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-02219/21-16
Praha 5. října 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 z 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) ve spojení s § 50 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů.

Kontrolující:

Ing. Zdeňka Filová – pověřená zaměstnankyně Úřadu, č. služebního průkazu: XXXXXX, jako vedoucí kontrolní skupiny na základě pověření ke kontrole ze 3. června 2021;

JUDr. Roman Recman – pověřený zaměstnanec Úřadu, č. služebního průkazu: XXXXX na základě pověření ke kontrole z 6. září 2021.

Kontrolovaná osoba:

XXXXXXXXXXXXX, a.s., se sídlem XXXXXXXXXXXXXX, XXXXXXXXXXXXXXXXXX, XXXXXXXXXXXXX, IČ: XXXXXXXXXX (dále také „kontrolovaný“).

Předmět kontroly:

Předmětem kontroly je dodržování povinností stanovených nařízením (EU) 2016/679 a zákonem č. 110/2019 Sb. v souvislosti se zpracováním osobních údajů při nabízení zprostředkování či prodeji energií.

První kontrolní úkon:

Oznámení o zahájení kontroly z 10. června 2021, Čj. UOOU-02219/21-3, které bylo doručeno kontrolované osobě 10. června 2021.

Poslední kontrolní úkon:

Úřední záznam – pořízení dokumentace ze 14. září 2021, Čj. UOOU-00765/21-15.

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. *Strana 4, písm. a. bod 3. kontrolního plánu Úřadu pro rok 2021. 4. února 2021. 1 s.*
2. *XXXXXXXX. Doložení informací a podkladů ke kontrole... Čj. UOOU-02219/21-6. 7. července 2021. 3 listy. 1 CD.*
3. *XXXXXXXXXXXX. Poskytnutí součinnosti. Čj. UOOU-02219/21-8. 24. srpna 2021. 2 listy. 5 příloh.*
4. *XXXXXXXXXX. Dodatečné doložení informací. Čj. UOOU-02219/21-11. 19. září 2021. 2 listy. 1 příloha.*
5. *XXXXXXXXXXX. Smlouva o zpracování osobních údajů. Čj. UOOU-02219/21-12. 17. července 2018. 3 listy.*
6. *XXXXXXXXX. E-mailová informace o změně v seznamu zpracovatelů. Čj. UOOU-02219/21-13. 29. září 2021. 1 list.*
7. *XXXXXXXXXl. Dohoda o zpracování údajů. Čj. UOOU-02219/21-14. 4. října 2021. 6 listů.*
8. *Úřední záznam – pořízení dokumentace ze dne 5. října 2021. Čj. UOOU-00765/21-15. 2 s. 12 příloh.*
   - 8.1. *Výpis z obchodního rejstříku, vedeného Krajským soudem v Ústí nad Labem. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX 22. března 2021. 2 listy.*
   - 8.2. *Vyhledávání v registru (Whois). XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX. 18. června 2021. 2 listy.*
   - 8.3. *XXXXXXXXXXXX. Sdělení o jmenování pověřence. Č.j.: UOOU - 00005/21-318. UOOUX00ELW1J. 4. března 2021. 1 list.*
   - 8.4. *Informace o množství klientů. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX. 23. června 2021. 6 listů.*
   - 8.5. *XXXXXXXXXX. Informace pro zákazníky o zpracování osobních údajů společností XXXXXXXXXXXXXXXXXXX, a.s. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX. 22. června 2021. 14 listů.*
   - 8.6. *Seznam zpracovatelů osobních údajů zákazníka. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX. 22. června 2021. 28 listů.*
   - 8.7. *XXXXXXXXX. Zpracování osobních údajů společností XXXXXXXXX, a.s., 22. března 2021. Zpracování osobních údajů společností XXXXXXXXXXX, a.s. (marketingové účely). XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX 20180719.pdf. 22. června 2021. 3 listy.*

8.8. *Žádost o přenesení osobních údajů, XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX. 22. března 2021. 1 list.*
8.9. *XXXXXXXXX. Na stránce používáme XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX. 12. července 2021. 1list.*
8.10. *Zpracování cookies. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX. 22. března. 16 listů.*
8.11. *Seznam zpracovatelů osobních údajů zákazníka. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX. 28. července 2021. 20 listů.*
8.12. *XXXXXXXXX Informace pro zákazníky o zpracování osobních údajů společností XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, a.s. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX. 9. srpna 2021. 12 listů.*
8.13. *Seznam zpracovatelů osobních údajů zákazníka. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX. 30. září 2021. 16 listů.*

V rámci kontroly je posuzováno výhradně zpracování osobních údajů v rozsahu stanoveném v předmětu kontroly, pokud není níže uvedeno jinak, v čase provedení kontroly. Z výše uvedených podkladů jsou pro kontrolní zjištění v protokolu o kontrole výslovně vyhodnoceny pouze ty podklady, případně jejich části, v nichž jsou uvedeny relevantní informace.

II. Důvod kontroly:

Kontrola byla provedena na základě Kontrolního plánu Úřadu pro ochranu osobních údajů pro rok 2021.

III. Kontrolní zjištění:

Skutečnosti zjištěné z veřejných zdrojů a činnosti Úřadu

1. XXXXXXXXXXXXX, a. s., se sídlem XXXXXXXXXXXXXXXXX, XXXXXXXXXXXXXXXXX, XXXXXXXXXXXXX, IČO: XXXXXXXXXXXX, je zapsán v obchodním rejstříku, vedeném Městským soudem v Praze od XXXXXXXXXXXX. Předmětem podnikání je mimo jiné obchod s elektřinou a obchod s plynem, veřejně dostupná telefonní služba, služby přístupu k síti Internet, služby přenosu dat (*I.8.1.).*

2. Podle XXXXXXXXXXXXXXXXXXXXXX je držitelem domény XXXXXXXXXXXXXXX společnost XXXXXXXXXXXXXX, a.s., registrace domény provedena XXXXXXXXXXXXX (*I.8.2.).*

3. Kontrolovaný 5. března 2021 sdělil Úřadu informaci o jmenování pověřence pro ochranu osobních údajů, a to XXXXXXXXXXX, XXXXXXXXXX, XXXXXXX, telefon: + XXXXXXXXXXXX, e-mail: *XXXXXXXXXXXXXXXXXXXXXXXXXX, XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX (I.8.3.).*

4. Na webové stránce kontrolovaného *XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX* byla 23. června 2021 nalezena informace o počtu klientů kontrolovaného – *věří nám přes 262 000 klientů (I.8.4.).*
5. Na webové stránce kontrolovaného byl 22. června 2021 v záložce *ověřte si, jestli nepřeplácíte,* uveden odkaz na *XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX*, obsahující dokument *Informace pro zákazníky o zpracování osobních údajů společnosti XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, a.s.*, účinná od XXXXXXXXXXX. V dokumentu kontrolovaný podává informace o zpracování osobních údajů.

Dokument v bodě č. 7 odkazuje na seznam zpracovatelů a mimo jiné uvádí, že:
předává osobní údaje svých zákazníků ke zpracování do třetí země mimo EHP, avšak pouze za předpokladu, že správce nebo zpracovatel poskytli vhodné záruky jejich ochrany a v cílové zemi jsou k dispozici vymahatelná práva subjektu údajů a účinná právní ochrana subjektů údajů.

Dne 9. srpna 2021 byl na webové stránce kontrolovaného XXXXXXXXXXX kontrolujícími nalezen dokument *Informace pro zákazníky o zpracování osobních údajů společnosti XXXXXXXXXXX, a.s.*, účinný od XXXXXXXXXXX, s datem poslední aktualizace červenec 2021.

Informace popisují účely a způsoby zpracování osobních údajů, informují o kategoriích zpracovávaných osobních údajů, případných příjemcích, době uchování osobních údajů a právech subjektů údajů.

V bodě 3. uvádí kontrolovaný jako účely zpracování: předsmluvní jednání, plnění smlouvy, k plnění právních povinností, ochrana oprávněného zájmu správce, vyřizování požadavků zadaných prostřednictvím e-mailu, zákaznické linky nebo webových formulářů a zasílání obchodních sdělení a cílení reklamy.

V bodě 4. dokumentu jsou uvedeny zpracovávané osobní údaje v rozsahu:

- *XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.*

Účelem zpracování je *XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX*

V případě dodávky elektřiny a plynu zpracovává osobní údaje v rozsahu: *spojovací číslo SIPO*, v případě telekomunikačních služeb: *heslo, číslo SIM karty, PUK, PIN*.

Účelem zpracování je *XXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX,*

V případě telekomunikačních služeb zpracovává kontrolovaný *provozní údaje* (např. *telefonní číslo volaného, telefonní číslo volajícího, začátek a konec spojení, datum a frekvence uskutečněného spojení, IMEI, typ zařízení, konfigurační údaje, adresa datového spojení (např. URL), IP adresa, druh, způsob a objem využívání služeb, cena za službu, typové chování), provozní lokalizační údaje (zeměpisná poloha koncového zařízení*), a to za účelem plnění právních povinností.

Kontrolovaný dále zpracovává

- *číslo účtu, IČO, datum narození* pro účely *předsmluvní jednání, plnění smlouvy, plnění právních povinností, ochrana oprávněného zájmu správce,*

- elektronický podpis (bez biometrických údajů) pro účel plnění smlouvy,

- *rodné číslo* (pokud to zákon umožňuje), *údaje o dokladu totožnosti* pro účel plnění právní povinnosti,

- *údaje o odběrném místě* zejména adresa odběrného místa, EAN/EIC, popř. číslo elektroměru/plynoměru pro účel *plnění smlouvy, plnění právních povinností, ochrana oprávněného zájmu správce, vyřizování požadavků zadaných prostřednictvím zákaznické linky, e-mailu nebo webového formuláře,*

- *XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXX*

- záznam z kamerového systému pro účel *ochrana oprávněného zájmu – doložení dokladů příslušnému správnímu orgánu ČR nebo orgánů činných v trestním řízení,*

- informace uvedené v životopise pro účel *opatření před uzavřením smlouvy (v případě uchazečů o zaměstnání).*

Dále dokument obsahuje informaci o tom, že kontrolovaný zpracovává osobní údaje jak manuálně, tak automatizovaně. *XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.*

Doba uchování je v dokumentu uvedena podle účelu zpracování, a to mimo jiné:

plnění smlouvy – *po dobu trvání smlouvy a po dobu 10 let od ukončení smlouvy,*

plnění právních povinnost – *po dobu stanovenou příslušným právním předpisem*,

ochrana oprávněného zájmu správce – maximálně *po dobu 3 let od doby počátku zpracování údajů, nestanoví-li zvláštní právní předpisy jinak,*

-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXX

- XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX,

vyřizování požadavků zadaných prostřednictvím zákaznické linky, e-mailu nebo webového formuláře *- po dobu nezbytnou pro vyřízení příslušného požadavku,*

zasílání obchodních sdělení a cílení reklamy *- po dobu uděleného souhlasu se zasíláním obchodních sdělení a cílením reklamy, případně do odvolání souhlasu se zpracováním,*

opatření před uzavřením smlouvy – *po dobu jednání o uzavření smlouvy a dále maximálně po dobu XXXXXXXX.*

Dokument dále mimo jiné informuje subjekt údajů o příjemcích a zpracovatelích jeho osobních údajů, o jeho právech v souvislosti se zpracováním jeho osobních údajů, včetně způsobu odhlášení se z odběru obchodních sdělení (odkaz v závěru posledního obchodního sdělení – newsletteru).

V bodě 8. *Veřejné rejstříky a rejstříky vedené soukromými osobami* je mimo jiné uvedena *informace o dlužnických registrech* (SOLUS), a to na základě zákona č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů.

V závěru dokumentu je dále uveden kontakt na pověřence pro ochranu osobních údajů, a to:

Společnost XXXXXXXXXXXXXXX jmenovala pověřence pro ochranu osobních údajů XXXXXXXXXXXXXXX, kterého můžete kontaktovat níže uvedenými způsoby.

Písemně na adrese: XXXXXXXXXXXXXX, a.s.
Pověřenec pro ochranu osobních údajů
XXXXXXXXXXXXXXXXXXXXXXXXXXXX

Telefonicky: XXXXXXXXXXXXXXXXX

E-mailem: XXXXXXXXXXXXXXXXXXXXXX

Prostřednictvím kontaktního formuláře: XXXXXXXXXXXXXXXXXXXXXXXXXXXX

Zveřejněné kontaktní údaje pověřence se oproti dokumentu, který kontrolovaný zaslal Úřadu 4. března 2021 (*Sdělení o jmenování pověřence*) neliší. Dokument je popsán v bodě 3. kontrolních zjištění *(I.8.5. a 12.*).

6. V *Seznamu zpracovatelů osobních údajů zákazníka,* nalezeném 22. června 2021 na webových stránkách kontrolovaného (popsáno v bodě 5. kontrolních zjištění – proklikem v bodě č. 7) byl uveden abecedně seřazený výčet XXX zpracovatelů.

Na webové stránce kontrolovaného byl dne 28. července 2021 pořízen seznam zpracovatelů, obsahující XXX zpracovatelů. Kontrolovaný zde jako *správce informuje zákazníky – fyzické osoby* o zapojení do zpracování jejich osobních údajů další zpracovatele. Oproti seznamu, popsanému výše se liší o více než 200 položek. Seznam obsahuje informaci: název/jméno zpracovatele, IČO a sídlo, forma zpracování (např. *zasílání leadů ke zpracování komoditních smluv, zprostředkovatelská smlouva, partnerská smlouva, smlouva o spolupráci, rámcová smlouva).* U každého zpracovatele je uveden účel zpracování, a to např. *generuje leady, zprostředkování komoditních smluv, uzavírání obchodních smluv, předávání dat osobních údajů na základě plnění ze smlouvy, o připojení).* Seznam zde jako zpracovatele označuje mimo jiné společnost XXXXXXXX a.s.

Na webové stránce kontrolovaného byl dne 30. září 2021 pořízen seznam zpracovatelů, obsahující XXX zpracovatelů. Kontrolovaný zde jako *správce informuje zákazníky – fyzické osoby* o zapojení do zpracování jejich osobních údajů další zpracovatele. Z abecedně seřazeného seznamu bylo vypuštěno cca. 50 společností, např. XXXXXXXX, XXXXXXX, XXXXXXX) *(I.8.6., 11. a 13.).*

7. Na webových stránkách kontrolovaného byl 22. března 2021 v záložce *XXXXXXXXXXX a XXXXXXX,* nalezen dokument *Zpracování osobních údajů společností XXXXXXX, a.s., který* obsahuje osobní údaje zákazníka v rozsahu *jméno a příjmení, datum narození, ulice, číslo popisné a orientační, obec, PSČ, mobil, pevná linka e-mail.*

Zákazník uděluje *souhlas se zpracováním osobních údajů pro marketingové účely*, kdy zaškrtnutím jednoho či více uvedených komunikačních kanálů souhlasí se zpracováním svých osobních údajů a dále je zde *ukázka správného zaškrtnutí pole.*

Kontrolovaný zde informuje, že *v rámci zpracování bude docházet k profilování*, které bude cílené na marketingové sdělení. Osobní údaje budou kontrolovaným *zpracovávány po dobu trvání smlouvy a po dobu 5 let od jejího ukončení.* Dále je zde uvedeno, že souhlas zákazníka se zpracováním pro marketingové účely je dobrovolný a nemá vliv na uzavření smlouvy.

V další části dokumentu kontrolovaný informuje o zpracování osobních údajů zákazníka, účelu, rozsahu a době zpracování jeho osobních údajů, o zpracovatelích a příjemcích osobních údajů. Dále uvádí výčet práv zákazníků v souvislosti se zpracováním osobních údajů. Tyto informace o zpracování osobních údajů podané kontrolovaným jsou shodné s informacemi podanými kontrolovaným v dokumentu *Informace pro zákazníky o zpracování osobních údajů společností XXXXXXXXXXXXX, a.s.* a podrobně popsaném v bodech 5. a 6. kontrolních zjištění. Závěr formuláře tvoří prostor pro místo, datum a podpis zákazníka, který jím prohlašuje, že *se seznámil s podmínkami souhlasu a informacemi o zpracování svých osobních údajů. Zákazník bere na vědomí, že tyto informace jsou též dostupné na XXXXXXXXXXXXXXXXXXX.*

Dne 22. června 2021 byl na stejném místě nalezen dokument aktualizovaný *(I.8.7. a 12.).*

8. Na webových stránkách kontrolovaného byl 22. března 2021 nalezen v záložce *Ke stažení, Žádosti a smlouvy* bianko formulář *Žádost o přenesení osobních údajů,* který obsahuje údaje o současném správci osobních údajů (kontrolovaném), osobní údaje subjektu údajů (v rozsahu *jméno a příjmení, datum narození, adresa bydliště*), údaje o novém správci. Kontrolovaný ve formuláři upozorňuje, že *XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.* Formulář zákazník vlastnoručně podepisuje *(I.8.8).*

9. Na webových stránkách kontrolovaného byl 22. března 2021 v záložce *Ke stažení, Podmínky a prohlášení* dokument *Zpracování cookies,* který informuje o tom, že webové stránky XXXXXXXXXXXXXXX využívají cookies a co jsou cookies. Stránky lze používat i v režimu, který neumožňuje sbírání údajů o chování návštěvníků webu. Souhlas zákazník uděluje kliknutím na tlačítko *„OK, rozumím"* v okně ve spodní části stránky, souhlas je udělen na dobu, která je uvedena u jednotlivých cookies, souhlas se sbíráním údajů souborů cookies pro marketingové účely lze vzít kdykoliv zpět. Kontrolovaný dále uvádí výčet jednotlivých cookies (26), u každé cookies je přehledně uvedeno, *kdo má přístup k informacím*, *účel* a dobu uchování (od 1 min - 540 dní).

Shromážděné cookies jsou zpracovány prostřednictvím:

- *služby Google Analytics, provozované společností Google Inc.*
- *služby Facebook Pixel, provozované společností Facebook Inc.*

Dále zveřejňuje možnosti ukončení využívání *souborů cookies nebo identifikátorů zařízení*. V závěru dokumentu je uveden výčet práv subjektů údajů.

V zápatí webové stránky XXXXXXXXXXXXXXXX je uvedena informace pro návštěvníka stránky o používání cookies. Jednoduchým a přehledným výběrem (nutné, preferenční, statistické, marketingové), nebo *pouze nutné*, *povolit výběr*, *povolit všechny cookies*, může návštěvník stránek jejich používání ovlivnit.

Kliknutím na nabízené *Zobrazit detaily* podává kontrolovaný obecnou informaci o cookies. Oproti výběru povolení cookies je zde navíc uveden typ *neklasifikované cookies.* U každého jednotlivého typu cookies je uvedena informace o jménu, poskytovateli, účelu (v angličtině), doby uchování a typu *(I.8.9 a 10).*

Skutečnosti zjištěné u kontrolovaného

10. Kontrolovaný 24. srpna 2021 předložil dokument *Zpráva o vztazích za účetní období roku 2020 (*zveřejněný ve sbírce veřejných listin) a písemně uvedl, že v rámci společností skupiny *propojených osob tvořících koncern* nedochází k předávání osobních údajů zákazníků *(I.3.).*

11. Kontrolovaný 7. července 2021 uvedl, že k systematickému zpracování osobních údajů dochází v souvislosti se zpracováním osobních údajů zákazníků a zaměstnanců kontrolovaného. To doložil diagramy, které zachycují hlavní procesy zpracování osobních údajů a kontrolovaný je vytvořil v rámci analýzy zpracování osobních údajů.

Dále uvedl, že k 2. únoru 2021 jmenoval do funkce pověřence pro ochranu osobních údajů zaměstnance XXXXXXXXXXXXXXX, Ph.D. (*I.2.).*

12. Kontrolovaný 7. července 2021 písemně uvedl, že informační systém, zpracovávající zákaznická data je tvořen z dílčích informačních systémů, a to:

XXX– koncentruje veškerá data o zákaznících kontrolovaného, jejich smlouvách, vzájemné interakci a fakturačních jednotkách zákazníků. V tomto informačním systému pracuje větší část uživatelů kontrolovaného.

Karta zákazníka obsahuje osobní údaje v rozsahu: *jméno, příjmení, titul, rodné číslo, číslo OP, datum narození, adresa, mobil, e-mail, partner, úmrtí, datum úmrtí, dědické usnesení, insolvence, schválení oddlužení.* Dále aktivity (*změna dodavatele, záznamy hovorů, hlasové záznamy hovorů, záznam návštěv, nabídky*), údaje ve vztahu ke smlouvě, odběrnému místu, fakturační jednotce, produktům.

Smluvní formulář obsahuje osobní údaje v rozsahu: *ID formuláře, VIP (ano, ne), sken formuláře (číslo)*, *obchodní podmínky (název verze), typ zákazníka*, *název zákazníka* (*jméno, a příjmení), titul, rodné číslo, číslo pasu, datum narození, IČ/DIČ, telefon, mobil, e-mail, datová schránka, adresa zákazníka, odběrná místa, způsob uzavření sml. (M-mimo prostory obvyklé), partner, pořizovatel,* datum a místo podpisu*, neúplný formulář (ano/ne), vlastník.*

Tento informační systém obsahuje dále mimo jiné i data o segmentaci zákazníka (segment, přínos, celková roční spotřeba, celkový roční výnos), o kontrolách a interní „black list" zákazníků.

XXXXXX – informační systém využívaný především pro fakturaci, distribuci faktur a platebních kalendářů. *Čerpá data o zákaznících a smlouvách přes integrační rozhraní z XXX.*

XXXXXX – ekonomický informační systém. Z pohledu zákaznických dat zpracovává vystavené faktury, komunikace probíhá zabezpečeným šifrovaným kanálem v aplikaci Crypta.

XXXXXXX – komunikační kanál s partnery (obchodními zástupci XXXXXXX a.s.), kterým se do XXX dostávají nové smlouvy se zákazníky, pořízené elektronicky přes aplikaci v tabletu včetně elektronického podpisu zákazníka. Obchodním zástupcům zůstane po odeslání smlouvy (do XXX) k dispozici pouze omezené množství informací o daném zákazníkovi a smlouvě.
Součástí aplikace XXXXXXXXX je aplikace XXXXXXXX, která tvoří mezičlánek mezi tabletem a XXX. Smlouva, která se uzavře na tabletu se propíše nejdříve do XXXXXXXX a odtud poté do XXX. K této části mobilního obchodníka mají přístup interní zaměstnanci XXXXXXXXXX a.s., příp. administrativní pracovníci partnera, pro kontrolu smluvních údajů a následné potvrzení přesunu nové smlouvy do XXX. Část aplikace XXXXXXX slouží také ke správě samotných tabletů a uživatelů (zakládání přístupových hesel, blokování uživatelů a tabletů atp., zobrazení polohy tabletu/uživatele).

XXX vrstva – informační systém pro řízení kontaktního centra XXXXXXXXXXXXXX a.s. Z pohledu zpracovávaných dat jsou zde uloženy veškeré probíhající i historicky uzavřené telefonické kampaně. Tato data se do XXX dostávají prostřednictvím xls sestav (obsahujících osobní údaje zákazníků) generovaných z XXX a následně importovaných do XXX. V systému XXX jsou také spravovány zvukové nahrávky hovorů (uloženy v aplikaci XXXXXXXX) a vyhodnocení realizovaného kontaktu s klientem.

XXX– do XXX jsou ukládány veškeré dokumenty získané v souvislosti s uzavřením a případnou změnou smlouvy. Dále také veškerá korespondence se zákazníky. Uložené scany jsou dostupné z XXX (odkazem z karty zákazníka).

Provize – účelová aplikace využívaná mimo jiné i externím subjektem k výpočtu provizí partnerům – obchodním zástupcům společnosti XXXXXXXXXXXXXX a.s. Aplikace čerpá data o zákaznících a uzavřených smlouvách z XXX. V této aplikaci však dochází pouze k předzpracování, finální přepočet provize je prováděn mimo tento systém (I.2.).

13. K tomu kontrolovaný 7. července 2021 předložil grafický přehled jednotlivých procesů zpracování a jim odpovídající pracovní zařazení/role, provádějící zpracování dat. U externích rolí *se jedná o případy využívání služeb dalších zpracovatelů nebo případ spolupráce s dalšími správci. V obou těchto případech je tato spolupráce smluvně ošetřena s odpovídajícím vymezením povinností dle nařízení (EU) 2016/679.*

Přístupová oprávnění jsou udělována v souladu s interní podnikovou metodikou, do aplikací se přihlašuje uživatel uživatelským jménem a heslem, *výměna hesel je do počítačové techniky prováděna vždy na výzvu systému 1 x za 3 měsíce, nebo uživatelem kdykoliv.*

To kontrolovaný doložil seznamem zaměstnanců a jejich pracovních pozicí s vyznačením jejich konkrétních přístupů do informačních systémů. Dále předložil popis jednotlivých pracovních míst *(I.2.).*

14. Kontrolovaný 7. července 2021 předložil interní dokument *Směrnice XXXX, zpracování osobních údajů zákazníků a potenciálních zákazníků*, účinný od 1. března 2021. Směrnice stanovuje závazné pokyny, instrukce a postupy, práva a povinnosti zaměstnanců kontrolovaného při zpracování osobních údajů zákazníků a případně potenciálních zákazníků kontrolovaného. Směrnice je platná pro všechny útvary, vedoucí zaměstnance a ostatní zaměstnance kontrolovaného a další osoby v obdobném vztahu k němu, kteří v rámci své pracovní činnosti provádějí zpracování osobních údajů. Je zde stanovena povinnost

mlčenlivosti o osobních údajích a o bezpečnostních opatřeních k jejich ochraně, která trvá i po skončení zaměstnaneckého poměru.

V bodě 6.1. je mimo jiné uvedeno, že kontrolovaný je správcem osobních údajů svých zákazníků, správcem registru SOLUS je sdružení SOLUS, zájmové sdružení právnických osob, IČ: 69346925.

Osobní údaje zákazníka kontrolovaný dále předá pouze v případě, *pokud příjemcům bude svědčit zákonný důvod pro přístup k osobním údajům (orgány činné v trestním řízení, Energetický regulační úřad, jiné kontrolní orgány se zákonným zmocněním pro přístup k informacím) nebo pokud to bude nezbytné pro ochranu jeho práv (soudní nebo správní řízení) nebo se souhlasem zákazníků.*
Jestliže dochází k předávání osobních údajů třetím osobám, kontrolovaný *bez zbytečného odkladu informuje příjemce osobních údajů, kterým údaje zpřístupnila, o blokování, opravě, doplnění nebo likvidaci takových osobních údajů v souladu se zásadou zajištění přesnosti a úplnosti zpracovávaných údajů.*
V bodě 6.3. *Zpracovávané osobní údaje* je mimo jiné uvedeno, že obecně může kontrolovaný pořizovat kopie dokladu totožnosti pouze se souhlasem zákazníka. Zákazník mu není povinen udělit takovýto souhlas s pořízením kopie svého dokladu totožnosti. V takovémto případě pořídí pouze výpis z předložených dokladů včetně záznamu o tom, kdo, kdy a z jakého dokladu provedl ověření totožnosti zákazníka.

V bodě 6.6.1 je mimo jiné uvedeno, že kontrolovaný vede záznamy o činnostech zpracování, které tvoří přílohu směrnice.

Záznamy o činnostech jsou zpracovány zvlášť ke každému procesu zpracování osobních údajů, a to:
- *XXXXXXX, Kontaktní centrum. Řízení obchodních kampaní a zákaznických center* Účel zpracování – *uzavření, změny a ukončení smluv se zákazníky,* čl. 6. odst.1 písm. b) nařízení (EU) 2016/679).
Kategorie subjektů údajů – aktivní zákazníci (uzavřená smlouva o poskytování služeb, nebo mobilní službu XXXX), potenciální zákazníci (telefonickým, e-mailovým nebo webovým kanálem vyjádřili požadavek na uzavření smlouvy o dodávce služeb), ztracení zákazníci (mají s kontrolovaným ukončenou/odvolanou smlouvu o poskytování služeb, nebo *mobilní službu XXXXXX)*.
Dále dokument obsahuje rozsah osobních údajů, výčet příjemců osobních údajů, *plánované* lhůty pro výmaz osobních údajů (5 let od ukončení smlouvy, 1 rok u smluv, které nenabyly účinnosti a jsou ukončené).
Bod VI. uvádí způsob zpracování osobních údajů a popis technických a organizačních bezpečnostních opatření.

- *Procesy Finance zákazníků*
Účel zpracování – *správa zákaznických smluv, zpracování plateb, saldo, účtování, pohledávky,* čl. 6. odst.1 písm. b) a f) nařízení (EU) 2016/679).
Kategorie subjektů údajů – aktivní zákazníci (uzavřená smlouva o poskytování služeb, nebo mobilní službu XXXXX), ztracení zákazníci (mají s kontrolovaným ukončenou/odvolanou smlouvu o poskytování služeb, nebo *mobilní službu XXXXX)*.
Dále dokument obsahuje rozsah osobních údajů, výčet příjemců osobních údajů, *plánované* lhůty pro výmaz osobních údajů (nejdéle 10 let od ukončení posledního smluvního vztahu).

Bod VI. uvádí způsob zpracování osobních údajů a popis technických a organizačních bezpečnostních opatření.

- *Procesy Řízení vztahů se zákazníky*

Účel zpracování – *nabídka produktů a služeb, přímý marketing,*
čl. 6. odst.1 písm. f) nařízení (EU) 2016/679), *propagace služeb svým zákazníkům.*
Kategorie subjektů údajů – aktivní zákazníci (uzavřená smlouva o poskytování služeb, nebo mobilní službu XXXXX), potenciální zákazníci (telefonickým, e-mailovým nebo webovým kanálem vyjádřili požadavek na uzavření smlouvy o dodávce služeb), ztracení zákazníci (mají s kontrolovaným ukončenou/odvolanou smlouvu o poskytování služeb, nebo *mobilní službu XXXXX),* ztracení zákazníci (mají s kontrolovaným ukončenou/odvolanou smlouvu o poskytování služeb, nebo *mobilní službu XXXXXX)*.
Dále dokument obsahuje rozsah osobních údajů, výčet příjemců osobních údajů, *plánované* lhůty pro výmaz osobních údajů (doba uchování po dobu trvání smlouvy, pokud smlouva nenabyla účinnosti, je doba uchování záznamů *5 let (od data plánované účinnosti u smluv, které nenabyly účinnosti a zároveň nejsou ukončené (smlouvy jsou stále v platnosti) nebo do opt-out zákazníka.*
Bod VI. uvádí způsob zpracování osobních údajů a popis technických a organizačních bezpečnostních opatření.

Účel zpracování – *nabídka produktů a služeb, marketing,*
čl. 6. odst.1 písm. a) nařízení (EU) 2016/679), souhlas je kontrolovanému *udělován pro zasílání obchodních sdělení.*
Kategorie subjektů údajů – zákazníci, potenciální zákazníci (telefonickým, e-mailovým nebo webovým kanálem vyjádřili souhlas s nabízením obchodu a služeb).
Dále dokument obsahuje rozsah osobních údajů, výčet příjemců osobních údajů, *plánované* lhůty pro výmaz osobních údajů (doba uchování po dobu udělení souhlasu nebo do jeho odvolání).
Bod VI. uvádí způsob zpracování osobních údajů a popis technických a organizačních bezpečnostních opatření.

- *Procesy útvaru Marketingu*

Účel zpracování – *jednání s potenciálními zákazníky,*
čl. 6. odst.1 písm. a) nařízení (EU) 2016/679) – *opatření nezbytná před uzavřením smlouvy na žádost subjektu údajů.*
Kategorie subjektů údajů – potenciální zákazník (jakákoliv osoba, *která projeví zájem o uzavření smluvního vztahu na prodej komodit* s kontrolovaným*)*.
Dále dokument obsahuje rozsah osobních údajů, výčet příjemců osobních údajů (zprostředkovatelé, call centrum), *plánované* lhůty pro výmaz osobních údajů (doba uchování záznamů 6 měsíců).
Bod VI. uvádí způsob zpracování osobních údajů a popis technických a organizačních bezpečnostních opatření.

- *Procesy útvaru Podpora a rozvoj obchodu*

Účel zpracování – *uzavření a změny smlouvy se zákazníky*
čl. 6. odst.1 písm. b) nařízení (EU) 2016/679),
Kategorie subjektů údajů – aktivní zákazníci (uzavřená smlouva o poskytování služeb, nebo mobilní službu XXXXX), potenciální zákazníci (telefonickým, e-mailovým nebo webovým

kanálem vyjádřili požadavek na uzavření smlouvy o dodávce služeb), ztracení zákazníci (mají s kontrolovaným ukončenou/odvolanou smlouvu o poskytování služeb, nebo *mobilní službu XXXXX),* ztracení zákazníci (mají s kontrolovaným ukončenou/odvolanou smlouvu o poskytování služeb, nebo *mobilní službu XXXXX)*.
Dále dokument obsahuje rozsah osobních údajů, výčet příjemců osobních údajů, *plánované* lhůty pro výmaz osobních údajů (doba uchování záznamů 5 let od ukončení smlouvy, 1 rok u smluv, které nenabyly účinnosti a jsou ukončené, 5 let *(od data plánované účinnosti u smluv, které nenabyly účinnosti a zároveň nejsou ukončené (smlouvy jsou stále v platnosti).*
Bod VI. uvádí způsob zpracování osobních údajů a popis technických a organizačních bezpečnostních opatření.

Kontrolovaný má dále zpracované záznamy o činnostech
- *Procesy útvaru Péče o zaměstnance (docházkový a přístupový systém, nábor zaměstnanců, provoz kamerového systému se záznamem, správa pracovního poměru,*
čl. 6. odst.1 písm. b) a f) nařízení (EU) 2016/679)

V bodě 7.2 směrnice je podrobně popsán proces při vyřizování žádostí o výkon práva subjektu údajů *(I.2.).*

15. Kontrolovaný 7. července 2021 předložil interní dokumenty:
Pracovní postup GDPR Anonymizace, platný od 23.7.2020, upravující pravidla anonymizace od zákazníků přijímaných fyzických dokumentů (např. občanský průkaz, rodný list, oddací list, výpis bankovního účtu, nájemní smlouva, výpis z katastru nemovitostí a další).
Pracovní postup GDPR Elektronická anonymizace, platný od 29. července 2020, upravující pravidla anonymizace osobních údajů z PDF dokumentu, nebo datového souboru. To doložil otisky obrazovek z informačního systému XXX, ze kterých je patné, že kontrolovaný používá začerňování nadbytečných osobních údajů (úmrtní list, občanský průkaz, oddací list) (*I.2. a 3.).*

16. Kontrolovaný 7. července 2021 předložil interní dokument *Směrnice LZ07, Pokyny pro uživatele ICT vybavení*, účinný od 1.7.2020, stanovující závazné pokyny instrukce a postupy pro uživatele pro zajištění bezpečnosti a důvěrnosti informací. Dokument je závazný pro všechny zaměstnance kontrolovaného *(I.2.).*

17. Dalším předloženým dokumentem 7. července 2021 je *Směrnice LZ10, Spisový, archivační a skartační řád*, účinný od 25.5.2018 *(I.2.).*

18. Kontrolovaný 7. července 2021 písemně uvedl, že získává osobní údaje *od:*
- smluvních partnerů *(*rozsah osobních údajů – nezbytný pro uzavření smlouvy*).* Právní základ zpracování čl. 6 odst. 1 písm. b) plnění smlouvy / opatření nezbytná před uzavřením smlouvy na žádost subjektu údajů;
- ze svých webových stránek (subjekt údajů projeví zájem o služby a zadá své kontaktní údaje (telefonní číslo) do kontaktního formuláře (rozsah – jméno, příjmení, telefonní číslo). Právní základ zpracování čl. 6 odst. 1 písm. b) opatření nezbytná před uzavřením smlouvy na žádost subjektu údajů;
- smluvních call center – *na základě volání na náhodně generovaná čísla z rozsahu zveřejněného Českým telekomunikačním úřadem, pokud držitel čísla projeví zájem o námi nabízené komodity/služby a pokud tento souhlasí s předáním jeho osobních údajů*

kontrolovanému *pro účely oslovení s nabídkou* (rozsah – jméno, příjmení, PSČ, informace o odběru komodit, telefonní číslo*), právní základ zpracování čl. 6 odst. 1 písm. a) souhlas subjektů údajů.*

Kontrolovaný písemně uvedl, že *nevyužívá pro získání osobních údajů fyzických osob žádné komerční databáze a důsledně dbá na to, aby pro každý ze subjektů údajů vždy věděl, z jakého zdroje byly osobní údaje získány (a na základě jakého právního základu jsou zpracovávány).*
K tomu kontrolovaný doložil seznam konkrétních zdrojů osobních údajů, a to v rozsahu název/jméno, IČ, sídlo, forma zpracování (např. Zasílání leadů ke zpracování komoditních smluv, zprostředkovatelská smlouva, partnerská smlouva, *XXXX - Partnerská smlouva)* a účel zpracování (např. *generuje leady*, uzavírání obchodních smluv, zprostředkování a uzavírání komoditních smluv).

Kontrolovaný předložil otisk obrazovky z databáze XXX, ze které je patrné, že v části *podrobnosti* je uveden zdroj (Ušetřeno.cz s.r.o.), způsob uzavření smlouvy – *M – mimo prostory obvyklé.*

Dále předložil dva záznamy telefonního hovoru *smluvního call centra* při získávání osobních údajů pro kontrolovaného. Volající se představil svým jménem, uvedl, že je energetický poradce a volaného neoslovil jménem (pane). Mimo jiné uvedl, zda by mu mohl zavolat specialista ze společnosti XXXXXX. V hovoru zazní i rozsah předávaných osobních údajů, které XXXXXXX předají, a to jméno, příjmení, PSČ a tel. číslo.

Ve druhém záznamu telefonního hovoru se volající představil jménem a uvedl, že volá ze společnosti XXXXX. Volaného jménem neoslovil, sám volaný mu sdělil v průběhu hovoru svoje jméno, příjmení, číslo telefonu a PSČ a souhlasil s voláním specialisty XXXXXXXXXXX a.s. v domluveném termínu (volající uvedl začátek tel. čísla, ze kterého bude volat a to, že zákazníci XXXXXXXXXXXX ušetří ročně…). V obou hovorech volající uvedl odkaz na webové stránky kontrolovaného, kde jsou uvedeny informace o zpracování osobních údajů a o jeho právech na odvolání souhlasu. Na závěr se zeptal, zda s tím volaný souhlasí. *(I.2.).*

19. Kontrolovaný 7. července 2021 *písemně* uvedl, že využívá zpracovatele především pro uzavírání smluv se zákazníky. *Vzhledem k tomu, že smlouvy jsou těmito zpracovateli uzavírány mimo obchodní prostory, dochází ke zpracování i mimo místo, kde má zpracovatel sídlo. Místo uzavření smlouvy je určitelné prostřednictvím GPS souřadnic tabletu, který mají tito zpracovatelé k dispozici. Jedná se o tablet, prostřednictvím kterého jsou uzavřené smlouvy při zapojení datového přenosu předávány do XXX. V ostatních případech dochází ke zpracování v místech sídla zpracovatele.*

Předložený seznam zpracovatelů (XXX zpracovatelů) a míst zpracování odpovídá k 28. červenci 2021 zveřejněnému seznamu zpracovatelů, popsanému v bodě 6. kontrolních zjištění.

Pro aktualizaci seznamu zpracovatelů má kontrolovaný vytvořen interní dokument *Pracovní postup, GDPR – Aktualizace seznamu zpracovatelů*, platný od 23. července 2020.

V reakci na dotaz Úřadu ve věci zařazení distributorů komodit do seznamu zpracovatelů a žádosti zaslání *Rámcové smlouvy o zajištění služby distribuční soustavy* a *Smlouvy o zpracování osobních údajů* se společností XXXXXXXXX, a.s., kontrolovaný dne 29. září 2021 Úřad písemně informoval o změně seznamu zpracovatelů osobních údajů, a to o *vyřazení*

osob, které mají vlastnické či jiné právo k distribuční soustavě dle z. č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů. Nový seznam je popsán v bodě 6. kontrolních zjištění a liší se oproti seznamu z 28. července 2021 o cca. 50 právnických osob, o které byl seznam ponížen *(I.2. a I.8.13).*

20. Kontrolovaný 7. července 2021 předložil bianko jednotlivé typy zpracovatelských smluv, a to např.:

- *Smlouva o obchodní spolupráci,* ve které je kontrolovaný v roli *poskytovatel*e a zpracovatel je označen jako *partner.*

V bodě IV. smlouvy je mimo jiné ujednání o tom, že partner bude jako zpracovatel zpracovávat osobní údaje zákazníků kontrolovaného/správce v souladu s nařízením (EU) 2016/679. Dokument dále v bodě V. obsahuje povinnost mlčenlivosti.

Nedílnou součástí smlouvy je mimo jiné příloha č. 2 *Etický kodex* a příloha č. 4 *Zpracování osobních údajů.* V něm se zpracovatel zavazuje na základě pověření správce a v souladu s právními předpisy a touto přílohou provádět zpracování. V příloze jsou upraveny podmínky zpracování osobních údajů, práva a povinnosti správce a závazků zpracovatele vůči správci, mimo jiné o vzájemném informování o průběhu a závěrech kontroly ze strany Úřadu.

Dokument obsahuje mimo jiné ujednání o technických a organizačních opatřeních, zaručujících přiměřený stupeň zabezpečení s ohledem na riziko týkající se důvěrnosti, integrity, disponibility a odolnosti systémů. Smlouva zakazuje zpracovateli zapojit dalšího zpracovatele bez předchozího písemného povolení kontrolovaného. Osobní údaje zpracovávané zpracovatelem jsou v rozsahu jméno, příjmení, bydliště, kontaktní adresa, datum narození, rodné číslo, bankovní spojení, e-mail, telefonní číslo. Údaje o odběrném místě a údaje o smluvním vztahu subjektu údajů. Součástí dodatku je uveden výčet technických a organizačních opatření, která se zpracovatel zavazuje přijmout a dodržovat po celou dobu trvání smlouvy.

- *Smlouva o obchodní spolupráci pro hypoteční makléře a finanční poradce č.,* ve které je kontrolovaný v roli *poskytovatel*e a zpracovatel je označen jako *partner.*

V bodě IV. smlouvy je mimo jiné ujednání o tom, že partner bude jako zpracovatel zpracovávat osobní údaje zákazníků kontrolovaného v souladu s nařízením (EU) 2016/679. Dokument dále v bodě V. obsahuje povinnost mlčenlivosti.

Nedílnou součástí smlouvy je mimo jiné příloha č. 2 *Etický kodex* a příloha č. 4 *Zpracování osobních údajů.* V něm se zpracovatel zavazuje na základě pověření správce a v souladu s právními předpisy a touto přílohou provádět zpracování. V příloze jsou upraveny podmínky zpracování osobních údajů, práva a povinnosti správce a závazků zpracovatele vůči správci, mimo jiné o vzájemném informování o průběhu a závěrech kontroly ze strany Úřadu.

Dokument obsahuje mimo jiné ujednání o technických a organizačních opatřeních, zaručujících přiměřený stupeň zabezpečení s ohledem na riziko týkající se důvěrnosti, integrity, disponibility a odolnosti systémů. Dokument zakazuje zpracovateli zapojit dalšího zpracovatele bez předchozího písemného povolení kontrolovaného. Osobní údaje zpracovávané zpracovatelem jsou v rozsahu jméno, příjmení, bydliště, kontaktní adresa, datum narození, rodné číslo, bankovní spojení, e-mail, telefonní číslo. Údaje o odběrném místě a údaje o smluvním vztahu subjektu údajů. Součástí dodatku je výčet technických a organizačních opatření, která se zpracovatel zavazuje přijmout a dodržovat po celou dobu trvání smlouvy.

- *Smlouva o obchodní spolupráci – místo obvyklé č.:,* ve které je kontrolovaný v roli poskytovatele/správce a zpracovatel je označen jako partner.
V bodě V. smlouvy je mimo jiné ujednání o tom, že partner bude jako zpracovatel zpracovávat osobní údaje zákazníků kontrolovaného v souladu s nařízením (EU) 2016/679. Dokument dále v bodě VI. obsahuje povinnost mlčenlivosti.
Nedílnou součástí smlouvy je mimo jiné příloha č. 2 *Etický kodex* a příloha č. 4 *Zpracování osobních údajů*. V něm se zpracovatel zavazuje na základě pověření správce a v souladu s právními předpisy a touto přílohou provádět zpracování. V příloze jsou upraveny podmínky zpracování osobních údajů, práva a povinnosti správce a závazků zpracovatele vůči správci, mimo jiné o vzájemném informování o průběhu a závěrech kontroly ze strany Úřadu.
Dokument obsahuje mimo jiné ujednání o technických a organizačních opatřeních, zaručujících přiměřený stupeň zabezpečení s ohledem na riziko týkající se důvěrnosti, integrity, disponibility a odolnosti systémů. Dokument zakazuje zpracovateli zapojit dalšího zpracovatele bez předchozího písemného povolení kontrolovaného. Osobní údaje zpracovávané zpracovatelem jsou v rozsahu jméno, příjmení, bydliště, kontaktní adresa, datum narození, rodné číslo, bankovní spojení, e-mail, telefonní číslo. Údaje o odběrném místě a údaje o smluvním vztahu subjektu údajů. Součástí dodatku je výčet technických a organizačních opatření, která se zpracovatel zavazuje přijmout a dodržovat po celou dobu trvání smlouvy.

- *Smlouva o zprostředkování,* ve které je kontrolovaný v roli poskytovatele/správce a zprostředkovatel je v roli zpracovatele.
V bodě IV. smlouvy je mimo jiné ujednání o tom, že bude jako zpracovatel zpracovávat osobní údaje zákazníků kontrolovaného v souladu s nařízením (EU) 2016/679. Dokument dále v bodě V. obsahuje povinnost mlčenlivosti.
Nedílnou součástí smlouvy je mimo jiné příloha č. 1 *Zpracování osobních údajů zákazníků*. V něm se zpracovatel zavazuje na základě pověření správce a v souladu s právními předpisy a touto přílohou provádět zpracování. V příloze jsou upraveny podmínky zpracování osobních údajů, práva a povinnosti správce a závazků zpracovatele vůči správci, mimo jiné o vzájemném informování o průběhu a závěrech kontroly ze strany Úřadu.
Dokument obsahuje mimo jiné ujednání o technických a organizačních opatřeních, zaručujících přiměřený stupeň zabezpečení s ohledem na riziko týkající se důvěrnosti, integrity, disponibility a odolnosti systémů. Dokument zakazuje zpracovateli zapojit dalšího zpracovatele bez předchozího písemného povolení kontrolovaného. Osobní údaje zpracovávané zpracovatelem jsou v rozsahu jméno, příjmení, bydliště, kontaktní adresa, datum narození, rodné číslo, bankovní spojení, e-mail, telefonní číslo. Údaje o odběrném místě a údaje o smluvním vztahu subjektu údajů. Součástí dodatku je výčet technických a organizačních opatření, která se zpracovatel zavazuje přijmout a dodržovat po celou dobu trvání smlouvy *(I.2.).*

- *Smlouva o zprostředkování,* ve které je kontrolovaný v roli poskytovatele/správce a zpracovatel je označen jako zprostředkovatel.
V bodě IV. smlouvy je mimo jiné ujednání o tom, že bude jako zpracovatel zpracovávat osobní údaje zákazníků kontrolovaného v souladu s nařízením (EU) 2016/679. Dokument dále v bodě V. obsahuje povinnost mlčenlivosti.
Nedílnou součástí smlouvy je mimo jiné příloha č. 1 *Zpracování osobních údajů zákazníků*. V něm se zpracovatel zavazuje zpracovávat osobní údaje pouze pro účely plnění smlouvy,

a to v rozsahu *jméno, příjmení, bydliště, kontaktní adresa, datum narození, rodné číslo, bankovní spojení, e-mail, tel. číslo ad.), údaje o odběrném místě subjektu údajů (adresa odběrného místa, EAN/EIC, popř. číslo elektroměru/plynoměru ad.), a údaje o smluvním vztahu subjektu údajů (výše záloh, plateb, ročních vyúčtování, spotřeb včetně historie a údajů o případném porušení smluvní povinnosti zákazníkem ad.).*
V příloze jsou upraveny podmínky zpracování osobních údajů, práva a povinnosti správce a závazků zpracovatele vůči správci, mimo jiné o vzájemném informování o průběhu a závěrech kontroly ze strany Úřadu.
Dokument obsahuje mimo jiné ujednání o technických a organizačních opatřeních, zaručujících přiměřený stupeň zabezpečení osobních údajů. Dokument zakazuje zpracovateli zapojit dalšího zpracovatele bez předchozího písemného povolení kontrolovaného. Součástí dodatku je výčet technických a organizačních opatření, která se zpracovatel zavazuje přijmout a dodržovat po celou dobu trvání smlouvy *(I.2.).*

21. Kontrolovaný 7. července 2021 předložil *Smlouvu o zpracování osobních údajů*, uzavřenou se společností XXXXXXXXXXX s.r.o., 23. prosince 2019, která je přílohou *Podkladové smlouvy* – smlouvy o spolupráci. Zpracovatel (XXXXXXXX s.r.o.) bude pro správce/kontrolovaného zpracovávat osobní údaje v rozsahu rodného čísla, které správce – kontrolovaný získal, nebo získá v souvislosti se svou podnikatelkou činností, nebo které pro správce za tímto účelem získá samotný zpracovatel. Smlouva mimo jiné obsahuje ujednání o zárukách technického a organizačního a zabezpečení ochrany osobních údajů.
V bodě 6.3. smlouvy je mimo jiné uvedeno, že zpracovatel je oprávněn pověřit zpracováním osobních údajů dalšího zpracovatele. Je zde uvedeno šest společností, což vzal kontrolovaný ve smlouvě na vědomí.

K tomu kontrolovaný 24. srpna 2021 písemně uvedl, že nebyl společností XXXXXXXXX s.r.o., informován o zapojení dalších zpracovatelů.
Dále uvedl, že XXXXXXX *s.r.o., má i další zpracovatele, avšak ti nevykonávají zpracování osobních údajů upravené Smlouvou o zpracování osobních údajů,* ze dne 23. prosince 2019*.*
- Zpracovatel XXXXXXXXXX pro XXXXXXX s.r.o., zajišťuje mechanickou skartaci vyřazených dokumentů na základě Smlouvy o mechanické likvidaci dokumentů ze dne 22. 2. 2018;
- Zpracovatel XXXXXXXXXX s.r.o., zajišťuje kurýrní/zasilatelské služby v rámci sjednávání smluv s klienty na základě Smlouvy o poskytování zasilatelských služeb ze dne 4. 8. 2017;
- Zpracovatel XXXXXX pro XXXXXXX s.r.o., zajišťuje služby v souvislosti s provozováním callcentra (virtuální ústředna, nahrávání hovorů apod.) na základě Smlouvy o poskytování telekomunikačních služeb;
- Zpracovatel XXXXXXX pro XXXXXXX s.r.o., zajišťuje služby v souvislosti s provozem on premise cloudu na základě Smlouvy o poskytování telekomunikačních služeb ze dne 24. 2. 2016;
- Zpracovatel MICROSOFT pro XXXXXXXXXX s.r.o., zajišťuje zejména licencování a služby v oblasti produktů MS Office na základě licenčních smluv uzavíraných v souladu s Podmínkami pro produkty, Podmínkami pro služby online a Dodatkem k ochraně osobních údajů;
- Zpracovatel Google pro XXXXXXXX s.r.o., zajišťoval zejména licencování a služby v oblasti produktů XXXX na základě Smlouvy o používání služby XXXXX (online), nicméně uvedené řešení bylo v průběhu nahrazeno řešením od MICROSOFT.

Dne 4. října 2021 kontrolovaný (správce) předložil *Dohodu o zpracování údajů (dále také „Dohoda“) v souladu s ustanoveními článku 28 obecného nařízení o ochraně osobních údajů (dále také „GDPR“),* uzavřenou se společností XXXXXXXXXXXXXXXXXXXXXX, a.s.

(zpracovatel) dne 18. března 2020. Předmětem dohody je zpracování osobních údajů v souvislosti s uzavíráním obchodů na trhu zpracovatele pro konečné zákazníky, a to na základě účastnické smlouvy. Dokument obsahuje mimo jiné ujednání o technických a organizačních opatřeních. Porušení dohody je sankcionováno.

22. Kontrolovaný dále 17. září 2021 předložil *Smlouvu o zpracování osobních údajů* č. P3A18000014197, uzavřenou společností XXXXXXXXXXXXXXX, a.s., dne 17. července 2018 (jako distributorem/správcem) s kontrolovaným (jako dodavatelem/zpracovatelem) ve vazbě na *Rámcovou smlouvu o zajištění služby distribuční soustavy* č. 13250354_RSD_2016_D_00 (předložena kontrolovaným).

Účelem smlouvy je závazek kontrolovaného provádět zpracování osobních údajů pro distributora. V čl. II smlouvy distributor pověřuje kontrolovaného ke zpracování osobních údajů v rozsahu *jméno, příjmení, titul, název společnosti, zastupující osoba/osoby, e-mail, telefonní spojení, datum narození, IČO, DIČ, EAN, adresa trvalého bydliště obec, adresa trvalého bydliště místní část, adresa trvalého bydliště ulice, adresa trvalého bydliště č.p./č.o., adresa trvalého bydliště PSČ, adresa fakturační/zasílací obec, adresa fakturační/zasílací místní část, adresa fakturační /zasílací ulice, adresa fakturační/zasílací č.p./č.o., adresa fakturační/zasílací PSČ, adresa odběrného místa obec, adresa odběrného místa místní část, adresa odběrného místa ulice, adresa odběrného místa č.p/č.o., adresa odběrného místa PSČ, katastrální území, parcelní číslo, patro/ č. bytu, jméno a příjmení - kontaktní osoba pro zpřístupnění, e-mail - kontaktní osoba pro zpřístupnění, telefonní číslo - kontaktní osoba pro zpřístupnění, jméno a příjmení - kontaktní osoba pro technická jednání, e-mail - kontaktní osoba pro technické záležitosti, telefonní spojení - kontaktní osoba pro technické záležitosti, typ měření, číslo elektroměru, stav elektroměru, zákaznické číslo, podpis.*
Smlouva obsahuje mimo jiné ujednání o povinnosti kontrolovaného zavedení vhodných technických a organizačních opatření, povinnosti mlčenlivosti. Porušení smlouvy je sankcionováno. Jedná se o smlouvu jednocestnou, z žádného ustanovení nevyplývá jiný vztah.
K tomu kontrolovaný 17. září 2021 písemně doplnil, že ve vztahu k osobním zákazníkům se distributor a kontrolovaný *mohou nacházet v pozici dvou samostatných správců osobních údajů* (kontrolovaný pro účely dodávky komodity, distributor pro účely dodání technického vybavení) a v pozici správce a zpracovatele osobních údajů, a to pokud distributor pro kontrolovaného prostřednictvím svého technického vybavení získává informace nezbytné pro fakturaci *(např. objem odebrané komodity, kterou XXX zákazníkovi fakturuje)* a naopak v případě, pokud kontrolovaný pro distributora získává osobní údaje nezbytné pro účely umístění technického zařízení, za které je zákazník odpovědný přímo distributorovi *(I.2. - I.5.).*
23. Kontrolovaný 7. července 2021 písemně uvedl, že ke dni zahájení kontroly zpracovával osobní údaje 179810 subjektů údajů, z toho 333 zaměstnanců, včetně osob v obdobném postavení.
Potenciální zákazníky nelze přesně identifikovat; odhad leadů (zpracováno 50–100 denně), které jsou zpracovávány nejdéle 6 měsíců (pokud není uzavřena smlouva, nebo neprobíhá jednání o uzavření smlouvy) *(I.2.).*

24. Dále kontrolovaný 7. července 2021 písemně uvedl, že *k ochraně osobních údajů, řízení aktiv společnosti a jejího know-how využívá systém ochrany dat (Data Loss Protection –* dále také „DLS*"), který řídí i jednotlivé činnosti zaměstnanců. Jedná se o nadstavbu systému,*

kde na základě nastavené hodnoty systém vyhodnocuje rizikovost (kritičnost) dat nebo zamezuje přístupům či nakládání s těmito daty.
Systém řídí a kontroluje *(online i ad hoc report) i ostatní periferie, které jsou-li připojené k uživatelské stanici, jež porušují interní obecná pravidla společnosti XXXXXXXXXXXXXXXXXXX a.s. Systém vyhodnotí, že mohlo dojít k porušení bezpečnostní politiky, která byla v systému nastavena (např. USB pro vložení média) a tuto aktivitu zablokuje. Jedná se o prevenci exportu jakékoliv databáze společnosti, aktiv společnosti.*
Systém je nastaven na tři úrovně, blokace, justifikace, notifikace. Obsluha bezpečnostního systému je informována o porušení bezpečnostní politiky a dle nastavené struktury žádá podání zprávy od uživatele (zaměstnance), ale i nadřízeného uživatele. Na základě takto vyhodnocené situace je přijato opatření k uvedení věci do pokojného stavu. K tomu kontrolovaný předložil popis jeho nastavení.

Kontrolovaný předložil otisk obrazovky z logu XXX systému; je z něj patrné datum a čas změny (20.5.2021), událost (*aktualizovat, nastavit stav, přiřadit*), který uživatel změnu provedl, záznam (*doložené usnesení, potvrzení přijetí reklamace*), nad jakou entitou XXX systému (*formulář, tel. hovor, dopis*), typ operace. K tomu kontrolovaný předložil seznam uživatelů s přístupem do systému XXX a jim přidělených systémových rolí.
K aplikaci mobilní obchodník (aplikační nástavba XXX určená pro tabletové řešení) kontrolovaný uvedl, že tato poskytuje obchodníkům v terénu *nástroj pro podepisování komoditních smluv se zákazníky. Podepsané smlouvy jsou napárovány do XXX systému. Logování je zajištěno v centrálním systému XXX.*

Z důvodu odcizení *dat, neoprávněné manipulaci na tabletu je na chytrém zařízení instalována aplikace XXXXXXXXXXXXX XXXXXXXXXXXXX od společnosti XXXXXXXXXXX, která tvoří chráněné, šifrované uložiště v tabletu. Aplikace v případě* odcizení *tabletu umožnuje smazání celé chráněné části, veškerého obsahu tabletu (reset do továrního nastavení). Po uzavření smluvního vztahu a podpisu smlouvy jsou tato data exportována včetně podpisu do XXX šifrovaným kanálem.* Dále uvedl, že šifrovací klíč (certifikát) využívá *v případě zabezpečené komunikace v důvěrné obchodní korespondenci mezi bankou a společností XXXXXXXXXX a.s., a to zejména při převodu nebo zadávání finančních transakcí.*

Kontrolovaný má stanovenou minimální dobu pro uchování elektronických záznamů na 6 měsíců pro všechny IT systémy a aplikace, maximální doba pro uchování elektronických záznamů je nastavena na 18 měsíců. *Přístup k elektronickým záznamům je omezen na roli administrátora příslušného systému/aplikace a vedoucího příslušného oddělení nebo jeho zástupce.*

Výstupy ze zastřešujícího bezpečnostního nástroje DLP pravidelně zpětně vyhodnocuje *(I.2.).*

25. Kontrolovaný 7. července 2021 mimo jiné písemně uvedl, že *v roce 2019 byla provedena analýza rizik ve vztahu k IT systémům XXXXXXXXXXXXX, a.s., která identifikovala další rizikové oblasti. Na základě této analýzy byla přijata dodatečná bezpečnostní zařízení. Zahájena byla příprava společnosti na certifikaci ISO 2700 (stále v procesu) a bylo dokončeno zavedení systému DLP (I.2.).*

26. K plnění informační povinnosti kontrolovaný 7. července 2021 písemně uvedl, že zákazníci a potenciální zákazníci jsou informováni prostřednictvím:
- informace umístěné na jeho webových stránkách (popsáno v bodě 5. kontrolních zjištění),

- informací umístěnou ve smluvních formulářích, kterou kontrolovaný předložil (odkaz na *Zpracování osobních údajů společností XXXXXXXXXXXXXXX, a.s.“,* který je též dostupný na webových stránkách XXXXXXXXXXXXXXXXXXXXX),
- informace umístěná v předsmluvní informaci (odkaz na *webovou stránku XXXXXXXXXXXXXX),* schváleno k implementaci,
- v rámci telefonních hovorů, což doložil nahrávkami (popsáno v bodě 18. kontrolních zjištění).

Informační povinnost vůči zaměstnancům (*Metodický postup, GDPR – LZ06 Zpracování osobních údajů zaměstnanců,* platný od 1. září 2020); kontrolovaný předložil dokument *Seznámení se směrnicemi* ze dne 15. června 2021, ze kterého je patné, že zaměstnanec podepisuje, že byl seznámen s obsahem směrnic kontrolovaného (včetně směrnic týkajících se ochrany osobních údajů).

Informační povinnost vůči partnerům je uvedena ve smlouvách o obchodní spolupráci (popsáno v bodě 19. kontrolních zjištění).

Informační povinnost vůči návštěvníkům webových stránek XXXXXXXXXXXX je plněna prostřednictvím cookies banneru s možností volby nastavení a podrobnými informacemi o nasazených cookies (popsáno v bodě 9. kontrolních zjištění).

K tomu kontrolovaný doplnil, že od roku 2020 *pracují kompetentní zaměstnanci společnosti XXXXXXXXXXXXXXXXX a.s. na aktualizaci smluvní a informační dokumentace (I.2.).*

Kontrolovaný 24. srpna 2021 písemně uvedl, že proces aktualizace zveřejněných informací, popsaných v bodě 5. a 6. kontrolních zjištění byl (před zahájením kontroly) *postaven na tom*, *že v zájmu komplexnosti jednotlivé útvary XXX doplňovaly do seznamu zpracovatelů zpracovatele autonomně* s cílem, aby seznam zpracovatelů uvedený na webových stránkách kontrolovaného byl zveřejněn vždy v aktuální podobě. Nesoulad byl způsoben aktualizací seznamu zpracovatelů. Na základě zahájení kontroly *byla provedena revize nastavení procesů a bylo zjištěno, že právě autonomie aktualizace seznamu zpracovatelů, kdy nedocházelo k průběžné revizi zadaných údajů, vedla k tomu, že došlo k chybnému zařazení některých entit do seznamu zpracovatelů, přestože tam být uvedeny neměly.*
Kontrolovaný dále uvedl, že přijal v této souvislosti technická o organizační opatření, a to mimo jiné připravuje *školení odpovědných pracovníků jednotlivých útvarů a nastavení kontroly aktualizovaného seznamu pověřencem pro ochranu osobních údajů před jeho zveřejněním.*
K dokumentu *Informace pro zákazníky o zpracování osobních údajů společností XXXXXXXXXXXXXXXXXXX, a.s.*, účinnému od 25. května 2018 a popsanému v bodě 5. kontrolních zjištění, kontrolovaný 24. srpna 2021 písemně uvedl, že *na podzim 2020 byl zahájen proces nastavení nového způsobu a aktualizace obsahu plnění informační povinnosti vůči subjektům údajů. Původní předpoklad realizace byl duben 2021. Proces byl současně spojen s aktualizací obsahu a vizuální úpravou veškeré zákaznické smluvní dokumentace, což však bohužel celý proces poněkud prodloužilo a k realizaci tak došlo až na přelomu června a července 2021 (I.3.).*

27. Kontrolovaný 7. července 2021 písemně uvedl, že do 10. června 2021 přijal celkem *42 žádostí podle obecného nařízení (EU) 2016/679, z čehož bylo jedno uplatněné právo dle čl. 21 (námitka), ostatní uplatněná práva byla dle čl. 17 (výmaz).*

Doložil, že vede evidenci uplatněných žádostí (obsahuje datum, označení v XXX a stav, v jakém se daná žádost nachází) a přijal a předložil metodický pokyn obsahující vzorové odpovědi pro žádosti uplatněné podle nařízení (EU) 2016/679. Postup při vypořádání žádostí upravuje interní závazný předpis *Směrnice LZ09*, popsaný v bodě 13. kontrolních zjištění.

Kontrolovaný předložil dvě odpovědi stěžovatelům, a to
- paní XXXXXXXXXXXXX, která 31. března 2021 požádala (e-mailem) o nahrávku a vyjádření k nevyžádanému hovoru a požádala o nepoužívání jejího telefonního čísla k marketingovým účelům. Kontrolovaný jí dne 30. dubna 2021 písemně (e-mailem) sdělil, že byla volána jeho smluvním partnerem – společností XXXXX s.r.o. a uvedl, že číslo *bylo náhodně vygenerováno z databáze možných rozsahů telefonních čísel zveřejněné Českým telekomunikačním úřadem. Vaše takto náhodně vygenerované telefonní číslo není evidováno v žádné společnosti XXXXXXXXX dostupné databázi, a není tak spojené s žádným či jiným identifikačním údajem konkrétní osoby. V našem systému tedy neevidujeme žádné Vaše osobní údaje. Taktéž sdělujeme, že hovor byl vymazán po splnění účelu, neboť subjekt údajů nedal souhlas s nahrávaným hovorem…*
- pana XXXXXXXXXX, který 15. ledna 2021 e-mailem požádal o vymazání svého tel. čísla z databáze, kontrolovaný (pověřenec) mu 12. února 2021 stejnou cestou sdělil, že na základě jeho žádosti o výmaz jakýchkoliv osobních údajů, které o něm zpracovává, provedl veškeré kroky ke zjištění, zda byl nebo nebyl z jeho strany, či strany jeho spolupracujících subjektů kontaktován, na základě čehož mu sdělil, že jeho osobní údaje kontrolovaný, ani jeho spolupracující subjekty nezpracovávají *(I.2.).*

28. Kontrolovaný 7. července 2021 písemně uvedl, že každý zaměstnanec je informován o problematice nakládání s osobními údaji v rámci vstupního školení, které se koná po nástupu na pracovní pozici. V rámci úvodního školení jsou zaměstnanci seznámeni se směrnicemi společnosti, které jsou pro zaměstnance závazné. Seznámení se směrnicemi stvrzuje zaměstnanec podpisem dokumentu *Seznámení se směrnicemi;* to kontrolovaný doložil kopií *Seznámení se směrnicemi* ze dne 15. června 2021, ze kterého je patné, že zaměstnankyně JB svým podpisem stvrdila, že byla seznámena s obsahem v dokumentu vyjmenovaných směrnic, mj. *Zpracování osobních údajů zákazníků a potenciálních zákazníků* a že rozumí jejich obsahu. Dále předložil přehled přijatých opatření k zabezpečení osobních údajů s vyznačením, zda jsou aplikována, nebo částečně aplikována.

Kontrolovaný předložil interní dokument *Pracovní postup GDPR na ZC*, platný od 22. července 2020, ve kterém je mimo jiné stanovena povinnost vedení registru incidentů a *Pracovní postup Registr bezpečnostních incidentů OÚ GDPR*, platný od 30.7.2020, který vedení záznamů o bezpečnostních incidentech podrobně upravuje. Bod 3. pracovního postupu upravuje vyhodnocení míry rizika a následných kroků (*I.2.).*

Hodnocení zjištěných skutečností

29. <u>k čl. 4 bodu 1 nařízení (EU) 2016/679</u>

Kontrolou bylo zjištěno, že v souvislosti s předmětem kontroly jsou zpracovávány osobní údaje subjektů údajů minimálně v rozsahu: jméno a příjmení, adresa trvalého bydliště, kontaktní adresa, e-mail, telefonní číslo, datová schránka, v případě dodávky elektřiny a plynu číslo zákaznického účtu, údaje o smluvním vztahu, zejména výše záloh, plateb, měsíčních a ročních vyúčtováních, spotřebě, včetně historie produktu, typ a objem

využívaných služeb, informace o využívání produktu, adrese odběrného místa, o údajích případného porušení smluvní povinnosti, výši plateb, o telefonním čísle, rodném čísle, čísle OP, datu narození, adrese, telefonním čísle, e-mailu, partnerovi, o datu úmrtí, dědickém usnesení, insolvenci, schválení oddlužení, údaje o čerpaných a využitých bodech, odměnách, výhodách, o historii nákupů, komunikaci, informace o IP adrese zákazníka, o čísle SIPO, cookies, záznamy z kamerového systému, nahlížení a vkládání údajů do registru dlužníků SOLUS.

V případě telekomunikačních služeb zpracovává kontrolovaný údaje v rozsahu telefonní číslo volaného, telefonní číslo volajícího, začátek a konec spojení, datum a frekvence uskutečněného spojení, IMEI, typ zařízení, konfigurační údaje, adresa datového spojení (např. URL), IP adresa, druh, způsob a objem využívání služeb, cena za službu, typové chování), provozní lokalizační údaje (zeměpisná poloha koncového zařízení), a to za účelem plnění právních povinností (kontrolní zjištění 5).

Jedná se o osobní údaje podle ustanovení čl. 4 bod 1 nařízení (EU) 2016/679.

30. k čl. 4 bod 2 nařízení (EU) 2016/679

Kontrolovaný zpracovává osobní údaje subjektů údajů jak manuálně, tak automatizovaně (např. shromažďuje, vyhledává, uchovává, přenáší data) v rozsahu nezbytném pro daný účel (kontrolní zjištění 5.).

Nakládání s osobními údaji kontrolovaným vykazuje pojmové znaky zpracování podle čl. 4 bodu 2 nařízení (EU) 2016/679.

31. k čl. 4 bod 7 nařízení (EU) 2016/679

Z kontrolního zjištění uvedeného v bodu 5. vyplývá, že se v případě kontrolovaného jedná o správce osobních údajů podle čl. 4 bod 7 nařízení (EU) 2016/679, který určuje účely zpracování osobních údajů a rozsah zpracovávaných osobních údajů. Hlavním účelem zpracování osobních údajů kontrolovaným je především jeho podnikatelská činnost v oblasti obchodu s elektřinou a zemním plynem, a s tím související zpracování osobních údajů, zejména za účelem předsmluvního jednání, plnění smlouvy, plnění právních povinností správce, ochrany oprávněného zájmu správce a marketingu.

Kontrolovaný má určeny účely zpracování osobních údajů, je tedy v pozici správce podle ustanovení čl. 4 bod 7 nařízení (EU) 2016/679.

32. k čl. 4 bod 8 nařízení (EU) 2016/679

Z kontrolního zjištění uvedeném v bodech 19. a 20. vyplývá, že pro kontrolovaného, jakožto správce osobních údajů, jsou osobní údaje zpracovávány velkým počtem zpracovatelů (více než 500), se kterými má kontrolovaný uzavřené např. smlouvy o zprostředkování, smlouvy o obchodní spolupráci a smlouvy o obchodní spolupráci pro hypoteční makléře a finanční poradce. Subjekty, které zpracovávají osobní údaje pro kontrolovaného jsou v pozici zpracovatelů podle ustanovení čl. 4 bod 8 nařízení (EU) 2016/679.

V případě společnost XXXXXXXXXXXXXX, a.s. a cca 50 dalších subjektů je kontrolovaný v pozici zpracovatele (kontrolní zjištění 6. a 22.).

Porovnání zjištěného stavu věci s relevantním ustanovením nařízení EU 2016/679

33. k čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679

Kontrolou bylo zjištěno, že kontrolovaný zpracovává osobní údaje zákonným způsobem k legitimním účelům. Subjekt údajů je srozumitelně a transparentně informován o účelech zpracování, rozsahu zpracovávaných údajů, době zpracování, právních titulech zpracování, o zdrojích osobních údajů, právech subjektů údajů a dalších záležitostech v zájmu zajištění zákonného a spravedlivého zpracování ve vztahu k dotčeným subjektům údajů. Kontrolou bylo zjištěno, že se v období od 28. července 2021 do 29. září 2021 nacházela v seznamu zpracovatelů umístěném na webových stránkách kontrolovaného nesprávná informace o tom, že jsou společnost XXXXXXXXXXXXXXX, a.s. a cca 50 dalších subjektů zpracovateli kontrolovaného, přičemž podle obsahu jednotlivých smluv byli tito v postavení správců a kontrolovaný zpracovatel. Tato nesprávná informace byla kontrolovaným dne 29. září 2021 napravena tak, že ze seznamu zpracovatelů společnost XXXXXXXXXXXXXXX, a.s. a cca 50 dalších subjektů odstranil. Kontrolující vyhodnotili výše uvedenou nesprávnou informaci kontrolovaného jako porušení čl. 12 odst. 1 nařízení (EU) 2016/679, popsanou v bodě 38. kontrolních zjištění.

Nebylo zjištěno porušení čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679.

34. k čl. 5 odst. 1 písm. b) nařízení (EU) 2016/679

Kontrolou nebylo zjištěno, že by kontrolovaný shromažďoval či zpracovával osobní údaje pro jiné než výslovně stanovené a legitimní účely, kterými jsou zejména předsmluvní jednání, plnění smlouvy, plnění právních povinností správce, ochrana oprávněných zájmů správce a zasílání obchodních sdělení, marketing a ověřování bonity či platební morálky zákazníka v registru dlužníků SOLUS (kontrolní zjištění č. 5). Nebylo prokázáno, že by zpracovatelé kontrolovaného zpracovávali osobní údaje v rozporu s účely stanovenými kontrolovaným ve *Smlouvách o zpracování osobních údajů*.

Nebylo zjištěno porušení čl. 5 odst. 1 písm. b) nařízení (EU) 2016/679.

35. k čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679

Podle čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679 *osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů“).* Bylo zjištěno, že kontrolovaný zpracovává relevantní a přiměřené osobní údaje a v rozsahu nezbytném ve vztahu k jednotlivým účelům zpracování.

Nebylo zjištěno porušení čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679.

36. k čl. 5 odst. 1 písm. e) nařízení (EU) 2016/679

Kontrolovaný má jednotlivé doby uchovávání osobních údajů uvedeny na svých webových stránkách XXXXXXXXXXXXXXX, v dokumentu *Informace pro zákazníky o zpracování osobních údajů společností XXXXXXXXXXXXXXX.* Doby uchovávání osobních údajů jsou v dokumentu uvedeny podle účelu zpracování osobních údajů. (např. zasílání obchodních sdělení se souhlasem zákazníka je ukončeno odvoláním souhlasu zákazníka a dále se např. v případech ochrany oprávněného zájmu správce osobní údaje mažou maximálně po 3 létech od doby počátku zpracování údajů, nestanoví-li zvláštní právní předpisy jinak. Nebylo prokázáno, že by kontrolovaný uchovával osobní údaje subjektů údajů po dobu delší, než je nezbytné pro účely, pro které jsou stanoveny (blíže kontrolní zjištění 5. a 27.).

Nebylo zjištěno porušení čl. 5 odst. 1 písm. e) nařízení (EU) 2016/679.

37. k čl. 6 nařízení (EU) 2016/679, zákonnost zpracování

Podle čl. 6 odst. 1 nařízení (EU) 2016/679 je *zpracování zákonné, v případě, že byla splněna nejméně jedna z podmínek uvedených v č. 6 odst. 1 písm. a) až f)* nařízení (EU) 2016/679.
Z kontrolního zjištění 5. vyplývá, že kontrolovaný zpracovává osobní údaje v souvislosti se zasíláním obchodních sdělení a marketingem pouze se souhlasem zákazníka podle čl. 6 odst. 1 písm. a) nařízení (EU) 2016/679. Zákazník je kontrolovaným informován prostřednictvím formuláře *Zpracování osobních údajů společnosti XXXXXXXXXXXX, a.s*. (popsaným v bodě 7. kontrolních zjištění) o účelu poskytování souhlasu, rozsahu poskytovaných osobních údajů, době zpracování, jakož i o jeho právech souvisejících se zpracováním osobních údajů. Kontrolovaný splňuje podmínky k tomu, aby jeho zákazník/fyzická osoba mohl uplatnit svobodný, konkrétní a jednoznačný projev vůle při poskytování souhlasu ve smyslu čl. 4 odst. 11) nařízení (EU) 2016/679. Souhlas zákazníka kontrolovaného je dobrovolný a nemá vliv na uzavření smlouvy.
Podle čl. 6 odst. 1 písm. b) nařízení (EU) 2016/679 zpracovává kontrolovaný osobní údaje za účelem předsmluvních jednání a plnění smluv. Za účelem plnění právní povinnosti správce podle čl. 6 odst. 1 písm. c) nařízení (EU) 2016/679, jsou kontrolovaným zpracovávány osobní údaje, jejichž zpracování vyplývá z obecně platných právních předpisů. Dále kontrolovaný zpracovává osobní údaje ve veřejném zájmu podle čl. 6 odst. 1 písm. e) nařízení (EU) 2016/679, který se jako právní titul zpracování osobních údajů uplatní tam, kde převažují legitimní zájmy/práva správce nad zájmy/právy zákazníků, a to při zohlednění přiměřeného očekávání zákazníků na základě jeho vztahu se správcem. Jedná se zejména o ochranu základních či jiných důležitých práv kontrolovaného vyplývajících z obecně závazných právních předpisů a smluv v rámci různých sporů, kontrol, šetření, řízení a ve vztahu k smluvním partnerům a třetím osobám, dále o ochranu majetku kontrolovaného, vymáhání pohledávek právní cestou a ochranu zájmu správce v souvislosti s vyhodnocováním bonity či platební morálky zákazníka (kontrolní zjištění 7.)

Nebylo zjištěno porušení čl. 6 odst. 1 nařízení (EU) 2016/679.

38. k čl. 12 nařízení (EU) 2016/679 - Transparentní informace, sdělení a postupy pro výkon práv subjektu údajů v souvislosti s poskytováním informací v rozsahu čl. 13 a 14 nařízení (EU) 2016/679

Povinností kontrolovaného je zajistit, aby zákazník obdržel transparentním, srozumitelným a snadno přístupným způsobem veškeré potřebné informace týkající se zpracování jeho osobních údajů. Informace týkající se ochrany osobních údajů jsou uvedeny na webových

stránkách kontrolovaného v dokumentu *Zpracování osobních údajů společností XXXXXXXXXXXX, a.s*. a dále jsou obsaženy v předsmluvní informaci, která je umístěna na webových stránkách kontrolovaného (kontrolní zjištění č. 5.) a dále ve formulářích smluv. Informace pro zaměstnance kontrolovaného o nakládání s osobními údaji a jejich zpracováním a ochranou je kontrolovaným doložena dokumentem *Seznámení se směrnicemi,* ze dne 15. června 2021, jehož obsahem je také ochrana osobních údajů (kontrolní zjištění č. 26. a 28.). Informační povinnost vůči partnerům je uvedena ve smlouvách o obchodní spolupráci (kontrolní zjištění bod 19. a 20.). Informační povinnost vůči návštěvníkům webových stránek kontrolovaného je plněna prostřednictvím cookies banneru s možností volby nastavení a podrobnými informacemi o nasazených cookies. Kontrolovaný uvedl, že od roku 2020 pracuje na aktualizaci smluvní a informační dokumentace, která bude ukončena ve třetím čtvrtletí roku 2021. Kontrolovaný má zpracovaný interní dokument *Směrnice LZ09*, *zpracování osobních údajů zákazníků a potenciálních zákazníků*, ve kterém je v bodě 7.2 podrobně popsán proces při vyřizování žádostí o výkon práva subjektu údajů. Dále má zpracovaný interní dokument *Pracovní postup GDPR na ZC*, ve kterém je mimo jiné stanovena povinnost vedení registru incidentů a *Pracovní postup Registr bezpečnostních incidentů OÚ GDPR*, který vedení záznamů o bezpečnostních incidentech podrobně upravuje. Bod 3. pracovního postupu upravuje vyhodnocení míry rizika bezpečnostních incidentů a následných kroků (kontrolní zjištění č. 28.).

V seznamu zpracovatelů, který kontrolovaný zveřejňuje na svých webových stránkách se minimálně od 28. července 2021 do 29. září 2021 nacházela nesprávná informace o cca 50 zpracovatelích kontrolovaného, kteří jsou ve *Smlouvách o zpracování osobních údajů* označeni jako správci a kontrolovaný jako zpracovatel osobních údajů, čemuž také odpovídají jeho povinnosti při zpracování, zabezpečení a ochraně osobních údajů, které pro něj ze smluv vyplývají. Tato nesprávná informace byla kontrolovaným napravena tím, že ze seznamu svých zpracovatelů odstranil ke dni 29. září 2021 cca 50 subjektů, které jsou ve *Smlouvách o zpracování osobních údajů* označeni jako správci osobních údajů (kontrolní zjištění 19. a 21.). Kontrolovaný se zveřejněním seznamu zpracovatelů sám označil za správce, jak je popsáno v bodě 6. kontrolních zjištění.

Informace, které je kontrolovaný jako správce osobních údajů povinen poskytnout subjektům údajů podle čl. 13 a 14 nařízení (EU) 2016/679, jsou kontrolovaným uvedeny v dokumentu *Zpracování osobních údajů společností XXXXXXXXXXXXXXX, a.s*., který je zveřejněn na webových stránkách kontrolovaného.

Bylo zjištěno porušení čl. 12 odst. 1 nařízení (EU) 2016/679, jelikož kontrolovaný uváděl minimálně od 28. července 2021 do 29. září 2021 na svých webových stránkách v seznamu zpracovatelů nesprávnou informaci o cca 50 zpracovatelích, kteří jsou podle obsahu *Smluv o zpracování osobních údajů* správci osobních údajů, nikoli zpracovatelé, přičemž se zveřejněním seznamu zpracovatelů sám označil za správce.

39. <u>k čl. 15 až 21 nařízení (EU) 2016/679, práva subjektu údajů</u>

V dokumentu zveřejněném na webových stránkách kontrolovaného *Informace pro zákazníky o zpracování osobních údajů společností XXXXXXXXXXXXXXXXXX, a.s*., poskytuje kontrolovaný zákazníkům podrobné informace o jejich právech v souvislosti s ochranou osobních údajů podle článku 15 až 21 nařízení (EU) 2016/679, včetně příslušného komentáře (kontrolní zjištění 5.).

Kontrolou nebylo zjištěno porušení povinností stanovených v čl. 15 až 21 nařízení (EU) 2016/679.

40. k čl. 28 nařízení (EU) 2016/679 - zpracovatel

Z kontrolních zjištění vyplývá, že kontrolovaný má velký počet zpracovatelů, kteří se podílejí na zpracování osobních údajů, které kontrolovaný využívá ke své obchodní činnosti. Kontrolovaný využívá zpracovatele především pro uzavírání smluv se zákazníky. Kontrolovaný má se zpracovateli uzavřené např. smlouvy o zprostředkování, smlouvy o obchodní spolupráci a smlouvy o obchodní spolupráci pro hypoteční makléře a finanční poradce. Kontrolovaným uzavřené smlouvy se zpracovateli obsahují požadované náležitosti podle článku 28 odst. 3 nařízení (EU) 2016/679. Seznam zpracovatelů je uveden na webových stránkách kontrolovaného XXXXXXXXXXXXXXXXXXXXXXX. Nedílnou součástí každé smlouvy se zpracovatelem je příloha č. 1 - *Zpracování osobních údajů zákazníků*, kde se zpracovatel zavazuje na základě pověření správce a v souladu s právními předpisy a touto přílohou provádět zpracování osobních údajů dle platných právních předpisů. V příloze smlouvy jsou upraveny podmínky zpracování osobních údajů, práva a povinnosti správce a závazků zpracovatele vůči správci a dále ujednání o technický a organizačních opatřeních, zaručujících přiměřený stupeň zabezpečení s ohledem na riziko týkající se důvěrnosti, integrity, disponibility a odolnosti systémů. Podle přílohy se zpracovateli zakazuje zapojit dalšího zpracovatele bez předchozího písemného povolení kontrolovaného. Součástí přílohy je výčet technických a organizačních opatření, která se zpracovatel zavazuje přijmout a dodržovat po celou dobu trvání smlouvy. Pro aktualizaci seznamu zpracovatelů má kontrolovaný vytvořen interní dokument *Pracovní postup, GDPR – Aktualizace seznamu zpracovatelů*. V příloze č. 2 smlouvy je Etický kodex, podle kterého se zpracovatel zavazuje na základě pověření správce a v souladu s právními předpisy a touto přílohou provádět zpracování osobních údajů (kontrolní zjištění 19. a 20.).

Nebylo zjištěno porušení ustanovení čl. 28 nařízení (EU) 2016/679.

41. k čl. 30 nařízení (EU) 2016/679, záznamy o činnostech pracování

Záznamy o činnostech zpracování osobních údajů upravuje kontrolovaný v příloze interní Směrnice *LZ09* – zpracování *osobních údajů zákazníků a potenciálních zákazníků*. Záznamy o činnostech jsou zpracovány zvlášť ke každému procesu zpracování osobních údajů.
Záznamy o činnostech obsahují kontaktní údaje správce, zástupce správce, pověřence pro ochranu osobních údajů, dále obsahují účely zpracování osobních údajů, popis jednotlivých kategorií subjektů údajů, výčet příjemců osobních údajů, *plánované* lhůty pro výmaz osobních údajů, způsob zpracování osobních údajů a popis technických a organizačních bezpečnostních opatření (kontrolní zjištění 14.).

Nebylo zjištěno porušení povinností stanovených v čl. 30 nařízení (EU) 2016/679.

42. k čl. 32. (EU) 2016/679, zabezpečení zpracování

Dokument *Informace pro zákazníky o zpracování osobních údajů XXXXXXXXXXXXXX, a.s*. obsahuje v úvodu informaci pro zákazníky, a to, že *kontrolovaný chrání veškeré*

zpracovávané údaje jako přísně důvěrné a nakládá s nimi v souladu s platnými právními předpisy v oblasti ochrany osobních údajů. Informace pro zaměstnance kontrolovaného o nakládání s osobními údaji a jejich zpracováním a ochranou je kontrolovaným doložena dokumentem *Seznámení se směrnicemi,* ze dne 15. června 2021, jehož obsahem je také ochrana osobních údajů. Zaměstnanec podepisuje, že byl seznámen s obsahem směrnic týkajících se ochrany osobních údajů. Ujednání o ochraně osobních údajů a jejich zabezpečení je součástí jednotlivých smluv uzavřených se zpracovateli. Na formuláři *Žádosti o přenesení osobních údajů*, který je dostupný na webových stránkách kontrolovaného je informace, že přenášené osobní údaje jsou zabezpečené šifrováním.

Kontrolovaný provádí logování přístupů v systému XXX, přičemž předložil seznam uživatelů s přístupem do systému XXX a jim přidělených systémových rolí (kontrolní zjištění 24.).

Nebylo zjištěno porušení povinností stanovených v čl. 32 nařízení (EU) 2016/679.

43. K čl. 37 a 38 nařízení (EU) 2016/679

Kontrolovaný má jmenovaného pověřence pro ochranu osobních údajů dle čl. 37 nařízení (EU) 2016/679, aniž by mu povinnost jeho jmenování z tohoto ustanovení vyplývala. Jeho kontaktní údaje zveřejnuje a tuto skutečnost oznámil Úřadu. V průběhu kontroly byl pověřenec zapojen do záležitostí souvisejících s ochranou osobních údajů (kontrolní zjištění 2., 7. a 15.).

Kontrolou nebylo zjištěno porušení čl. 37 a 38. nařízení (EU) 2016/679.

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:

Ing. Zdeňka Filová	vedoucí kontrolní skupiny pověřená zaměstnankyně Úřadu	*(podepsáno elektronicky)* podpis
JUDr. Roman Recman	pověřený zaměstnanec Úřadu	*(podepsáno elektronicky)* podpis