Příloha – Informační bezpečnost a požadavky na ochranu dat pro konzultantské služby

1 Požadavky na informační bezpečnost

Požadavky na informační bezpečnost jsou platné pro veškerý majetek, vlastněný dodavatelem, za který je odpovědný dodavatel.

1.1 **Solidnost zdrojů**: Dodavatel zajistí, že hardware a software jsou odebírány ze známých a solidních zdrojů a že existuje spolehlivá technická podpora a sledovatelný dodavatelský řetězec.

1.2 **Řízení aktiv (assets management)**: Dodavatel zajistí, že (i) majetek (hardware a software), který je využíván pro vytvoření, zpracování, uložení nebo přenos informací spol. E.ON je chráněn proti korupci, ztrátě, krádeži a neoprávněnému předání informací po dobu celé životnosti/celého životního cyklu. Dodavatel zajistí, že všechen majetek je přidělen vlastníkovi, který je odpovědný za provoz tohoto majetku.

1.3 **Přístup k systému**: Dodavatel omezí přístup k aktivům/majetku, kde jsou informace společnosti E.ON vytvářeny, zpracovávány, ukládány nebo přenášeny oprávněným osobám pro specifické obchodní účely. To zahrnuje minimálně, že (i) pouze oprávnění uživatelé mohou získat přístup k relevantním informacím, (ii) přístupová práva jsou omezena na schválenou funkci systému, (iii) existuje příslušná segregace povinností, (iv) přístupová privilegia nejsou přidělována kolektivně (uživatelská ID a hesla nesmí být sdílena). Dodavatel zajistí, že administrativní přístup k systémům, které uchovávají nebo zpracovávají informace společnosti E.ON jsou (v) omezeny na minimální počet administrátorů.

1.4 **Management systému**: Dodavatel provozuje systémy, které tvoří, uchovávají, zpracovávají nebo přenášejí informace společnosti E.ON, aby (i) splnil současnou a predikovanou pracovní zátěž a (ii) konfiguruje je konzistentním, přesným způsobem, aby je mohl chránit, stejně jako informace, které zpracovávají, ukládají nebo přenášejí proti nesprávné funkci, cyber-útoku, neoprávněnému předání, korupci, krádeži a ztrátě.

1.5 **Management technické bezpečnosti**: Dodavatel instaluje řešení pro ochranu proti malware na systémech, kde mohou být informace společnosti E.ON vystaveny malware, včetně a v závislosti na použitelnosti se jedná o (i) servery (např. se jedná o aplikační servery, databázové servery, servery pro soubory, servery pro tisk, webové servery), (ii) počítačové přístroje (např. stolní počítače, laptopy a jiné mobilní přístroje) a (iii) kancelářské zařízení (např. síťové tiskárny, fotokopírky, multifunkční přístroje). (iv) Software na ochranu proti malware by mělo chránit proti všem formám malware (např. viry, worms, trojské koně, spyware, rootkits, botnet software, software keylogger „keystroke loggers“, ransomware). (v) Software na ochranu proti malware by mělo být distribuováno automaticky a v rámci definovaného časového rámce. Dodavatel zajišťuje a pravidelně reviduje a kontroluje, že (vi) software na ochranu proti malware nebyl deaktivován ani nebyla minimalizována jeho funkčnost, (vii) konfigurace software na ochranu proti malware je správná, (viii) aktualizace jsou použity správně v rámci definovaných časových limitů, (ix) skeny jsou prováděny v předem určenou dobu, a (x) je poskytnuta adekvátní informace o identifikovaných událostech malware.

1.6 **Aktualizace úrovní Patch**: Dodavatel zajistí nápravu technicky citlivých míst realizací procesu patch management, který zajistí (i) identifikování a získání patches z autorizovaných zdrojů, jakmile jsou dostupné (ii) rozhodnutí, kdy patches rozmístit, (iii) testování patches vůči známým kritériím, (iv) včasné rozmístění patches, (v) Dodavatel je zmocněn aplikovat

patches v IT prostředí, včetně hypervisorů virtualizace,

virtuálních strojů, operačních systémů a aplikací, pokud nemají negativní vliv na mlčenlivost, integritu/neporušenost nebo dostupnost informací společnosti E.ON.

1.7 **Posílení**: Všechny informace a síťové systémy musí být posíleny. To zahrnuje (i) znemožnění běhu zbytečných aplikací, služeb, nástrojů, protokolů a rozhraní, (ii) vynechání nebo minimálně změnu defaultních uživatelských jmen a hesel dodávaných prodávajícím, (iii) aktivaci možností zvyšujících bezpečnost a (iv) prevenci transferu technických informací externím subjektům.

1.8 **Bezpečná likvidace a opětovné využití**: Dodavatel zajistí, aby hardware uváděné mimo provoz
(i) bylo před opětovným využitím, prodejem nebo vrácením ošetřeno tak, aby byly informace společnosti E.ON Information bezpečně a komplexně vymazány (ii) nebo bezpečně zničeny. (iii) Toto ošetření nebo zničení bude provedeno bezpečným způsobem s použitím moderní techniky a postupů, jako jsou nástroje a postupy, definované v NIST 800-88 "Směrnice pro ošetření médií".

1.9 **Spolupráce v oblasti IT bezpečnosti:** Obě strany souhlasí s tím, že budou spolupracovat a vyměňovat si informace v rámci oblasti bezpečnosti.

2 Požadavky na ochranu dat

2.1 Dodavatel se zavazuje, že splní zákonná ustanovení o ochraně údajů (např. General Data Protection Regulation (GDPR)).

2.2 Dodavatel zpracovává nebo využívá osobní údaje společnosti E.ON výlučně v rámci smluvní dohody; zvláště nepředává údaje třetím stranám. Strany předpokládají, že Dodavatel provede své služby pro spol. E.ON na svou výlučnou odpovědnost v souladu s článkem 4 č. 7 GDPR. Dodavatel ochrání osobní údaje, které dostane od společnosti E.ON před přístupem neoprávněných třetích stran s pomocí vhodných technických a organizačních opatření (jak je popsáno v odstavci 1). Dodavatel okamžitě informuje spol. E.ON v případě závažného narušení provozu, podezření na porušení ochrany údajů nebo jiné problémy ve zpracování osobních údajů společnosti E.ON.

2.3 Pokud, v důsledku změny v původním zadání Dodavateli se posouzení ochrany údajů liší od článku 2.2; strany musí, v rámci tohoto spouštění a před zpracováním osobních údajů Dodavatelem uzavřít odpovídající Dohodu o ochraně údajů (Dohoda o zpracování spuštěných dat dle článku 28 GDPR nebo Dohodu o společné kontrole dle článku 26 GDPR).

2.4 Nároky datových subjektů, jejichž údaje jsou zpracovávány společností E.ON a Dodavatelem jsou vznášeny vůči společnosti E.ON za jakékoliv neodpovídající nebo nepřesné zpracování dat dle GDPR nebo jiné legislativy na ochranu dat a lhostejno, zdali dojde k porušení ochrany údajů na straně společnosti E.ON nebo Dodavatele, spočívá důkazní břemeno neexistence odpovědnosti Dodavatele na Dodavateli.