VNITŘNÍ PŘEDPIS O OCHRANĚ OSOBNÍCH ÚDAJŮ

(dále jen „**směrnice**“)

Strong energy s.r.o., IČO: 06000134

EVIDENCE REVIZÍ A ÚPRAV SMĚRNICE

Verze	Datum platnosti	Připravil	Schválil
1.0	29.3.2021		

1. ÚČEL

1.1. Strong energy s.r.o., IČO: 06000134**,** se sídlem Bezručova 146/10, Vnitřní Město, 301 00 Plzeň, zapsaná v obchodním rejstříku vedená u Krajského soudu v Plzni, oddíl C, vložka 34428 (dále jen „**Podnikatel**“) zavádí tuto směrnici pro naplnění požadavků a uplatňování GDPR.

1.2. Účelem této směrnice je stanovit základní pravidla zpracování osobních údajů Podnikatelem. Tato směrnice je jedním z organizačních opatření ochrany osobních údajů ve smyslu článku 32 GDPR.

1.3. Tato směrnice dále upravuje procesy realizace práva subjektu údajů na přístup k osobním údajům ve smyslu článku 15 GDPR a ohlašování případů porušení zabezpečení osobních údajů ve smyslu článku 33 a 34 GDPR.

2. PŮSOBNOST

2.1. Tato směrnice se vztahuje na každého pracovníka Podnikatele, když zpracovává osobní údaje nebo plní jinou činnost, která je upravena v GDPR.

3. TERMÍNY, DEFINICE A ZKRATKY

3.1. V této směrnici mají níže uvedené pojmy následující význam:

3.1.1. **Dozorový úřad** – Úřad pro ochranu osobních údajů;

3.1.2. **GDPR** – Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů);

3.1.3. **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;

3.1.4. **Zvláštní kategorie osobních údajů** – osobní 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;

3.1.5. **Pracovník** – je každá osoba, zejména zaměstnanec a fyzická osoba podnikající, která pro Společnost vykonává činnost související s její podnikatelskou činností, a při své činnosti zpracovává osobní údaje nebo plní jinou činnost upravenou v GDPR;

3.1.6. **Subjekt údajů** – každá fyzická osoba, včetně osob samostatně výdělečně činných;

3.1.7. **Zpracování osobních údajů** – je 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.

4. ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

4.1. Podnikatel určuje účely a prostředky zpracování osobních údajů každé jím vykonávané činnosti. Podnikatel dále určí dobu, po kterou bude každý osobní údaj zpracováván, nebo kritéria, pomocí kterých se tato doba určí. Osobní údaje jsou zpracovávány po dobu určenou právními předpisy nebo po dobu trvání licence ke zpracovávání osobních údajů správcem. Účel jakožto i retenční doba zpracovávání osobních údajů jsou evidovány v záznamech o činnostech zpracování vedených Společností dle čl. 30 GDPR.

4.2. Má-li pracovník podezření, nebo dozví-li se, že jsou osobní údaje jakéhokoliv subjektu údajů nepřesné, neúplné či zastaralé, ohlásí to Podnikateli.

4.3. Má-li pracovník podezření, nebo dozví-li se, že jsou osobní údaje zpracovávány déle, než je nezbytné pro účely, pro které jsou zpracovávány, ohlásí to Podnikateli.

4.4. Při zpracování osobních údajů u Podnikatele pracovníci dodržují následující zásady:

4.4.1. ve vztahu k subjektu údajů musí být osobní údaje zpracovávány korektně, zákonným a transparentním způsobem;

4.4.2. osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný;

4.4.3. zpracování musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou osobní údaje zpracovávány – tzv. minimalizace údajů;

4.4.4. 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;

4.4.5. osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány;

4.4.6. osobní údaje musí být zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

5. POVINNOSTI PRACOVNÍKŮ

5.1. Pracovníci jsou oprávněni zpracovávat osobní údaje pouze v souladu se zákonem, pokyny Podnikatele a vnitřními předpisy provádějícími GDPR. Pracovníci smí zpracovávat pouze osobní údaje nezbytné pro plnění svých povinností. Podnikatel za tímto účelem zřizuje pracovníkům přístup pouze k nezbytně nutným evidencím osobních údajů.

5.2. Každý pracovník odpovídá za to, že zpracování osobních údajů provádí v souladu s právními předpisy, pokyny Podnikatele a tímto interním předpisem.

5.3. Každý pracovník je povinen zachovávat mlčenlivost o osobních údajích a opatřeních přijatých k jejich ochraně, o nichž se v souvislosti s výkonem svého zaměstnání, či obdobné činnosti dozvěděl, a to i po skončení pracovního poměru či jiného vztahu s Podnikatelem.

5.4. Každý pracovník je povinen chránit dokumenty obsahující osobní údaje, se kterými pracuje, před odcizením či zneužitím ze strany neoprávněné osoby, a to zejména tak, že se při odchodu ze svého místa odhlásí ze svého uživatelského účtu na počítači, pokud jej k práci využívá, a uzamkne dokumenty obsahující osobní údaje subjektu údajů na určené místo.

5.5. Při tisku na síťové tiskárně je pracovník povinen dokumenty obsahující osobní údaje subjektu údajů odebrat z tiskárny bez zbytečného odkladu.

6. TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ PRO OCHRANU OSOBNÍCH ÚDAJŮ

6.1 Systém ochrany osobních údajů je tvořen komplexem organizačních a technických opatření, která jsou realizována za účelem zabezpečení ochrany a bezpečnosti osobních údajů.

6.2 Podnikatel vede a uchovává záznamy o činnostech zpracování.

6.3 **Technická opatření**:

a. elektronické zabezpečení prostor Podnikatele;

b. zamezení přístupu neoprávněným osobám;

c. zabezpečení serveru před odcizením a neoprávněným přístupem;

d. přístup do všech počítačů a mobilních zařízení pod heslem;

e. ochrana zařízení antivirem, firewallem;

f. nastavené oprávněné přístupy do systému Podnikatele jen pro pověřené osoby;

g. záznamová zařízení a listinné evidence jsou umístěny v uzamykatelných místnostech. Vstup do místnosti mají pouze oprávněné osoby, které při opuštění místnosti tuto vždy zamykají. Ostatní osoby mají přístup do místnosti pouze v doprovodu oprávněných osob;

h. vzdálený přístup je umožněn prostřednictvím zabezpečeného připojení jen oprávněným osobám (pracovníkům vyřizujícím danou agendu);

6.4 **Organizační opatření**:

a. pracovníci jsou pravidelně školeni na zásady a principy ochrany osobních údajů a kybernetickou bezpečnost;

b. Podnikatel přijal tuto vnitropodnikovou směrnici pro nakládání s osobními údaji;

c. všichni pracovníci jsou vázáni mlčenlivostí ohledně předaných osobních údajů;

6.5 **Řízení rizik**

Společnost provádí pravidelnou kontrolu, testování a hodnocení účinnosti zavedených technických a organizačních opatření pro zjištění bezpečnosti zpracování a možných nedostatků formou interního auditu

Vyhodnocení rizik je následující:

a. Riziko vůči právům a svobodám subjektů údajů z následujících pohledů

1. porušení principů přiměřenosti a nezbytnosti zpracování;

2. porušení práv subjektů údajů;

3. neoprávněný přístup k osobním údajům;

4. neoprávněná změna osobních údajů;

5. nedostupnost nebo výmaz osobních údajů.

b. Hodnocení závažnosti dopadu: Na základě definice možných dopadů v bodě b) je určena jedna z následujících kategorií identifikovaných rizik.

1. **Zanedbatelné**: Subjekty údajů nebudou dotčeny, nebo budou dotčeny minimálně bez jakýchkoliv větších problémů (např. opětovné zadávání informací do systému, obtěžování při opětovném marketingovém sdělení).

2. **Omezené**: Subjekty údajů se mohou setkat s nepříjemnostmi, které budou schopny relativně snadno vyřešit (dodatečné náklady, popření přístupu k obchodním službám, strach, nedostatek porozumění, stres atd.).

3. **Významné**: Událost může mít významný důsledek pro subjekty údajů. Tyto důsledky by subjekty měly být schopné překonat, ačkoliv s vážnými obtížemi (např. zneužití finančních prostředků, škody na majetku, ztráta zaměstnaní, zhoršení zdravotního stavu atd.).

4. **Vysoké**: Událost může mít vysoké nebo nezvratné důsledky pro subjekty údajů, které nemusí být možné překonat (např. finanční potíže, značný dluh, pracovní neschopnost, dlouhodobé fyzické nebo psychické nemoci, smrt atd.).

c. Zavedená a plánovaná ochranná, resp. nápravná opatření.

6.6 **Narušení zabezpečení osobních údajů**

V případě zjištění porušení zabezpečení osobních údajů je nezbytné:

a. Zamezit dalšímu úniku – fyzickým zamčením dokumentů nebo v případě elektronické formy zamezením přístupu nebo vypnutím IT systémů;

b. Případ narušení zabezpečení posoudit a zdokumentovat (co se stalo, jaké a čí osobní údaje unikly, možné následky, popis přijatých opatření s cílem vyřešit daný případ, identifikace rizika/vysokého rizika);

c. postupovat dle čl. 7. této směrnice, pokud jsou splněny podmínky pro takový postup.

7. OZNAMOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

7.1. Jakékoli porušení zabezpečení osobních údajů dle ustanovení čl. 4 odst. 12 GDPR Podnikatel bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, ač tomu tak mělo být, musí být současně s ním uvedeny důvody tohoto zpoždění.

7.2. Ohlášení dozorovému úřadu podle tohoto článku musí přinejmenším obsahovat:

7.2.1. popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;

7.2.2. kontaktní místo, které může poskytnout bližší informace;

7.2.3. popis pravděpodobných důsledků porušení zabezpečení osobních údajů;

7.2.4. popis opatření, která Společnost přijala nebo navrhla k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

7.3. Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí Podnikatel toto porušení bez zbytečného odkladu dotčenému subjektu údajů.

7.4. Zaznamenání incidentů bude na základě předložených informací zpracovávat pověřenec nebo jiná pověřená osoba ve formě seznamu incidentů s popisem události.

8. VZDĚLÁVÁNÍ

8.1. Podnikatel zajistí školení pracovníků na zásady dodržování ochrany osobních údajů ve smyslu GDPR. Každý pracovník, kterému to bude uloženo, je povinen účastnit se školení a potvrdit svou účast na školení.

9. ARCHIVACE

10.1. Podnikatel archivuje veškerou dokumentaci získanou v souvislosti se zpracováním osobních údajů po dobu předepsanou obecně závaznými právními předpisy, příp. dle archivačního a skartačního řádu.

10. LIKVIDACE OSOBNÍCH ÚDAJŮ

10.2. Podnikatel provádí likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovávány, případně na základě žádosti subjektu údajů. Při likvidaci jsou dodržovány zákonné výjimky týkající se uchovávání osobních údajů pro účely archivnictví a uplatňování práv v občanském soudním řízení, trestním řízení a správním řízení.

10.3. Pověřenec nebo jiná pověřená osoba vyhotoví záznam o likvidaci osobních údajů.

V Plzni dne 29.3.2021

_____

Strong energy s.r.o.
Dana Votýpková, jednatelka