

1. Společnost

1.1 Společnost se zabývá prodejem elektřiny a zemního plynu

2. Úvodní ustanovení

2.1 Účel a působnost

2.1.1 Cílem této směrnice (dále jen "**Směrnice**") je vytvořit rámec standardů a postupů pro ochranu osobních údajů v rámci činností Společnosti.

2.1.2 Směrnice upravuje povinnosti Společnosti, jejích funkcionářů a zaměstnanců, kteří se podílejí na zpracování osobních údajů v rámci činnosti Společnosti při zpracovávání osobních údajů.

2.1.3 Ustanovení Směrnice jsou závazná pro všechny osoby, při jejichž činnosti dochází ke zpracování osobních údajů ve Společnosti, tedy k jakékoliv operaci s osobními údaji, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení; nebo jejichž činnost souvisí se zabezpečením (zajištěním ochrany) osobních údajů.

2.1.4 Ustanovení Směrnice doplňují Záznamy o činnostech zpracování (dále jen "**Záznamy**") podrobně upravující nakládání s osobními údaji v rámci Společnosti. Metodický pokyn musí být v souladu se Směrnicí a jeho součástí jsou Záznamy o činnostech zpracování.¹ Metodický pokyn schvaluje tajemník Společnosti.

2.1.5 Směrnice nabývá účinnosti dne 25. května 2018.

2.2 Vymezení právních předpisů

2.2.1 Právní předpisy EU a výkladová stanoviska pracovních skupin

- (i) 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/EU ("**Nařízení GDPR**");
- (ii) Pokyny a Vodítka Pracovní skupiny pro ochranu údajů zřízenou podle článku 29 ("**Pokyny WP 29**");
- (iii) směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV ("**Směrnice GDPR**");
- (iv) směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti ("**Směrnice PNRD**").

2.2.2 Národní legislativa a výkladová stanoviska

- (i) Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů;
- (ii) Návrh zákona o zpracování osobních údajů;
- (iii) Návrh zákona o změně zákonů související s přijetím zákona o zpracování osobních údajů.

¹ Dokument povinně vypracovává Společnosti podle čl. 30 Nařízení GDPR.

3. Vymezení Pojmů

Analýza rizik	prověření, jaká rizika představuje zpracování osobních údajů pro dotčené subjekty údajů;
Automatizované zpracování	zpracování uskutečňované zcela nebo zčásti pomocí automatizovaných postupů, zahrnuje operace jako ukládání na nosiče dat, provádění logických operací s těmito daty, jejich změny, vymazání, vyhledávání nebo rozšiřování;
DPIA	pokud je na základě analýzy rizik pravděpodobné, že určitý druh zpracování představuje, byť potenciálně, vysoké riziko pro práva a svobody dotčených subjektů údajů, musí být provedena detailní analýza rizik, která se nazývá DPIA neboli posouzení vlivu. DPIA má předepsaný obsah a postup dle čl. 35-36 Nařízení GDPR;
Evidence	jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska; není-li řečeno jinak, v podmínkách Společnosti se evidencí rozumí každá evidence listinná (spisová) i elektronická, jejíž součástí jsou osobní údaje;
Likvidace osobních údajů	nezvratné zničení, jehož cílem je znemožnění dalšího zpracování;
Osobní údaj	veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;
Porušení zabezpečení osobních údajů	porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;
Pověřenec pro ochranu osobních údajů (DPO)	řádně jmenovaná osoba, jejímž úkolem je plnit funkci koordinátora ochrany osobních údajů a zároveň funkci kontaktního bodu pro komunikaci s dozorovým úřadem;
Příjemce	fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli; ²

² Orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují, zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování.

Pseudonymizace	zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.
Souhlas subjektu údajů	jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;
Správce	fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení; není-li řečeno jinak, v podmínkách Společnosti se správcem rozumí Společnosti;
Subjekt údajů	každá fyzická osoba, jejíž osobní údaje jsou zpracovávány.
Třetí strana	fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jenž je oprávněna ke zpracování osobních údajů;
Úřad	Úřad pro ochranu osobních údajů jakožto příslušný dozorový úřad v oblasti ochrany osobních údajů;
Vlastník procesů	zaměstnanec nebo organizační jednotka Společnosti, která v rámci své činnosti provádí nebo bude provádět zpracování osobních údajů a současně za něj zodpovídá;
Zpracování osobních údajů	jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;
Zpracovatel	fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce; není-li řečeno jinak, v podmínkách Společnosti se zpracovateli rozumí dodavatelé služeb a další osoby, které v rámci plnění pro Společnosti zpracovávají osobní údaje předávané Společnosti;

Zvláštní kategorie osobních údajů

údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby;

4. Zásady zpracování osobních údajů ve společnosti

Níže uvedené zásady zpracování osobních údajů ve Společnosti jsou základními principy, které musí být pro každé zpracování osobních údajů v rámci Společnosti vždy dodržovány. Žádné nové zpracování osobních údajů ve Společnosti nesmí být zahájeno, pokud není v souladu s těmito zásadami. Při zpracování osobních údajů Společnost a další osoby, které se podílejí na zpracování osobních údajů a jsou vázány touto Směrnicí, dbají na to, aby zpracování osobních údajů probíhalo v souladu se zásadami pro zpracování osobních údajů, které jsou stanoveny níže v tomto článku. Společnost ctí základní práva a svobody subjektů údajů, zejména respektování jejich soukromého a rodinného života, obydli a komunikace.

4.1 Zásady zpracování osobních údajů

4.1.1 Společnost jako správce osobních údajů odpovídá za to, že zpracování osobních údajů bude probíhat v souladu s níže uvedenými zásadami a musí být schopna toto dodržení souladu doložit a prokázat ("**zásada odpovědnosti**").

Směrnice spolu s Metodickým pokynem a procesy kontroly jejich dodržování jsou hlavními dokumenty, jež plnění zásady odpovědnosti v rámci Společnosti dokládají.

4.1.2 Jakékoliv zpracování osobních údajů ve Společnosti musí být prováděno korektně a zákonným, spravedlivým a transparentním způsobem ("**zásada zákonnosti, korektnosti a transparentnosti**"). Zásada zákonnosti znamená, že osobní údaje mohou být zpracovávány pouze na základě jednoho nebo více právních titulů vyjmenovaných v čl. 6 Nařízení GDPR, zejména ke splnění smlouvy se subjektem osobních údajů, k naplnění právní povinnosti uložené Společnosti, při výkonu veřejné moci, kterým je pověřena Společnost, na základě oprávněného zájmu Společnosti, souhlasu svobodně daného subjektem anebo pro další vyjmenované právní tituly. O tom, pro jaký právní titul jsou osobní údaje zpracovávány, vede Společnost záznam v příslušném dokumentu Záznamy o činnostech zpracování.

4.1.3 Zásada korektnosti a transparentnosti vyžaduje, aby všechny informace a všechna sdělení týkající se zpracování těchto osobních údajů byly snadno přístupné a srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků. Pro subjekty údajů musí být transparentní, jak jsou osobní údaje, které se jich týkají, shromažďovány, používány, konzultovány nebo jinak zpracovávány, jakož i v jakém rozsahu tyto osobní údaje jsou či budou zpracovány.

Tato zásada se dotýká zejména informování subjektů údajů o totožnosti správce a účelech zpracování a o dalších záležitostech v zájmu zajištění spravedlivého a transparentního zpracování ve vztahu k dotčeným fyzickým osobám, včetně jejich práva získat informace o zpracovávaných osobních údajích, které se jich týkají. Fyzické osoby by měly být upozorněny na to, jaká rizika, pravidla, záruky a práva existují v souvislosti se zpracováním jejich osobních údajů a jak mají v souvislosti s tímto zpracováním uplatňovat svá práva. Zejména je zapotřebí, aby konkrétní účely, pro které jsou osobní údaje zpracovávány, byly jednoznačné a legitimní a aby byly stanoveny v okamžiku shromažďování osobních údajů.

Osobní údaje by měly být zpracovány pouze tehdy, nemůže-li být účelu zpracování přiměřeně dosaženo jinými prostředky. Aby se zajistilo, že osobní údaje nebudou uchovávány déle, než je nezbytné, stanoví Společnost lhůty pro výmaz nebo pravidelný přezkum platnosti a potřebnosti osobních údajů, a to ve Skartačním řádu Společnosti. Měla by být přijata veškerá vhodná opatření, aby nepřesné osobní údaje byly opraveny nebo vymazány. Osobní údaje by měly být zpracovávány způsobem, který zaručí náležitou bezpečnost a důvěrnost těchto údajů, mimo jiné za účelem zabránění neoprávněnému přístupu k osobním údajům a k zařízení používanému k jejich zpracování nebo jejich neoprávněnému použití.

4.1.4 Osobní údaje musí být shromažďovány pro určité konkrétní, výslovně a jednoznačně vyjádřené a legitimní účely, které mají být stanoveny v okamžiku shromažďování osobních údajů a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný ("**zásada účelového omezení**").

4.1.5 Zpracovávané osobní údaje musí být přiměřené, relevantní a omezené na to, co je nezbytné z hlediska účelů, pro které jsou zpracovávány ("**zásada minimalizace údajů**").

- 4.1.6 Zpracovávané osobní údaje musí být přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny ("**zásada přesnosti**").
- 4.1.7 Osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány ("**zásada omezení uložení**"). Tato zásada je v podmínkách Společnosti naplňována především důsledným naplňováním a dodržováním lhůt obsažených ve Skartačním řádu Společnosti;
- 4.1.8 Osobní údaje musí být zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických a organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením ("**zásada integrity a důvěrnosti**").

5. Naplňování práv subjektů údajů

- 5.1 Společnosti řádně a včas naplňuje práva subjektů údajů vymezená v čl. 15 – 22 Nařízení GDPR. Podrobnosti naplňování práv subjektů údajů stanoví Metodický pokyn.
- 5.2 Společnost nezpracovává citlivé osobní údaje ve smyslu čl. 9 Nařízení GDPR.
- 5.3 Všichni funkcionáři a zaměstnanci Společnosti odpovídají ve svěřené oblasti činností Společnosti za vedení evidencí a procesů zpracování osobních údajů tak, aby umožňovaly řádně a hladké naplňování práv subjektů údajů.

6. Pověřenec pro ochranu osobních údajů

- 6.1 Pověřenec pro ochranu osobních údajů (DPO) musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a své schopnosti plnit úkoly DPO.
- 6.2 DPO je zaměstnancem Společnosti nebo vykonává činnost na základě příkazní smlouvy. Výkon funkce DPO je osobní.
- 6.3 DPO vykonává tyto úkoly:
- 6.3.1 poskytování informací a poradenství funkcionářům a členům orgánů Společnosti, zaměstnancům a dodavatelům Společnosti, kteří provádějí zpracování osobních údajů, o jejich povinnostech podle Nařízení GDPR a dalších právních předpisů v oblasti ochrany osobních údajů;
- 6.3.2 monitorování souladu činnosti Společnosti s Nařízením GDPR a dalšími právními předpisy v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy funkcionářů a zaměstnanců zapojených do operací zpracování a souvisejících auditů; v rámci této odpovědnosti bude DPO zejména:
- (i) předkládat předsedovi představenstva Společnosti jedenkrát ročně hodnotící zprávu o stavu ochrany osobních údajů ve Společnosti za uplynulé období;
 - (ii) dohlížet na soulad činnosti Společnosti s GDPR a dalšími předpisy v oblasti ochrany osobních údajů podle vlastního plánu dohledové činnosti a navrhnout organizaci opatření k dosahování plného souladu s GDPR a dalšími předpisy v oblasti ochrany osobních údajů.
 - (iii) poskytovat Společnosti a jejím zaměstnancům informace z oboru své působnosti podle aktuálních potřeb formou písemných stanovisek, příp. zajistit proškolení a také formou vyjádření a připomínek ke konkrétním otázkám předloženým mu Společnosti.
 - (iv) sledovat vývoj právní úpravy, stanoviska Úřadu pro ochranu osobních údajů a orgánů Evropské unie a rozhodovací činnost soudů v oblasti ochrany osobních údajů a přiměřeným způsobem o těchto skutečnostech informovat Společnosti.
 - (v) posuzovat návrhy významných dokumentů Společnosti týkajících se ochrany osobních údajů, zejména politik ochrany osobních údajů (směrnice pro ochranu osobních údajů, Záznamy) a dalších vnitřních předpisů, vzorů souhlasů se zpracováním osobních údajů, návrhů smluv o zpracování osobních údajů, vzorů podání a vyřízení, pokud jde o uplatňování práv subjektů údajů.
 - (vi) sledovat vývoj technologií souvisejících s ochranou osobních údajů a přiměřeným způsobem o něm informovat Společnosti.

- (vii) posuzovat soulad navrhovaných řešení v oblasti informačních a komunikačních technologií s pravidly ochrany osobních údajů.
 - (viii) přijímat a vyhodnocovat podání subjektů údajů v záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle GDPR. V případě, že nemůže podání vyřídit sám, vyžádá si od příslušných odborů podkladová stanoviska a následně zajistí řádné a včasné vyřízení předložených podání.
 - (ix) vést záznamy o činnostech zpracování podle čl. 30 GDPR.
 - (x) iniciovat audity bezpečnosti zpracování osobních údajů ve Společnosti a u jejích dodavatelů a evidovat záznamy o provedených auditech.
 - (xi) podílet se na plnění povinností organizace hlásit porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů (čl. 33 GDPR) a oznamovat porušení zabezpečení osobních údajů subjektům osobních údajů (čl. 34 GDPR).
- 6.3.3 poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle článku 35 Nařízení GDPR, příprava posudku ke každému připravovanému posouzení vlivu (DPIA);
- 6.3.4 zajišťování spolupráce s dozorovými úřady v oblasti ochrany osobních údajů (Úřad pro ochranu osobních údajů a Úřady práce); a
- 6.3.5 působení jako kontaktní místo pro dozorové úřady (zejména pro Úřad pro ochranu osobních údajů) v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36 Nařízení GDPR, a případně vedení konzultací v jakékoli jiné věci.
- 6.4 DPO bere při plnění svých úkolů patřičný ohled na riziko spojené s operacemi zpracování a současně přihlíží k povaze, rozsahu, kontextu a účelům zpracování.
- 6.5 Společnosti zajistí, aby byl DPO náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů v rámci Společnosti. Všichni funkcionáři a zaměstnanci Společnosti (včetně příslušných Vlastníků procesů) jsou povinni s DPO všestranně spolupracovat a poskytnout mu veškerou potřebnou součinnost.
- 6.6 Společnosti poskytne DPO odpovídající zdroje nezbytné k plnění jeho úkolů, k přístupu k osobním údajům a operacím zpracování a k udržování jeho odborných znalostí.
- 6.7 Společnosti zajistí, aby DPO nedostával žádné pokyny týkající se výkonu úkolů vymezených v odst. 5.3 výše. Pokud je DPO zaměstnancem Společnosti, v souvislosti s plněním svých úkolů nemůže být propuštěn ani sankcionován.
- 6.8 DPO je organizačně přímo podřízen předsedovi představenstva Společnosti, při výkonu funkce je nezávislý.
- 6.9 DPO působí jako kontaktní osoba organizace pro subjekty údajů ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle nařízení GDPR.
- 6.10 DPO je v souvislosti s výkonem svých úkolů vázán povinností mlčenlivosti v souladu se vzájemnou smlouvou, případně dohodou o mlčenlivosti, právem Evropské unie nebo České republiky.
- 6.11 DPO může plnit i jiné úkoly a povinnosti v rámci společnosti. Společnosti zajistí, aby žádné z těchto úkolů a povinností nevedly ke střetu zájmů.

7. Spolupráce s dozorovými úřady

- 7.1 Jakoukoliv komunikaci s dozorovými úřady včetně hlášení bezpečnostních incidentů na poli ochrany osobních údajů v rámci činnosti Společnosti vede výlučně DPO, popř. jeho zástupce nebo jiná určená osoba.
- 7.2 Všichni ostatní funkcionáři a zaměstnanci Společnosti jsou povinni poskytnout veškerou potřebnou součinnost k tomu, aby byla spolupráce s dozorovými orgány hladká a v rámci zákonných pravidel efektivní a s pozitivními výsledky pro Společnost.

8. Zásady vztahů společnosti se zpracovateli osobních údajů

- 8.1 Společnost spolupracuje pouze s těmi zpracovateli, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby prováděné zpracování splňovalo požadavky Nařízení GDPR a aby byla zajištěna ochrana práv subjektu údajů.
- 8.2 Zpracování zpracovatelem se řídí smlouvou o zpracování osobních údajů uzavřenou mezi příslušným zpracovatelem a Společností.
- 8.3 Při zpracování osobních údajů je zpracovatel povinen dbát, aby subjekty údajů, jejichž osobní údaje zpracovatel zpracovává, neutrpěli újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a dále je povinen dbát na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektů údajů.
- 8.4 Zpracovatel je povinen poskytnout veškerou potřebnou součinnost Společnosti tak, aby Společnosti byla schopna řádně a včas reagovat na žádosti fyzických osob o výkon jejich práv stanovených zejména v Nařízení GDPR (například práva na obdržení informací o zpracovávaných osobních údajích; práva na přístup k osobním údajům; práva být zapomenut; práva na omezení zpracování; práva na přenositelnost osobních údajů; práva vznést námitku); práva na opravu. Zpracovatel je dále povinen poskytnout veškerou potřebnou součinnost k zajištění zabezpečení zpracování osobních údajů, ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu, oznamování případů porušení zabezpečení osobních údajů fyzické osobě, jejíž osobní údaje jsou zpracovávány, posouzení vlivu na ochranu osobních údajů (tzv. „DPIA“), předběžných konzultací zpracování s dozorovým úřadem.
- 8.5 Zpracovateli mohou být subjekty s bydlištěm a/nebo sídlem jak na území České republiky, tak s bydlištěm a/nebo sídlem v členském státě Evropské unie. K předání a zpracování osobních údajů v zemích mimo území Evropské unie dochází vždy v souladu s platnými a účinnými právními předpisy.

9. Závěrečná ustanovení

Revize směrnice bude prováděna podle potřeby, nejméně však jednou ročně.

10. Související dokumenty a přílohy:

- 10.1 Záznamy o činnostech zpracování

V Pardubicích dne 24. 05. 2018

Clever Energies s.r.o.