Příloha č. 7

Smlouva o ochraně osobních údajů

mezi

Smluvní strany:

EG.D, a.s.

se sídlem: Lidická 1873/36, Černá Pole, 602 00 Brno

IČO: 28085400, DIČ: CZ28085400

bank. spojení: 27-9426120297/0100, Komerční banka a.s.

zastoupená: Ing. Zdeňkem Bauerem, předsedou představenstva a Ing. Pavlem Čadou, Ph.D.,

místopředsedou představenstva – jako správce

(dále jen „Objednatel“),

a

**[ ● DOPLNÍ ÚČASTNÍK V NABÍDCE]**

se sídlem: **[ ● DOPLNÍ ÚČASTNÍK V NABÍDCE]**

IČO: , DIČ: **[ ● DOPLNÍ ÚČASTNÍK V NABÍDCE]**

společnost zapsaná v obchodním rejstříku vedeném Krajským soudem v ,

oddíl , vložka **[ ● DOPLNÍ ÚČASTNÍK V NABÍDCE]**

bank. spojení: , č. účtu: **[ ● DOPLNÍ ÚČASTNÍK V NABÍDCE]**

zastoupený: **[ ● DOPLNÍ ÚČASTNÍK V NABÍDCE]**

(dále jen „Zhotovitel “),

– jako zpracovatel údajů, dále jen **„Zhotovitel “–**

– společně dále jen „Smluvní strany“ –

– dále jen „Smlouva“ –

**Obsah**

[Preambule 3](#_Toc534876757)

[§ 1 Předmět, doba trvání a specifikace Zpracování údajů 3](#_Toc534876758)

[§ 2 Odpovědnost a rozsah oprávnění ke stanovení pokynů 4](#_Toc534876759)

[§ 3 Technická a organizační opatření 5](#_Toc534876760)

[§ 4 Oprava, omezení zpracování, výmaz a vrácení osobních údajů 6](#_Toc534876761)

[§ 5 Ostatní povinnosti Zhotovitele 6](#_Toc534876762)

[§ 6 Vztahy se subdodavateli (dílčími zpracovateli) 8](#_Toc534876763)

[§ 7 Předání do třetích zemí 8](#_Toc534876764)

[§ 8 Monitoring 9](#_Toc534876765)

[§ 9 Odpovědnost 9](#_Toc534876766)

[§ 10 Odměna, dodatky Smlouvy, salvatorní doložka 10](#_Toc534876767)

Preambule

Tato Smlouva stanoví práva a povinnosti Smluvních stran při ochraně osobních údajů v případě, kdy Zhotovitel zpracovává osobní údaje poskytnuté Objednatelem v rámci plnění smluv jejichž předmětem je dodávka datové centrály (software i hardware), která bude sloužit především k dálkovému odečtu dat a řízení odběru elektrické energie na odběrných místech s instalovaným smart metrem, jejichž cílový stav bude cca 1,5 mil. kusů, které byly mezi Objednatelem a Zhotovitelem po účinnosti této Smlouvy užavřeny (dále společně jen jako „smlouva “). Tato Smlouva zohledňuje právní úpravu platnou ke dni jejího uzavření na území České republiky, zejména zákon č. 101/2000 Sb., o ochraně osobních údajů a obecné nařízení o ochraně údajů (GDPR), a zajišťuje ochranu, kterou je nezbytné zajistit dle těchto právních předpisů při zpracovávání osobních údajů (dále jen „Zpracování údajů“) ze strany Zhotovitele nebo třetích osob, které Zhotovitel zapojil do poskytování plnění dle smlouvy jako subdodavatele.

Ustanovení této Smlouvy se uplatní obdobně tehdy, pokud Zhotovitel kontroluje nebo spravuje určitý automatizovaný postup nebo zařízení na zpracování osobních údajů v zastoupení Objednatele, kdy nelze tedy zaručit zamezení přístupu k osobním údajům Objednatele.

Tato Smlouva se nevztahuje na případy, kdy Zhotovitel zpracovává osobní údaje jako správce osobních údajů, a to na základě samostatného souhlasu, který byl Zhotoviteli platně udělen příslušným subjektem údajů, nebo na základě jiného právního titulu, který mu v souladu s předpisy stanovenými na ochranu osobních údajů svědčí.

1. Předmět, doba trvání a specifikace Zpracování údajů
2. Předmět Zpracování údajů vyplývá z Věcné smlouvy. Zpracování údajů se týká zejména osobních údajů v následujícím rozsahu:

|  |  |  |
| --- | --- | --- |
| Kategorie subjektů údajů | Kategorie osobních údajů | Účel  Zpracování údajů |
| Zákazníci Objednatele/ Potenciální zákazníci objednatele | **Identifikační údaje**  jméno a příjmení / titul / datum narození / místo narození / rodné číslo / ulice / číslo domu / město/obec / PSČ / země / telefon / mobilní telefon / fax / emailová adresa / číslo průkazu totožnosti (občanský průkaz, pas) / platnost (občanského průkazu, pasu)  **Personální údaje**  rodné číslo / osobní číslo / údaje o organizaci zaměstnance (telefon, mobilní telefon, fax, email) / údaje o umístění zaměstnance (číslo budovy, ulice, město, PSČ) / interní bezpečnostní údaje (identifikační číslo skupiny, identifikační číslo zaměstnance, osvědčení, přístupová práva) / oddělení / role / číslo sociálního pojištění / národnost / jazyk / rodinný stav / informace o manželovi/manželce nebo dětech / příjem / plat / majetek / důchod / důchodové dávky / informace o bance/kreditní kartě související se zaměstnancem / kariérní a profesní rozvoj ve firmě / číslo smlouvy o účtu / číslo obchodního partnera / stav odběru / měřicí místo    **Údaje o zaměstnanosti**  výkonnost / výpověď / písemné výstrahy / absence  **Individuální údaje**  údaje o provozu / údaje o telefonní lince / data protokolu (přihlášení / odhlášení) / hesla / údaje o aktivitě v síti / fotografie a videa / zvukové záznamy řeči / obsah emailů / číslo SIM karty/PUK / biometrické údaje / trestní rejstřík / adresa MAC (je-li osobní) / systémová data (údaje o konfiguraci, údaje o aktualizaci, výstrahy, jsou-li osobní) / údaje o konfiguraci protokolu IP, údaje o identifikaci v síti, jsou-li osobní    **Zvláštní typy osobních údajů**  rasový nebo etnický původ / politické názory / náboženské nebo filozofické přesvědčení / členství v odborech / zdravotní / lékařské údaje / údaje o sexuálním životě  **Osobní údaje vyplývající z používání konkrétní služby**  parametry smluv / údaje z měřičů / identifikační čísla/ číslo smlouvy uzavřené mezi Objednatelem a fyzickou osobou / číslo smlouvy zákazníka Objednatele / adresa odběrného místa / údaje o technických parametrech a o stavu odběrného místa / číslo odběrného místa a kód EAN/EIC | Plnění definované ve smlouvě |

1. Doba platnosti této Zpracovatelské smlouvy je určena dobou platnosti smluv, pokud dále z této Zpracovatelské smlouvy nevyplývá jinak.
2. Zhotovitel se zavazuje osobní údaje zpracovávat v elektronické i písemné podobě.
3. Objednatel bude předávat Zhotoviteli osobní údaje o subjektech údajů, buď elektronicky nebo v písemné podobě. V případě elektronického předání osobních údajů zajistí Zhotovitel jejich vytištění a souběžné smazání elektronických dat. Dále bude zhotovitel zpracovávat osobní údaje pouze v listinné písemné podobě.
4. Odpovědnost a rozsah oprávnění ke stanovení pokynů
5. Zhotovitel se zavazuje zpracovávat osobní údaje pro Objednatele, který je jediným správcem údajů ve smyslu čl. 4 odst. 7 GDPR.
6. Objednatel bude ukládat Zhotoviteli pokyny o povaze, rozsahu a způsobu Zpracování údajů a opatření k zajištění bezpečnosti údajů, které je nezbytné přijmout. Rozsah činností, které podléhají pokynům, vyplývá z Věcné smlouvy. Zhotovitel je oprávněn zpracovávat osobní údaje pouze dle pokynů Objednatele.
7. Přístup k záznamům údajů a právo provádět Zpracování údajů bude v každém případě uděleno pouze v rozsahu nezbytném k řádnému plnění smluvních povinností. Zejména nebudou bez vědomí a souhlasu Objednatele pořizovány kopie nebo duplikáty. To neplatí o logovacích souborech nebo cache, které se vytváří automaticky, jestliže jsou poté bez zbytečného odkladu automaticky vymazány a nejsou zpracovávány nebo užívány za jiným účelem než Zpracování údajů.
8. Pokyny Objednatele budou udělovány písemně nebo obdobnou formou (např. v elektronickém formátu). V případě potřeby může Objednatel dávat jednotlivé pokyny také ústně.
9. Jestliže některý Objednatelův pokyn porušuje dle názoru Zhotovitele ustanovení právních předpisů o ochraně údajů, musí takovou skutečnost Zhotovitel bez zbytečného odkladu písemně oznámit Objednateli. Objednatel v takovém případě bez zbytečného odkladu udělí Zhotoviteli nový pokyn nebo mu sdělí, ať se řídí původním pokynem. Práva Objednatele udělovat pokyny a provádět kontrolu dle této Smlouvy může vykonávat rovněž osoba pověřená Objednatelem.
10. Požadavek dodržovat pokyny se nevztahuje na případy uvedené v čl. 28 odst. 3 písm. a) GDPR (výjimka z požadavku plnit příkazy). Zhotovitel o takém případu musí informovat Objednatele před zahájením Zpracování údajů.
11. Pokud Zhotovitel poruší Objednatelův pokyn nebo nesplní povinnosti dle právních předpisů v oblasti ochrany osobních údajů tím, že určí účely a prostředky zpracování, považuje se Zhotovitel ve vztahu k takovému zpracování za správce.
12. Změny předmětu, rozsahu, povahy, doby trvání, účelu nebo kategorií subjektů údajů vyžadují uzavření příslušné dohody mezi Zhotovitelem a Objednatelem v písemné nebo obdobné formě.
13. Technická a organizační opatření
14. Zhotovitel se zavazuje nastavit svou interní politiku ve společnosti v souladu s Věcnou smlouvou tak, aby plnila příslušné požadavky na zabezpečení osobních údajů. Zhotovitel se zavazuje, že zajistí náležitou úroveň zabezpečení svých systémů a služeb zpracování údajů pomocí příslušných technických a organizačních opatření. V tomto ohledu je nutno přihlédnout ke stavu techniky, nákladům na provedení, povaze, rozsahu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob ve smyslu čl. 32 odst. 1 GDPR. Cílem implementace těchto technických a organizačních je to, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.
15. Zhotovitel se zavazuje dodržovat tato technická a organizační opatření (dále jen „**TOO“**) uvedená v **Příloze 1** této Smlouvy.
16. Z důvodu technického pokroku a legislativního vývoje může vyvstat potřeba přizpůsobit realizovaná technická a organizační opatření takovému technickému pokroku a vývoji legislativy. Zhotovitel za tímto účelem zavede postup pro pravidelnou kontrolu, posouzení a hodnocení TOO, aby tak zajistil ochranu práv subjektů údajů.

Zhotovitel je oprávněn za účelem přizpůsobení zabezpečení technickému pokroku přijmout náležitá alternativní TOO. V rámci daného přizpůsobení však nesmí poklesnout bezpečnostní úroveň dosažená původně stanovenými opatřeními.

Nezbytné přizpůsobení TOO změněným nebo novým legislativním požadavkům musí Zhotovitel provést v okamžiku, kdy tyto požadavky nabydou platnosti, pokud se Smluvní strany nedohodnou jinak.

Všechna přizpůsobení TOO musí být zdokumentována a sdělena v písemně nebo obdobné formě Objednateli ihned poté, co se Zhotovitel dozvěděl o nezbytnosti přizpůsobit TOO.

1. Náklady na přizpůsobení TOO ponese Zhotovitel.
2. Oprava, omezení zpracování, výmaz a vrácení osobních údajů
3. Zhotovitel nemůže opravovat, mazat nebo omezovat zpracování údajů poskytovaných Objednatelem, které pro něj zpracovává, na základě vlastního úsudku, ale pouze v souladu s doloženým pokynem Objednatele.
4. V případě doloženého pokynu Objednatele, který tak stanoví, musí Zhotovitel okamžitě zajistit naplnění požadavků na výmaz nebo splnění specifické žádosti o výmaz, omezení zpracování, právo být zapomenut, na opravu a přenositelnost údajů.
5. Osobě odpovědné ve věcech provozně-technických, která uzavřela smlouvu na straně Objednatele, musí Zhotovitel bez zbytečného odkladu odevzdat všechny dokumenty, které obdrží, vytvořené výsledky zpracování a užívání a záznamy údajů související se vztahem k Objednateli, v souladu s doloženým pokynem takové osoby nebo v souladu s požadavky na výmaz údajů a po ukončení Zpracování údajů.
6. Pokud takové předání není možné nebo by nebylo účelné, musí je Zhotovitel zničit v souladu s požadavky na ochranu osobních údajů. Totéž platí o testovacích a o odmítnutých materiálech. Jakmile budou osobní údaje odevzdány osobě odpovědné ve věcech provozně-technických, která uzavřela Smlouvu, musí Zhotovitel bez zbytečného odkladu zničit údaje uvedené v předchozí větě a veškeré kopie a duplikáty, které má u sebe, v souladu s požadavky na ochranu osobních údajů.

Plnění výše uvedených povinností musí být potvrzeno Objednateli na požádání v písemné nebo obdobné formě.

1. Smluvní strany jsou povinny dodržovat zákonné povinnosti ohledně uchovávání dokumentů.
2. Dokumentaci, která slouží k ověření řádného Zpracování údajů dle objednávky, Zhotovitel po ukončení Smlouvy předá Objednateli.
3. Ostatní povinnosti Zhotovitele
4. Zhotovitel se zavazuje nejpozději před zahájením Zpracování údajů písemně ustanovit pověřence pro ochranu osobních údajů v souladu s čl. 38 GDPR nebo zvláštním vnitrostátním předpisem a zajistí řádné plnění jeho povinností do doby splnění všech pokynů Objednatele dle této Smlouvy. V případě ukončení spolupráce s předchozím pověřencem pro ochranu osobních údajů se Zhotovitel zavazuje okamžitě jmenovat dalšího. Nebude-li Zhotovitel povinen dle ustanovení GDPR nebo zvláštního vnitrostátního předpisu jmenovat pověřence pro ochranu osobních údajů, zavazuje se jmenovat kontaktní osobu pro Objednatele pro otázky ochrany osobních údajů v rámci Smlouvy.
5. Zhotovitel je povinen poskytnout součinnost Objednateli při plnění povinností týkajících se bezpečnosti údajů, informační povinnosti v případě porušení zabezpečení údajů, při posuzování vlivu na ochranu údajů a při předchozích konzultacích.
6. Pokud některý subjekt údajů uplatní svá práva vůči Objednateli, zejména právo na přístup, přijme Zhotovitel všechna opatření nezbytná k tomu, aby byly povinnosti vůči subjektu údajů bez zbytečného odkladu splněny, a to v souladu se Smlouvou a s veškerými pokyny Objednatele. Jestliže nejsou ustanovení o vyřizování práv subjektů údajů uplatněnými vůči Zhotoviteli obsažena ve Smlouvě nebo v nějakém pokynu, dohodne se Zhotovitel na dalším postupu s Objednatelem. Jestliže subjekt údajů uplatní svá práva přímo u Zhotovitele, odkáže Zhotovitel subjekt údajů na Objednatele, bude-li to možné na základě informací poskytnutých ze strany subjektu údajů. V takovém případě postoupí Zhotovitel žádost bez zbytečného odkladu Objednateli.
7. Zhotovitel je povinen zajistit předání pokynů Objednatele všem zaměstnancům, kteří mají přístup k osobním údajům v souvislosti s plněním povinností Zhotovitele dle této Smlouvy. Zhotovitel je současně povinen zakázat těmto zaměstnancům zpracovávat nebo užívat osobní údaje v rozporu s pokyny Objednatele nebo za jiným účelem než plnění smluvních povinností vůči Objednateli, a to i po ukončení plnění jejich povinností. Zhotovitel zajistí, aby byly osoby oprávněné zpracovávat osobní údaje vázány povinností mlčenlivosti nebo aby se na ně vztahovala náležitá zákonem stanovená povinnost mlčenlivosti.
8. Zhotovitel není oprávněn zpřístupnit jakékoliv osobní údaje třetím osobám nebo je používat pro vlastní potřebu, zejména pro marketingové účely.
9. Pokud se Zhotovitel dozví, že došlo k porušení zabezpečení osobních údajů, oznámí to bez zbytečného odkladu Objednateli. Totéž platí v případě, že Zhotovitel nebo osoba, kterou zaměstnává, poruší ustanovení o ochraně osobních údajů nebo tuto Smlouvu nebo pokud o tom existuje důvodné podezření. Zhotovitel podnikne opatření nezbytná k zajištění bezpečnosti údajů a k minimalizaci potenciálních nepříznivých důsledků pro subjekty údajů a bude danou záležitost bez zbytečného odkladu koordinovat s Objednatelem. Zhotovitel je povinen poskytnout součinnost Objednateli všemi prostředky, které má k dispozici, aby Objednatel mohl splnit svou povinnost dle čl. 33 odst. 1 GDPR (povinnost učinit ohlášení do 72 hodin).

[Ohlášení bude zasláno na tuto adresu: gdpr@eon.cz, případně písemně na](mailto:gpdr@eon.cz) korespondenční adresu : Ing. Jindřich Veselý, E.ON Česká republika s.r.o., Cejl 42/44, 602 00 Brno.

Tel. kontakt Ing. Jindřich Veselý : +420 733 670 559

1. Oznámení uvedené v odstavci (6) musí obsahovat alespoň tyto informace:
   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 počtu dotčených záznamů osobních údajů,
   2. popis pravděpodobných důsledků porušení zabezpečení osobních údajů a
   3. popis opatření, která Zhotovitel přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.
2. Bude-li zabezpečení a důvěrná povaha osobních údajů, které zpracovává Zhotovitel, ohrožena zabavením, exekucí, insolvenčním nebo obdobným řízením nebo jinými událostmi nebo kroky podniknutými třetími osobami, musí o tom Zhotovitel informovat bez zbytečného odkladu Objednatele. Zhotovitel je v této souvislosti povinen informovat bez zbytečného odkladu všechny odpovědné osoby o tom, že správcem daných údajů je Objednatel.
3. Zhotovitel je povinen vést záznamy o činnostech zpracování, které vykonává na základě této Smlouvy. Tyto záznamy musí obsahovat alespoň tyto informace:
   1. jméno a kontaktní údaje Zhotovitele, Objednatele a případně jejich zástupců;
   2. kontaktní údaje pověřence pro ochranu osobních údajů Zhotovitele (pokud jej Zhotovitel má);
   3. kategorie zpracování prováděných pro Objednatele;
   4. informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci; a
   5. obecný popis technických a organizačních bezpečnostních opatření.
4. Zhotovitel se na základě písemné nebo obdobné výzvy Objednatele zavazuje zpřístupnit Objednateli vedené záznamy o činnostech zpracování.
5. Vztahy s poddodavateli (subdodavazeli - dílčími zpracovateli)
6. Zhotovitel je oprávněn do zpracování údajů zapojit poddodavatele (jakožto dalšího zpracovatele) pouze takové, kteří byli odsouhlaseni Objednatelem pro plnění Věcné smlouvy v souladu s ustanoveními Věcné smlouvy, nebo pokud o tom byl Objednatel předem písemnou nebo obdobnou formou vyrozuměn a dal k tomu výslovný souhlas.
7. Pokud je podle ustanovení výše uvedeného odstavce Zhotovitel oprávněn využít poddodavatele, musí jej Zhotovitel vybrat s řádnou péčí a před jeho zapojením si musí být jist tím, že takový poddodavatel je schopen plnit všechny povinnosti Zhotovitele stanovené v této Smlouvě. Zhotovitel je rovněž povinen uložit příslušnému poddodavateli povinnosti stanovené v této Smlouvě v tom rozsahu, v němž tento poddodavatel jedná za Zhotovitele. Zhotovitel je povinen rovněž smluvně zajistit, aby všechny činnosti stanovené v této Smlouvě mohl dle uvážení Objednatele vykonávat buď Zhotovitel v souladu s pokynem Objednatele, nebo sám Objednatel. Jestliže bude Zhotovitel vykonávat činnosti v souladu s pokynem Objednatele, je povinen předávat Objednateli bez zbytečného odkladu všechny informace, zejména dokumentaci a výsledky kontrol. Zhotovitel se zavazuje, že na žádost Objednatelova pověřence pro ochranu osobních údajů předloží písemný důkaz o tom, že zde stanovené povinnosti jsou plněny.

Povinnosti dle tohoto odstavce se vztahují rovněž na Zhotovitele ve vztahu ke všem osobám, které jsou zaměstnány na základě smluvního vztahu s Objednatelem, v rámci plnění smluvních povinností Zhotovitele a které mají přístup k osobním údajům.

1. V případě, že poddodavatel pochybí při plnění povinností ochrany osobních údajů, Zhotovitel zůstává vůči Objednateli plně odpovědný za nesplnění jeho povinností.
2. Předání do třetích zemí
3. Smluvně sjednané Zpracování údajů bude prováděno výhradně v některém členském státě Evropské unie (EU) nebo v členském státě Evropského hospodářského prostoru (EHP). Veškeré předání údajů do třetí země vyžaduje předchozí souhlas Objednatele a může k němu dojít pouze na základě splnění zvláštních předpokladů dle čl. 44 GDPR.
4. Zhotovitel nese veškeré náklady na plnění svých povinností dle této Smlouvy, které mohou vzniknout odchodem Spojeného království z EU. To zahrnuje zejména náklady na zajištění dodržování v dané době platných právních předpisů. Pokud tyto náklady budou mít, se zřetelem na ustanovení Věcné smlouvy a zájmů Objednatele na dodržování smluvních povinností ze strany Zhotovitele, za následek nepřiměřenou ekonomickou újmu pro Zhotovitele a Zhotovitel odpovídajícím způsobem doloží tyto náklady Objednateli, Smluvní strany se pokusí dosáhnout vzájemným jednáním dohody o rozdělení nákladů. Pokud se Smluvní strany nebudou moci dohodnout, mají právo vypovědět Smlouvu s tříměsíční výpovědní lhůtou v souladu s příslušnými smluvními ustanoveními.
5. Monitoring
6. Zhotovitel uděluje Objednateli a zejména jeho pověřenci pro ochranu osobních údajů nebo třetí osobě oprávněné Objednatelem právo kdykoli bez omezení monitorovat, zda je Zpracování údajů prováděno v souladu s právními předpisy o ochraně osobních údajů, s ustanoveními této Smlouvy a s pokyny danými Objednatelem. Zhotovitel se zavazuje podporovat Objednatele v nezbytném rozsahu v tomto procesu a zejména poskytovat potřebné informace a podnikat veškeré nezbytné kroky k tomuto účelu. Objednatel je oprávněn provádět výše uvedené monitorování s pomocí třetích osob, které jsou oprávněny monitorovat Objednatele (zejména zákazníci Objednatele a dozorové orgány).
7. Ověřovat dle odstavce 1 lze
   1. dodržováním schváleného kodexu chování v souladu s čl. 40 GDPR
   2. prováděním interního auditu
8. Zhotovitel rovněž poskytne před zahájení Zpracování údajů a v jeho průběhu součinnost a podporu při dokumentování zjištění z kontrol.
9. Odpovědnost
10. Jestliže subjekt údajů úspěšně uplatní náhradu škody proti jedné ze Smluvních stran z důvodu porušení ustanovení GDPR, uplatní se čl. 82 GDPR.
11. Za veškerou ostatní škodu, která bude způsobena Objednateli v důsledku nedodržení některého pokynu nebo nedodržením povinnosti dle této Smlouvy, odpovídá Zhotovitel v souladu s právními předpisy. Náhrada škody současně zahrnuje i správní pokutu, udělenou Objednateli dozorovým úřadem, která byla způsobena nesplněním pokynu Zhotovitelem, nebo neplněním povinností Zhotovitele dle právních předpisů v oblasti ochrany osobních údajů.
12. V případě nesplnění pokynů udělených Objednatelem, nedodržení povinnosti dle této Smlouvy, neplnění povinností Zhotovitele dle právních předpisů v oblasti ochrany osobních údajů, v případě, že Zhotovitel nezajistí potřebná opatření proti neoprávněnému nebo nahodilému přístupu k osobním údajům, které mu byly předány Objednatelem podle této Smlouvy, nebo dojde k neoprávněnému zpracování, změně, ztrátě nebo jinému zneužití osobních údajů (např. v případě použití osobních údajů pro jiný než sjednaný účel) nebo k jinému porušení povinnosti Zhotovitele dle této Smlouvy, Zhotovitel uhradí Objednateli smluvní pokutu ve výši 1.000.000,- Kč, a to za každé jednotlivé porušení těchto povinností. Úhradou smluvní pokuty není dotčeno právo Objednatele na náhradu škody v plné výši či nemajetkové újmy vzniklé porušením smluvní povinnosti, které se smluvní pokuta týká.
13. Ujednáním smluvních pokut dle této Smlouvy není dotčen nárok poškozené Smluvní strany na náhradu majetkové i nemajetkové újmy. Smluvní strany výslovně sjednávají povinnost odčinit vedle vzniklé škody také nemajetkovou újmu.
14. Odměna, dodatky Smlouvy, salvatorní doložka
15. Odměna za opatření a aktivity, které má Zhotovitel realizovat, povinnosti, které má plnit a součinnost, kterou má poskytnout, je zahrnuta do odměny poskytované Zhotoviteli v rámci Věcné smlouvy.
16. Změny a dodatky k této Smlouvě, včetně tohoto článku, mohou být provedeny pouze v písemné nebo obdobné formě.
17. Na uzavření této Smlouvy nebo jejích případných dodatků či jiných dohod navazujících na tuto Smlouvu navazujících se neaplikuje možnost modifikované akceptace dle ustanovení § 1740 odst. 3 věty první zákona č. 89/2012 Sb., občanského zákoníku.
18. Jestliže kterékoli ustanovení této Smlouvy je nebo se stane neúčinným nebo neurčitým, nebude touto okolností ovlivněna účinnost ani úplnost zbytku Smlouvy. Smluvní strany se v takovém případě dohodnou na ustanovení, kterým nahradí takové neúčinné nebo neúplné ustanovení a bude z finančního i právního hlediska co možná nejbližší cílům sledovaným touto Smlouvou a právně povoleným úmyslům Smluvních stran.
19. V případě změn požadavků stanovených v příslušných zákonech o ochraně údajů, zejména při nabytí platnosti Nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES a jeho prováděcích předpisů, se Zhotovitel zavazuje, že na žádost Objednatele změní nebo rozšíří ustanovení smluvních ujednání, včetně příslušné Smlouvy a technických a organizačních opatření tak, jak to bude nezbytné pro právoplatné provedení změn zákonných požadavků pro nakládání s osobními údaji nebo v důsledku vnitroskupinových předpisů, které se vztahují na Objednatele. Náklady na takovou realizaci hradí Zhotovitel.
20. Otázky touto smlouvou výslovně neupravené se řídí obecně závaznými právními předpisy České republiky.
21. Smluvní strany prohlašují, že souhlasí s obsahem Smlouvy, že tato Smlouva byla sepsána na základě pravdivých údajů, jejich pravé a svobodné vůle a nebyla ujednána v tísni ani za jinak jednostranně nevýhodných podmínek. Na důkaz toho připojují své podpisy.
22. Tato Smlouva vstupuje v platnost i účinnost dnem podpisu oprávněnými zástupci všech smluvních stran. Nebude-li tato Smlouva podepsána všemi smluvními stranami téhož dne, stává se platným i účinným dnem podpisu pozdějšího.

Součástí této Smlouvy je tato příloha:

Příloha 1: Popis technických a organizačních opatření dle § 3 Smlouvy (TOO)

|  |  |
| --- | --- |
|  |  |

**Příloha - Technicko-organizační opatření bezpečnosti informací a ochrany osobních údajů**

1. **Požadavky na bezpečnost informací**

Všeobecné požadavky, které se vztahují obecně na poskytování všech Služeb Zhotovitelem.

* 1. **Důvěryhodná dodávka**: Zhotovitel zajistí, aby jím používané hardwarové a softwarové produkty byly nakupovány ze známých a spolehlivých zdrojů a aby byla zajištěna spolehlivá technická podpora a identifikovatelný dodavatelský řetězec.
  2. **Správa bezpečnosti informací**: Zhotovitel zavede, udržuje a sleduje rámec řízení bezpečnosti informací. Ten umožňuje vedení společnosti Zhotovitele stanovit jasné směřování a cíle v oblasti bezpečnosti informací a řízení rizik. Tím vedení společnosti Zhotovitele dává najevo závazek s naplňováním těchto cílů.
  3. **Řízení rizika v oblasti bezpečnosti informací**: Zhotovitel zajistí, aby (i) před zavedením nových IT systémů, ve kterých jsou zpracovávány informace společnosti E.ON, (ii) před zavedením významných změn ve stávajících systémech (iii) před zavedením významných nových technologií, byla zjištěna, hodnocena, řešena, sledována a udržována související rizika v přijatelných mezích pro oblasti bezpečnosti informací. Zhotovitel bez zbytečného odkladu poskytne na vyžádání společnosti E.ON informace týkající se činností ve vztahu k procesu řízení rizik.
  4. **Řízení bezpečnosti**: Zhotovitel (i) zřídil specializovanou roli pro bezpečnost informací, která je na dostatečně vysoké úrovni řízení se svěřenými přiměřenými pravomocemi i zdroji k zajištění účinného a důsledného uplatňování osvědčených postupů v oblasti bezpečnosti informací v celé společnosti a dodržování právních, regulačních a smluvních požadavků, které se týkají bezpečnosti informací. Zhotovitel (ii) realizuje komplexní, průběžný program zvyšování bezpečnostního povědomí s cílem propagovat žádoucí chování v oblasti bezpečnosti ve vztahu ke všem osobám, které mají přístup k informacím společnosti E.ON, a toto chování jim vštěpovat.
  5. **Zdokumentované provozní postupy**: Zhotovitel stanovil odpovědnosti a postupy pro řízení a provozování svých Služeb s cílem zajistit, aby po dobu trvání této smlouvy tato dokumentace byla (i) v souladu s uznávanými oborovými normami a osvědčenými postupy, (ii) řádně písemně vyhotovena a (iii) průběžně aktualizována. Zhotovitel bez zbytečného odkladu poskytne na vyžádání společnosti E.ON dokumentaci provozních postupů.
  6. **Správa aktiv**: Zhotovitel zajistí, aby (i) aktiva (hardwarové a softwarové prostředky), která se používají k vytváření, zpracování, ukládání nebo předávání informací společnosti E.ON, byla během celého životního cyklu chráněna proti poškození, ztrátě, krádeži a neoprávněnému zpřístupnění. Zhotovitel zajistí, aby tato aktiva byla evidována v inventáři aktiv, který (ii) je chráněn proti neoprávněnému pozměňování, (iii) aktualizován, (iv) pravidelně zálohován (v) a obsahuje potřebné údaje o těchto hardwarových a softwarových aktivech a případně – požadavky na dodržování předpisů v souvislosti s těmito aktivy. Zhotovitel zajistí, aby (vi) každému aktivu byl přiřazen jeho vlastník, který je odpovědný za provozování daného aktiva.
  7. **Řízení přístupu**: Zhotovitel omezí přístup k aktivům, která slouží k vytváření, zpracování, ukládání nebo předávání informací společnosti E.ON, na oprávněné osoby a pro vyhrazené provozní činnosti. To přinejmenším znamená, že (i) přístup k příslušným informacím mohou získat pouze oprávnění uživatelé, (ii) přístupová oprávnění jsou omezena na schválenou funkčnost systému, (iii) existuje jasné určení zodpovědnosti, (iv) přístupová oprávnění jsou udělována jednotlivcům (ID uživatele a hesla nesmějí být sdíleny). Zhotovitel zajistí, aby přístup pro správu k systémům, které slouží k ukládání nebo zpracování informací společnosti E.ON, byl (v) omezen na minimální počet správců, (vi) chráněn dvoufaktorovou autentizací, nebo pokud není možné dvoufaktorovou autentizaci technicky implementovat, zajistí obdobnou úroveň bezpečnosti řízení přístupu (jako jsou generovaná dočasná hesla v systémech pro správu, vynucování politiky hesel, použití kryptografických klíčů). Zhotovitel dále zajistí, aby byl přístup pro správu (vii) vždy protokolován s cílem umožnit zjištění a přešetření neoprávněného přístupu k informacím společnosti E.ON a neoprávněné manipulace s nimi. (viii) Zhotovitel rovněž zajistí, aby byl zaveden a dodržován formální postup, který definuje, jak jsou vytvářeny, pravidelně kontrolovány, upravovány, uzamykány a odstraňovány role, účty, přístupová práva a oprávnění týkající se přístupu.
  8. **Správa systémů**: Zhotovitel provozuje systémy, které vytvářejí, ukládají, zpracovávají nebo předávají informace společnosti E.ON takovým způsobem, aby (i) bylo možné zvládnout aktuální i předpokládanou pracovní zátěž a (ii) byly důsledně a přesně nakonfigurovány s cílem chránit tyto systémy a informace, které zpracovávají, ukládají nebo předávají, proti selhání, kybernetickému útoku, neoprávněnému zpřístupnění, poškození, krádeži či ztrátě. Zhotovitel zajišťuje správu zabezpečení systémů (iii) zálohováním nezbytných informací a softwaru, (iv) důsledným uplatňováním procesu provádění změn a (v) sledováním dodržování sjednaných dohod o úrovni služeb.
  9. **Síť a komunikace**: Zhotovitel zajistí, aby fyzické, bezdrátové a případně i hlasové sítě byly navrženy takovým způsobem, aby (i) byly spolehlivé a odolné, (ii) zabránily neoprávněnému přístupu, (iii) využívaly šifrované spojení a (iv) odhalily podezřelý provoz v síti. (v) Zhotovitel zajistí nakonfigurování síťových zařízení (včetně směrovačů, firewallů a bezdrátových přístupových bodů) tak, aby fungovaly podle potřeby a zabránily neoprávněným a nesprávným aktualizacím. Zhotovitel zajistí ochranu elektronických komunikačních systémů (vi) stanovením zásad pro jejich používání, (vii) nakonfigurováním bezpečnostního nastavení, (viii) posílením bezpečnostního nastavení podpůrné technické infrastruktury. (ix) Zhotovitel zajistí, aby názvy a topologie počítačů a sítí zůstaly skryty externím subjektům. Zhotovitel zajistí omezení externího přístupu k informačním systémům a sítím (x) zřízením demilitarizovaných zón (DMZ) mezi nedůvěryhodnými sítěmi a interními sítěmi, (xi) směrováním síťového provozu prostřednictvím firewallů nebo proxy firewallů, (xii) omezením způsobů připojení na nezbytné minimum(xiii) poskytnutím přístupu výhradně k autorizovaným podnikovým aplikacím, informačním systémům nebo konkrétně určeným částem sítě.
  10. **Správa technických bezpečnostních opatření**: Zhotovitel instaluje řešení ochrany proti škodlivému kódu v systémech, ve kterých mohou být informace společnosti E.ON vystaveny škodlivému kódu, včetně (i) serverů (např. aplikační servery, databázové servery, souborové servery, tiskové servery, webové servery), (ii) výpočetních zařízení (např. stolní počítače, notebooky a další mobilní zařízení) a iii) kancelářských zařízení (např. síťové tiskárny, kopírky, multifunkční zařízení). (iv) Software pro ochranu proti škodlivému kódu by měl chránit proti všem formám škodlivého kódu (např. viry, červy, trojské koně, spyware, rootkity, botnetový software, keyloggery, ransomware). (v) Software pro ochranu proti škodlivému kódu by měl být distribuován automaticky a v určených časových intervalech. Zhotovitel zjišťuje a pravidelně kontroluje, zda (vi) software pro ochranu proti škodlivému kódu nebyl deaktivován nebo zda jeho funkčnost nebyla omezena (vii) software pro ochranu proti škodlivému kódu správně nakonfigurovaný, (viii) jsou správně aplikovány aktualizace v rámci definovaných časových intervalů, (ix) probíhají kontroly systému v předem určených časech (x) systém náležitě upozorňuje na zjištěné případy přítomnosti škodlivého kódu.
  11. **Vzájemné oddělení testovacích a produkčních systémů**: Zhotovitel zajistí, aby (i) testovací a produkční systémy byly alespoň logicky odděleny s cílem snížit riziko neoprávněného přístupu nebo neoprávněné změny produkčních systémů. (ii) V případě, že vzájemné oddělení není možné, Zhotovitel zajistí zavedení speciálně upravených postupů pro proces řízení změn a proces řešení incidentů a mimořádných situací, které umožní rychle a přiměřeně reagovat na narušení produkčních systémů a problémy v těchto systémech. (iii) V testovacích nebo vývojových prostředích nesmí být produkční data povolena a musí být anonymizována vždy, obsahují-li osobní údaje nebo osobně identifikovatelné informace (PII).
  12. **Vývoj/pořizování softwaru**: Zhotovitel zajistí, aby interně vyvinutý software nebo software získaný z externích zdrojů, který se používá ke zpracování, ukládání nebo předávání informací společnosti E.ON, nevykazoval žádné bezpečnostní chyby z hlediska kritérií „OWASP TOP Ten“ a „SANS Top 25 Most Dangerous Software Errors“.
  13. **Prověřování bezpečnostních zranitelností**: Zhotovitel zajistí, aby (i) veřejně přístupné systémy byly pravidelně (nejméně jednou ročně) testovány na zranitelnosti a chyby v nastavení provedením dynamických testů (penetrační test nebo prověřování zranitelností), (ii) společnost E.ON byla bez zbytečného odkladu informována o veškerých zjištěních z těchto testů, která jsou pro společnost E.ON relevantní; (iii) kritické zranitelnosti byly společnosti E.ON okamžitě oznámeny. (iv) Zhotovitel poskytne pomoc a podporu při kontrolách procesu správy bezpečnostních zranitelností a oprav (tzv. „záplat“) prováděné pro společnost E.ON. (v) Ošetření bezpečnostních zranitelností se řeší na základě úrovní rizika těchto zranitelností a dle příslušných časových harmonogramů smluvních stran.
  14. **Úroveň aktuálnosti bezpečnostních záplat (tzv. patchů)**: Zhotovitel zajistí odstranění zranitelností realizací procesu správy bezpečnostních záplat, v jehož rámci (i) identifikuje a získá bezpečnostní záplaty z autorizovaných zdrojů, jakmile jsou k dispozici, (ii) rozhodne, kdy je třeba bezpečnostní záplaty nasadit, (iii) otestuje bezpečnostní záplaty na základě známých kritérií, (iv) nasadí bezpečnostní záplaty v dohodnutém časovém rámci, (v) eviduje stav implementace bezpečnostních záplat (např. v konfigurační databázi CMDB). (vi) Zhotovitel je oprávněn bezpečnostní záplaty používat v prostředí IT, včetně virtualizačních hypervisorů, virtuálních počítačů, operačních systémů a aplikací, pokud to nepříznivě neovlivní zachování důvěrnosti, integrity nebo dostupnosti informací společnosti E.ON.
  15. **Minimální požadavky na přihlašovací údaje:** Zhotovitel zajistí splnění minimálních požadavků společnosti E.ON na přihlašovací údaje (doporučená je dvoufaktorová autentizace) prostřednictví E.ON Single-Sign-On federativních služeb. Musí být uplatňovány tyto zásady: princip minimálních oprávnění, udělení těchto oprávnění výhradně osobám, které je potřebují ke své činnosti (‚need-to-know princip“) a jasné oddělení zodpovědnosti („segregation of duties“). Dále je třeba uplatňovat koncepci řízení přístupu na základě rolí.
  16. **Požadavky na návrh sítí:** U aplikací, které jsou přístupné prostřednictvím internetu, musí být jak vícevrstvá architektura, tak služby umístěné v demilitarizované zóně (DMZ). Síťové segmenty musí být vhodnými bezpečnostními opatřeními odděleny od segmentů s nízkou a střední úrovní ochrany s cílem zabránit přenosu dat mezi segmenty. Síťové segmenty s velmi vysokou úrovní ochrany by měly být pokud možno také odděleny od segmentů s vysokou úrovní ochrany a vůči těmto segmentům zabezpečeny.
  17. **Standardy bezpečnostního nastavení (tzv. „hardening“)**: Všechny informačních a síťové systémy musí být standardně bezpečně nastaveny a řádně zabezpečeny. To zahrnuje: (i) zakázání a blokování nepotřebných aplikací, služeb, nástrojů, protokolů a rozhraní, (ii) vymazání nebo přinejmenším změna výchozích uživatelských jmen a hesel od výrobce, (iii) aktivace bezpečnostních nástrojů a konfigurací ke zvyšování zabezpečení a (iv) zabránění přenosu technických informací externím subjektům.
  18. **Protokolování bezpečnostních událostí**: V zájmu zjištění a vyšetřování neoprávněného přístupu k informacím společnosti E.ON a neoprávněné manipulace s nimi zajistí, aby (i) u všech systémů provozovaných Zhotovitelem za účelem vytváření, ukládání, zpracování a předávání informací společnosti E.ON bylo vždy povoleno protokolování událostí (logování), (ii) tyto systémy byly nakonfigurovány tak, aby generovaly bezpečnostní události (včetně událostí, jako jsou úspěšné a neúspěšné pokusy o přihlášení uživatele, vytvoření / úprava / odstranění služby, vytvoření / úprava / odstranění objekt, havárie systému, odstranění uživatelských účtů) a atributy událostí související s každou konkrétní událostí (např. datum, čas, ID uživatele, název souboru a IP adresa), (iii) konzistentní, důvěryhodné datové a časové zdroje byly zárukou, že protokoly událostí používají přesná časová razítka (např. pomocí serverů NTP), (iv) protokoly bezpečnostních událostí byly chráněny před neoprávněným přístupem a náhodnou nebo úmyslnou úpravou / přepsáním
  19. **Dodržování předpisů (compliance)**: Zhotovitel zajistí, aby (i) všechny systémy, které vytvářejí, ukládají, zpracovávají nebo předávají informace společnosti E.ON, byly pravidelně kontrolovány z hlediska dodržování vlastních „bezpečnostních politik/standardů“ Zhotovitele. (ii) Vlastní „bezpečnostní politiky/standardy“ Zhotovitele musí být v souladu s požadavky s certifikáty uvedenými v oddílech 2 a 3 této přílohy. (iii) Zhotovitel společnosti E.ON na vyžádání předloží prohlášení o technické shodě za účelem prokázání, že tyto technické kontroly shody proběhly pro každý prostředek (aktivum) v rámci prostředí IT. Prohlášení o shodě musí obsahovat přiřazení mezi souvisejícími kontrolami vyplývajícími z oddílů 2 a 3 této přílohy a kontrolou technické shody. (iv) Zhotovitel vlastní „bezpečnostní zásady / standardy“ zpřístupní před Datem účinnosti a poté na vyžádání společnosti E.ON.
  20. **Bezpečná likvidace a opětovné použití**: Zhotovitel zajistí, aby hardware, který má být vyřazen z provozu, (i) byl před jeho opětovným použitím, prodejem nebo vrácením vyčištěn tak, aby všechny informace společnosti E.ON byly v celém rozsahu bezpečně smazány (ii) nebo bezpečně zničeny. (iii) Smazání nebo zničení je třeba provést bezpečným způsobem pomocí nejmodernějších technologií a postupů, jako jsou nástroje a postupy definované v NIST SP 800-88 Guideline for Media Sanitization (Postupy pro odstraňování dat z médií). (iv) Zhotovitel na vyžádání společnosti E.ON předloží koncepci bezpečného odstraňování a smazání, jakož i důkazy o provedeném bezpečném odstranění a vymazání informací společnosti E.ON.
  21. **Bezpečnost lidských zdrojů:** Za každou osobu, která jedná jménem Zhotovitele a byla jí udělena přístupová oprávnění (místně nebo vzdáleně), musí být společnosti E.ON poskytnuty osobní identifikační údaje. Zhotovitel zajistí ověření totožnosti fyzických osob a dále zajistí, aby nikdo nezneužil přístupu nebo oprávnění udělených Zhotovitelem. Zhotovitel dále přejímá odpovědnost za případné škody způsobené neoprávněným přístupem a/nebo použitím informací společnosti E.ON. Zhotovitel pověří plněním zadaných úkolů výhradně pracovníky, kteří jsou k jejich plnění prokazatelně odborně způsobilí.
  22. **Bezpečnost v oblasti dodavatelského řetězce**: Zhotovitel zajistí identifikaci a řízení rizika bezpečnosti informací v každé fázi vztahů s externími zhotoviteli hardwaru a softwaru v celém dodavatelském řetězci tím, že (i) začlení požadavky na bezpečnost informací do formálních smluv a ii) ověří plnění těchto požadavků. (iii) Zhotovitel zajistí, aby subdodavatelé, kteří se podílejí na zpracování, ukládání, předávání nebo likvidaci informací společnosti E.ON, splňovali minimálně požadavky dohodnuté v této příloze. (iv) Zhotovitel je zodpovědný za zajištění náležitého řízení Subdodavatele(ů) a za dodržování opatření prováděných externě.

1. **Požadavky na ochranu osobních údajů** 
   1. Kontrola přenosu
      1. Požadavky na pracovníky v oblasti mlčenlivosti
         1. Všichni pracovníci, kteří zpracovávají osobní údaje pomocí automatizovaných procesů, musí dodržovat pravidla mlčenlivosti.
         2. Noví pracovníci musí být informováni o ochraně údajů pro potřeby nakládání s osobními údaji.
         3. Všechny zúčastněné strany si jsou vědomy otázek souvisejících s bezpečností a ochranou údajů.
         4. Osoby, které osobní údaje zpracovávají, jsou prokazatelně poučeni o bezpečném nakládání s osobními údaji na pracovišti.
         5. Jsou definována jasná pravidla pro postup v případě odchodu a propouštění pracovníků.
      2. Anonymizace / pseudonymizace
         1. Pro potřeby přenosu osobních údajů jsou využívány techniky anonymizace a pseudonymizace – pokud je to možné.
         2. V případě pseudonymizace údajů je nutné zajistit, aby pseudonym nebyl příjemci zasílán společně se skutečným jménem.
   2. Kontrola vstupů – Protokoly

(i) Pověřenec pro ochranu osobních údajů sleduje namátkově dodržování pokynů / zásad pro protokolování přístupů.

* 1. Kontrola objednávek
     1. Pověřenec pro ochranu osobních údajů (dle článků 37 až 39 obecného nařízení o ochraně osobních údajů (GDPR) a vnitrostátních právních předpisů)
        1. Je jmenován pověřenec pro ochranu osobních údajů, pokud je k tomu dodavatel povinen dle čl. 37 GDPR.
        2. U pověřenců pro ochranu osobních údajů nesmí docházet ke střetu zájmů.
        3. Pověřenec pro ochranu osobních údajů musí mít příslušnou kvalifikaci a musí být spolehlivý dle požadavků konkrétní společnosti.
        4. Pověřenec pro ochranu osobních údajů je jmenován písemnou formou.
        5. Vedení společnosti musí pověřence pro ochranu osobních údajů v jeho práci podporovat.
        6. Pověřenec pro ochranu osobních údajů je přímo podřízen vedení společnosti a přímo se mu zodpovídá.
        7. Pověřenec pro ochranu osobních údajů je včas informován o nových procesech či o modifikaci stávajících procesů a přímo se podílí na jejich plánování.
        8. Pověřenec pro ochranu osobních údajů aktivně přispívá k navrhování procesů.
  2. Smluvní požadavky
     1. Všichni subdodavatelé zapojení do zpracování objednávky jsou smluvně vázáni vůči Zhotoviteli.
     2. Smluvní dohoda mezi Zhotovitelem a subdodavatelem musí splňovat podmínky uvedené v článku 28, odstavci 3 GDPR.
  3. Výběr subdodavatelů
     1. Zhotovitel zdokumentuje rozhodnutí o subdodavateli a důvody pro jeho výběr.

**2.6** Další pravidla řízení ochrany osobních údajů

* + 1. Je zaveden systém ochrany osobních údajů a řízení rizik v souladu s požadavky GDPR. Externě zajišťované služby infrastruktury IT jsou do systému řízení rizik plně integrovány.
    2. V souvislosti se zpracováním osobních údajů probíhá analýza rizik dle předem stanovených transparentních kritérií a zjištěná rizika v bezpečnosti informací a ochrany osobních údajů jsou na základě těchto kritérií hodnocena a řádně řešena pomocí závazného a kontinuálního procesu. Účinnost přijatých opatření je hodnocena pravidelnými interními audity.
    3. Jsou vydávány pravidelné zprávy o ochraně osobních údajů popisující aktuální stav a účinnost systému řízení ochrany osobních údajů, včetně všech případných selhání či relevantních případů narušení ochrany osobních údajů/ bezpečnosti. Tyto zprávy jsou Zhotovitelem poskytnuty na vyžádání.
    4. Všechny dokumenty, které by měly být dostupné jsou vydávány v takové formě, aby mohly být poskytnuty třetí straně k posouzení zavedených opatření k ochraně osobních údajů a informací. Veškerá dokumentace je dle potřeby aktualizována. Dokumentace s upraveným obsahem je dostupná na vyžádání.
    5. Vedení společnosti Zhotovitele je plně informováno a zapojeno do informační bezpečnosti a ochrany osobních údajů formou příslušných komunikačních, eskalačních a rozhodovacích procesů. Vedení společnosti Zhotovitele zajistit, že činnosti a zodpovědnosti mohou být vykonávány v souladu s požadavky a v uspokojivé kvalitě.
    6. Jsou prokazatelně vyčleněny dostatečné zdroje na zřízení, implementaci, provozování, monitoring, hodnocení, údržbu a zlepšování systému řízení ochrany osobních údajů, stejně tak jako dostupného prokazování jeho existence.
    7. Do provozu systému řízení ochrany osobních údajů se mohou zapojit pouze zaměstnanci s dostatečnou kvalifikací a znalostmi nutnými pro realizaci příslušných úkolů. Tato kvalifikace a znalosti jsou zajišťovány formou pokynů a školení.
    8. Pravidelně, a alespoň jednou ročně, a nezávisle na hodnocení bezpečnosti IT a rizik probíhá interní audit stavu ochrany osobních údajů. Smyslem auditu je zjišťovat odchylky skutečného stavu ochrany údajů od smluvně garantované úrovně ochrany osobních údajů (tzn. všech dohodnutých technických a organizačních opatření). Tato zjištění pak dle potřeby slouží pro hodnocení rizika a lze je na vyžádání předložit.
    9. Výstupem auditu řízení ochrany osobních údajů je akční plán, který jasně definuje, jaké kroky je nutné přijmout a v jakém časovém horizontu tak, aby byly zjištěné problémy odstraněny.

Do plánu lze na vyžádání nahlédnout.

* + 1. Systém řízení ochrany osobních údajů je neustále zlepšován pomocí přístupu založeném na PDCA (naplánuj-proveď-ověřjednej), v jehož rámci je Společnost E.ON na vyžádání informována o fázi plánování a účastní se fáze realizace (Act – jednej), pokud se vyhrazené zdroje a zdroje pro více klientů týkají osobních údajů Společnosti E.ON.
    2. Účinnost systému řízení ochrany osobních údajů je ověřována interními a externími testy (audity).
    3. Jsou jmenovány příslušné kontaktní osoby a jsou poskytnuty konkrétní kontaktní informace a stanoveny postupy pro výměnu informací se Společností E.ON a koordinaci opatření k ochraně osobních údajů.

**2.7** Kontroly dostupnosti – Ukládání firemních dokumentů

**2.7.1** Dokumenty a elektronicky uložená data jsou po uplynutí zákonné, povinné nebo smluvní archivační doby skartovány a elektronicky uložená data vymazána dle plánu výmazu v souladu s příslušnými právními předpisy na ochranu osobních údajů.

1. **Normy** 
   1. Zhotovitel souhlasí s tím, že služby budou dodávány v souladu s těmito normami:
      1. ISO/IEC 27001: Všechna zařízení pro hostování dat a podpůrné služby, jakož i procesy, v jejichž rámci jsou ukládány nebo zpracovávány informace společnosti E.ON, musí být provozovány v souladu s normou ISO / IEC 27001 „Informační technologie – bezpečnostní techniky – systémy managementu bezpečnosti informací – požadavky“.
      2. Zhotovitel se zavazuje, že na vyžádání společnosti E.ON předloží příslušná prohlášení o shodě.
2. **Kontaktní osoby a výměna informací** 
   1. Obě Smluvní strany souhlasí se oznámením a poskytnutím kontaktních osob pro následující procesy bezpečnosti IT:
      1. Řízení shody s požadavky: průběžná výměna informací o dodržování požadavků, průběžné předkládání zpráv uvedených v této příloze a projednání a odsouhlasení opatření k řešení stávajících případů neshod s požadavky a souvisejících rizik.
      2. Řízení bezpečnostních incidentů: výměna informací o bezpečnostních incidentech nebo událostech, které by mohly vést k incidentu, který by ovlivnil nebo mohl ovlivnit prostředí IT provozované k ukládání nebo zpracování informací společnosti E.ON. „Řízení bezpečnostních incidentů“ zahrnuje také správu žádostí společnosti E.ON o forenzní analýzu.
      3. Řízení rizik: průběžná výměna informací o činnostech řízení rizik prováděných Zhotovitelem s cílem zajistit, aby rizika v oblasti bezpečnosti informací byla průběžně identifikována, hodnocena, ošetřována, monitorována a udržována v přijatelných mezích.
      4. Řízení zranitelností: výměna informací o zranitelnostech, které ovlivňují nebo by mohly ovlivnit prostředí IT provozované k ukládání nebo zpracování informací společnosti E.ON, a projednání a odsouhlasení opatření k odstranění / zmírnění stávajících zranitelností.
      5. Správa bezpečnostních záplat: výměna informací o dohodnutých časových obdobích údržby a instalace bezpečnostních záplat (tzv. „patchů“).
      6. Správa identit a přístupu: výměna informací o tématech souvisejících se správou identit a přístupu.
      7. Ochrana údajů: výměna informací o činnostech a incidentech souvisejících s ochranou osobních údajů.
   2. Obě Smluvní strany souhlasí s tím, že budou v rámci výše uvedených bezpečnostních procesů spolupracovat a vyměňovat si informace. Smluvní strany se dohodnou na technických prostředcích pro výměnu informací a klíčových ukazatelů výkonnosti (Key Performance Indicators, KPI) s cílem zajištění shody s dohodnutými bezpečnostními postupy.
   3. Obě Smluvní strany souhlasí s tím, že byly jmenovány kontaktní osoby pro výše uvedené bezpečnostní postupy a že může být provedena jejich personální výměna. V případě personální výměny kontaktní osoby Smluvní strana, která výměnu jmenované kontaktní osoby provede, o této skutečnosti bezodkladně uvědomí druhou Smluvní stranu.

*Kontaktní osoba společnosti E.ON*

Ochrana osobních údajů

Jméno a příjmení: Jindřich Veselý

Telefon: (+420) 733 670 559

E-mailová adresa: jindrich.vesely@eon.cz

Bezpečnost informací

Jméno a příjmení: Josef Ječmen

Telefon: (+420) 724 606 913

E-mailová adresa: josef.jecmen@eon.com

*Kontaktní osoba Zhotovitele*

Jméno a příjmení:

Telefon:

E-mailová adresa: