bezpečnostní požadavky: důvěryhodné vytvoření klíčového páru – odpovídající algoritmus a délka klíče, způsob vytvoření, získání a vystavení certifikátu veřejného klíče, bezpečné uložení soukromého klíče zajišťující jeho důvěryhodnost a požadovanou dostupnost, bezpečnost manipulaci se soukromým klíčem, protokolování každého kroku a pravidelnou kontrolu funkčnosti uchovávaného klíče.
Společnost XXXXXXXXXXXXXX provádí pouze úschovu soukromého klíče k šifrování a dešifrování údajů Společnosti, sama dokumenty s osobními údaji a DBP klientů Společnosti nezpracovává ani neuchovává.
Proces vytvoření a úschovy klíčů ve společnosti XXXXXXXXXXXXXXXXXX je vždy iniciován zástupcem zákazníka, který předem kontaktuje společnost XXXXXXXXXXXXXXXX. Proces musí probíhat důvěryhodným způsobem, tj. v průběhu vytváření klíčového páru, vytváření médií k úschově a rušení klíčů z personálního počítače, na kterém byly vytvořeny a musí být dodrženo pravidlo „čtyř očí“. Plnou odpovědnost za zadání autentizačních dat a hlesla nese zástupce zákazníka. Kontrolu plné moci zákazníka a další úkony provede společnost XXXXXXXXXXXXXXXXXXXX, která tak provádí po celou dobu při vytvoření a úschovy klíče kontrolu spolu se zástupcem zákazníka. Operační systém je nahrán za přítomnosti zákazníka do jeho počítače. Zástupce zákazníka může nahraný systém zkontrolovat.

Kontrolní zjištění č. I.

Podle čl. 4 bodu. 1 Nařízení EU se osobním údaje rozumí *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.*

Společnost jako zprostředkovatel finančních služeb shromažďuje osobní údaje za účelem uzavírání smluv v níže uvedených kategoriích a rozsahu:

a) Identifikační údaje (jméno a příjmení, rodné příjmení, rodné číslo, datum narození, místo a země narození, národnost, informace týkající se průkazu totožnosti).
b) Kontaktní údaje (např. trvalá adresa, korespondenční adresa, telefonní čísla, e-mail).
c) Údaje o stavu, rodině, zaměstnání (např. rodinný stav, děti, jiné závislé osoby, vzdělání, údaje o zaměstnání, PEP).
d) Elektronické údaje (např. IP adresy, časy připojení, vygenerovaná a zaslaná hesla, grafická podoba podpisu, cookies).
e) Finanční údaje (např. příjmy, hotovost, výdaje, číslo bankovního účtu, údaje o majetku, údaje o jiných smlouvách na finanční produkty, plány do budoucna, aktuální životní situace, investiční dotazník atd.
f) Odvozené údaje (např. jméno poradce, navržené řešení, ID klienta).

g) Zvláštní kategorie osobních údajů (údaje o zdravotním stavu a zašifrovaná biometrická data, tedy DBP).

Podle výše uvedených údajů lze fyzickou osobu přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor. Jedná se tedy o osobní údaje ve smyslu čl. 4 odst. 1 Nařízení EU.

Podle čl. 4 bodu 14 se Nařízení EU se biometrickými údaji rozumí osobní údaje vyplývající z konkrétního zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.
Podpis smlouvy, která je uzavírána v elektronické formě, kdy prostřednictvím elektronického zařízení dochází k zachycení a následnému uchování jednotlivých znaků podpisu, např. rychlost, tlak, dynamika pohybu pera, resp. pohybu ruky, je biometrickým údajem ve smyslu čl. 4 bodu 14 Nařízení EU.

Podle čl. 4 bodu 2 Nařízení EU se zpracováním rozumí *„jakákoliv operace nebo Soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomocí 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.“*
Společnost osobní údaje svých klientů systematicky shromažďuje, ukládá v rámci IT systému, třídí, vyhodnocuje, uchovává, používá a uchovává, a to včetně DBP. Jedná se tedy o zpracování osobních údajů ve smyslu čl. 4 odst. 2 Nařízení EU.

Podle čl. 4 bodu 7 Nařízení EU je *„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.“*
Podle čl. 4 bodu 8 Nařízení EU je zpracovatelem *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.“*

Společnost využívá osobní údaje klienta za účelem podepisování smluvní dokumentace. DBP využívá k vytvoření grafické podoby podpisu na dokumentech. Společnost zpracovává osobní údaje, včetně DBP za účelem zprostředkování nabízení finančních služeb tím, že shromážděné osobní údaje vyhodnocuje za účelem zprostředkování nejvýhodnější formy finančních služeb.
Společnost tedy zpracovává osobní údaje za účelem shromáždění a vyhodnocení osobních údajů klientů a je tedy ve smyslu čl. 4 bodu 7 Nařízení EU správcem osobních údajů, neboť určila účel i prostředky zpracování osobních údajů, přičemž k uzavření smlouvy o zajištění služeb využívá i DBP.
Současně Společnost shromažďuje a zpracovává osobní údaje v rozsahu a způsobem podle pokynů jednotlivých Společností, pro které zajišťuje zprostředkovávané poptávané finanční služby. Společnost je tedy současně zpracovatelem osobních údajů ve smyslu článku 4 bodu 8 Nařízení EU.

Kontrolní zjištění č. 2

Jsou-li biometrické údaje zpracovávány za účelem jedinečné identifikace fyzické osoby, jako je tomu v případě Společnosti, jedná se o zpracování zvláštní kategorie osobních údajů dle čl. 9 odst. 1 nařízení (EU) 2016/679. Zpracování zvláštní kategorie osobních údajů je s ohledem na jejich zvláštní charakter a hrubý zásah do soukromého a osobního života subjektu údajů v případě jejich zneužití obecně zakázáno. Výjimku z obecného zákazu zpracování zvláštní kategorie osobních údajů pak představuje splnění alespoň jednoho z taxativně vyčtených právních důvodů obsažených v čl. 9 odst. 2 písm. a) až j) nařízení (EU) 2016/679. Zároveň je vždy nezbytné mít pro zpracování osobních údajů také obecný právní titul pro zpracování dle čl. 6 odst. 1 nařízení (EU) 2016/679. Právním titulem pro zpracování osobních údajů klientů při poskytování finančních služeb je primárně plnění smlouvy, jejíž smluvní stranou je subjekt údajů dle čl. 6 odst. 1 písm. b) nařízení (EU) 2016/679. Ve vztahu k DBP, jakožto zvláštní kategorie osobních údajů, se pak uplatní právní důvod dle čl. 9 odst. 2 písm. a) ve spojení s čl. 6 odst. 1 písm. b) nařízení (EU) 2016/679. neboť klienti dali výslovný souhlas se zpracováním této zvláštní kategorie osobních údajů pro účely uzavření a uchování smluvní dokumentace též dynamický biometrický podpis klientů. Souhlas se zpracováním konkrétních osobních údajů, resp. v daném případě DBP nezbavuje Společnost povinnosti dodržovat všechny základní zásady zpracování osobních údajů, neboť soulad sledovaného účelu a k němu se vztahujícího minimálního rozsahu osobních údajů je nutno hodnotit objektivně, nikoli subjektivně, (tj. jako možný předmět dohody uzavřené mezi Společností a subjektem údajů). Současně je nezbytné odmítnout vyjádření kontrolované Společnosti o zpracování DBP na základě jiného právního titulu, než je souhlas, protože výslovný souhlas s účely zpracování DBP se vztahuje pouze k tomuto jedinému biometrickému osobnímu údaji, jehož odvolání nemění nic na platnosti uzavřené smlouvy, protože odvolání souhlasu se týká pouze odvolání zpracování biometrických údajů, a ne obsahu smluvního ujednání.

K rozsahu osobních údajů nezbytných pro identifikovatelnost subjektu údajů pro účely smluvního vztahu, jakož i pro plnění dalších povinností vyplývajících z něj pro Společnost, a to bez ohledu na to, zda osobní údaje shromažďuje a zpracovává jako správce, resp. zpracovatel osobních údajů, je zcela dostačující rozsah osobních údajů, které musí Společnost shromažďovat v souvislosti s plněním zákonných požadavků dle zvláštní právní úpravy. Dynamický biometrický podpis klientů není pro účely uzavření a uchování smluvní dokumentace, či zjednodušení tohoto procesu nezbytný, neboť v případě uzavírání smluv v listinné podobě není také vyžadován. Jako dostatečný pro výše uvedené účely je prostý obraz podpisu klienta na dematerializované smluvní dokumentaci, který je srovnatelný s podpisem na smluvní dokumentaci v listinné formě. Tuto nadbytečnost potvrzuje i vyjádření kontrolované Společnosti, ze dne 25. ledna 2019, že „*od počátku smlouvy s I. CA nebyl postup dešifrování použit ve vztahu k žádnému klientovi.*“

Kontrolovaná osoba nedodržela základní zásadu minimalizace údajů stanovenou v čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679 když shromažďovala a následně uchovávala dynamické biometrické podpisy svých klientů.

Kontrolní zjištění č. 3

A. Podle čl. 12 Nařízení EU *„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 článků 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".

Pokud se osobní údaje získávají od subjektu údajů podle čl. 13 odst. 1 písm. a) Nařízení EU, *„poskytne správce v okamžiku získávání osobních údajů subjektu údajů informace podle písm. a) až f) uvedeného ustanovení (totožnost správce nebo jeho zástupce, účel zpracování, včetně informace o oprávněných zájmech, případné příjemce a případného úmyslu o předávání osobních údajů do třetích zemí nebo mezinárodních organizací. Současně je dle čl. 13 odst. 2 poskytne správce subjektu údajů další informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování (dobu uchovávání, existenci práva požadovat od správce přístup k osobním údajům, právu na opravu, výmaz, omezení zpracování, vznést námitku proti zpracování, přenositelnost zpracování, včetně práva podat stížnost u dozorového úřadu)."*

B. O zpracování osobních údajů jsou subjekty údajů informováni bezplatně, transparentním a srozumitelným způsobem prostřednictvím dokumentu „Zásady zpracování osobních údajů" zveřejněného na webových stránkách Společnosti XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, který obsahuje informace o správci osobních údajů, jeho kontaktní údaje, údaje o pověřenci, účel zpracování, plnění právní povinnosti podle o zvláštních zákonů, informace o zpracování zvláštní kategorie osobních údajů (zdravotní a biometrické údaje), rozsah a způsob zpracování osobních údajů, informace o příjemcích, v souvislosti se zpracováním osobních údajů (přístup, oprava výmaz omezení zpracování, informace o možnosti podat námitku, přenositelnost údajů, právo odvolat souhlas se zpracováním osobních údajů, právo podat stížnost u Úřadu a informace o automatickém rozhodování včetně profilování). Jsou zde také jmenovitě uvedeni zpracovatelé Společnosti.

V souvislosti se zapracováním osobních údajů, včetně DBP plní Společnost podmínky uvedené v čl. 12 Nařízení EU a nebylo prokázáno porušení čl. 13 Nařízení (EU), přičemž se doporučuje ve smyslu recitálu bodu 60 Nařízeni (EU) rozšířit informaci poskytovanou klientům o tom, zda je klient DBM povinen pro stanovené účely poskytnout.

Kontrolní zjištění č. 4

A. Podle čl. 15 odst. 1 Nařízení EU, má subjekt údajů *„právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k následujícím informacím:*

- *a) účely zpracování;*
- *b) kategorie dotčených osobních údajů;*
- *c) příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích;*
- *d) plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;*
- *e) existence práva požadovat od správce opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování anebo vznést námitku proti tomuto zpracování;*
- *f) právo podat stížnost u dozorového úřadu;*

g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;

h) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů."

B. Informace k výše uvedeným bodům jsou přístupné na webových stránkách Společnosti XXXXXXXXXXXXXXXXXXXXXXXXxx, v dokumentu „Zásady zpracování osobních údajů" a v interním „Ochrana osobních údajů XXXXX." z května 2018. V dokumentu „Zásady zpracování osobních údajů" jsou subjekty údajů informováni o účelu zpracování, kategoriích osobních údajů, o zvláštní kategorii osobních údajů (zdravotní a biometrické údaje), a době zpracování, příjemcích osobních údajů, o právech subjektů údajů a informace o zpracovatelích.
V dokumentu jsou konkrétně rozvedena tato práva subjektu údajů:
a) právo na přístup k osobním údajům (čl. 15 Nařízení EU),
b) právo na opravu – doplnění (čl. 16 GDPR),
c) právo na výmaz (právo být zapomenut) – (čl. 17 Nařízení EU),
e) právo na omezení zpracování (čl. 18 Nařízení EU),
f) oznamovací povinnost – oprava nebo výmaz (čl. 19 Nařízení EU),
g) právo na přenositelnost osobních údajů (čl. 20 Nařízení EU),
h) právo vznést námitku proti zpracování (čl. 21 Nařízení EU),
ch) automatizované rozhodování, včetně profilování (čl. 22 Nařízení EU),
i) právo podat stížnost u Úřadu (čl. 77 Nařízení EU).

Kontrolující v daném případě konstatují že Společnost plní povinnosti správce osobních údajů v souvislosti s informacemi o právech subjektů údajů. Porušení čl. 15–22 Nařízení EU nebylo kontrolou prokázáno.

Kontrolní zjištění č. 5

A. Čl. 32 odst. 1 Nařízení EU obsahuje toto ustanovení *„S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku.*

B. Společnost má zpracovány vnitřní předpisy a další dokumenty, které upravují postupy při zpracování, zabezpečení a ochraně osobních údajů, včetně DBP.
Jedná se o interní předpis „Kontrolní a bezpečnostní opatření pro zpracování dat XXXX", ve kterém je upravena pravidelná kontrola základních funkcí technických a programových prostředků, které slouží jako operační infrastruktura pro informační systémy Společnosti. Dále tento předpis upravuje sledování jejich provozuschopnosti systémů a jejich aktualizaci především s ohledem na odstraňování bezpečnostních chyb v operačních systémech. Vedoucí oddělení IT je povinen zajistit maximální dosažitelnou bezpečnost informačních systémů a chránit je před neoprávněným vstupem, zásahem či útokem, a to jak interním, tak externím. Za tím účelem aplikuje technologické prostředky ochrany, jako jsou firewally, sledování abnormalit v síťovém provozu, důsledné vyžadování přihlašovacích údajů, implementaci antivirové ochrany apod.

Kontrolou bylo zjištěno, že výše uvedený předpis upravuje postupy Společnosti, které zajišťují elektronické zpracování informací. Jedná se o popis technických a softwarových požadavků na zabezpečení osobních údajů, popis jednotlivých povinností subjektů při práci s technologickým zařízením, včetně popisu přístupů k jednotlivým informačním systémům Společnosti (XXXXXXX, XXXXXXXX a XXXXXXXXXX). Poštovní server, který je hostován u společnosti XXXXXXXXXX. Veškerá správa poštovního serveru, včetně správy hesel je zcela v kompetenci IT Společnosti. Společnost má nastaven systém delegování pravomocí systémových správců serveru tak, aby nebyla všechna práva soustředěna u jedné osoby.
Dále bylo zjištěno, že síťové infrastruktury poradenských sítí jsou nezávislé a zcela mimo přímý vliv centrály Společnosti. Centrála ovlivňuje bezpečnostní pravidla využívání technických prostředků sítě stanovením práv a povinností poradců Společnosti a technickým nastavením příslušných oprávnění. Konkrétní pravidla jsou vynucována technickými prostředky ([redacted]).
Poradce Společnosti nemá implicitně žádná přístupová práva k prostředkům sítě Společnosti a připojení k Internetu přes vnitřní síť.
Serverové části infrastruktury jsou ošetřeny v interní, bezpečnostní směrnicí, kdy o hardware a data se stará interní a vymezená obsluha. Elektronické dokumenty jsou uloženy v elektronickém archivu, kde je dokumentovaný přístup. Existuje plán záloh, který dostatečně zajišťuje možnost obnovy v takovém čase, kdy je minimální riziko s dopadem na práva a svobody fyzických osob z hlediska dostupnosti (plnění ze smlouvy apod.).
DBP je zpracován tak, že údaje (biometrika podpisu) jsou připojeny k elektronickému dokumentu takovým způsobem, že je eliminováno riziko neoprávněného zpracování [redacted]

Kontrolující v daném případě konstatují, že Společnost má technická a organizační opatření k zabezpečení osobních údajů. Kontrolou nebylo prokázáno porušení čl. 32 odst. 1 Nařízení EU.

Kontrolní zjištění č. 6

A. Podle čl. 32 odst. 2 Nařízení EU *„správce osobních údajů 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.“*

B. Společnost má zpracovaná rizika při zpracování osobních údajů, včetně DBP v příloze č. 2 dopisu ze dne 25. ledna 2019 (č.j. UOOU-09654/18-8).
Analýza obsahuje popis rizik při zpracování osobních údajů včetně DBP, stupně rizik a jejich hodnocení: a) vysoce rizikové, b) zpracování s rizikem, c) ostatní zpracování.
DBP je zpracován tak, že údaje (biometrika podpisu) jsou připojeny k elektronickému dokumentu takovým způsobem, že je eliminováno riziko neoprávněného zpracování [redacted]

Kontrolující v daném případě konstatují, že má Společnost určena rizika v souvislosti se zpracováním osobních údajů. Provedenou kontrolou nabylo prokázáno porušení čl. 32 odst. 2 Nařízení EU.

Kontrolní zjištění č. 7

A. Podle čl. 32 odst. 4 Nařízení EU *„správce a zpracovatel přijmou opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu".*

B. Dokumenty jsou mezi informačními systémy předávány pomocí zabezpečených protokolů, kdy informační systémy jsou připravené omezit seznam uživatelů s přístupem ke konkrétním obchodním případům, tedy k datům obsahujícím osobní údaje konkrétních, identifikovaných fyzických osob. Přístup k osobním údajům je přidělen pouze oprávněným osobám. O schválení přístupu rozhoduje vždy člen představenstva Společnosti. Systém přístupu je pravidelně vyhodnocován a probíhá periodická kontrola autenticity a integrity uchovávaných dat. Jednou za rok probíhá ověření dostupnosti dokumentů a ověření zabezpečení biometrických dat. HW a SW infrastruktura zajišťuje minimální ztrátu dat v případě havárie. Dokumenty obsahující [redacted].

Přístup k dokumentům s DBP má:

Uživatel – který je poradce nebo manažer v poradenské struktuře Společnosti.

Klient – má právo na zpřístupnění dokumentů, které sám podepsal DBP.

Obchodní partner vstupuje do systémů Společnosti přes rozhraní XXXXXXXX nebo za využití jiného rozhraní určeného pro tento účel. Předání biometricky podepsaných dokumentů obchodnímu partnerovi je možné výhradně způsobem k tomu určeným za dodržení bezpečnosti přenášených dat.

Zaměstnanec a spolupracovník Společnosti má přístup do systémů spravujících dokumenty obsahující dynamické biometrické podpisy pouze s uděleným oprávněním

Zaměstnanci oddělení vývoje IT a SW.

Společnost má nastaven systém delegování pravomocí systémových správců serveru tak, aby nebyla všechna práva soustředěna u jedné osoby.

Každý vedoucí zaměstnanec Společnosti je povinen provádět průběžně kontrolu rozsahu přístupových práv jemu podřízených zaměstnanců. Kontrolu lze provádět dotazem na oddělení IT, které je povinno bezodkladně vyhotovit autorizovaný výpis všech přístupových práv (logování) u dané osoby v rámci firemní infrastruktury.

[redacted]

Poradce Společnosti nemá implicitně žádná přístupová práva k prostředkům sítě Společnosti a připojení k Internetu přes vnitřní síť.

Kontrolující v daném případě konstatují, že v souvislosti se zpracováním osobních údajů, včetně DBP, nebylo prokázáno porušení čl. 32 odst. 4 Nařízení EU.

Poučení o opravném prostředku:
Proti kontrolnímu zjištění uvedenému v protokolu o kontrole může kontrolovaná osoba podat Úřadu pro ochranu osobních údajů ve lhůtě 15 dnů ode dne doručení protokolu o kontrole námitky.

Námitky se podávají písemně a 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:

otisk
úředního
razítka

MVDr. František Bartoš	inspektor Úřadu	
…….	……	……..
jméno	funkce	podpis
		(dokument podepsán elektronicky)

	pověřený	
JUDr. Michal Jelínek	zaměstnanec Úřadu	
…….	……..	……..
jméno	funkce	podpis
		(dokument podepsán elektronicky)

	pověřený	
Ing. Max Gůt	zaměstnanec Úřadu	
…….	…….	……..
jméno	funkce	podpis
		(dokument podepsán elektronicky)