

Technicko-organizační opatření bezpečnosti informací a ochrany osobních údajů

Úroveň VYSOKÁ/VELMI VYSOKÁ

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.

1 Požadavky na bezpečnost 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.

1.3 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.

1.4 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.

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

1.6 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.

1.7 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 podpornými 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.

1.8 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.

1.9 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.

1.10 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.

1.11 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, (viii) 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.

1.12 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).

1.13 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“.

1.14 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 úrovně rizika těchto zranitelností a dle příslušných časových harmonogramů smluvních stran.

1.15 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 záplatu nasadit, (iii) otestuje bezpečnostní záplatu na základě známých kritérií, (iv) nasadí bezpečnostní záplatu 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.

1.16 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.

1.17 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.

1.18 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.

1.19 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.

1.20 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.

1.21 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

1.22 Fyzický hypervisor a virtuální počítač

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

1.23 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.

1.24 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.

1.25 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.

1.26 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 přístup 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.

1.27 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.

2 Požadavky na ochranu osobních údajů

2.1 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 zachování 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.

2.2 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).

2.3 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.

2.4 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 systému 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 (inspekce).

3 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 II¹).

4 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.

5 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.

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.

- 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.