Typ vnitřní normy:	**Směrnice č. 1**
Název:	**O ochraně osobních údajů**

Vazba na legislativu:	zákon č. 101/2000 Sb. o ochraně osobních údajů, evropská právní úprava Nařízením Evropského parlamentu a Rady (EU) č. 2016/679, obecné nařízení o ochraně osobních údajů, dále též jen „GDPR“
Závazné pro:	ENERGY XXI s.r.o. se sídlem P. Jilemnického 1803, 738 01 Frýdek – Místek
Odpovědná osoba:	Ing. Karel Holuša
Schváleno:	Ing. Holuša v. r.
Účinnost od:	25. 5. 2018
Účinnost do:	Neomezena

PREAMBULE

Firma s ohledem na jí ukládané povinnosti, a to jak českou právní úpravou (zákonem č. 101/2000 Sb. o ochraně osobních údajů), tak i evropskou právní úpravou (Nařízením Evropského parlamentu a Rady (EU) č. 2016/679, obecné nařízení o ochraně osobních údajů, dále též jen „GDPR“) tímto přijímá tuto směrnici, která stanoví pravidla pro všechny pracovníky firmy.

Účelem této směrnice je zajištění ochrany osobních údajů fyzických osob, s nimiž přijdou pracovníci firmy do styku, jakožto i naplnění dalších zákonných požadavků kladených na firmu.

Veškerá ustanovení této směrnice musí být vykládána v souladu s výše uvedeným účelem směrnice, když veškerá ustanovení musí být vyložena ve prospěch zajištění maximálního naplnění účelu této směrnice.

Pokud tato směrnice vymezuje konkrétní pojmy, skutečnosti, nebo vlastnosti úžeji, než vyplývá z rozhodných právních předpisů, pak toto zúžení nezakládá odlišný obsah pojmu, skutečnosti nebo vlastnosti, ale má sloužit pouze k jednoduššímu vysvětlení obsahu pojmu, skutečnosti nebo vlastnosti, a to pro účely této směrnice.

OBSAH

ČLÁNEK 1 – ÚVODNÍ USTANOVENÍ

1. Osobními údaji jsou veškeré informace o fyzické osobě, na jejichž základě je možné tuto osobu přímo nebo nepřímo identifikovat. Za takovýto osobní údaj se považuje kromě typicky identifikačních údajů (datum narození, jméno, příjmení, rodné číslo, apod.) taktéž údaj o její funkci v konkrétní právnické osobě, lokační nebo komunikační údaje, nebo jeden či více prvků fyzické, fyziologické, ekonomické, nebo společenské identity osoby.

2. Zpracováním osobních údajů je jejich jakékoliv zobrazení, užití, archivace, popřípadě prosté uvedení do databáze firmy.

3. K zpracování osobních údajů bude docházet výlučně u firmy s tím, že pokud by tato chtěla pověřit zpracováním osobních údajů externího zpracovatele (např. externí účetní, apod.), pak takovýto subjekt musí nakládat s osobními údaji v souladu se shora uvedenými právními předpisy.

4. Případný externí zpracovatel musí být smluvně zavázán k tomu, aby poskytoval firmě součinnost při výkonu práv subjektů údajů, oznamoval bezpečnostní incidenty ve smyslu ustanovení čl. 33 a 34 GDPR, a tyto řešil, a dále umožnil provádět firmě audity pro ni zpracovávaných údajů, včetně umožnění provádění inspekcí. Za tímto účelem bude do smluv s externími zpracovateli vkládána doložka, která bude znít následovně: *„Zpracovatel je povinen firmě poskytovat součinnost při výkonu práv subjektů údajů, písemně oznamovat bezpečnostní incidenty ve smyslu ustanovení čl. 33 a 34 GDPR, a tyto řešit, a umožnit firmě provádět audity pro ni zpracovávaných údajů, včetně umožnění provádění inspekcí u zpracovatele. Zpracovatel je taktéž povinen plnit veškeré povinnosti vyplývající přímo zpracovateli z rozhodných právních předpisů, tak také povinnosti ukládané firmě, která tyto povinnosti bude plnit prostřednictvím zpracovatele.“*

ČLÁNEK 2 – ZÁKLADNÍ ZÁSADY NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI

1. Osobní údaje mohou být firmou zpracovávány pouze na základě zákonného důvodu, typicky z důvodu nezbytnosti plnění smlouvy, popřípadě zákonné povinnosti, nebo subjekt poskytne firmě souhlas se zpracováním svých osobních údajů.

2. Osobní údaje mohou být zpracovány pouze pro účely sledování legitimního cíle – tedy zejména naplnění smluvních povinností, zákonných archivačních, účetních nebo daňových povinností, ostrahy a ochrany majetku. Pokud by osobní údaje měly být zpracovány i nad rámec důvodů uvedených výše, pak k tomuto zpracování musí firma získat souhlas konkrétní osoby.

3. Osobní údaje musí být zpracovávány přiměřeně, relevantně a omezeně s ohledem na účel jejich zpracování, tedy firma nebude zpracovávat větší objem osobních údajů, než je pro účely jejich zpracování nezbytné. Pokud to bude z povahy věci možné, tak osobní údaje budou v maximálním možném rozsahu pseudonymizovány či dokonce anonymizovány.

4. Pracovníci firmy budou i s ohledem na práva subjektu údajů ověřovat aktuálnost, a tedy přesnost zpracovávaných osobních údajů.

5. Osobní údaje budou ukládány u firmy v nezbytně nutném rozsahu k naplnění účelu jejich zpracování, a to při respektování skutečnosti, že k daným osobním údajům budou mít přístup pouze pracovníci, u nichž je dána potřeba zajištění přístupu k těmto osobním údajům.

6. Pracovníci firmy jsou povinni zajistit, aby osobní údaje jak obchodních partnerů, tak případně pracovníků firmy i dalších osob, byly konkrétní osobou zpracovávány s maximálním důrazem na zachování jejich ochrany.

ČLÁNEK 3 – INFORMOVÁNÍ SUBJEKTU ÚDAJŮ

1. Firma se zavazuje informovat své obchodní partnery o skutečnosti, že o nich zpracovávají osobní údaje, a to případně i ve smyslu citlivých osobních údajů. Firma je povinna dále informovat své obchodní partnery o veškerých právech, které jim z rozhodných právních předpisů vyplývají.

2. Obchodní partner bere na vědomí, že firma o něm eviduje a zpracovává osobní údaje zahrnující:
   a) identifikační údaje – jméno, příjmení, datum narození, bydliště/sídlo, identifikační číslo, údaje o zápisu do registrů (např. obchodní, živnostenský), identifikační údaje odpovědných osob,
   b) další údaje, pokud jejich zpracovávání je nezbytné pro účely plnění dalších povinností firmy (např. údaje nezbytné pro realizaci zakázky),
   c) údaje dotýkající se platební morálky, a to zejména za účelem řádného vedení účetnictví, sledování insolvenčních a jiných obdobných rejstříků.

   Zpracování osobních údajů obchodních partnerů je nezbytné pro plnění povinností vyplývajících z dotčených právních předpisů, případně plnění smluvních závazků

firmy. V případě nesdělení daných údajů nebude moci firma plnit předmětné povinnosti. Obchodní partner je povinen sdělovat firmě změny svých údajů, a to za účelem zajištění správnosti, úplnosti a autenticity údajů zpracovávaných firmou. Zároveň má obchodní partner právo požadovat opravu jednotlivých evidovaných údajů. Za účelem ověření správnosti a autenticity údajů je firma povinna vyhovět žádosti obchodního partnera o sdělení údajů, které o něm jsou zpracovávány, a to ve formě potvrzení o tom, jaké osobní údaje jsou o něm zpracovávány v jakém rozsahu, za jakým účelem, apod.

3. Každý ze subjektů, o němž firma zpracovává osobní údaje, je oprávněn se obrátit na dozorový orgán – Úřad pro ochranu osobních údajů, jakožto se případně také domáhat soudní ochrany, a to ve všech otázkách ochrany jeho osobních údajů. Jakmile odpadne důvod pro zpracování osobních údajů, tedy zejména po uplynutí 10 roků od ukončení kalendářního roku, kdy obchodní partner naposledy realizoval obchodní spolupráci s firmou, je firma povinna vymazat osobní údaje obchodního partnera. Obchodní partner má právo, aby firma odstranila osobní údaje o obchodním partnerovi před tímto datem, pokud tento je zpracovává neoprávněně, případně chybně, a k opravě chyby nedojde ani po výzvě k jejich opravě.

4. Firma není oprávněna činit jakékoliv rozhodování v záležitostech obchodního partnera toliko na základě automatizovaného zpracování jeho osobních údajů, ani provádět jakékoliv jeho profilování, a to vyjma případného posouzení termínu splatnosti jednotlivých závazků obchodního partnera.

5. Firma je povinna informovat obchodního partnera o jakémkoliv ohrožení jeho osobních údajů. Firma případy porušení ochrany osobních údajů ve smyslu čl. 33 GDPR ohlásí Úřadu pro ochranu osobních údajů do 72 hodin. Tuto povinnost firma nebude mít v případě, že je velmi nepravděpodobný vliv na riziko úniku osobních údajů.

6. Firma nezpracovává osobní údaje obchodního partnera z titulu jeho souhlasu, ale pouze z titulu plnění zákonných povinností, a to s výjimkou zpracování osobních údajů za účelem:
   a) zasílání obchodních sdělení v oblasti obchodu a poskytování služeb, které jsou předmětem podnikání firmy, na jím uvedenou e-mailovou adresu, k čemuž tímto obchodní partner dává výslovný souhlas, a to na dobu neurčitou, který však je oprávněn kdykoliv odvolat, a to sdělením na e-mail holusa@energyxxi.cz .
   b) pořízení audiovizuálních materiálů z realizovaných zakázek a jejich zveřejnění pro účely referencí.
   c) reklamační řízení
   d) řízení společných projektů.

7. Žádosti obchodních partnerů ohledně uplatnění práva na:
   přenositelnost,
   omezení zpracování (žádost o dočasný přesun do jiného systému nebo znepřístupnění),
   vydání potvrzení o zpracovávání údajů o něm,
   opravu,
   vymazání,
   informace o přijatých opatřeních,

vyřídí bez zbytečného odkladu, nejpozději však do 30 dnů pověřený pracovník, který předem písemně informuje svého nadřízeného a po odsouhlasení nadřízeným zašle obchodnímu partnerovi zprávu o způsobu a termínu vyřešení jeho žádosti.

8. Firma bude zpracovávat osobní údaje obchodních partnerů pouze pro účely zákonné archivační, daňové a účetní. V případě požadavku na zpracování osobních údajů i za jiným účelem, se firma zavazuje získat informovaný předchozí písemný souhlas.

ČLÁNEK 4 – NĚKTERÁ TECHNICKÁ OPATŘENÍ

1. Firma je povinna realizovat veškerá nezbytná technická opatření k zajištění náležité ochrany osobních údajů, a to jak svých pracovníků, tak obchodních partnerů.

2. Pracovníci firmy jsou povinni navrhovat svým jednotlivým vedoucím pracovníkům přijetí nezbytných opatření k zajištění náležité ochrany osobních údajů subjektu údajů.

3. Údaje o subjektech údajů budou likvidovány po uplynutí příslušných zákonných archivačních, účetních, popřípadě daňových lhůt. O tomto předem pracovník provádějící likvidaci informuje svého nadřízeného.

4. Pracovníci firmy nejsou oprávněni užívat vedením firmy či alespoň nadřízeným pracovníkem neschválený software, www aplikace či platformy.

5. Při zasílání jakýchkoliv osobních údajů elektronickou cestou, je příslušný odesílající pracovník povinen si nejprve ověřit soulad příslušné osoby adresáta a cílové elektronické adresy či úložiště dané osoby.

6. V případě, že firma provozuje nebo se chystá provozovat tzv. e-shop nebo jiný obdobný způsob prodeje, tak je povinna se bez zbytečného odkladu registrovat u Úřadu pro ochranu osobních údajů.

7. V případě, že by ve firmě byly shromažďovány biometrické údaje (např. otisky prstů v docházkových systémech), tak je příslušný pracovník, který za zavedení odpovídá, povinen o zavedení písemně informovat vedení společnosti (nejlépe přímo statutární orgán) a informovat o splnění povinností ve smyslu plnění předpisů na ochranu osobních údajů.

8. Firma případy porušení ochrany osobních údajů ve smyslu čl. 33 GDPR ohlásí Úřadu pro ochranu osobních údajů do 72 hodin. Tuto povinnost firma nebude mít v případě, že je velmi nepravděpodobný vliv na riziko úniku osobních údajů.