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

1 Požadavky na bezpečnosti informací

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

1.1 **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.

1.2 **Správa bezpečnosti informací**: Dodavatel zavede, udržuje a sleduje rámec řízení bezpečnosti informací. Ten umožňuje vedení společnosti Dodavatele stanovit jasné směřování a cíle v oblasti bezpečnosti informací a řízení rizik. Tím vedení společnosti Dodavatele dává najevo závazek s naplňováním těchto cílů.

1.3 **Řízení rizika v oblasti bezpečnosti informací**: Dodavatel 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. Dodavatel bez zbytečného odkladu poskytne na vyžádání společnosti E.ON informace týkající se činností ve vztahu k procesu řízení rizik.

1.4 **Řízení bezpečnosti**: Dodavatel (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. 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 společnosti E.ON, a toto chování jim vštěpovat.

1.5 **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. Dodavatel bez zbytečného odkladu poskytne na vyžádání společnosti E.ON dokumentaci provozních postupů.

1.6 **Správa aktiv**: Dodavatel 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. Dodavatel 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. Dodavatel zajistí, aby (vi) každému aktivu byl přiřazen jeho vlastník, který je odpovědný za provozování daného aktiva.

1.7 **Řízení přístupu**: Dodavatel 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). Dodavatel 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 dvoufaktorovu autentizací, nebo pokud není možné dvoufaktorouvou autentizaci technicky implementovat, zajistí obdobnou úroveň bezpečnosti řízení přístupu (jako jsou generovaná dočasná hesla v systémech pro správu, vynucování politiky hesel, použití kryptografických klíčů). Dodavatel 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) 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.

1.8 **Správa systémů**: Dodavatel 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 je nakonfigurovány s cílem chránit tyto systémy a informace, 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.

1.9 **Síť a komunikace**: Dodavatel 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) 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.

1.10 **Správa technických bezpečnostních opatření**: Dodavatel 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. 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 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.

1.11 **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).

1.12 **Vývoj/pořizování softwaru**: Dodavatel 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“.

1.13 **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 zranitelností), (ii) společnost E.ON byla bez zbytečného odkladu informována o veškerých zjištěních z těchto testů, která jsou pro společnost E.ON relevantní; (iii) kritická zranitelnost zabezpečení byla společnosti E.ON okamžitě oznámena. (iv) Dodavatel 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.

1.14 **Úroveň aktuálnosti bezpečnostních záplat (tzv. patchů)**: Dodavatel 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). (v) Dodavatel 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.

1.15 **Minimální požadavky na přihlašovací údaje:** Dodavatel 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.

1.16 **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.

1.17 **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.

1.18 **Dostupnost a podpora**: 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

1.19 **Fyzický hypervisor a virtuální počítač**: Pro provozování aplikace společnosti E.ON se používá vyhrazený hypervisor a vyhrazený virtuální počítač.

1.20 **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 Dodavatelem 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 služeb, vytvoření / úprava / odstranění objektů, 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 (v) protokoly bezpečnostních událostí byly extrahovány do centrálního úložiště provozovaného společností E.ON 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 společnosti E.ON, byly prováděny společně s pracovníkem útvaru pro bezpečnost IT společnosti E.ON, aby se vyhovělo zásadě „čtyř očí“, pokud si to společnost E.ON vyžádá.

1.21 **Dodržování předpisů (compliance)**: Dodavatel 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 Dodavatele“. (ii) Vlastní „bezpečnostní politiky/standardy“ Dodavatele musí být v souladu s požadavky s certifikáty uvedenými v oddílech 2 a 3 této přílohy. (iii) Dodavatel 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) Dodavatel vlastní „bezpečnostní zásady / standardy“ zpřístupní před Datem účinnosti a poté na žádost společnosti E.ON.

1.22 **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 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) Dodavatel na vyžádání společnosti E.ON předloží koncepce bezpečného odstraňování a smazání, jakož i důkazy o provedeném bezpečném odstranění a vymazání informací společnosti E.ON.

1.23 **Bezpečnost lidských zdrojů:** Za každou osobu, která jedná jménem Dodavatele a byla jí udělena přístupová oprávnění (místně nebo vzdáleně), musí být společnosti E.ON poskytnuty osobní identifikační údaje. Dodavatel zajistí ověření totožnosti fyzických osob a dále zajistí, aby nikdo nezneužil přístupu nebo oprávnění udělených Dodavatelem. Dodavatel dále přejímá odpovědnost za případné škody způsobené neoprávněným přístupem a/nebo použitím informací společnosti E.ON. Dodavatel pověří plněním zadaných úkolů výhradně pracovníky, kteří jsou k jejich plnění prokazatelně odborně způsobilí.

1.24 **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 podílejí na zpracování, ukládání, předávání nebo likvidaci informací společnosti E.ON, splňovali minimálně požadavky dohodnuté v této příloze. (iv) Dodavatel je zodpovědný za zajištění náležitého řízení Subdodavatele(ů) a za dodržování opatření prováděných externě.

2 Požadavky na ochranu osobních údajů

2.1 Kontrola fyzického přístupu

2.1.1 Přístupové protokoly jsou uchovávány pouze v případě, že jsou zapotřebí pro zamýšlený povolený účel.

2.1.2 Vyhodnocování přístupových protokolů je v souladu s předpisy o ochraně osobních údajů.

2.2 Opatření ochrany přístupu k datům

2.2.1 Uživateli se zobrazuje čas posledního použití.

2.3 Kontrola přenosu

2.3.1 Požadavky na pracovníky v oblasti mlčenlivosti

(i) Všichni pracovníci, kteří zpracovávají osobní údaje pomocí automatizovaných procesů, musí dodržovat pravidla mlčenlivosti.

(ii) Noví pracovníci musí být informováni o ochraně údajů pro potřeby nakládání s osobními údaji.

(iii) Všechny zúčastněné strany si jsou vědomy otázek souvisejících s bezpečností a ochranou údajů.

(iv) Osoby, které osobní údaje zpracovávají, jsou prokazatelně poučeni o bezpečném nakládání s osobními údaji na pracovišti.

(v) Jsou definována jasná pravidla pro postup v případě odchodu a propouštění pracovníků.

2.3.2 Anonymizace / pseudonymizace

(i) Pro potřeby přenosu osobních údajů jsou využívány techniky anonymizace a pseudonymizace.

(ii) V případě pseudonymizace dokumentačních údajů je nutné zajistit, aby pseudonym nebyl příjemci zasílán společně se skutečným jménem.

2.4 Kontrola vstupů – Protokoly

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

2.5 Kontrola objednávek

2.5.1 Pověřenec pro ochranu osobních údajů (dle článků 37 až 39 obecného nařízení o ochraně osobních údajů (GDPR) a vnitrostátních právních předpisů)

(i) Je jmenován pověřenec pro ochranu osobních údajů.

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

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

(iv) Pověřenec pro ochranu osobních údajů je jmenován písemnou formou.

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

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

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

(viii) Pověřenec pro ochranu osobních údajů aktivně přispívá k navrhování procesů.

2.6 Smluvní požadavky

2.6.1 Všichni subdodavatelé zapojení do zpracování objednávky jsou smluvně vázáni vůči Dodavateli.

2.6.2 Smluvní dohoda mezi Dodavatelem a subdodavatelem musí splňovat podmínky uvedené v článku 28, odstavci 3 GDPR.

2.7 Výběr subdodavatelů

2.7.1 Dodavatel zdokumentuje rozhodnutí o subdodavateli a důvody pro jeho výběr.

2.8 Systém řízení ochrany osobních údajů

2.8.1 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.

2.8.2 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.

2.8.3 Jsou vydávány čtvrtletní 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 Dodavatelem poskytnuty na vyžádání.

2.8.4 Všechny dokumenty, které by měly být dostupné jsou vydávány v takové formě, aby mohly být poskytnuty třetí straně k posouzení vykonávaných zavedená opatření k ochraně osobních údajů a informací. Veškerá dokumentace je dle potřeby aktualizována. Dokumentace s upraveným obsahem je dostupná na vyžádání.

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

2.8.6 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.

2.8.7 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.

2.8.8 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.

2.8.9 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.

2.8.10 Systém řízení ochrany osobních údajů je neustále zlepšován pomocí přístupu založeném na PDCA (naplánuj-proveď-ověř-jednej), 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.

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

2.8.12 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.

2.8.13 Tento proces chrání práva subjektů údajů na posouzení vlivu na ochranu údajů (proces analýzy rizika), pokud je pravděpodobné, že zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob s ohledem na povahu, rozsah, kontext a účely zpracování.

2.9 Kontroly dostupnosti – Ukládání firemních dokumentů

2.9.1 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.

3 Certifikace

3.1 Dodavatel souhlasí s tím, že po Dobu trvání smlouvy zajistí, aby udržoval v platnosti následující certifikace:

3.1.1 ISO/IEC 27001: Všechna zařízení pro hostování dat a podpůrné služby, ve kterých jsou ukládány nebo zpracovávány informace společnosti E.ON, jsou certifikována podle normy ISO / IEC 27001 „Informační technologie – bezpečnostní techniky – systémy managementu bezpečnosti informací – požadavky“.

3.1.2 ISO/IEC 22301: Všechna zařízení pro hostování dat a podpůrné služby, ve kterých jsou ukládány nebo zpracovávány informace společnosti E.ON, jsou certifikována podle normy ISO/IEC 22301 „Ochrana společnosti – Systémy managementu kontinuity podnikání – požadavky“.

3.2 Dodavatel se zavazuje, že předloží společnosti E.ON před datem účinnosti této Smlouvy příslušný certifikát, jakož i „Prohlášení o aplikovatelnosti“ a tento certifikát společnosti E.ON předloží rovněž po jeho obnovení a na vyžádání společnosti E.ON kdykoli během Doby trvání této Smlouvy.

3.3 Dodavatel se zavazuje, že zajistí, aby „Prohlášení o aplikovatelnosti“ pokrývalo veškerá hostingová a provozní zařízení, aplikace a procesy, v jejichž rámci jsou zpracovávány nebo ukládány informace společnosti E.ON.

4 Zpráva o kontrole organizace zaměřené na služby (Zpráva SOC)

4.1.1 Dodavatel se zavazuje, že společnosti E.ON předloží zprávu AICPA SOC2 Typ II (AICPA=Americký institut certifikovaných veřejných účetních) 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.

4.1.2 Dodavatel se zavazuje, že příslušnou zprávu předloží společnosti E.ON před Datem účinnosti této Smlouvy, po opětovném vydání této zprávy a na vyžádání společnosti E.ON kdykoli během Doby trvání této Smlouvy.

5 Kontaktní osoby a výměna informací

5.1 Obě Smluvní strany souhlasí se oznámením a poskytnutím kontaktních osob pro následující procesy bezpečnosti IT:

5.1.1 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 případů neshod s požadavky a souvisejících rizik.

5.1.2 Řízení bezpečnostních incidentů: průběžná 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.

5.1.3 Řízení rizik: průběžná výměna informací o činnostech řízení rizik prováděných Dodavatelem s cílem zajistit, aby rizika v oblasti bezpečnosti informací byla průběžně identifikována, hodnocena, ošetřována, monitorována a udržována v přijatelných mezích.

5.1.4 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.

5.1.5 Správa bezpečnostních záplat: výměna informací o dohodnutých časových obdobích údržby a instalace bezpečnostních záplat (tzv. „patchů“).

5.1.6 Správa identit a přístupu: výměna informací o tématech souvisejících se správou identit a přístupu.

5.1.7 Ochrana údajů: výměna informací o činnostech a incidentech souvisejících s ochranou osobních údajů.

5.2 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.

5.3 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 Dodavatele

Jméno a příjmení:

Telefon:

E-mailová adresa: