Příloha č. 6. – DPA smlouva

Smlouva o ochraně osobních údajů

mezi

**EG.D, s.r.o.,**se sídlem Lidická 1873/36, Brno – Černá Pole, 602 00 Brno, zapsanou v obchodním rejstříku vedeném Krajským soudem v Brně, sp. zn. C 142374 IČO 21055050

* jako správce, dále jen „Objednatel“–

a

doplní účastník**,**  
se sídlem doplní účastník,zapsanou v obchodním rejstříku vedeném doplní účastník soudem v doplní účastník, sp. zn. doplní účastník, IČO doplní účastník,

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

– společně dále jen „Smluvní strany“ –

– dále jen „Zpracovatelská smlouva“ –

**Obsah**

[Preambule 3](#_Toc155334795)

[§ 1 Předmět, doba trvání a specifikace Zpracování údajů 3](#_Toc155334796)

[§ 2 Odpovědnost a rozsah oprávnění ke stanovení pokynů 3](#_Toc155334797)

[§ 3 Technická a organizační opatření 4](#_Toc155334798)

[§ 4 Oprava, omezení zpracování, výmaz a vrácení osobních údajů 5](#_Toc155334799)

[§ 5 Ostatní povinnosti Zhotovitele 5](#_Toc155334800)

[§ 6 Vztahy se subdodavateli (dílčími zpracovateli) 7](#_Toc155334801)

[§ 7 Předání do třetích zemí 7](#_Toc155334802)

[§ 8 Monitoring 8](#_Toc155334803)

[§ 9 Odpovědnost 8](#_Toc155334804)

[§ 10 Odměna, dodatky Zpracovatelské smlouvy, salvatorní doložka 9](#_Toc155334805)

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 Rámcové dohody na poskytování služeb mobilní hlasové a datové komunikaceze dne včetně jejích příloh (dále jen „**Rámcová smlouva**“). Tato Smlouva zohledňuje právní úpravu platnou ke dni jejího uzavření na území České republiky, zejména 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 Rámcové smlouvy jako subdodavatele.

Ustanovení této Zpracovatelské 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 Zpracovatelská 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 Rámcové smlouvy. Konkrétně se Zpracování údajů týká zejména osobních údajů v následujícím rozsahu:

|  |  |  |
| --- | --- | --- |
| **Kategorie subjektů údajů** | **Kategorie osobních údajů** | **Účel  Zpracování údajů** |
| Stávající zaměstnanci (včetně agenturních) | ***Identifikační údaje***  *jméno a příjmení / telefon / mobilní telefon*  ***Individuální údaje***  *zvukové záznamy (nahrávky hovorů) / poloha GPS* | **"Provozní potřeby zaměstnavatele**  **Vnitřní evidence a kontrola"** |

1. Doba platnosti této Zpracovatelské smlouvy je určena dobou platnosti Rámcové smlouvy, 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.
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 Rámcové 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 Zpracovatelské 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 Rámcovou smlouvu 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 č. X.1** této Zpracovatelské 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. Pokud tyto náklady budou mít se zřetelem k ustanovením této Zpracovatelské smlouvy a zájmům Objednatele na dodržování smluvních povinností ze strany Zhotovitele za následek nepřiměřenou ekonomickou újmu pro Zhotovitele a současně Zhotovitel odpovídajícím způsobem doloží tyto náklady Objednateli, pokusí se Smluvní strany dosáhnout vzájemným jednáním dohody o rozdělení nákladů.
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. V souladu s doloženým pokynem Objednatele nebo s požadavky na výmaz údajů a po ukončení Zpracování údajů musí Zhotovitel bez zbytečného odkladu odevzdat Objednateli všechny dokumenty, které obdrží, vytvořené výsledky zpracování a užívání a záznamy údajů související se smluvním vztahem k Objednateli. 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 Objednateli, 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 povinni dodržovat zákonné povinnosti ohledně uchovávání dokumentů.
2. Dokumentaci, která slouží k ověření řádného Zpracování údajů dle objednávky, bude Zhotovitel uchovávat i po ukončení Zpracovatelské smlouvy v souladu s příslušnými lhůtami pro uchovávání nebo ji 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 Zpracovatelské 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 Zpracovatelské 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 Zpracovatelskou smlouvou a s veškerými pokyny Objednatele. Jestliže nejsou ustanovení o vyřizování práv subjektů údajů uplatněnými vůči Zhotoviteli obsažena ve Zpracovatelské 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 Zpracovatelské 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 Zpracovatelskou 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:

E.ON Česká republika, s.r.o.

Ing. Jindřich Veselý

gpdr@eon.cz

+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 Zpracovatelské 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 se subdodavateli (dílčími zpracovateli)
6. Zhotovitel je oprávněn do zpracování údajů zapojit subdodavatele (jakožto dalšího zpracovatele) pouze tehdy, pokud o tom byl Objednatel předem písemnou nebo obdobnou formou vyrozuměn a dal k tomu souhlas.
7. Pokud je podle ustanovení výše uvedeného odstavce Zhotovitel oprávněn využít subdodavatele, musí jej Zhotovitel vybrat s řádnou péčí a před jeho zapojením si musí být jist tím, že takový subdodavatel je schopen plnit všechny povinnosti Zhotovitele stanovené v této Zpracovatelské smlouvě. Zhotovitel je rovněž povinen uložit příslušnému subdodavateli povinnosti stanovené v této Zpracovatelské smlouvě v tom rozsahu, v němž tento subdodavatel jedná za Zhotovitele. Zhotovitel je povinen rovněž smluvně zajistit, aby všechny činnosti stanovené v této Zpracovatelské 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 subdodavatel 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 Zpracovatelské 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 této Rámcové 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 Zpracovatelskou 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 Zpracovatelské 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 Zpracovatelské 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 Zpracovatelské 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 Zpracovatelské 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 Zpracovatelské 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 Zpracovatelské 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 Zpracovatelské smlouvy, salvatorní doložka
15. Zpracovateli náleží odměna za opatření a aktivity, které má realizovat, povinnosti, které má plnit a součinnost, kterou má poskytnout dle této Zpracovatelské smlouvy. Tato odměna je stanovená v Rámcové smlouvě.
16. Změny a dodatky k této Zpracovatelské smlouvě, včetně tohoto článku, mohou být provedeny pouze v písemné nebo obdobné formě.
17. Na uzavření této Zpracovatelské smlouvy nebo jejích případných dodatků či jiných dohod navazujících na tuto Zpracovatelskou 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 Zpracovatelské smlouvy je nebo se stane neúčinným nebo neurčitým, nebude touto okolností ovlivněna účinnost ani úplnost zbytku Zpracovatelské 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 Zpracovatelskou 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 Zpracovatelské 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 Zpracovatelskou smlouvou výslovně neupravené se řídí obecně závaznými právními předpisy České republiky.
21. Smluvní strany prohlašují, že souhlasí s obsahem Zpracovatelské smlouvy, že tato Zpracovatelská 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.

Součástí této Zpracovatelské smlouvy je tato příloha:

Příloha č. X.1: Technicko-organizační opatření bezpečnosti informací a ochrany osobních údajů dle článku 3 Zpracovatelské smlouvy

**Příloha č. X.1 - Technicko-organizační opatření bezpečnosti informací a ochrany osobních údajů**

Technicko-organizační opatření bezpečnosti informací a ochrany osobních údajů

Technicko-organizační opatření bezpečnosti informací a ochrany osobních údajů zde uvedená byla ve smyslu odst. 1.1. Všeobecných nákupních podmínek společností E.ON Czech sjednána mezi některou ze společností skupiny E.ON Czech jako KLIENTEM a zhotovitelem, poskytovatelem či dodavatelem nebo prodávajícím na straně druhé jako DODAVATELEM v souvislosti s uzavřením a plněním Smlouvy.

# Požadavky na bezpečnost informací

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

## Důvěryhodná dodávka

DODAVATEL zajistí, aby hardwarové a softwarové produkty byly nakupovány ze známých a spolehlivých zdrojů a aby byla zajištěna spolehlivá technická podpora a identifikovatelný dodavatelský řetězec.

## Správa bezpečnosti informací

DODAVATEL zavede, udržuje a sleduje rámec řízení bezpečnosti informací. Ten umožňuje vedení společnosti DODAVATELE stanovit jasné směrování a cíle v oblasti bezpečnosti informací a řízení rizik.

## Řízení rizik v oblasti bezpečnosti informací

DODAVATEL zajistí, aby

(i) před zavedením nových IT systémů, ve kterých jsou zpracovávány informace KLIENTA, včetně jeho osobních údajů (dále označovaných jako „informace KLIENTA“),

(ii) před zavedením významných změn ve stávajících systémech a

(iii) před zavedením významných nových technologií,

byla zjištěna, hodnocena, řešena, sledována a udržována související rizika v přijatelných mezích pro oblasti bezpečnosti informací.

Informace týkající se činností ve vztahu k řízení rizik budou na vyžádání poskytnuty KLIENTOVI, a to bez zbytečného odkladu.

## Řízení bezpečnosti

DODAVATEL (i) zřídil specializovanou roli pro bezpečnost informací, která je na dostatečně vysoké úrovni řízení se svěřenými přiměřenými pravomocemi a 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. DODAVATEL (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 KLIENTA, a toto chování jim vštěpovat, a to v pravidelných intervalech, alespoň 1krát ročně nebo při významných změnách.

## Zdokumentované provozní postupy

DODAVATEL 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. Dokumentace provozních postupů bude na vyžádání poskytnuta KLIENTOVI, a to bez zbytečného odkladu.

## Správa aktiv

DODAVATEL zajistí, aby (i) aktiva (hardwarové a softwarové prostředky, dále označované jako „aktiva“), která se používají k vytváření, zpracování, ukládání nebo předávání informací KLIENTA, byla během celého životního cyklu chráněna proti poškození, ztrátě, krádeži a neoprávněnému zpřístupnění. DODAVATEL zajistí, aby tato aktiva byla evidována v inventáři aktiv, který (ii) je chráněn proti neoprávněnému pozměňování, (iii) aktualizován, (iv) pravidelně zálohován a (v) obsahuje potřebné údaje o těchto aktivech a případně i požadavky na dodržování předpisů v souvislosti s těmito aktivy. DODAVATEL zajistí, aby (vi) každému aktivu byl přiřazen jeho vlastník, který je odpovědný za provozování daného aktiva.

## Fyzická bezpečnost

DODAVATEL musí přijmout příslušná opatření pro zajištění fyzické bezpečnosti a ochranu přístupu. Musí být zejména přijata opatření k ochraně před ohněm a vodou, ochraně před extrémními teplotami nebo k zamezení jejich výskytu (klimatizace), k zajištění nouzového napájení. Přístup do prostor s informacemi nebo systémy zpracovávajícími informace KLIENTA nebo s podpůrnými procesy, které mají vliv na bezpečnost informací KLIENTA, může mít jen skupina oprávněných osob (se zásadou co nejomezenějších práv). To zahrnuje i opatření na ochranu přístupu do datových center, včetně sledování kritických oblastí, záznamů o přístupu, přístupu zaměstnanců externích společností pouze s doprovodem a bezpečnostní opatření proti vniknutí.

## Řízení přístupu

DODAVATEL omezí přístup k aktivům, která slouží k vytváření, zpracování, ukládání nebo předávání informací KLIENTA na oprávněné osoby a pro vyhrazené provozní činnosti. To přinejmenším znamená, že (i) přístup k informacím KLIENTA 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 a výchozí hesla musí být změněna při prvním použití). DODAVATEL zajistí, aby přístup pro správu k systémům, které slouží k ukládání nebo zpracování informací KLIENTA, byl (v) omezen na minimální počet správců, (vi) chráněn dvoufaktorovou autentizací, nebo pokud není možné dvoufaktorovou autentizaci technicky implementovat, zajistí obdobnou úroveň bezpečnosti (jako jsou generovaná dočasná hesla ve správě systémů). DODAVATEL dále zajistí, aby byl přístup pro správu (vii) vždy protokolován s cílem umožnit zjištění a přešetření neoprávněného přístupu k informacím KLIENTA a neoprávněné manipulaci s nimi. (viii) DODAVATEL 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.

## Správa systémů

DODAVATEL provozuje systémy, které vytvářejí, ukládají, zpracovávají nebo předávají informace KLIENTA takovým způsobem, aby (i) bylo možné zvládnout aktuální i předpokládanou pracovní zátěž a (ii) a byly důsledně a přesně nakonfigurovány s cílem chránit tyto systémy a informace KLIENTA, které zpracovávají, ukládají nebo předávají, proti selhání, kybernetickému útoku, neoprávněnému zpřístupnění, poškození, krádeži či ztrátě. DODAVATEL 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.

## Síť a komunikace

DODAVATEL zajistí, aby fyzické, bezdrátové a případně i hlasové sítě byly navrženy takový způsobem, aby (i) byly spolehlivé a odolné, (ii) zabránily neoprávněnému přístupu, (iii) využívaly šifrované spojení a (iv) odhalily podezřelý provoz v síti. (v) DODAVATEL zajistí nakonfigurování síťových zařízení (včetně směrovačů, firewallů a bezdrátových přístupových bodů) tak, aby fungovaly podle potřeby a zabránily neoprávněným a nesprávným aktualizacím. DODAVATEL zajistí ochranu elektronických komunikačních systémů (vi) stanovením zásad pro jejich používání, (vii) nakonfigurováním bezpečnostního nastavení, (viii) posílením bezpečnostního nastavení podpůrné technické infrastruktury. (ix) DODAVATEL zajistí, aby názvy a topologie počítačů a sítí zůstaly skryty externím subjektům. DODAVATEL 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.

## Správa technických bezpečnostních opatření

DODAVATEL instaluje řešení ochrany proti škodlivému kódu v systémech, ve kterých mohou být informace KLIENTA 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. DODAVATEL 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 je správně nakonfigurovaný, (vii) jsou správně aplikovány aktualizace v rámci definovaných časových intervalů, (ix) probíhají kontroly systému v předem určených časech a (x) systém náležitě upozorňuje na zjištěné případy přítomnosti škodlivého kódu.

## Vzájemné oddělení testovacích a produkčních systémů

DODAVATEL 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, DODAVATEL 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).

## Vývoj/pořizování softwaru

DODAVATEL zajistí, aby interně vyvinutý software nebo software získaný z externích zdrojů, který se používá ke zpracování, ukládání nebo předávání informací KLIENTA, nevykazoval žádné bezpečnostní chyby z hlediska kritérií „OWASP TOP Ten” a “SANS Top 25 Most Dangerous Software Errors”.

## Prověřování bezpečnostních zranitelností

DODAVATEL zajistí, aby (i) veřejně přístupné systémy byly pravidelně (nejméně jednou měsíčně) testovány na zranitelnosti a chyby v nastavení provedením dynamických testů (penetrační test nebo prověřování zranitelnosti). (ii) KLIENT byl bez zbytečného odkladu, informován o veškerých zjištěních z těchto testů, které jsou pro KLIENTA relevantní; (iii) kritické zranitelnosti byly KLIENTOVI okamžitě oznámeny. (iv) DODAVATEL poskytne pomoc a podporu při kontrolách procesu správy bezpečnostních zranitelností a oprav (tzv. „záplat“) prováděných KLIENTEM. (v) Ošetření bezpečnostních zranitelností se řeší na základě úrovní rizika těchto zranitelností a dle příslušných časových harmonogramů smluvních stran.

## Úroveň aktuálnosti bezpečnostních záplat (tzv. patchů)

DODAVATEL zajistí odstranění technických 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 v databázi CMDB. (vi) DODAVATEL je oprávněn bezpečnostní záplaty používat v IT prostředí, včetně virtualizačních hypervisorů, virtuálních počítačů, operačních systémů a aplikací, pokud to nepříznivě neovlivní zachování důvěrnosti, integrity nebo dostupnosti informací KLIENTA.

## Minimální požadavky na přihlašovací údaje

DODAVATEL zajistí, že minimální požadavky KLIENTA na přihlašovací údaje (dvoufaktorová autentizace) jsou vynuceny prostřednictvím KLIENTOVA federativního Single-Sign-On řešení pro IT prostředí, které je používáno k ukládání nebo zpracování informací KLIENTA. 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.

## Požadavky na návrh sítí

Aplikace, které jsou přístupné prostřednictvím internetu, musí mít vícevrstvou architekturu a musí být umístěny 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.

## Vzdálený přístup a mobilní pracoviště

DODAVATEL zajistí, aby byly možnosti vzdáleného přístupu chráněny dle aktuálních technických standardů „state of the art“. Mobilní pracoviště zaměstnanců DODAVATELE, kteří mají přístup k informacím KLIENTA, musí být KLIENTOVI předem oznámena (obecně, nikoliv za jednotlivé zaměstnance) a mohou být využívána pouze v případě, že zaměstnanci byli proškoleni a písemně se zavázali dodržovat předpisy o ochraně osobních údajů a provozní předpisy. DODAVATEL musí zaměstnancům za tímto účelem poskytnout software a hardware, který lze používat výhradně pro obchodní účely nebo který podporuje účinné oddělení obchodních a soukromých údajů (např. kontejnerové řešení). Důvěrné dokumenty musí být uchovávány bezpečně tak, aby k nim neměly přístup třetí strany. Dokumenty mohou být skartovány pouze v prostorách DODAVATELE v rámci likvidace/zničení dokumentů v souladu s předpisy pro ochranu osobních údajů. Zároveň musí být při poskytování Služeb v rámci mobilní práce dodržována dohodnutá bezpečnostní opatření. Musí být zabráněno odposlouchávání a čtení informací neoprávněnými osobami. DODAVATEL KLIENTOVI na požádání poskytne veškeré informace nezbytné k prokázání dodržování specifikací pro mobilní pracoviště.

## Šifrování

Uložené (Data-at-Rest) a přenášené (Data-in-Motion) údaje mohou být uchovávány a přenášeny pouze prostřednictvím bezpečnostních protokolů a nejmodernějšího šifrování. Autentizační prvky (hesla, PIN kódy) mohou být po síti přenášeny pouze v zašifrované podobě. Kromě toho musí být fyzická přeprava paměťových médií zabezpečena fyzickou ochranou a šifrováním.

## Standardy bezpečnostního nastavení (tzv. hardening)

Všechny informační 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.

## Dostupnost a podpora

Nedohodnou-li se strany jinak, DODAVATEL zajistí splnění následujících požadavků na dostupnost, podporu parametry RPO (Recovery Point Objective) a RTO (Recovery Time Objective):

* dostupnost 99,6 % nebo vyšší
* podpora 24/7
* parametr Recovery Point Objective (RPO) < 8 hodin
* parametr Recovery Time Objective (RTO) < 24 hodin

## Fyzický hypervisor a virtuální počítač

Pro provozování aplikace KLIENTA se používá vyhrazený fyzický hypervisor a vyhrazený virtuální počítač.

## Protokolování bezpečnostních událostí

V zájmu zjištění a vyšetřování neoprávněného přístupu k informacím KLIENTA a neoprávněné manipulace s nimi DODAVATEL zajistí, aby (i) u všech systémů provozovaných DODAVATELEM za účelem vytváření, ukládání, zpracování a předávání informací KLIENTA bylo vždy povoleno protokolování událostí (logování), (ii) tyto systémy byly nakonfigurovány tak, aby generovaly bezpečnostní události a události významné z pohledu integrity dat (včetně událostí, jako jsou změny informací KLIENTA, úspěšné a neúspěšné pokusy o přihlášení uživatele, vytvoření/úprava/odstranění Služby, vytvoření/úprava/odstranění objektu, 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 serveru NTP), (iv) protokoly bezpečnostních událostí a událostí významných z pohledu integrity a důvěrnosti údajů byly chráněny před neoprávněným přístupem a náhodnou nebo úmyslnou úpravou/přepsáním, (v) protokoly bezpečnostních událostí byly extrahovány do centrálního úložiště provozovaného KLIENTEM v reálném čase. Obě Smluvní strany se dohodly, že pro tyto účely společně definují a zavedou koncepci, která podrobně stanoví, jak budou extrahovány protokoly událostí, a zároveň se dohodly, že tuto koncepci budou společně v celém průběhu poskytování Služeb dodržovat s cílem zajistit, aby změny prostředí IT neovlivňovaly dostupnost protokolů událostí nebo typy reportovaných událostí (Use Cases) pro účely správy událostí zabezpečení. (vi) DODAVATEL dále zajistí, aby jakékoli forenzní analýzy/činnosti mající dopad na systémy, které vytvářejí, ukládají, zpracovávají nebo předávají informace KLIENTA byly prováděny společně s pracovníkem útvaru KLIENTA pro bezpečnost IT, aby se vyhovělo zásadě „čtyř očí“, je-li to vyžadováno.

## Dodržování předpisů

DODAVATEL zajistí, aby (i) všechny systémy, které vytvářejí, ukládají, zpracovávají nebo předávají informace KLIENTA, byly pravidelně kontrolovány z hlediska dodržování vlastních „bezpečnostních politik/standardů“ DODAVATELE. (ii) Vlastní „bezpečnostní politiky/standardy“ DODAVATELE musí být v souladu s certifikáty uvedenými v oddílech 2 a 3 této přílohy. (iii) KLIENT na vyžádání bez zbytečného odkladu obdrží 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) DODAVATEL vlastní „bezpečnostní zásady/standardy“ zpřístupní KLIENTOVI před Datem účinnosti a poté na žádost KLIENTA bez zbytečného odkladu.

## Bezpečná likvidace a opětovné použití

DODAVATEL zajistí, aby hardware, který má být vyřazen z provozu, (i) byl před jeho opětovným použitím, prodejem nebo vrácením vyčištěn tak, aby všechny informace KLIENTA 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 s NIST 800-88 "Guidelines for Media Sanitization" (Postupy pro odstraňování dat z médií). (iv) Koncepce bezpečného odstraňování a smazání, jakož i důkazy o provedeném bezpečném odstranění a vymazání informací KLIENTA jsou na vyžádání předloženy KLIENTOVI bez zbytečného odkladu.

## Bezpečnost lidských zdrojů

Za každou osobu, která jedná jménem DODAVATELE a byla jí udělena přístupová oprávnění (místně nebo vzdáleně), musí být KLIENTOVI poskytnuty osobní identifikační údaje. DODAVATEL zajistí ověření totožnosti fyzických osob a dále zajistí, aby nikdo nezneužil přístupu nebo oprávnění udělených DODAVATELEM. DODAVATEL zajistí, aby byla udělená oprávnění okamžitě odebrána po ukončení smlouvy nebo změně osob anebo odpovědností. DODAVATEL dále přejímá odpovědnost za případné škody způsobené neoprávněným přístupem anebo použitím informací KLIENTA. DODAVATEL pověří plněním zadaných úkolů výhradně pracovníky, kteří jsou k jejich plnění prokazatelně odborně způsobilí.

## Bezpečnost v oblasti dodavatelského řetězce

DODAVATEL zajistí identifikaci a řízení rizika bezpečnosti informací v každé fázi vztahů s externími dodavateli 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) DODAVATEL zajistí, aby subdodavatelé, kteří se podílí na zpracování, ukládání, předávání nebo likvidaci informací KLIENTA, splňovali minimálně požadavky dohodnuté v této příloze. (iv) DODAVATEL je zodpovědný za zajištění náležitého řízení subdodavatele(ů) a za dodržování opatření prováděných externě.

# Požadavky na ochranu osobních údajů

## Závazek k mlčenlivosti

DODAVATEL musí písemně zavázat všechny své zaměstnance a další osoby podílející se na plnění Smlouvy, kteří zpracovávají osobní údaje KLIENTA nebo mají k takovým údajům přístup, aby zachovávali mlčenlivost při nakládání s osobními údaji alespoň v takovém rozsahu, v jakém je DODAVATEL povinen vůči KLIENTOVI.

Pokud to stanoví Smlouva nebo to vyžaduje všeobecně závazný právní předpis, musí DODAVATEL rovněž zajistit ochranu osobních, provozních a lokalizačních údajů a důvěrnost komunikací k zachovávání telekomunikačního tajemství (v souladu s ust. § 87 a násl. zákona č. 127/2005 Sb. o elektronických komunikacích, ve znění pozdějších předpisů) nebo podle jiného všeobecně závazného právního předpisu.

DODAVATEL proškolí všechny zaměstnance, kteří zpracovávají osobní údaje KLIENTA nebo mají k takovým údajům přístup na bezpečnost a ochranu údajů. Jména účastníků školení budou dokumentována.

## Záměrná ochrana osobních údajů

DODAVATEL přijme předpisy o „záměrné ochraně osobních údajů“ s cílem zohlednit při vývoji a návrhu výrobků, Služeb a aplikací právo na ochranu údajů (takovými opatřeními, jako například minimalizací údajů, pseudonymizací, výchozím nastavením vhodným pro ochranu údajů).

## Pověřenec pro ochranu osobních údajů

V souladu s právními požadavky (dle článků 37 až 39 obecného nařízení o ochraně osobních údajů (GDPR) a vnitrostátních právních předpisů) je jmenován pověřenec pro ochranu osobních údajů.

U pověřenců pro ochranu osobních údajů nesmí docházet ke střetu zájmů.

Pověřenec pro ochranu osobních údajů musí mít příslušnou kvalifikaci a musí být spolehlivý dle požadavků konkrétní společnosti.

Vedení společnosti musí pověřence pro ochranu osobních údajů v jeho práci podporovat.

Pověřenec pro ochranu osobních údajů je přímo podřízen vedení společnosti a přímo se mu zodpovídá.

Pověřenec pro ochranu osobních údajů je včas informován o nových procesech či o modifikaci stávajících procesů a přímo se podílí na jejich plánování.

Pověřenec pro ochranu osobních údajů aktivně přispívá k navrhování procesů.

## Systém řízení ochrany osobních údajů

DODAVATEL zavedl systém ochrany osobních údajů splňující požadavky GDPR a podléhá průběžnému procesu testování a zlepšování.

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.

Jsou vydávány čtvrtletní zprávy o ochraně osobních údajů popisující aktuální stav a účinnost sytému řízení ochrany osobních údajů, včetně všech případných selhání či relevantních případů narušení ochrany osobních údajů/bezpečnosti. Tyto zprávy jsou poskytnuty na vyžádání.

Vedení je plně informováno a zapojeno do informační bezpečnosti a ochrany osobních údajů formou příslušných komunikačních, eskalačních a rozhodovacích procesů. Vedení společnosti zajistí, že činnosti a zodpovědnosti mohou být vykonávány v souladu s požadavky a v uspokojivé kvalitě.

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.

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.

Pravidelně, minimálně 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.

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.

Systém řízení ochrany osobních údajů je neustále zlepšován pomocí přístupu založeném na PDCA (naplánuj-proveď-ověř-jednej), v jehož rámci je zmocnitel na vyžádání informován o fázi plánování a účastní se fáze realizace (Act – jednej), pokud se vyhrazené zdroje a zdroje pro více klientů týkají osobních údajů zmocnitele.

Účinnost systému řízení ochrany osobních údajů je ověřována interními a externími testy (inspekcemi).

# Certifikace

DODAVATEL souhlasí s tím, že zajistí, aby po celou dobu plnění Smlouvy udržoval v platnosti následující certifikace:

* ISO/IEC 27001: Všechna zařízení pro hostování dat a podpůrné služby, v jejichž rámci jsou ukládány nebo zpracovávány informace KLIENTA jsou certifikovány dle normy ISO/IEC 27001 „Informační technologie – bezpečnostní techniky – systémy managementu bezpečnosti informací – požadavky”.

DODAVATEL se zavazuje, že předloží KLIENTOVI před Datem účinnosti této Smlouvy příslušný certifikát, jakož i „Prohlášení o aplikovatelnosti“ a tento certifikát předloží KLIENTOVI rovněž po jeho obnovení a na vyžádání KLIENTA bez zbytečného odkladu kdykoli během Doby trvání této Smlouvy.

Odchylka od požadavků na Certifikace je možná formou výjimky, která musí být součástí Smlouvy.

Pokud má KLIENT dodatečné požadavky na certifikace s ohledem na poskytovanou službu DODAVATELEM, budou specifikovány v předmětu smlouvy (například ISO/IEC 22301 (Ochrana společnosti – systémy managementu kontinuity podnikání – požadavky), AICPA SOC2 Typ II[[1]](#footnote-1)).

# Zpráva o kontrole organizace zaměřené na Služby (Zpráva SOC)

Pokud je ve Smlouvě požadován soulad s AICPA SOC2 Typ II, DODAVATEL se zavazuje, že předloží zprávu AICPA SOC2 Typ II s cílem prokázat, jak prosazuje klíčové kontroly a cíle v oblasti dodržování předpisů (ve vztahu k zabezpečení, dostupnosti, integritě zpracování, důvěrnosti a ochraně údajů), a tuto zprávu si nechá přezkoumat nezávislou třetí stranou, která vydá v této souvislosti kontrolní zprávu.

DODAVATEL se zavazuje, že příslušnou zprávu předloží KLIENTOVI před Datem účinnosti této Smlouvy, po opětovném vydání této zprávy a na vyžádání KLIENTA bez zbytečného odkladu kdykoli během Doby trvání této Smlouvy.

# Rozhraní bezpečnostních procesů v oblasti IT

Obě strany souhlasí s oznamováním a poskytnutím kontaktních osob pro následující procesy bezpečnosti IT:

* Řízení shody s požadavky: průběžná výměna informací o dodržování požadavků, průběžné předávání certifikací a zpráv uvedených v této příloze a projednání a odsouhlasení opatření k řešení stávajících případů neshod s požadavky a souvisejících rizik. Pravdivé odpovědi v dotazníku „sebehodnocení dodavatele“ v platformě pro řízení rizik KLIENTA. Poskytnutí zvláštních informací o dodržování požadavků ze strany subdodavatelů DODAVATELE, je-li to požadováno.
* Řízení bezpečnostních incidentů v oblasti IT a porušení zabezpečení osobních údajů: výměna informací o bezpečnostních incidentech nebo událostech v IT oblasti, které by mohly vést k incidentu, který by ovlivnil nebo mohl ovlivnit prostředí IT provozované k ukládání nebo zpracování informací KLIENTA. „Řízení bezpečnostních incidentů v oblasti IT” zahrnuje také správu žádostí KLIENTA o forenzní analýzu. Porušení zabezpečení osobních údajů a bezpečnostní incidenty v IT oblasti ovlivňující ochranu osobních údajů musí DODAVATEL okamžitě oznámit KLIENTOVI, nejdéle do zákonem stanovené lhůty. V tomto ohledu se odkazuje na příslušná ustanovení dohody o ochraně údajů.
* Řízení rizik: průběžná výměna informací o činnostech řízení rizik prováděných DODAVATELEM s cílem zajistit, aby byla rizika v oblasti bezpečnosti informací průběžně identifikována, hodnocena, ošetřována, monitorována a udržována v přijatelných mezích.
* Řízení zranitelností: výměna informací o zranitelnostech, které ovlivňují nebo by mohly ovlivnit prostředí IT provozované k ukládání nebo zpracování informací KLIENTA a projednání a odsouhlasení opatření k odstranění/zmírnění stávajících zranitelností.
* Řízení bezpečnostních záplat: výměna informací o dohodnutých časových obdobích údržby a instalace bezpečnostních záplat (tzv. patchů).
* Správa identit a přístupu: výměna informací o tématech souvisejících se správou identit a přístupu.

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.

1. AICPA (American Institute of Certified Public Accountants). SOC 2 Type II je auditorský standard a zpráva, která hodnotí kontroly a procesy související s bezpečností, dostupností, integritou zpracování, důvěrností a ochranou údajů v servisní organizaci. [↑](#footnote-ref-1)