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-03219/20-28
Praha 2. listopadu 2021

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 (obecné nařízení o ochraně osobních údajů), [dále jen „nařízení (EU) 2016/679“] ve spojení s § 50 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů (dále jen „zákon č. 110/2019 Sb.“).

Kontrolující:
Mgr. Eva Cupáková – pověřená zaměstnankyně Úřadu, č. průkazu: [redacted], jako vedoucí kontrolní skupiny na základě pověření ke kontrole ze 13. srpna 2020;

Mgr. Marek Šnajdr – pověřený zaměstnanec Úřadu, č. průkazu: [redacted], na základě pověření ke kontrole ze 13. srpna 2020;

Josef Polák – pověřený zaměstnanec Úřadu, č. průkazu: [redacted], na základě pověření ke kontrole ze 13. srpna 2020, které bylo ukončeno 31. srpna 2021;

Mgr. Barbora Šnajderová, pověřená zaměstnankyně Úřadu, č. průkazu: [redacted], na základě pověření ke kontrole ze 13. srpna 2020;
(dále jen „kontrolující“).

Kontrolovaná osoba:
[redacted] (dále jen „kontrolovaná osoba“).

Místo provedení kontroly:
- sídlo Úřadu
- provozovna kontrolované osoby – [redacted]
- provozovna kontrolované osoby – [redacted]
- sídlo kontrolované osoby

Předmět kontroly:
Předmětem kontroly je dodržování povinností stanovených nařízením (EU) 2016/679 v souvislosti se zpracováním osobních údajů při uzavírání pojištění odpovědnosti za újmu způsobenou provozem vozidla (dále jen „povinného ručení“), a to především se zaměřením na zpracování osobních údajů spolupracujícími osobami (např. zprostředkovateli, kteří uzavírají pojistné smlouvy), plnění informační povinnosti, doložení pokynů pro zpracování a zabezpečení osobních údajů dle nařízení (EU) 2016/679.

První kontrolní úkon:
Doručení *Oznámení o zahájení kontroly* kontrolované osobě 31. srpna 2020.

Poslední kontrolní úkon:
Kontrola podkladů doložených kontrolovanou osobou v rámci *Vyjádření kontrolované osoby k protokolu z ústního jednání a místního šetření* z 25. června 2021, čj. UOOU-3219/20-26.

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

1. *Kontrolní plán pro rok 2020*, čj. UOOU-03219/20-1, počet listů 1;
2. *Pověření ke kontrole* z 13. srpna 2020, čj. UOOU-03219/20-2, počet listů 1;
3. *Oznámení o zahájení kontroly* z 28. srpna 2020, čj. UOOU-03219/20-3, doručené kontrolované osobě 31. srpna 2020 počet listů 2;
4. *Potvrzení přijetí oznámení o zahájení kontroly* z 2. září 2020, čj. UOOU-03219/20-4, počet listů 1;
5. *Úřední záznam* ze 8. září 2020, čj. UOOU-03219/20-5, počet listů 1;
   5.1. Výtisk webové stránky (dokumentu) Informace o zpracování osobních údajů z 8. září 2020, počet listů 24;
6. *Vyjádření kontrolované osoby k žádosti o poskytnutí součinnosti* z 10. září 2021, čj. UOOU-03219/20-6, počet listů 10;
   6.1. *Politika ochrany osobních údajů* [redacted], počet listů 4;
   6.2. *Směrnice o ochraně osobních údajů* [redacted], počet listů 13;
   6.3. *Oznámení pověřence pro ochranu osobních údajů*, počet listů 1;
   6.4. Vzorová smlouva o obchodním zastoupení, počet listů 7;
   6.5. *Vnější metodický pokyn* [redacted], počet listů 4;
   6.6. *Metodický pokyn* [redacted], počet listů 10;
   6.7. *Metodický pokyn* [redacted], počet listů 7;
   6.8. *Metodický pokyn* [redacted] *příloha č. 5*, počet listů 2;
   6.9. *Záznamy o činnostech zpracování*, počet listů 5;
   6.10. *Základní pokyny pro pojišťovací zprostředkovatele*, počet listů 3;
   6.11. Záznam obrazovky sjednávací nástroj [redacted], počet listů 1;
   6.12. Vzor pojistné smlouvy, počet listů 2;

6.13. *Posouzení oprávněného zájmu – zpracování OÚ zájemců o pojištění*, počet listů 5;
6.14. *Posouzení oprávněného zájmu – zpracování OÚ pojistníků*, počet listů 5;
6.15. *Posouzení oprávněného zájmu – zpracování OÚ pojištěných osob*, počet listů 6;
6.16. *Informace o zpracování OÚ v pojištění vozidel*, počet listů 4;
6.17. *Směrnice bezpečnostní požadavky na informační systémy*, počet listů 20;
6.18. , počet listů 1;
6.19. *Metodický pokyn* , počet listů 3;
6.20. *Informace o roli PZ při zpracování OÚ*, počet listů 2;
6.21. *Pokyny ke zpracování osobních údajů*, počet listů 2;

7. *Úřední záznam* z 11. září 2020, čj. UOOU-03219/20-7, počet listů 1;
7.1. Výtisk webové stránky (dokumentu) informace o zpracování osobních údajů, počet listů 24;
7.2. Uložené cookies bez souhlasu, počet listů 1;
7.3. Uložené soubory cookies po souhlasu, počet listů 1;

8. *Úřední záznam – analýza dodaných smluv* z 1. října 2020, čj. UOOU-03219/20-8, počet listů 1;

9. *Protokol z ústního jednání a místního šetření* z 6. října 2020, čj. UOOU-03219/20-9, počet listů 3;
9.1. *Směrnice* , počet listů 20;
9.2. *Směrnice* , počet listů 6;
9.3. *Směrnice* , počet listů 13;
9.4. *Metodický pokyn* , počet listů 11;
9.5. *Vnější metodický pokyn* , počet listů 18;
9.6. *Interní sdělení* , počet listů 2;
9.7. *Interní sdělení* , počet listů 2;
9.8. *Interní sdělení* , počet listů 2;
9.9. *Interní sdělení* , počet listů 3;
9.10. *Vnější metodický pokyn* , počet listů 3;
9.11. *Informace GDPR*, počet listů 3;
9.12. *Pokyny k návrhu pojistné smlouvy*, počet listů 5;
9.13. *Informace o zpracování osobních údajů v pojištění vozidel*, počet listů 3;
9.14. *Informace přepážkové služby* , počet listů 2;
9.15. *Oznámení o změně osobních údajů klienta*, počet listů 1;
9.16. *Certifikát o úspěšném absolvování školení*, počet listů 1;
9.17. Snímek obrazovky - oznámení o změně osobních údajů klienta, počet listů 2;
9.18. Snímek obrazovky - informace klient, počet listů 1;
9.19. Snímek obrazovky - , počet listů 2;

10. *Vyjádření kontrolované osoby k protokolu z ústního jednání a místního šetření* z 19. října 2020, čj. UOOU-03219/20-10, počet listů 4;
10.1. Vzor prohlášení zaměstnance, počet listů 1;
10.2. *Pracovní řád* , počet listů 12;
10.3. Záznam týdenního souhrnu interní komunikace, počet listů 1;
10.4. Záznam obrazovky s upozorněním na nové vnitřní předpisy, počet listů 1;
10.5. *Protokol o výsledku kontroly*, počet listů 1;
10.6. Záznam obrazovky se záznamy o absolvování e-learningových kurzů, počet listů 1;
10.7. Záznam komunikace pověřence o sjednání nápravy, počet listů 1;

10.8. Prezenční listina ze školení [redacted], počet listů 1;
10.9. Seznam zaměstnanců účastnících se školení [redacted], počet listů 1;
10.10. Vzor pracovní smlouvy, počet listů 1;

11. *Žádost o součinnost* z 20. října 2020, čj. UOOU-3219/20-11, počet listů 1;
12. *Odpověď na žádost o součinnost* z 23. října 2020, čj. UOOU-03219/20-12, počet listů 1;
    12.1. *Seznam pojišťovacích zprostředkovatelů včetně spolupracujících osob v povinném ručení*, počet listů 12;
13. *Protokol z ústního jednání a místního šetření* z 15. prosince 2020, čj. UOOU-03219/20-15, počet listů 5;
    13.1. Snímek obrazovky – interní systém (formulář), počet listů 2;
    13.2. Snímek obrazovky – interní systém (souhlas s marketingem), počet listů 1;
    13.3. Snímek obrazovky – interní systém (vysvětlivky k údajům povinné osoby), počet listů 1;
14. *Sdělení povinné osoby*, čj. UOOU-03219/20-16, počet listů 1;
    14.1. *Smlouva o výhradním obchodním zastoupení*, počet listů 8;
15. *Sdělení povinné osoby*, čj. UOOU-03219/20-17, počet listů 1;
    15.1. *Záznamy o činnostech zpracování v pozici zpracovatele*, počet listů 1;
16. *Úřední záznam* z 10. února 2021 – analýza *Smlouvy o výhradním obchodním zastoupení* [redacted], čj. UOOU-03219/20-18, počet listů 2;
17. *Úřední záznam* ze 7. května 2021 – pořízení dokumentace o signpadech[1], čj. UOOU-03219/20-19, počet listů 1;
    17.1. Výtisk webové stránky (dokumentu) [redacted], počet listů 2;
    17.2. Výtisk webové stránky (dokumentu) *LCD* [redacted] *tablet* [redacted], počet listů 1;
    17.3. Výtisk webové stránky (dokumentu) [redacted], počet listů 1;
18. *Žádost o součinnost* ze 7. května 2021, čj. UOOU-03219/20-20, počet listů 1;
19. *Vyjádření kontrolované osoby k žádosti o součinnost* z 12. května 2021, čj. UOOU-03219/20-21, počet listů 7;
    19.1. *Postup uzavření pojistné smlouvy s využitím* [redacted], počet listů 2;
    19.2. *Schéma procesu vlastnoručního digitálního podepisování*, počet listů 1;
    19.3. *Informace o zpracování osobních údajů v pojištění vozidel*, počet listů 4;
    19.4. *Posouzení souladu s GDPR a vlivu na ochranu osobních údajů*, počet listů 14;
    19.5. *Minimální rozsah ročního kontrolního plánu agentury pro oblast obchodní činnosti*, počet listů 6;
    19.6. *Zpráva o kontrole plnění povinností dle GDPR pojišťovacím zprostředkovatelem*, počet listů 2;
    19.7. *Zpráva o kontrole plnění povinností dle čl. 28 Nařízení GDPR se zpracovatelem osobních údajů*, počet listů 3;
    19.8. *Přehled soudních řízení*, počet listů 1;
20. *Protokol z ústního jednání a místního šetření* ze 17. června 2021, čj. UOOU-03219/20-24, počet listů 6;

[1] Čtečka digitálních podpisů.

20.1. *Posouzení oprávněného zájmu – zpracování údajů o zdravotním stavu*, počet listů 10;

20.2. *Posouzení oprávněného zájmu – zpracování biometrických údajů*, počet listů 10;

21. *Vyjádření kontrolované osoby k protokolu z ústního jednání a místního šetření* z 25. června 2021, čj. UOOU-03219/20-26, počet listů 9;

21.1. *Směrnice* [redacted] *Archivační a skartační řád společnosti*, počet listů 27;

21.2. [redacted], počet listů 5;

21.3. E-mail – zpochybnění podpisu, počet listů 1.

22. *Odpověď na Vyjádření kontrolované osoby k protokolu z ústního jednání a místního šetření* z 23. července 2021, č. j. UOOU-03219/20-27, počet listů 1.

Z výše uvedených podkladů jsou pro kontrolní zjištění v protokolu o kontrole výslovně vyhodnoceny ty části, v nichž jsou uvedeny informace se vztahem k předmětu kontroly.

II. Důvod a průběh kontroly:

Kontrola byla zahájena na základě kontrolního plánu Úřadu pro ochranu osobních údajů pro rok 2020 oprávnění vyplývajícího z čl. 58 odst. 1 písm. b) nařízení (EU) 2016/679 ve spojení s § 50 zákona č. 110/2019 Sb.

Kontrolovaná osoba je zapsána v obchodním rejstříku pod spisovou značkou [redacted] s datem vzniku a zápisu [redacted] a jako [redacted] má uvedeny následující předměty podnikání:

1. Pojišťovací činnost a jako její součást činnosti z ní přímo vyplývající ve smyslu § 3, odst. 1, písm. f) zákona č. 277/2009 Sb., o pojišťovnictví, v platném znění (dále jen „zákon č. 277/2009 Sb.")
   - v rozsahu pojistných odvětví životních pojištění uvedených v části A bodech I, II, III, VI, VII a IX přílohy č. 1 k zákonu č. 277/2009 Sb., a dále
   - v rozsahu pojistných odvětví neživotních pojištění uvedených v části B bodu 1 až 18 přílohy č. 1 k zákonu č. 277/2009 Sb.,
2. Zajišťovací činnost ve smyslu § 3, odst. 1, písm. (l) zákona č. 277/2009 Sb. pro všechny typy zajišťovacích činností.

Pověření ke kontrole bylo kontrolujícím uděleno předsedkyní Úřadu 13. srpna 2020. Na základě tohoto pověření byla zahájena kontrola doručením oznámení o zahájení kontroly z 28. srpna 2020. Kontrolovaná osoba 3. září 2020 potvrdila přijetí oznámení o zahájení kontroly. Dne 8. září 2020 byla kontrolujícími provedena kontrola webových stránek kontrolované osoby, zaměřená primárně na plnění informační povinnost vůči subjektům údajů. Kontrolovaná osoba dále 10. září 2020 předložila vyjádření k otázkám položeným kontrolujícími v oznámení o zahájení kontroly a doložila jej přílohami. Dne 1. října 2020 byla provedena analýza doložené vzorové smlouvy o obchodním zastoupení. Kontrolující dále 6. října 2020 provedli ústní jednání a místní šetření v [redacted] pobočce kontrolované osoby. Ta 19. října 2020 předložila doplňující vyjádření s přílohami. Kontrolující si 20. října 2020 vyžádali od kontrolované osoby seznam zprostředkovatelů pojištění, kteří jejím jménem uzavírají smlouvy o povinném ručení, dokument byl doručen 23. října 2020.

Dne 15. prosince 2020 bylo provedeno ústní jednání a místní šetření u náhodně vybraného zprostředkovatele povinného ručení [redacted] [povinná osoba dle § 5 odst. 2 písm. a) zákona č. 255/2012 Sb., o kontrole (kontrolní řád, dále jen „zákon č. 255/2012 Sb.“), v souladu s § 10 odst. 3 zákona č. 255/2012 Sb.]. Zprostředkovatel povinného ručení 22. prosince 2020 doložil další požadované dokumenty. Dne 11. února 2020 byla provedena analýza smlouvy o obchodním zastoupení uzavřená mezi kontrolovanou osobou a zprostředkovatelem povinného ručení. Kontrolující následně 7. května 2021 pořídili dokumentaci týkající se technických specifikací signpadů využívaných kontrolovanou osobou. Ta byla téhož dne požádána o součinnost zejména ve věci využití signpadů, načež 12. května 2021 poskytla své vyjádření. Následně bylo 17. června 2021 v sídle kontrolované osoby uskutečněno ústní jednání a místní šetření, při kterém byly položeny dotazy vztahující se zejména ke zpracování zvláštních kategorií osobních údajů a k právním titulům jednotlivých zpracování. Kontrolovaná osoba se následně 25. června 2021 k ústnímu jednání vyjádřila i písemně.

III. Kontrolní zjištění:

Identifikace zpracování, charakter údajů, postavení kontrolované osoby:

V souvislosti s procesem zákonného pojištění vozidla (předmětem kontroly) uvádí kontrolovaná osoba (mj. k provedení úkolů jí uložených právními předpisy, zejména zákonem č. 277/2009 Sb.) veřejně své postavení prostřednictvím dokumentu *Informace o zpracování osobních údajů v pojištění vozidel* (viz body č. 6.16. a č. 19.3. přehledu podkladů), obsahující popis účelů zpracování osobních údajů. Jednotlivé účely, v souvislosti s předmětem kontroly, jsou kontrolujícími dále specifikovány v části *Zákonnost zpracování*. Z dokumentu je zřejmé, že kontrolovaná osoba zpracovává identifikační a kontaktní údaje, dále údaje o využívání služeb, údaje pro ocenění rizika při vstupu do pojištění a údaje o zdravotním stavu a genetické údaje. Dle vyjádření zprostředkovatele povinného ručení se z jeho strany jedná o zadání jména, příjmení, rodného čísla, titulu, bydliště a údajů z „velkého“ technického průkazu vozidla klienta do [redacted] (viz bod. č. 13, str. 2 přehledu podkladů, dále ověřeno dle bodu 13.1. přehledu podkladů).

Prostředky zpracování jsou uvedeny v *Metodickém pokynu* [redacted] (viz bod 6.19. přehledu podkladů). Je zde vymezeno využívání tzv. *nástroje získatele* (dále jen [redacted], tedy využití elektronických zařízení a programového vybavení určeného pro administraci sjednávaných pojistek (nezbytných pro činnost zprostředkovatelů pojištění).

V rámci uvedeného nástroje je pak využíván [redacted]. Zprostředkovatel pojištění v rámci [redacted] vygeneruje záznam z jednání a návrh pojistné smlouvy, která obsahuje osobní údaje klienta zaznamenané do nástroje [redacted]. Pro podpis těchto dokumentů elektronicky je využíváno čtečky digitálních podpisů (zaznamenává a ukládá do interního systému kontrolované osoby osobní údaje spojené s konkrétním podpisem), v případě vyhotovení fyzických kopií jsou tyto vytištěny tiskárnou (na pobočkách se jedná o vybavení kontrolované osoby, zprostředkovatel využívá přenosnou tiskárnu, viz bod č. 6.10. přehledu podkladů, str. 2-3).

Vztah se zprostředkovateli pojištění (včetně povinného ručení) je nastaven skrze *Smlouvu o obchodním zastoupení* (viz bod č. 14.1. přehledu podkladů). Dle [redacted] zprostředkovatel pojištění zpracovává osobní údaje v pozici zpracovatele a v souladu s odstavcem 5. zpracovává osobní údaje výlučně na základě pokynů kontrolované osoby. Zpracovává osobní údaje zájemců o pojištění, pojištěných, pojistníků, obmyšlených osob a rodinných příslušníků pojištěných, a to pro účely:

a) předkládání nabídek pojistných smluv, provádění přípravných prací směřujících k uzavření pojistné smlouvy a uzavírání pojistných smluv se zájemci jménem a na účet pojišťovny,
b) zajišťování klientského servisu ve vztahu k pojistným smlouvám uzavřeným prostřednictvím obchodního zástupce, resp. jiným pojistným smlouvám, které budou obchodnímu zástupci přiděleny do stálé péče nebo
c) pomoci při uplatňování práv z pojištění.

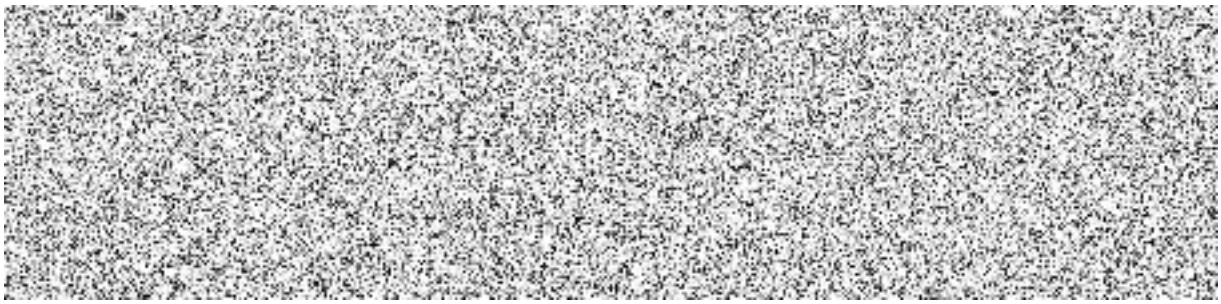
Obsah smluv mezi kontrolovanou osobou a zprostředkovateli povinného ručení z hlediska plnění požadavků na zpracovatelskou smlouvu dle čl. 28 odst. 3 nařízení (EU) 2016/679 je předmětem části [redacted].

Kontrolující konstatují, že ve vztahu k předmětu kontroly je kontrolovaná osoba v postavení správce podle čl. 4 bod 7 nařízení (EU) 2016/679, zpracovává osobní údaje ve smyslu čl. 4 bod 1, 2 nařízení (EU) 2016/679 a zprostředkovatel povinného ručení je pak zpracovatelem podle čl. 4 bod 8 nařízení (EU) 2016/679, neboť zpracovává osobní údaje pro správce (kontrolovanou osobu).

Zákonnost zpracování

K právním titulům zpracování kontrolovaná osoba uvedla (viz bod č. 6, str. 9-10 přehledu podkladů), že zpracování osobních údajů zájemce o pojištění, pojistníka a dále vlastníka a provozovatele vozidla, pokud se liší od pojistníka, a pojištěných osob je nezbytné:

[redacted]



Ke zpracování osobních údajů zájemců o pojištění dochází na základě žádosti (aktivního jednání) subjektu údajů, který projeví zájem o uzavření pojistné smlouvy. Dále kontrolovaná osoba uvedla, že tímto zpracováním chrání svoji činnost a rizika s provozováním pojištění. Uvádí, že její postup je při tom v souladu s platnou legislativou[2]. Zájemci o pojištění, pojistníci i pojištěné osoby jsou o účelech zpracování informováni prostřednictvím informací uvedených v předsmluvní dokumentaci a také prostřednictvím informačních memorand. Kontrolovaná osoba též dle vlastního vyjádření umožňuje subjektům údajů výkon jejich práv (viz *Práva subjektů údajů*). Dle tvrzení kontrolované osoby při tom dochází pouze ke zpracování, které může subjekt údajů očekávat.

Kontrolovaná osoba ve svém vyjádření (viz bod 6. přehledu podkladů, [redacted] uvádí, že na základě oprávněných zájmů zpracovává osobní údaje za účelem prevence a odhalování pojistných podvodů a jiných protiprávních jednání, kdy odkazuje na [redacted] téhož vyjádření. V uvedeném bodu je dále odkaz na část záznamů o činnostech zpracování pod [redacted]. V dané části záznamů o činnostech zpracování je uvedeno, že účelem tohoto zpracování je vyšetřování a prevence podvodů, příprava statistik o pojistných podvodech, prověřování rizikovosti smlouvy, scoring a tvorba vstupních dat pro prevenci a odhalování pojistných podvodů. Kontrolovaná osoba ve svém vyjádření (viz bod 6. přehledu podkladů, bod 23.) uvádí, že záznamy o činnostech zpracování (rovněž v této definované části) obsahuje aspekty zpracování pro všechny druhy pojištění, tj. i pro neživotní a životní pojištění.

K danému zpracování byly předloženy celkem 3 (tři) posouzení oprávněného zájmu [jedná se o tři dokumenty (balanční testy) - viz body 6.13. – 6.15. přehledu podkladů]: a) zpracování osobních údajů zájemců o pojištění, b) zpracování osobních údajů pojistníků, c) zpracování osobních údajů pojištěných osob.

Kontrolující však obsah těchto balančních testů v rámci kontroly neposuzovali, neboť zpracování osobních údajů v rámci zákonného pojištění reálně probíhá na základě právního titulu plnění právní povinnosti dle čl. 6 odst. 1 písm. c) nařízení (EU) 2016/679. Pro posouzení zákonnosti zpracování tedy tyto dokumenty nejsou relevantní.

[2] Vzhledem k legitimitě účelů zpracování se jedná především o § 6 odst. 5 (Pojišťovna a zajišťovna při provozování pojišťovací nebo zajišťovací činnosti zpracovává osobní údaje včetně rodných čísel; takové zpracování osobních údajů se považuje za zpracování nezbytné pro dodržení právní povinnosti správce podle zákona upravujícího ochranu osobních údajů.), § 127 odst. 1 (Členové statutárního a kontrolního orgánu a zaměstnanci pojišťovny a zajišťovny, likvidátor, správce a jeho zástupce podle § 100, jakož i osoby činné pro pojišťovnu nebo zajišťovnu zachovávají mlčenlivost o skutečnostech týkajících se pojištění fyzických a právnických osob. Povinnost zachovávat mlčenlivost mají tyto osoby i po skončení pracovního nebo jiného než pracovního poměru.) a § 129b odst. 1 (Za účelem prevence a odhalování pojistného podvodu a dalšího protiprávního jednání se pojišťovny vzájemně informují a sdílejí informace o skutečnostech týkajících se pojištění fyzických a právnických osob a jeho zprostředkování, včetně informací o zmocněncích účastníků pojištění a dalších osobách zúčastněných na škodné nebo pojistné události, a to i prostřednictvím právnické osoby, která není pojišťovnou, zajišťovnou ani pojišťovacím zprostředkovatelem.) zákona č. 277/2009 Sb.

Kontrolující se zabývali otázkou legálního právního titulu pro zpracování osobních údajů v rámci pojištění odpovědnosti z provozu vozidla, a to především z důvodu specifičnosti takového zpracování. Předem je třeba konstatovat, že pojištění odpovědnosti z provozu motorového vozidla upravuje zákon č. 168/1999 Sb. o pojištění odpovědnosti za újmu způsobenou provozem vozidla a o změně některých souvisejících zákonů (dále jen „zákon č. 168/1999 Sb.“), přičemž tento zákon je v postavení zákona speciálního vůči ustanovením zákona č. 89/2012 Sb., občanský zákoník (dále jen „zákon č. 89/2012 Sb.“), konkrétněji především ustanovení § 2758 a následujících. Toto pojištění je dle § 3 odst. 2 zákona č. 168/1999 Sb. pojištěním povinným, které musí uzavřít každý vlastník tuzemského motorového vozidla nebo řidič vozidla cizozemského, nestanoví-li zákon jinak.

Hlavními účely tohoto pojištění[3] je zabezpečit, aby poškozenému, kterému byla při dopravní nehodě způsobena újma, byla tato újma nahrazena a pomoct viníkovi dopravní nehody, aby mohl využít svého pojištění a nemusel veškerou způsobenou škodu hradit sám.

Zákon č. 168/1999 Sb. stanoví rozsah pojištění tak, že *„Pojištění odpovědnosti se vztahuje na každou osobu, která je povinna nahradit újmu způsobenou provozem vozidla uvedeného v pojistné smlouvě“.* To znamená, že způsobí-li dopravní nehodu osoba odlišná od pojistníka, tj. od osoby, která s pojistitelem pojistnou smlouvu sjednala (zpravidla se jedná o majitele vozidla), tak i na tuto třetí osobu se pojištění vztahuje.

Vzhledem k tomu, že pojištění odpovědnosti z provozu motorového vozidla je zákonné pojištění, které musí uzavřít zákonem stanovené subjekty, je zpracování osobních údajů účastníků smlouvy uzavřené za účelem pojištění odpovědnosti z provozu motorového vozidla a rovněž třetích osob (pojištěný odlišný od pojistníka a poškozený) plně pod dikcí zákonného titulu ve smyslu čl. 6 odst. 1 písm. c) nařízení (EU) 2016/679, je třeba konstatovat, že tento zákonný titul je aplikovatelný na celý rozsah „povinných činností“, vč. likvidací pojistných událostí, s výjimkou přípravy předsmluvní dokumentace, kterou lze podřadit pod zákonný titul plnění smlouvy dle čl. 6. odst. 1 písm. b) nařízení (EU) 2016/679.
Z pohledu zpracování osobních údajů pak může nastat situace, kdy je v rámci pojištění odpovědnosti uzavíráno i jiné připojištění, kdy toto připojištění (mimo zákonnou formulaci tohoto pojištění) je zpracováním mimo zákonnou povinnost, tudíž probíhá na základě zákonného titulu čl. 6 odst. 1 písm. b) nařízení (EU) 2016/679.

Bylo zjištěno, že kontrolovaná sice reálně zpracovává osobní údaje na základě zákonného titulu ve smyslu čl. 6 odst. 1 písm. b) nařízení (EU) 2016/679 pro období před uzavřením smluvního vztahu, čl. 6, odst. 1 písm. c) nařízení (EU) 2016/679 po uzavření smluvního vztahu (jedná se o zákonné zpracování), avšak zákonnost zpracování má v případě pojištění odpovědnosti za újmu způsobenou provozem vozidla špatně nastavenu, kdy dané zpracování zahrnula mylně pod čl. 6 odst. 1 písm. b) a f) nařízení (EU) 2016/679.

Jak je popsáno v části *Plnění zásady minimalizace, přesnosti a omezení uložení, část c) zásada omezení uložení,* kontrolovaná uchovává osobní údaje reálně na základě zákonného titulu čl. 6 odst. 1 písm. c) nařízení (EU) 2016/679, kdy jsou zákonem stanoveny lhůty pro archivaci předmětných dokumentů a dále na základě zákonného titulu podle čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679, kdy je zákonem stanovená lhůta prodloužena o 1 rok. Patnáctiletou

[3] Viz judikát Nejvyššího soudu ČR z 19. července 2012, sp. zn. 25 Cdo 3086/2011.

lhůtu má v interních dokumentech ovšem mylně zařazenu pod zpracování ve smyslu čl. 6 odst. 1 písm. b) nařízení (EU) 2016/679.

Zvláštní kategorie osobních údajů

a) Údaje o zdravotním stavu

Kontrolovaná osoba zpracovává též zvláštní kategorie osobních údajů (viz bod č. 6.13., str. 3 přehledu podkladů). Uvedla k tomu, že u tohoto typu pojištění (povinné ručení) je zpracování zvláštních kategorií osobních údajů (údajů o zdravotním stavu) prováděno až v okamžiku bezprostředně navazujícím na nahlášení možné pojistné události, kdy kontrolovaná osoba zjišťuje, zda újma na zdraví vznikla na základě pojistné události, za účelem prevence a odhalování pojistných podvodů [redacted]. Kontrolovaná osoba deklaruje [redacted], že nedochází ke zpracování, které by nemohl subjekt údajů očekávat.

Šíře zpracovávaných údajů se liší dle rozsahu nároku – újmy na zdraví. Jsou to údaje o tělesném a duševním zdraví, včetně údajů o poskytnutí zdravotních služeb vypovídajících o zdravotním stavu a jsou-li součástí zdravotnické dokumentace, pak i genetické údaje zahrnující zejména predispozice k různým chorobám a onemocněním. Tyto údaje však kontrolovaná osoba zpracovává pouze v případě, že je pojistné plnění vázáno na zjišťování zdravotního stavu (tj. při dopravní nehodě došlo k újmě na zdraví, [redacted]. Kontrolovaná osoba tímto ověřuje, zda pojistná událost způsobila újmu v rozsahu, který uvádí poškozený (ten je jediným subjektem údajů při tomto zpracování). Zpracovávány jsou posudky o zdravotním stavu a zdravotní dokumentaci či lékařské zprávy. Příjemcem údajů mohou být smluvní lékaři pro případ posouzení (ti disponují zpracovatelskou doložkou), Česká asociace pojišťoven, IČ 49624024, se sídlem Milevská 2095/5, 140 00 Praha 4 při sdílení informací dle § 129b odst. 1 zákona č. 277/2007 Sb., ostatní pojišťovny při přímém sdílení informací dle § 129b odst. 1 zákona č. 277/2007 Sb. a Policie ČR, dospěje-li kontrolovaná osoba k závěru, že je dáno podezření ze spáchání trestného činu [redacted].

Toto zpracování je kontrolovanou osobou založeno na čl. 6 odst. 1 písm. b) nařízení (EU) 2016/679 (pro potřebu šetření pojistné události), na čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679 (pro potřebu prevence a odhalování pojistných podvodů a jiného protiprávního jednání, viz bod č. 21, strana 4 přehledu podkladů) a v souvislosti s tím na výjimce dle čl. 9 odst. 2 písm. f) nařízení (EU) 2016/679. Kontrolovaná osoba k danému zpracování předložila *Posouzení oprávněného zájmu zpracování údajů o zdravotním stavu*. Jak je však popsáno výše, vzhledem k tomu, že celé zpracování, a to i řešení pojistných událostí je v reálně v dikci čl. 6 odst. 1 písm. c) a u zvláštní kategorie osobních údajů dále na základě výjimky dle čl. 9 odst. 2 písm. f) nařízení (EU) 2016/679, toto zpracování nepodléhá potřebě vypracování balančního testu.

Kontrolující konstatují, že dochází k nesprávnému internímu stanovení zákonného titulu pro zpracování zvláštní kategorie osobních údajů, jenž neodpovídá reálnému charakteru zpracování. V případě zpracování osobních údajů o zdravotním stavu dle výjimky dle čl. 9 odst. 2 písm. f) nedochází k porušení čl. 6 odst. 1 nařízení (EU) 2016/679, pouze interně je jeden zákonný titul zaměněn za druhý.

b) Biometrické údaje získané využitím signpadů

Kontrolující během ústních jednání a místních šetření u kontrolované osoby 6. října 2020 a u zprostředkovatele povinného ručení 15. prosince 2020 zjistili, že pro podepisování smluv elektronicky je využíváno signpadů [redacted] a [redacted]. Z informačních brožur, které výrobce k tomuto modelu vydal, je zjevné, že tyto zpracovávají biometrické údaje [redacted]

Z textu vzorové smlouvy o povinném ručení, která byla kontrolovanou osobou předložena kontrolujícím [redacted] není zřejmé, že by subjekt údajů uděloval souhlas se zpracováním jeho biometrických dat spojených s elektronickým podpisem předmětné smlouvy dle čl. 6 odst. 1 písm. a) nařízení (EU) 2016/679 v souladu s výjimkou dle čl. 9. Subjekt údajů sice dostává k dispozici (k nahlédnutí) *Informace o zpracování osobních údajů v pojištění vozidel* [redacted], kde je uvedeno zpracování biometrických údajů v rámci elektronického podepsání předmětné smlouvy, nicméně toto zpracování není kontrolovanou osobou v rámci zákonného titulu zpracování nikterak řešeno, ačkoli toto zpracování je možné založit pouze na základě výjimky dle čl. 9 odst. 2 písm. a) nařízení (EU) 2016/679. Ve verzi platné k 10. září 2020 bylo uvedeno [redacted] přehledu podkladů): *„V případě, že podepisujete pojistnou smlouvu nebo jiný dokument prostřednictvím podepisovacího zařízení, zpracováváme také biometrické údaje v tomto podpisu obsažené. Jde například o rychlost, tlak, zrychlení a sklon pera v jednotlivých částech podpisu.“* A dále: *„Ať jste pojistník, pojištěný, nebo jakákoliv jiná osoba podepisující smlouvu nebo jiný dokument prostřednictvím podepisovacího zařízení, zpracováváme biometrické údaje obsažené ve Vašem podpisu také na základě nezbytnosti pro určení, výkon nebo obhajobu právních nároků, a to pro účel:*

- *ochrany našich právních nároků (jinak řečeno pro to, abychom mohli hájit naše právní nároky v soudním, mimosoudním nebo vykonávacím řízení).*

Pro tento účel osobní údaje uchováváme po dobu, po kterou je to nezbytné k realizaci práv a povinností plynoucích ze vzájemného smluvního vztahu (tedy po dobu trvání pojištění) a po dobu trvání promlčecí doby (v délce maximálně 15 let od skončení pojištění) nároků vyplývajících z pojištění nebo s ním souvisejících prodlouženou o další jeden rok s ohledem na ochranu našich právních nároků. V případě zahájení soudního, správního nebo jiného řízení zpracováváme Vaše osobní údaje v nezbytném rozsahu po celou dobu trvání takových řízení.“

Verze aktuální k datu vyhotovení *Vyjádření kontrolované osoby k žádosti o součinnost* (jedná se o datum 12. května 2021, [redacted] obsahuje drobnou odchylku v prvním citovaném odstavci: *„V případě, že podepisujete pojistnou smlouvu nebo jiný dokument prostřednictvím podepisovacího zařízení, zpracováváme také biometrické údaje v tomto podpisu obsažené. Jde například o rychlost, zrychlení a dobu podpisu v jednotlivých částech podpisu.“*

Předložení tohoto dokumentu k prostudování však není souhlasem dle čl. 4 bodu 11) nařízení (EU) 2016/679 a nesplňuje podmínky vyjádření souhlasu popsané v čl. 7 nařízení (EU) 2016/679.

Kontrolovaná osoba ke zpracování biometrických údajů dále uvedla (informace uvedené v následujících odstavcích dostupné z *Vyjádření kontrolované osoby k žádosti o poskytnutí*

součinnosti, [redacted], že do nástroje [redacted] zprostředkovatelé zaznamenávají konkrétní údaje týkající se pojištění a v rámci tohoto procesu seznamují zájemce o pojištění s kalkulací pojistného a dále pak s povinnými předsmluvními informacemi včetně *Informací o zpracování osobních údajů*, které tvoří nedílnou součást pojistné smlouvy. Závěrečnou fázi jednání tvoří rekapitulace jednání, poskytnutí doporučení zprostředkovatelem a případně i vytvoření dokumentu záznamu z jednání a návrhu pojistné smlouvy ve sjednávacím nástroji [redacted]. Pokud zájemce o pojištění souhlasí se všemi podmínkami pojištění, dochází k uzavření pojistné smlouvy (a předání veškeré smluvní dokumentace klientovi). Pojistná smlouva je uzavírána jedním z následujících způsobů:

a) okamžitým zaplacením pojistného s využitím platebního terminálu [redacted], kdy nedochází k podepsání smlouvy, jelikož smlouva je uzavřena zaplacením pojistného;

b) vlastnoručním digitálním podpisem pojistné smlouvy, který je proveden prostřednictvím zařízení, které za tímto účelem zprostředkovatel předloží zájemci o pojištění; nebo

c) vlastnoručním podpisem vytištěné verze pojistné smlouvy zejm. v případě, že klient nechce podepsat smlouvu prostřednictvím zařízení nebo nechce pojistnou smlouvu a související informace zaslat na e-mailovou adresu.

V případě podpisu pojistné smlouvy prostřednictvím zařízení zaškrtne zprostředkovatel pole *„Použít vlastnoruční digitální podpis“* a připojí zařízení pomocí USB ke své pracovní stanici (PC, notebook). Před samotným podpisem je zprostředkovatel nástrojem [redacted] vyzván k ověření e-mailové adresy zájemce o pojištění. V dalším kroku se vygeneruje pojistná smlouva, která je zájemci o pojištění zobrazena na monitoru zprostředkovatele a ke které zájemce připojí svůj vlastnoruční digitální podpis prostřednictvím zařízení. Vlastnoruční digitální podpis je vždy spjat s podepisovanou pojistnou smlouvou, jejíž součástí jsou i podpisová data[5] v zašifrované podobě, a tento dokument je ve formátu PDF uložen v zabezpečeném datovém archivu kontrolované osoby. Pojistná smlouva zabezpečená [redacted] a související informace jsou klientovi zaslány na jeho ověřenou e-mailovou adresu, včetně odkazu na zabezpečené úložiště, kde si klient může stáhnout, po zadání přístupového kódu z SMS, dokument se zašifrovanými podpisovými daty.

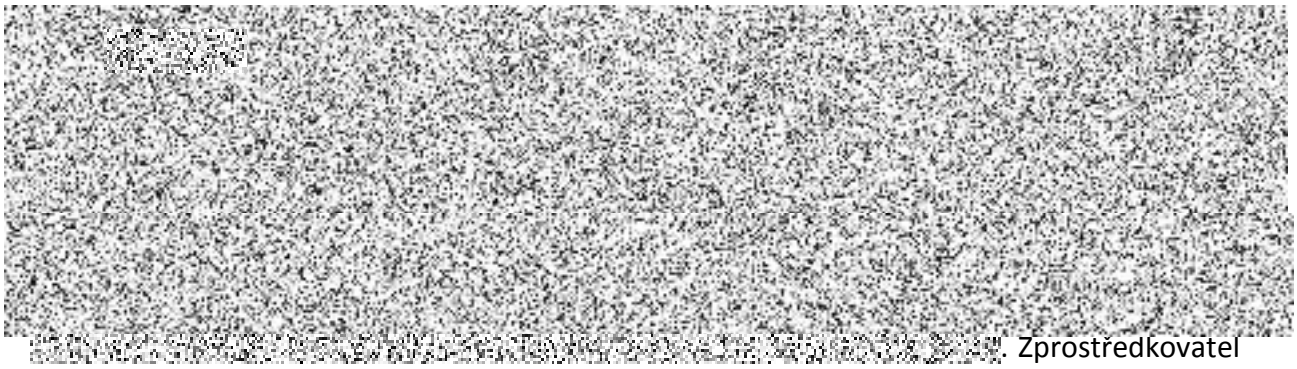
Z technického hlediska je postup vytváření a uložení vlastnoručního digitálního podpisu následující:

a) Poté, co zájemce o pojištění vyjádří vůli podepsat pojistnou smlouvu, zprostředkovatel zahájí podepisovací proces ve webové aplikaci [redacted].

[redacted]

[redacted]

[5] Při uzavírání pojistné smlouvy prostřednictvím zařízení dochází ke sběru 2D obrázku podpisu a dále informací o vektorech, které obsahují souřadnice x a y, časovou značku a příznak, zda se jedná o pohyb perem po zařízení nebo nad ním. Pomocí zmíněných informací je následně zpětně (v případě sporu o pravost podpisu) možné získat informace o rychlosti pohybu elektronického pera v jednotlivých částech podpisu.

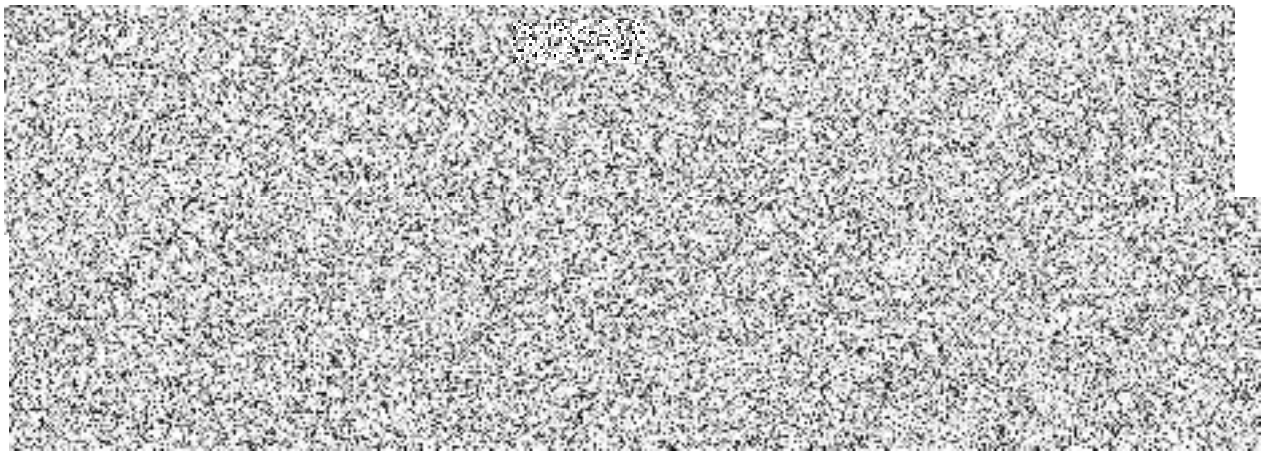


. Zprostředkovatel předá kontrolu nad zařízením zájemci o pojištění, který provede svůj vlastnoruční digitální podpis pomocí zařízení.

e) Podpisová data se přenáší ze zařízení . Sejmutá data se v obrazové podobě online zobrazují zájemci o pojištění ve webové aplikaci .

f) Zájemce o pojištění potvrdí podobu svého podpisu tlačítkem na zařízení nebo v rámci webové aplikace . Podpisová data se následně odešlou , který zajistí jejich spojení s podepisovaným dokumentem.

g) . Dokument je vrácen ve dvou kopiích, přičemž jedna z nich obsahuje zašifrovaná podpisová data a druhá obsahuje pouze vizuální reprezentaci podpisu (dále jen „vyžehlená kopie“).



j) Klientovi je dále odeslán e-mail s unikátním odkazem , jehož prostřednictvím si může stáhnout podepsaný dokument obsahující zašifrovaná podpisová data po omezenou dobu 90 dnů. .

Jak bylo uvedeno již výše, kontrolovaná osoba dle svého vyjádření zpracovává podpisová data za účelem ochrany svých právních nároků, konkrétně za účelem prokázání podpisu pojistné smlouvy danou osobou v případech, kdy tato osoba pravost digitálního podpisu zpochybní.

Kontrolovaná osoba tvrdí, že obecně dochází (např. v rámci vymáhání nezaplaceného pojistného) ke zpochybňování pravosti podpisů ze strany klientů. Dle jejích informací obecně dochází i ke zpochybňování platnosti podpisů elektronických (podobných těm, které používá kontrolovaná osoba). V takovém případném sporu bude kontrolovaná osoba prostřednictvím podpisových dat (a případně dalších důkazů, pokud jsou k dispozici) plnit svoji důkazní povinnost a realizovat tak své právo na obhajobu.

Obecné tvrzení o zpochybňování elektronických podpisů sice kontrolovaná osoba nikterak nepodložila, nicméně vzhledem k formulaci [redacted]: *„Dle našich informací obecně dochází i ke zpochybňování platnosti podpisů elektronických (podobných těm, které používá naše společnost)“* toto tvrzení nerozporují, neboť z něj není zjevná informace o počtu zpochybnění. Nevyplývá z něj tedy ani to, že by mělo např. docházet ke zpochybňování ve větší míře, než je tomu u podpisů fyzických kopií smluv.

K danému zpracování bylo předloženo *Posouzení souladu s GDPR a vlivu na ochranu osobních údajů, Zpracování – podepisování na signpadech u získatelů/zpracovatelů* [redacted] přehledu podkladů). Již v počáteční části tohoto posouzení (viz otázka č. 1) je uvedeno, že *„v případě tohoto zpracování nedojde ke změně v rozsahu využití zpracovávaných osobních údajů“*. S tímto kontrolující nemohou souhlasit, neboť oproti běžně podepisovaným smlouvám jsou navíc zpracovávány zvláštní kategorie osobních údajů a s tímto musí zákonitě souviset i další technická a organizační opatření (jak je patrné z postupu vytváření a uchovávání viz výše) a využití dalších prostředků zpracování (viz popis průběhu podpisu), přičemž tyto aspekty byly kontrolovanou osobou vyhodnoceny negativně, tedy že k těmto nedochází.
Biometrický podpis není v českém právním řádu definován. V oboru informačních a komunikačních technologií je definován dynamický biometrický podpis jako datová struktura, která vzniká působením podepisující osoby na podepisovací zařízení (nejčastěji na podpisovém grafickém tabletu, a to vlastní rukou, případně za pomocí dotykového pera), která kromě výsledné podoby samotného podpisu sleduje a zaznamenává biometrii podepisující se osoby (rychlost tahů, přítlak atp.), která je pro každého charakteristická (ovšem v čase proměnlivá, např. stárnutím ovlivňujícím změny biometrické techniky či aktuálním zdravotním stavem). Dynamický biometrický podpis tak zachycuje nejen samotnou podobu podpisu (statický prvek), ale také dynamický prvek (rychlost, dobu podpisu, délku trvání podpisu). Hlavním problémem zpracovávání dynamického biometrického podpisu obecně je, že podepisující se subjekt zpravidla, na rozdíl od podpisu vlastnoručního, nemůže ověřit, k jakému dokumentu je jeho podpis připojen, nemá tedy nad zpracováním svých osobních údajů kontrolu, neboť s příslušnými prostředky disponuje druhá strana, nikoliv podepisující se osoba. Při případném zpochybnění pravosti podpisu by též nestačil pouze znalec z oboru písmoznalectví, který by přezkoumal vedení a křivky podpisové linie, ale zapotřebí by bylo též znalce z oboru kybernetiky, který stanoví, zda nebylo do dat charakterizujících biometrický podpis zasaženo. Pro vyloučení nesrovnalostí při uzavření smlouvy by bylo vhodné doplnit též další nepřímé důkazy (např. vzájemná korespondence s klientem).

Dle ustanovení § 561 odst. 1 zákona č. 89/2012 Sb., občanský zákoník, … „*K platnosti právního jednání učiněného v písemné formě se vyžaduje podpis jednajícího. Podpis může být nahrazen mechanickými prostředky tam, kde je to obvyklé. Jiný právní předpis stanoví, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat*.“ Tímto zvláštním právním předpisem byl myšlen zákon č. 227/2000 Sb., o elektronickém podpisu, jenž

přestal platit 19. září 2016, a který výslovnou právní úpravu dynamického biometrického podpisu a jeho užití neobsahoval a byl nahrazen tzv. adaptačním zákonem k nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále jen „nařízení eIDAS“), tedy zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (dále jen „zákon č. 297/2016 Sb.“), který rovněž právní úpravu biometrického podpisu a jeho užití neobsahuje. Občanský zákoník ani zvláštní právní úprava tedy vysloveně nevyžadují pro platnost právního jednání v písemné formě dynamický biometrický podpis. Dostatečný pro výše uvedené účely je tak prostý obraz podpisu klienta na dematerializované smluvní dokumentaci, který je srovnatelný s podpisem na smluvní dokumentaci v listinné podobě.

Ohledně dynamického biometrického podpisu lze dále uvést, že zpravidla bývá označován za druh elektronického podpisu (a to zejména s ohledem na formu jeho pořízení a zpracování), přičemž při této interpretaci bývá odkazováno, na již výše zmíněné nařízení eIDAS. Toto nařízení v čl. 3 odst. 10, které definuje elektronický podpis jako „*data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání*“, rozeznává tři druhy těchto podpisů – prostý, zaručený (čl. 3 odst. 11 nařízení eIDAS) a kvalifikovaný (čl. 3 odst. 12 nařízení eIDAS). Právní účinek rovnocenný vlastnoručnímu podpisu přiznává nařízení eIDAS v čl. 25 odst. 2 pouze kvalifikovanému elektronickému podpisu, o jiných podpisech nic neuvádí. Dynamický biometrický podpis není kvalifikovaným elektronickým podpisem, neboť v rozporu s čl. 3 odst. 12 nařízení eIDAS není vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a není založen na kvalifikovaném certifikátu pro elektronické podpisy. Z pohledu této právní úpravy by mohl být označen pouze jako podpis prostý, který ovšem nařízení eIDAS definuje velmi obecně. V každém případě není dynamický biometrický podpis běžným podpisem, neboť je založen na jiných mechanismech, než je tomu u elektronických podpisů a shromažďuje zvláštní kategorii osobních údajů. Biometrická identifikace/autentizace je založena toliko na pravděpodobnosti, nikoliv na 100 % přesnosti.

V případě elektronického podpisu nařízení eIDAS i zákon č. 297/2016 Sb. vyžadují, aby ochrana osobních údajů byla zohledněna. Pokud dochází ke zpracovávání biometrických údajů, je vždy potřebné, aby správce zvážil, s ohledem na práva a svobody fyzické osoby, rizika spojená se zpracováním takových údajů, zda je skutečně nezbytné použití této kategorie osobních údajů při daném zpracování. Zejména je nutno brát v úvahu, že zpracování biometrických údajů je spojeno s určitými riziky, jež vyplývají ze samotné podstaty těchto údajů. Takové riziko přestavuje zejména možnost jejich dalšího použití, včetně skrytého shromažďování, a to včetně tzv. inverzních útoků.

Dalším aspektem je délka uchování takového podpisu a jeho „využitelnost“ vzhledem ke změnám fyziologické identity subjektu údajů po deklarované době uchování 15 + 1 rok, kdy se zákonitě biometrický podpis a jeho charakteristiky s tímto aspektem musí měnit.

Kontrolovaná osoba má vnitřně nastavenu možnost podepisování smluv skrze signpady s využitím biometrických údajů subjektů údajů, přičemž zpracování biometrických údajů má postaveno na základě čl. 9 odst. 2 písm. f) nařízení (EU) 2016/679. Podmínka nezbytnosti zpracování zde však není naplněna, neboť kontrolovaná osoba považuje vlastnoruční podpis subjektu údajů na listinné podobě smlouvy za rovnocenný podpisu skrze signpad, jenž

zpracovává též biometrické údaje [redacted]. Ze strany kontrolované osoby by připadalo v úvahu využití zákonného titulu souhlasu dle čl. 6 odst. 1 písm. a) nařízení (EU) 2016/679. Kontrolovaná osoba však v souvislosti s tímto zpracováním jeho využití neuvádí a ani jej nikterak nedoložila. Případný souhlas musí splňovat znaky, které uvádí čl. 7 nařízení (EU) 2016/679. Především musí být dle čl. 7 odst. 2 nařízení (EU) 2016/679 jasně odlišitelný od jiných skutečností, srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků a svobodný v souladu s čl. 7 odst. 4 nařízení (EU) 2016/679. Souhlas se zpracováním osobních údajů, který je součástí smluv o povinném ručení podepisovaných skrze signpady, tyto atributy nesplňuje. S ohledem na to, že elektronické podpisy smluv o povinném ručení jsou zpracovávány bez řádného zákonného titulu, dochází v této souvislosti k porušení čl. 6 odst. 1 ve spojení čl. 9 odst. 2 nařízení (EU) 2016/679.

Plnění zásady minimalizace, přesnosti a omezení uložení

a) Zásada minimalizace

Kontrolovaná osoba uvádí, že stanovuje rozsah zpracovávaných osobních údajů přiměřený konkrétním účelům zpracování a požadavkům relevantních právních předpisů (viz bod č. 6, str. 7 přehledu podkladů).

Ve vztahu k předmětu kontroly stanovila rozsah zpracovávaných osobních údajů následovně (zájemce o uzavření povinného ručení uvádí následující údaje, [redacted]:

a) údaje o pojistníkovi (titul, jméno, příjmení, rodné číslo, bydliště, státní příslušnost, kontaktní telefon a e-mail),
b) údaje ve stejném rozsahu o vlastníkovi vozidla/pojištěném a provozovateli vozidla a
c) údaje o vozidle (registrační značka, rozlišovací značka státu, druh vozidla, tovární značka, obchodní označení, počet míst k sezení, měsíc a rok první registrace, způsob užívání, současná a předchozí poškození, registrace vozidla mimo ČR, leasing, série a číslo technického průkazu, VIN, druh registrační značky, kategorie vozidla, zdvihový objem, výkon motoru, největší povolená hmotnost, palivo)

Kontrolujícími byl při ústním jednání a místním šetření u zprostředkovatele povinného ručení 15. prosince 2020 ověřen rozsah zpracovávaných údajů dotazem [redacted] a nahlédnutím do interního elektronického systému pro sjednávání pojištění [redacted].

Zprostředkovatel povinného ručení uvedl, že „*Do smlouvy* (myšleno *Pojistná smlouva o komplexním pojištění vozidla* [redacted] *se zadávají následující údaje: rodné číslo, jméno, příjmení, případně titul, bydliště, telefon a e-mail (poslední dva údaje nepovinné). Dále údaje z velkého technického průkazu*“ [redacted].

Náhledem do [redacted] nástroje získatele kontrolující ověřili, že jsou do něj vkládány údaje v rozsahu, který uvádí výše uvedená vzorová *Pojistná smlouva o komplexním pojištění vozidla* [redacted] (rodné číslo, titul, jméno, příjmení, státní příslušnost, adresa, e-mail, mobil, telefon, korespondenční adresa, SPZ, VIN, druh registrační značky, rozlišovací značka státu,

způsob užívání, číslo technického průkazu, měsíc a rok registrace, druh vozidla, palivo, výkon motoru, počet míst k sezení, zdvihový objem, největší povolená hmotnost, stav počítadla, informace o předchozím vážném poškození, současném poškození a o místě první registrace vozidla).

Kontrolující konstatují, že rozsah zpracovávaných údajů je určen zejména § 80 odst. 7 zákona č. 170/2018 Sb. (včetně uvedení rodného čísla)[6] a dále též § 1[7] vyhlášky č. 205/1999 Sb., Ministerstva financí, kterou se provádí zákon č. 168/1999Sb., o pojištění odpovědnosti za škodu způsobenou provozem vozidla a o změně některých souvisejících zákonů (zákon o pojištění odpovědnosti z provozu vozidla).

Údaje, které ve výše uvedených právních předpisech nejsou výslovně uvedeny, pak kontrolovaná osoba získává dle vlastního vyjádření [redacted] na základě stanovených právních titulů plnění smlouvy (pro účely modelace, návrhu a uzavření pojistné smlouvy a posouzení přijatelnosti do pojištění) a oprávněných zájmů správce (účel prevence a odhalování pojistných podvodů a jiných protiprávních jednání a zájem na řádném plnění smlouvy s pojistníkem a dále oprávněný zájem třetí osoby, tj. pojistníka). K problematice určení zákonnosti zpracování blíže *Zákonnost zpracování*.

Kontrolovaná osoba dle svého vyjádření [redacted] za účelem prevence a odhalování pojistných podvodů a jiných protiprávních jednání dále navíc zpracovává identifikační údaje lékařů, zprostředkovatelů pojištění poškozené osoby a viníka pojistné události a kontaktní údaje těchto osob, informace o škodném průběhu pojištění odpovědnosti, včetně originálů nebo kopií dokumentů poskytnutých za tímto účelem, údaje o využívání služeb kontrolované osoby a údaje o zdravotním stavu a genetické údaje (pouze v případě, že je pojistné plnění vázáno na zjišťování zdravotního stavu, tedy pokud při dopravní nehodě došlo k újmě na zdraví). Ze strany zprostředkovatelů jsou zpracovávány též logy aplikací, přístupy do systémů, produkce pojistných smluv a výplaty provizí.

---

[6] Při distribuci pojištění zpracovává pojišťovací zprostředkovatel osobní údaje týkající se fyzických osob zúčastněných na vzniku a změnách jím distribuovaného pojištění, a to včetně jejich rodných čísel. Takové zpracování osobních údajů se považuje za zpracování nezbytné pro splnění právní povinnosti správce podle přímo použitelného předpisu EU5) a zákona o zpracování osobních údajů.

[7] Rozsah údajů o pojištění odpovědnosti sdělovaných pojistitelem České kanceláři pojistitelů - Pojistitel sděluje České kanceláři pojistitelů tyto údaje o vzniku, době přerušení, změně a zániku pojištění odpovědnosti:
a) číslo zelené karty, datum jejího vystavení, dobu její platnosti,
b) jméno, popřípadě jména, a příjmení nebo obchodní firmu nebo název provozovatele vozidla podle technického průkazu vozidla a jméno, popřípadě jména, příjmení a bydliště vlastníka vozidla anebo obchodní firmu nebo název a sídlo vlastníka vozidla a jméno, popřípadě jména, příjmení a bydliště pojistníka anebo obchodní firmu nebo název a sídlo pojistníka; jedná-li se o vozidlo, které nepodléhá evidenci silničních vozidel podle zákona upravujícího podmínky provozu vozidel na pozemních komunikacích, pouze jméno, popřípadě jména, příjmení a bydliště vlastníka vozidla anebo obchodní firmu nebo název a sídlo vlastníka vozidla a jméno, popřípadě jména, příjmení a bydliště pojistníka anebo obchodní firmu nebo název a sídlo pojistníka,
c) obchodní firmu a sídlo pojistitele,
d) dobu trvání pojištění a dobu přerušení pojištění, bylo-li sjednáno,
e) druh vozidla, jeho tovární značku a jeho typ,
f) identifikační číslo vozidla; nebylo-li přiděleno, číslo karoserie nebo podvozku vozidla,
g) státní poznávací značku nebo vojenskou poznávací značku vozidla,
h) číslo technického průkazu vozidla,
i) číslo pojistné smlouvy.

Kontrolující k tomu uvádějí, že rozsah výše uvedených zpracovávaných osobních údajů není vzhledem k účelům zpracování nadbytečný.

Kontrolující dále neshledali, že by biometrický podpis klientů byl pro účely ochrany právních nároků nezbytný. Toto své tvrzení opírají jednak o doložené posouzení oprávněného zájmu, které neřeší všechny aspekty tohoto zpracování, a dále o fakt, že v případě uzavírání smluv v listinné podobě takový druh podpisu není vyžadován, stejně jako v případě uzavření smlouvy okamžitým zaplacením pojistného s využitím platebního terminálu [redacted]. Kontrolovaná osoba tedy považuje za rovnocenné podepsání skrze signpad i listinnou podobu podpisu. Listinnou podobu podpisu povolí vždy, když si o ni klient požádá (namísto podpisu skrze signpad). Ze strany kontrolované osoby tedy není nezbytné vyžadovat biometrický podpis.

Na základě výše uvedeného kontrolující konstatují, že kontrolovaná osoba neplní ve vztahu ke zpracovávaným osobním údajům, zásadu minimalizace dle čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679, a to v případě biometrických údajů obsažených v elektronických podpisech pořizovaných skrze signpady.

b) Zásada přesnosti

Pro uzavírání smluvního vztahu s klientem i při jakékoliv změně pojistné smlouvy je pojišťovacímu zprostředkovateli nařízena kontrola návrhu pojistné smlouvy včetně uvedených osobních údajů[8]. Takový postup je zaveden v souladu s plněním zásady přesnosti dle čl. 5 odst. 1 písm. d) nařízení (EU) 2016/679. Pojišťovací zprostředkovatel musí jednat s odbornou péčí, jejíž součástí je též každoroční povinné setkání s klientem, během nějž je prováděna aktualizace údajů. Nad rámec povinností ve smlouvách a interních pokynech jsou pojišťovací zprostředkovatelé vedeni k ověření osobních údajů a případnému provedení jejich aktualizace přímo ve sjednávacím nástroji [redacted]. Pojistná smlouva (myšleno *Pojistná smlouva o komplexním pojištění vozidla* [redacted]) též obsahuje prohlášení, že zadaná adresa a kontakty uvedené ve smlouvě jsou aktuální a souhlasí, že tyto údaje budou využívány i v případě předchozích smluv, liší-li se tyto údaje. Při uzavírání smluv tedy dochází k aktualizaci osobních údajů klienta i u dalších existujících smluv.

Plnění výše uvedeného bylo kontrolujícími ověřeno při ústním jednání a místním šetření u kontrolované osoby 6. října 2020 [redacted]. Kontrolovanou osobou bylo sděleno, že: „*Klient telefonicky, e-mailem či osobně nahlásí potřebné údaje. Při osobní návštěvě jsou údaje ověřeny shlédnutím průkazu totožnosti, případně též technického průkazu vozidla.*“

Při ústním jednání a místním šetření provedeném 15. prosince 2020 u zprostředkovatele povinného ručení [redacted], bylo kontrolujícími při kontrole zadávaných údajů do *Pojistné smlouvy o komplexním pojištění vozidla* [redacted] zjištěno, že do této smlouvy jsou zadávány následující údaje: rodné číslo, jméno, příjmení, případně titul, bydliště, nepovinně telefon a e-mail, dále údaje z velkého technického průkazu vozidla, kdy jsou tyto údaje kontrolovány shlédnutím příslušného dokladu.

[8] Povinnost stanovená dokumentem *Základní pokyny pro pojišťovací zprostředkovatele* [redacted]

[9] [redacted]

Na základě výše uvedeného kontrolující konstatují, že kontrolovaná osoba plní ve vztahu ke zpracovávaným osobním údajům zásadu přesnosti dle čl. 5 odst. 1 písm. d) nařízení (EU) 2016/679.

c) Zásada omezení uložení

Kontrolovaná osoba v záznamech o činnostech zpracování uvedla délky doby zpracování, které jsou určeny následovně [redacted]:

- u účelů modelace, návrh a uzavření pojistné smlouvy a posouzení přijatelnosti do pojištění se jedná o konec druhého kalendářního roku od aktualizace předsmluvní dokumentace či uzavření pojistné smlouvy (dle § 80 odst. 4 zákona č. 170/2018 Sb.), tato lhůta zpracování platí i pro zpracování osobních údajů v případě neuzavření smlouvy (do konce druhého kalendářního roku následujícího od poslední komunikace se zákazníkem, [redacted];
- pro účel prevence a odhalování pojistných podvodů a jiných protiprávních jednání je stanoven jako konec lhůty konec druhého kalendářního roku od aktualizace předsmluvní dokumentace či 16 let [redacted] promlčecí doba v délce maximálně 15 let od skončení pojištění podle § 636 odst. 2 zákona č. 89/2012 Sb., přičemž tuto dobu kontrolovaná osoba prodlužuje ještě o rok, který slouží jako ochranná doba pro případ, že by došlo k uplatnění nároků z pojištění až v závěru běhu této promlčecí doby, [redacted] od ukončení pojistné smlouvy či pojistné události;
- v rámci plnění právních povinností se vzhledem k předmětu kontroly jedná o konec druhého kalendářního roku od aktualizace předsmluvní dokumentace nebo 10 let po ukončení pojistné smlouvy, pojistné události, stížnosti, regresu nebo pohledávky z pojistného (dle § 80 odst. 4 zákona č. 170/2018 Sb.).

V návaznosti na uplynutí těchto lhůt dochází k ukončení zpracování. Přičemž dokumenty jsou následně skartovány a vymazány.

Kontrolující v rámci *Žádosti o součinnost* [redacted] kontrolovanou osobu požádali o upřesnění doby zpracování pro účel prevence a odhalování pojistných podvodů a jiných protiprávních jednání. Kontrolovaná osoba k tomu uvedla [redacted], že dodatečná jednoroční lhůta slouží jako ochranná doba pro případ, že by ze strany žalobce (subjekt údajů) došlo k uplatnění právních nároků, zejména nároků z pojištění, až v závěru běhu této promlčecí doby a současně by byla kontrolované osobě žaloba doručena až s výraznějším časovým odstupem.

Stanovení této dodatečné lhůty vychází z praktických zkušeností, kdy byla kontrolovaná osoba v minulosti opakovaně účastníkem soudních řízení, o jejichž zahájení se doručením žaloby dozvěděla až několik měsíců, resp. v některých případech dokonce až několik let po jejím podání u soudu. Takové vybrané případy z oblasti povinného ručení přiložila formou *Přehledu soudních řízení* [redacted], ve kterém je kromě relevantních časových údajů uvedeno i označení každého příslušného soudního sporu spisovou značkou. Kontrolující k tomu uvádějí, že kontrolovaná osoba dodala seznam celkem 35 žalob, u kterých byl časový interval mezi podáním a doručením žaloby v rozmezí šesti (6) měsíců až šesti (6) let čtyř (4)

měsíců, 28 dní. Celkem 22 z nich bylo doručeno v časovém rozmezí šesti (6) měsíců až jednoho (1) roku.

Kontrolovaná osoba dále uvedla, že údaje po tuto dodatečnou dobu zpracovává v rámci svého práva na obhajobu – pokud by totiž dané osobní údaje vymazala uplynutím promlčení doby, mohla by se dostat do situace, kdy by v zahájeném soudním sporu nebyla schopná unést své břemeno tvrzení a/nebo břemeno důkazní. Osobní údaje jsou tedy po tuto dodatečnou jednoroční dobu zpracovávány za účelem ochrany právních nároků a prevence pojistných podvodů.

V dokumentu *Archivační a skartační řád společnosti* [redacted] kontrolovaná osoba určuje osoby, které jsou odpovědné za vyřazování dokumentů a spisů (skartační komise) a obecně stanovuje postupy při procesu skartace a archivace, nejsou zde přímo stanoveny lhůty, po kterých se k jednotlivým krokům přistupuje.

Lhůty pro zpracování osobních údajů jsou zmíněny v dokumentu [redacted]. Zde je vždy uveden typ objektu (předsmluvní dokumentace, pojistná smlouva, pojistná událost), případně zpřesnění objektu (zdravotní údaje, biometrické údaje), konkrétní účel, role (subjekt údajů), právní titul, začátek účelu, trigger (spouštěč) doby expirace a doba, po které účel expiruje. Kontrolující k tomuto dokumentu uvádějí, že lhůty zpracování osobních údajů zde uvedené korespondují se lhůtami výše uvedenými, nicméně k tomuto dodávají, že určení právního titulu pro zpracování (oprávněný zájem) v případech uvedených v části *Zákonnost zpracování* neodpovídá reálnému stavu.

U osob, se kterými nedojde k uzavření pojistné smlouvy, uchovává kontrolovaná osoba osobní údaje po dobu, kterou stanoví § 80 odst. 4 zákona č. 170/2018 Sb. pro uchovávání dokumentů a záznamů (do konce druhého kalendářního roku od poslední komunikace se zákazníkem). Osobní údaje pojistníků a pojištěných osob jsou zpracovávány po celou dobu trvání smluvního vztahu (po celou dobu trvání pojištění a po dobu, po kterou je to nezbytné k realizaci práv a povinností plynoucích z takového pojištění). V případě ochrany právních nároků kontrolované osoby a prevence pojistných podvodů je dále prodloužena o promlčecí dobu v délce maximálně 15 let od skončení pojištění, přičemž tuto dobu kontrolovaná osoba prodlužuje ještě o rok, který slouží jako ochranná doba pro případ, že by došlo k uplatnění nároků z pojištění až v závěru běhu této promlčecí doby. V době zahájení kontroly měla kontrolovaná nastaveno zpracování (archivaci po dobu 16 let) mylně pod zákonným titulem čl. 6 odst. 1 písm. b) po dobu 15 let, jak je patrné z *Protokolu z místního šetření a ústního jednání* (viz bod 20. přehledu podkladů, otázka č. 1, písm. b. bod ii a iii) a dále správně nastavený 1 rok na základě čl. 6 odst. 1 písm. f) oprávněný zájem správce.

Na základě výše uvedeného kontrolující konstatují, že kontrolovaná osoba zpracovává osobní údaje ve smyslu zásady omezení uložení dle čl. 5 odst. 1 písm. e) nařízení (EU) 2016/679.

Plnění informační povinnosti

Pojistná smlouva o komplexním pojištění vozidla [redacted] obsahuje identifikační údaje správce, účely zpracování, právní tituly a kategorie osobních údajů [redacted]

[redacted] a plní tak dle vyjádření kontrolované osoby *první vrstvu plnění informační povinnosti správce*.

Předmětná pojistná smlouva dále odkazuje na *druhou informační vrstvu*, kterou tvoří dokument *Informace o zpracování osobních údajů v pojištění vozidel*. Ten obsahuje upřesňující informace, především bližší popis příjemců osobních údajů, doby zpracování a práva subjektů údajů. Dokument je trvale umístěn na webových stránkách kontrolované osoby [redacted].

Postup *aktivního* poskytování informací o zpracování osobních údajů je kontrolovanou osobou uveden v *Základních pokynech pro pojišťovací zprostředkovatele* [redacted]. Pojišťovací zprostředkovatel je dle tohoto dokumentu povinen seznámit klienta s *Informacemi pro klienta*, jejichž součástí jsou též *Informace o zpracování osobních údajů v pojištění vozidel* a které jsou nedílnou součástí pojistné smlouvy, ať už je předána fyzicky či zaslána e-mailem.

Platí to i v případech, kdy jsou dokumenty předávány v elektronické podobě (pokud si tuto formu klient zvolí). Před uzavřením smlouvy se klient seznámí s dokumenty alespoň jedním z následujících způsobů [redacted]:

a) nahlédnutím na předložené listinné dokumenty nebo
b) zpřístupněním na monitoru počítače při osobní přítomnosti, popř.
c) předáním dokumentů v předstihu v elektronické podobě (např. zasláním na e-mail).

Zprostředkovatel povinného ručení při ústním jednání a místním šetření 15. prosince 2020 sdělil, že předmětné údaje jsou zřejmé z uzavírané smlouvy, doprovodných materiálů a z internetových stránek kontrolované osoby. Dokumenty je možno zpřístupnit např. nahlédnutím prostřednictvím počítače povinné osoby či vytištěním [redacted].

V rámci výše uvedené *Informace o zpracování osobních údajů v pojištění vozidel* uvádí kontrolovaná osoba své kontaktní údaje včetně pověřence, účely a právní základ zpracování včetně oprávněných zájmů správce, informace o příjemcích osobních údajů, dobu zpracování osobních údajů, informace o právech subjektů údajů, o existenci práva podat stížnost u dozorového úřadu, skutečnost, že poskytování osobních údajů je zákonným či smluvním požadavkem, a že dochází k automatizovanému rozhodování, čímž rámcově plní svou informační povinnost dle odst. 1 a 2 čl. 13 nařízení (EU) 2016/679.

Subjekty údajů jsou ve výše uvedených dokumentech informovány též o zpracování biometrických údajů (vč. biometrických podpisů). Pojistník je také zavázán k tomu, aby pojištěné osoby informoval o zpracování jejich osobních údajů (liší-li se pojistník a pojištěná osoba).

K tomu však kontrolující dodávají, že kvůli nesprávnému určení právních titulů pro zpracování, jak jsou rozebrány v části *Zákonnost zpracování*, dostávají subjekty údajů nepřesné informace o právních titulech, na základě, kterých jsou jejich osobní údaje zpracovávány. Výše zmíněná *Pojistná smlouva o komplexním pojištění vozidla* [redacted] obsahuje informaci [redacted]: *„Pojistník bere na vědomí, že jeho identifikační a kontaktní údaje, údaje pro ocenění rizika při vstupu do pojištění a údaje o využívání služeb zpracovává pojistitel:*
- pro účely modelace, návrhu a uzavření pojistné smlouvy, posouzení přijatelnosti do pojištění,

správy a ukončení pojistné smlouvy a likvidace pojistných událostí, když v těchto případech jde o zpracování nezbytné pro plnění smlouvy, a – pro účely zajištění řádného nastavení a plnění smluvních vztahů s pojistníkem, zajištění a soupojištění, statistiky a cenotvorby produktů, ochrany právních nároků pojistitele a odhalování pojistných podvodů a jiných protiprávních jednání, když v těchto případech jde o zpracování založené na základě oprávněných zájmů pojistitele." Tato informace je ve věci určení právních titulů pro zpracování nesprávná (s výjimkou zpracování pro účel odhalování pojistných podvodů a jiných protiprávních jednání po dovršení lhůty 15 let od skončení pojištění podle § 636 odst. 2 zákona č. 89/2012 Sb.). Stejné vymezení právních titulů je v těchto případech uvedeno i v dokumentu *Informace o zpracování osobních údajů v pojištění vozidel* [redacted]. Subjekt údajů tedy i v druhé informační vrstvě dostává nesprávné informace o právních titulech k předmětným zpracováním.

Kontrolující vyhodnotili zjištěný stav tak, že dochází k porušení povinností vyplývajících z čl. 13 a 14 nařízení (EU) 2016/679 týkajících se informační povinnosti ze strany kontrolované osoby jako správce, protože subjekty údajů sice informuje, ale informace v souvislosti s uvedením nesprávného právního titulu obsahují chybné údaje.

Práva subjektů údajů

Subjekt údajů se dle vyjádření kontrolované osoby při uplatnění svých práv může na kontrolovanou osobu obrátit několika způsoby [redacted]. Zvolit může osobní návštěvu pobočky, kontaktovat se prostřednictvím e-mailu či telefonu, prostřednictvím poštovních služeb, datovou schránkou nebo prostřednictvím zaměstnance „v terénu" či pojišťovacího zprostředkovatele.

O těchto možnostech je informován prostřednictvím dokumentu *Informace o zpracování osobních údajů v pojištění vozidel* a také webových stránek kontrolované osoby. Na webových stránkách jsou též zveřejněny formuláře pro uplatnění práv subjektů údajů. Tyto formuláře však není nutné využít, je-li žádost zaslána e-mailem a je-li z dané žádosti zjevný předmět.

Při podání žádosti, jak vyplývá z pokynů, je po žadateli požadováno uvedení jména, příjmení, rodného čísla nebo data narození, popis žádosti, specifikace požadavku a dále IČO, číslo smlouvy (jde-li o současného či bývalého klienta kontrolované osoby), a podpis, pokud je žádost podána v listinné podobě. Žádosti jsou vyřizovány bezodkladně, nejpozději do jednoho měsíce od podání žádosti.

Při ústním jednání a místním šetření u zprostředkovatele povinného ručení 15. prosince 2020 bylo zjištěno, že uplatnění práv subjektů údajů zatím nezaznamenal [redacted]. V případě, že by se subjekt údajů dožadoval řešení této žádosti skrze zprostředkovatele povinného ručení, byla by při osobním setkání sepsána žádost. Kvůli identifikaci by byl požadováno předložení dokladu obsahující fotografii subjektu údajů[10] a dále údaje potřebné k řešení žádosti.

[10] Pojišťovací zprostředkovatel při ústním jednání uvedl, že by shlédnutím fotografie na průkazu ověřil totožnost osoby žádající o využití svých práv.

Kontrolující vyhodnotili zjištěný stav tak, že kontrolovaná osoba plní své povinnosti vyplývající z čl. 15-22 nařízení (EU) 2016/679.

Zpracovatelský vztah

Za účelem prověření plnění podmínek daných čl. 28 odst. 3 nařízení (EU) 2016/679 si kontrolující od kontrolované osoby vyžádali vzor zpracovatelské smlouvy. Kontrolovanou osobou byla předložena *Smlouva o obchodním zastoupení*, která [redacted] uvádí informace a podmínky stanovené výše uvedeným ustanovením [redacted].

Ve smlouvě je uveden předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce a zpracovatele (zpracovává údaje pouze na základě doložených pokynů správce, pokud mu toto zpracování neukládají právo Unie nebo členského státu, zajišťuje mlčenlivost osob oprávněných zpracovávat osobní údaje, přijme opatření podle článku 32, dodržuje podmínky pro zapojení dalšího zpracovatele, je nápomocen správci prostřednictvím vhodných technických a organizačních opatření, při povinnosti reagovat na žádosti o výkon práv subjektů údajů a povinností dle článků 32 až 36, vymaže nebo vrátí správci všechny osobní údaje po ukončení poskytování služeb spojených se zpracováním a vymaže existující kopie, poskytne správci veškeré informace potřebné k doložení splnění povinností plynoucích z čl. 28 nařízení (EU) 2016/679 a umožní též audity prováděné správcem či pověřeným auditorem).

Nastavení vztahu kontrolované osoby se zpracovatelem bylo kontrolujícími prověřeno při ústním jednání a místním šetření 15. prosince 2020. Kontrolující si vyžádali od kontrolované osoby seznam zprostředkovatelů povinného ručení, z něhož náhodně vybrali jednoho zprostředkovatele – povinnou osobu, u které pak provedli předmětné místní šetření. Tento zprostředkovatel uvedl, že jeho vztah ke kontrolované osobě je realizován na základě *Smlouvy o výhradním obchodním zastoupení* [redacted], která ho opravňuje poskytovat všechny typy pojištění, které nabízí kontrolovaná osoba [redacted], přičemž předmětnou smlouvu kontrolujícím na místě předložil.

Předložená *Smlouva o výhradním obchodním zastoupení* [redacted] je [redacted] totožná s dříve předloženým vzorem smlouvy a obsahuje všechny náležitosti uvedené ve výše uvedeném ustanovení (předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce a zpracovatele v rozsahu čl. 28 odst. 3 písm. a) až h) nařízení (EU) 2016/679.

Kontrolující tedy konstatují, že kontrolovaná osoba má uzavřeny smlouvy se zpracovateli (součást *Smlouvy o obchodním zastoupení*), ve smyslu ustanovení čl. 28 bod 3 nařízení (EU) 2016/679, které obsahují všechny náležitosti uvedené v tomto ustanovení.

Zabezpečení zpracování, zásada integrity a důvěrnosti

Kontrolovaná osoba vypracovala vnitřní politiky zabezpečení osobních údajů, které zahrnují i požadavky integrity a důvěrnosti (jak je patrné z vyjádření kontrolované osoby [redacted], [redacted].

Klíčovými prvky politiky jsou řízení přístupů a uložení dat. V rámci systému využívaného pro práci zprostředkovatelů pojištění je integrita a důvěrnost zajištěna prostřednictvím [redacted].

Metodicky je plnění zásad pojišťovacími zprostředkovateli realizováno především prostřednictvím dokumentů *Základní pokyny pro pojišťovací zprostředkovatele*, *Informace o roli pojišťovacího zprostředkovatele při zpracování osobních údajů, Pokyny ke zpracování osobních údajů* a *Metodický pokyn* [redacted] *- Spolupráce s externími partnery (zejména pojišťovacími zprostředkovateli) při zprostředkování pojištění* [redacted].

Vzhledem k výměně údajů mezi kontrolovanou osobou jakožto správcem a zprostředkovatelem povinného ručení jako zpracovatelem osobních údajů, bylo dále prověřeno zabezpečení zpracování osobních údajů na obou stranách tohoto vztahu.

Systém řízení bezpečnosti informací je kontrolovanou osobou zakotven ve *Směrnici* [redacted]. V této směrnici je popsána odpovědnost a povinnosti jednotlivých vlastníků informačních aktiv a kontrolní role Úseku interního auditu. Jsou zde též popsána konkrétní cílová bezpečnostní opatření.

Řízení přístupů (Identity management)

Přístupy do uživatelských systémů [redacted], využívaných kontrolovanou osobou, [redacted]

Uložení dat

Data systémů jsou uložena [redacted]

[11] IDM je zkratka pro identity management (řízení přístupů). [redacted]

[12] [redacted]

[redacted]

Organizační a technická opatření aplikovaná zprostředkovatelem povinného ručení

Kontrolovaná osoba zprostředkovatelům povinného ručení ukládá povinnost[21] zajistit zabezpečení zpracování osobních údajů a doložení provedení tohoto zabezpečení. Jedná se především o tvorbu a vedení srozumitelné dokumentace o provedeném zpracování, šifrování, zálohování, testování zabezpečení, antivirové ochraně či fyzickém zabezpečení papírových dokumentů.

V dokumentu *Pokyny ke zpracování osobních údajů* [redacted] pak kontrolovaná osoba uvádí konkrétní technická a organizační opatření ochrany osobních údajů. [redacted]. Zprostředkovatel povinného ručení musí zajistit, aby přístup k osobním údajům měly pouze pověřené osoby, a musí též zabránit neoprávněnému přístupu k datovým nosičům.

[redacted]

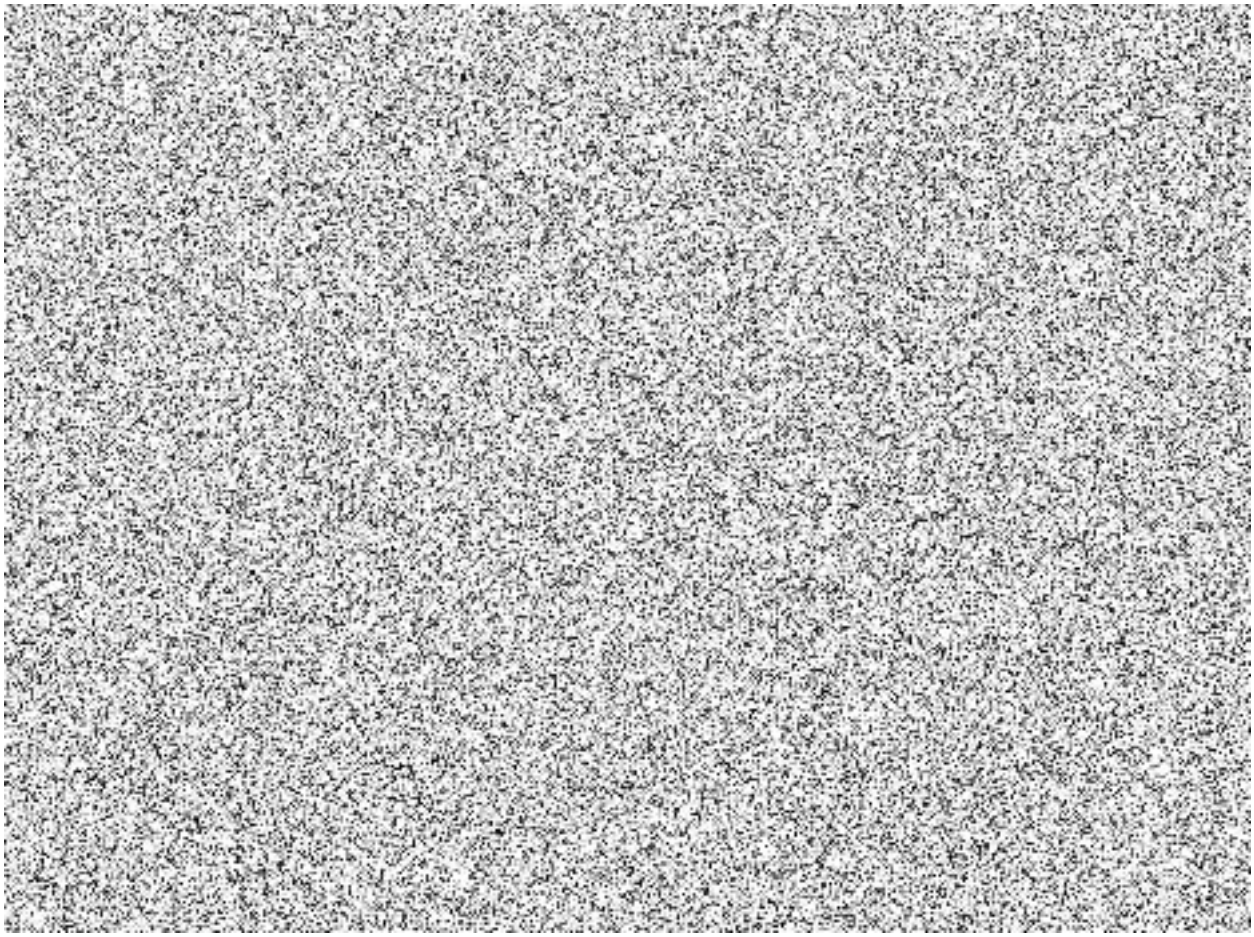
[redacted]

[redacted]

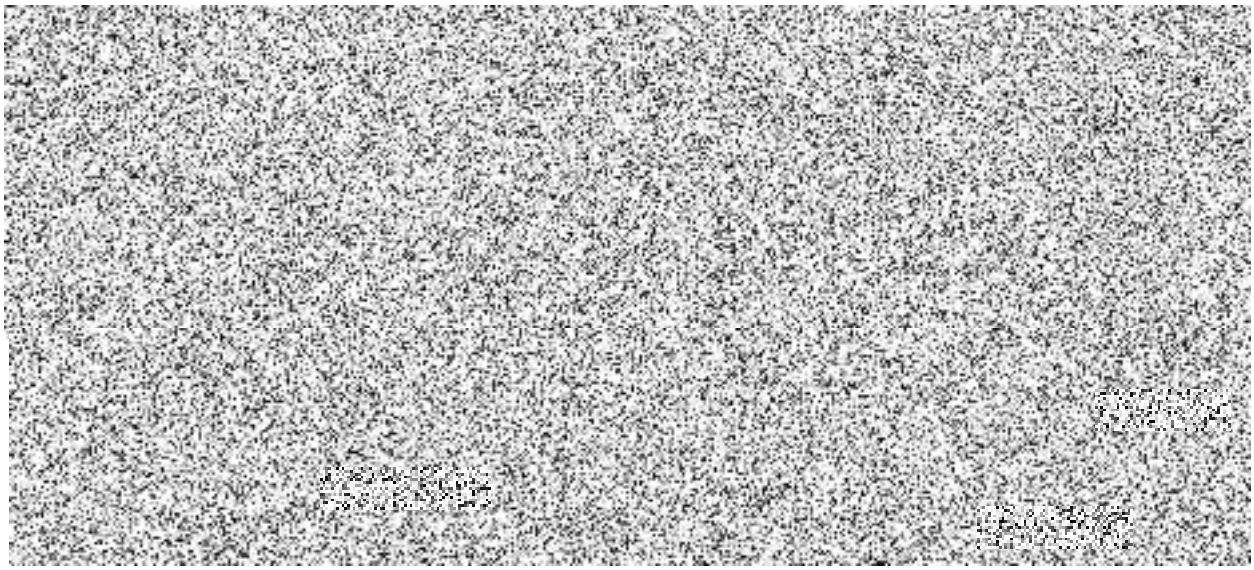
[redacted]

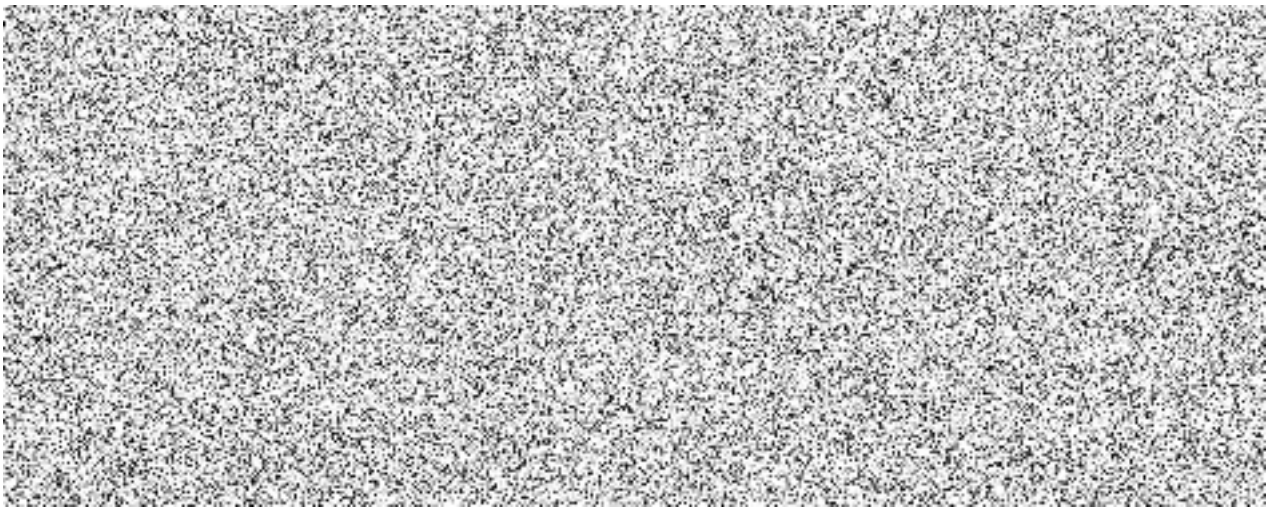
[21] Zjevné z dokumentu *Informace o roli pojišťovacího zprostředkovatele při zpracování osobních údajů* [redacted]

Dalšími prvky zabezpečení jsou dle výše uvedeného dokumentu:



Při zpracování osobních údajů v jiné, než elektronické podobě jsou pak dle tohoto předpisu osobní údaje uchovány v místnostech s náležitou úrovní zabezpečení, do kterých budou mít přístup výlučně pověřené osoby. Pojišťovací zprostředkovatel je povinen na písemnou žádost kontrolované osoby přijmout v přiměřené lhůtě stanovené kontrolovanou osobou další záruky za účelem technického a organizačního zabezpečení osobních údajů, zejména přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům.





Vzhledem k předepsanému technickému vybavení kontrolovaná osoba dále uvádí, že daná zařízení sama o sobě neisou schopna shromažďovat či ukládat žádné osobní či jiné údaje.

- zprostředkovatel má povinnost používat k podepisování pouze zařízení, která jsou kompatibilní se systémy kontrolované osoby,
- úsek informačních technologií stanovuje pro potřeby obchodní služby doporučené modely IT techniky a pro potřeby zprostředkovatelů minimální hardwarové a systémové/softwarové požadavky pro garantovaný chod sjednávací aplikace. Úsek informačních technologií dále stanovuje na základě odzkoušeného provozu typy podepisovacích zařízení, které spolupracují se sjednávací aplikací, a
- v případě, že zprostředkovatel nesplní minimální hardwarové a softwarové požadavky, není mu umožněno zařízení používat ke sjednání pojistných smluv.

Během ústního jednání a místního šetření u zprostředkovatele povinného ručení 15. prosince 2020 bylo zjištěno, že zprostředkovatel zadává údaje získané od klientů do systému [redacted], ke kterému má vlastní přístup [redacted]. Jakožto zprostředkovatel povinného ručení má přístup k údajům, které jsou nezbytné ke sjednání smlouvy [redacted]; jedná se o rodné číslo, titul, jméno, příjmení, státní příslušnost, adresu, e-mail, mobil, telefon, korespondenční adresu, SPZ, VIN, druh registrační značky, rozlišovací značku státu, způsob užívání, číslo technického průkazu, měsíc a rok registrace, druh vozidla, palivo, výkon motoru, počet míst k sezení, zdvihový objem, největší povolenou hmotnost, stav počítadla, informaci o předchozím vážném poškození, současném poškození a o místě první registrace vozidla).

Pokud je smlouva uzavřena v listinné podobě, je uchována po dobu nejdéle 24 hodin, poté je pověřenou osobou převezena na centrálu kontrolované osoby. Zprostředkovatel povinného ručení má v mezidobí smlouvu pod neustálým dohledem, případně je uložena v uzamčeném prostoru. Pro podepisování smluv elektronicky je využito [redacted].

Organizační a technická opatření přijatá v souvislosti s využitím signpadů

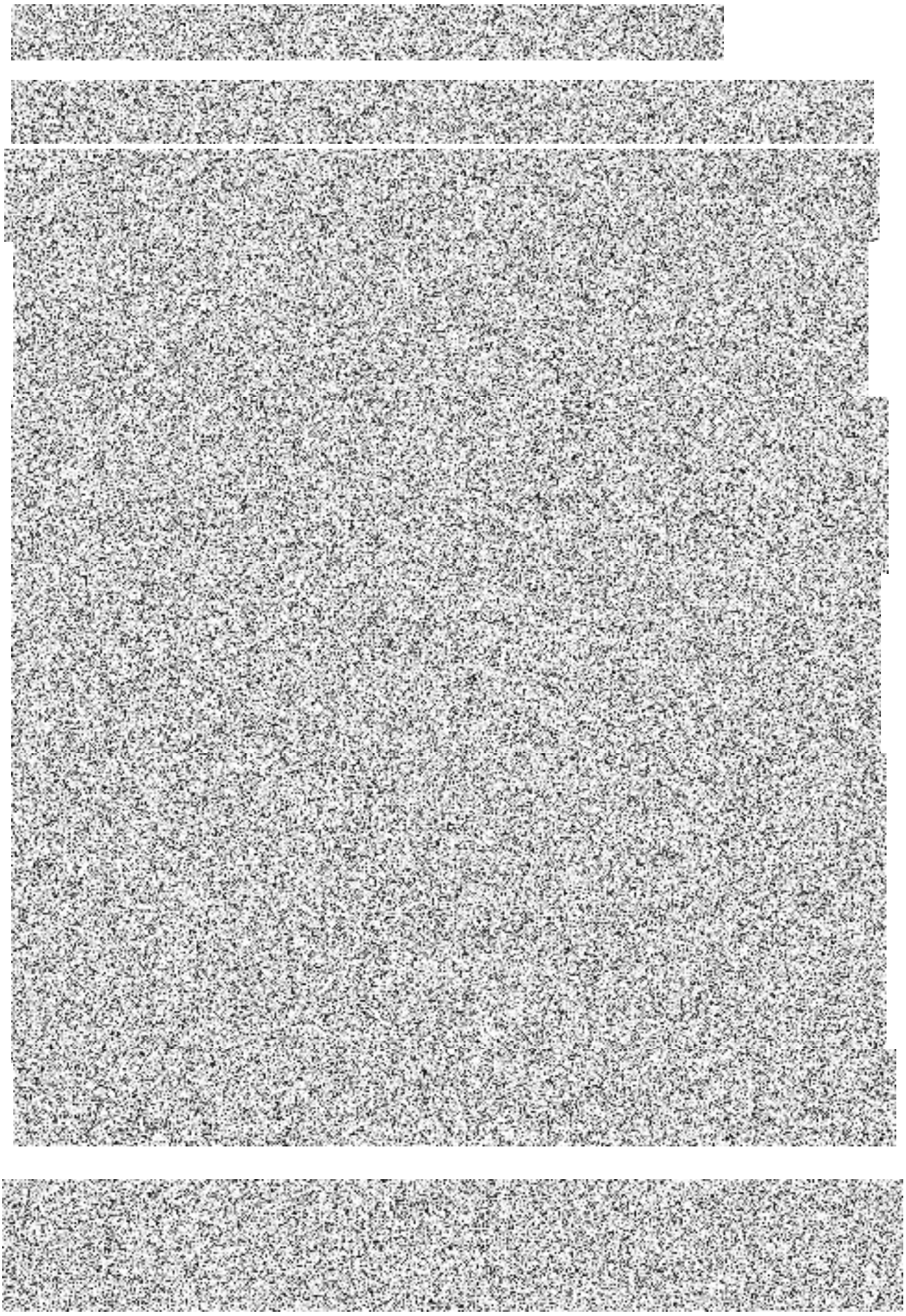
Kontrolovaná osoba uvádí (informace v následujících odstavcích dostupné z *Vyjádření kontrolované osoby k žádosti o poskytnutí součinnosti*, [redacted], že signpady jsou určeny ke snímání digitálního podpisu, který je proveden prostřednictvím podepisovacího pera na LCD displeji zařízení. Obě využívaná zařízení [redacted] fungují na principu elektromagnetické rezonance, kdy dochází ke snímání pohybů pera prostřednictvím senzorů umístěných v displeji. Modely zařízení se liší v několika aspektech, [redacted].

Zařízení sama o sobě nejsou schopna shromažďovat či ukládat žádné osobní či jiné údaje, nedisponují vlastní interní pamětí. [redacted]

Veškerá komunikace mezi zařízením a komponentami [redacted] je šifrovaná [redacted].

[redacted]

[redacted]



K pojistné smlouvě obsahující zašifrované informace o podpisu nemá přístup ani zprostředkovatel, který s klientem smlouvu uzavřel, tomu je poskytována pouze vyžehlená kopie.

Podpisová data nejsou poskytována žádným příjemcům. V případě sporu o pravost podpisu mohou být podpisová data poskytnuta orgánu, který daný spor rozhoduje, jak je uvedeno výše.

Kontrolující na základě výše uvedených zjištění konstatují, že kontrolovaná osoba má nastaveny procesy směřující k plnění povinností dle čl. 32 nařízení (EU) 2016/679 týkající se zabezpečení zpracování. Kontrolovaná osoba 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 provádí vhodná technická a organizační opatření, aby zajistila úroveň zabezpečení odpovídající danému riziku, zohledňuje rizika, která představuje zpracování, a přijala opatření aby jakákoliv fyzická osoba, která jedná z pověření kontrolované osoby nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn kontrolované osoby, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu. V důsledku toho nebylo zjištěno porušení plnění zásady integrity a důvěrnosti dle čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679.

Kontrolní závěry:

1) Zpracování biometrických údajů v souvislosti s elektronickým podepisováním smluv o povinném ručení signpady provádí kontrolovaná osoba bez řádného zákonného titulu, čímž porušuje čl. 6 odst. 1 nařízení EU) 2016/679,

2) U zpracování zvláštní kategorie osobních údajů v případě biometrických podpisů u podpisů smluv o povinném ručení kontrolující konstatují, že daným zpracováním kontrolovaná osoba porušuje ustanovení čl. 5 odst. 1. písm. c) nařízení (EU) 2016/679, a to z důvodu, že zpracování biometrických údajů není nezbytné pro dané zpracování.

3) Dochází k porušení povinností vyplývajících z čl. 13 a 14 nařízení (EU) 2016/679 týkajících se informační povinnosti ze strany kontrolované osoby jako správce, protože subjekty údajů sice informuje, ale informace v souvislosti s uvedením nesprávného právního titulu obsahují chybné údaje.

IV. 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, musí z nich být zřejmé, proti jakému kontrolnímu zjištění směřují, a musí obsahovat odůvodnění nesouhlasu s tímto kontrolním zjištěním.

Podpisová doložka:

Mgr. Eva Cupáková	vedoucí kontrolní skupiny	*(podepsáno elektronicky)* podpis
Mgr. Marek Šnajdr	pověřený zaměstnanec Úřadu	*(podepsáno elektronicky)* podpis
Mgr. Barbora Šnajderová	pověřená zaměstnankyně Úřadu	*(podepsáno elektronicky)* podpis