Příloha č. 2 – Technická specifikace infrastruktury

Tento dokument obsahuje požadavky zadavatele na systém z pohledu HW a SW infrastruktury a také další požadavky kladené na předmět plnění jako celek.

Zadavatel požaduje, aby součástí nabídkové ceny a specifikace nabízené HW a SW infrastruktury byly všechny služby, licence (včetně potřebných licencí a maintenance databází, operačních systémů, nástrojů pro virtualizaci a podobně) i HW komponenty tvořící řešení. Součástí nabídky musí být i podpora systému po celou dobu trvání smlouvy.

Systém bude provozován na HW dodavatele na náklady dodavatele. Zadavatel neumožní umístění HW (serverů) ve svém sídle. HW musí být umístěn na území EU. V případě, že bude pro provoz HW využito služeb provozovatele cloudových služeb, musí být zpracovávaná data šifrována a provozovatel cloudových služeb nesmí mít přístup k šifrovacímu klíči.

Architektura systému
Architektura systému musí vycházet ze zásad a principů servisně orientované architektury (SOA) s důrazem na silnou podporu tvorby a řízení oběhu dokumentů.

Prostředí systému
Dodávka systému musí obsahovat oddělené testovací a produkční prostředí. Testovací prostředí musí běžet na jiných HW a SW prostředcích (serverech) než produkční prostředí. Je povoleno, aby testovací prostředí běželo v záložním systému.

Produkční prostředí
Produkční prostředí musí být oddělené na dvě samostatné části:

Část 1 - Modul zpracování dat z měřících zařízení měření rychlosti.

Část 2 - Statistický modul systému měření rychlosti.

Část 1 a Část 2 nesmí být provozována na stejných HW a SW prostředcích (serverech).

Oddělení produkčního prostředí na dvě části (Část 1 a Část 2) vychází z logiky práce s daty v jednotlivých částech systému, požadavku zadavatele na zajištění dostupnosti dat a požadavku obecně závazných právních předpisů na ochraně osobních údajů. V Části 1 se zpracovávají výhradně data z měření ve smyslu přestupkového a správního řízení (ze zařízení jsou předávána data označená jako potencionální přestupek), zatím co v Části 2 se pracuje s on-line daty v kompletním telematickém rozsahu a data z této části jsou propagována do jiných systémů zadavatele, než data z části určené pro práci s přestupky.

Pro produkční prostředí pro Část 1 se požaduje:
Produkční prostředí jako celek musí být replikováno na záložní systém. Záložní systém nesmí být provozován na stejných HW a SW prostředcích (serverech) jako primární.

Provoz produkčního a záložního systému musí být minimálně v režimu Active/Passive.

V případě výpadku primárního systému musí být provoz přesměrován na záložní systém do 4 pracovních hodin od zjištění a nahlášení takového výpadku dodavateli. Pro hlášení výpadků (poruch a závad) zajistí dodavatel standardní HelpDesk.

Řešení musí provádět replikaci dat do záložního systému. Data na záložní server MUSÍ být přenášena průběžně, přičemž záloha dat z produkčního systému nesmí být starší více jak 30 minut. Záložní systém musí z výkonového pohledu mít minimálně 50% výkon z pohledu uživatelské odezvy systému oproti primárnímu systému.

Pro produkční prostředí pro Část 2 se požaduje:
Produkční prostředí jako celek musí být replikováno na záložní systém. Záložní systém nesmí být provozován na stejných HW a SW prostředcích (serverech) jako primární.

V případě výpadku primárního systému musí být možné přesměrovat provoz na záložní systém do 4 pracovních hodin od zjištění a nahlášení takového výpadku dodavateli. Pro hlášení výpadků (poruch a závad) zajistí dodavatel standardní HelpDesk.

Řešení musí provádět replikaci dat do záložního systému. Data na záložní server MUSÍ být přenášena průběžně, přičemž záloha dat z produkčního systému nesmí být starší více jak 60 minut. Záložní systém musí z výkonového pohledu mít minimálně 50% výkon z pohledu uživatelské odezvy systému oproti primárnímu systému.

Provoz produkčního a záložního systému musí být minimálně v režimu Active/Passive.

Doplnění:
Shora uvedené požadavky na Část 1 a Část 2 jsou chápány jako minimální a zájemce neomezuje dodavatele v nabídce kvalitnějšího systému, například s vyšší dostupností či provozu v režimu Active/Active.

Produkční a záložní prostředí musí být provozováno na fyzicky odlišných serverech. Části 1 a 2 produkčního prostředí mohou být provozovány na virtuálních serverech v rámci jednoho fyzického serveru. Požadavky na výkon tímto nejsou dotčeny.

Testovací prostředí
Testovací prostředí musí být konfiguračně shodné s provozním prostředím. Testovací prostředí nemusí splňovat výkonnostní požadavky kladené na provozní prostředí.

Požadavky na výkon
Systém musí být navržen tak, aby respektoval následující očekávané provozní parametry:

- Počet registrovaných uživatelů (počet uživatelů bude neomezený, tento údaj je počtem, kdy systém ještě musí pracovat s níže popsanou délkou odezvy)
    - 7 pro modul zpracování dat z měřících systémů
    - 7 pro statistický modul
- Datový objem
    - uchování veškerých dat po dobu 5 let
- Počet detekcí/přestupků
    - 85.000 přestupků ročně/1 měřící zařízení v rámci detekce překročení maximální povolené rychlosti
    - 20.000.000 detekcí ročně/1 měřící zařízení pro účely uchovávání statistických informací o měření

Délka doby odezvy systému musí při uvedeném zatížení odpovídat běžným zvyklostem obdobných informačních systémů a je měřena na straně serveru. Měření odezev systému bude probíhat v průběhu řádného provozu. Řešení musí mít garantované odezvy při založení/úpravě/zrušení jednoho záznamu v jednotkách sekund. Vícenásobné operace v případě zobrazování přehledů záznamů musí být realizováno v časovém horizontu nepřekračujícím běžné časy jiných informačních systémů pracujících s evidenčními záznamy DRMS v závislosti na množství zobrazovaných záznamů.

Systém musí vykazovat stabilní provoz. Případné dlouhodobější odstávky (např. servisní zásahy, upgrade apod.) jsou přípustné pouze mimo provozní dobu zadavatele.

Výkon systému nesmí klesat v průběhu provozu systému, tj. nesmí se prodlužovat doby odezev na jednotlivé funkcionality systému.

Požadavky na spolehlivost a dostupnost systému
Provoz systému (včetně zařízení popsaného v příloze č. 1 zadávací dokumentace) se z pohledu spolehlivosti systému a návazných SLA parametrů může nacházet v jednom ze tří následujících stavů:

- V provozu – systém je v provozu v případě, že se uživatelé mohou do systému přihlásit a využívat veškeré funkcionality, které jsou předmětem technické specifikace, nebo je pro nedostupné funkcionality (např. z důvodu jejich chyby) nabídnuto náhradní řešení umožňující dosažení shodného výsledku jako v případě, kdy by uživatel mohl tyto funkcionality využít. Délka doby odezvy odpovídá výše uvedeným podmínkám.
- Mimo provoz – systém je mimo provoz v případě, že se uživatelé nemohou do systému přihlásit
- Omezení funkcionality - systém se nachází v stavu „omezení funkcionality“, když nejsou splněny podmínky ani pro jeden z předešlých stavů

Systém nabývá "omezení funkcionality" či stavu "mimo provoz" v případě, kdy alespoň jeden uživatel (nebo případná automatická pravidelná kontrola systému) identifikuje nedostupnost funkcionality systému nebo systému jako celku, tento stav nahlásí dodavateli prostřednictvím systému HelpDesk a zároveň tento stav není způsoben uživatelem (tj. uživatel splňuje veškeré náležitosti pro přístup a práci se systémem).

Systém musí být, včetně HW infrastruktury a provozních postupů, navržen a vytvořen tak, aby umožnil zajištění následujících parametrů dostupnosti:

- Dostupnost produkčního prostředí musí být v obvyklé pracovní době (pracovní dny od 07:00 do 18:00) 99%
- Dostupnost produkčního prostředí musí být mimo obvyklou pracovní dobu 95%

Systém bude považován za nedostupný v době trvání systémového stavu "mimo provoz" a "omezení funkcionality" od okamžiku oprávněného nahlášení nedostupnosti či nesprávné funkčnosti uživatelem systému dodavateli prostřednictvím služby HelpDesk až do okamžiku obnovení provozu nebo nabídnutí náhradního řešení pro nedostupnou či nesprávně fungující funkcionalitu systému.

Celková plánovaná doba dostupnosti je definována jako počet hodin v daném kalendářním měsíci. Servisní okno systému je stanoveno od 20:00 do 24:00 v pracovní den.

V rámci služby HelpDesk je dodavatel povinen evidovat každé uživatelské hlášení nedostupnosti systému s informací, zda se jednalo o oprávněné či neoprávněné hlášení. Dodavatel je povinen tyto informace zpřístupnit zadavateli. Hlášení poruch a závad ze strany zadavatele, stejně jako dalších požadavků souvisejících se službou podpory a servisu, musí být možné elektronicky a telefonicky, s využitím nástroje, který každý požadavek zadavatele zaznamená, k požadavku doplní datum a čas nahlášení požadavku a následně bude pomocí tohoto nástroje možné sledovat způsob řešení takového požadavku ze strany dodavatele, případně prostřednictvím tohoto nástroje vést mezi zadavatelem a dodavatelem další komunikaci ve smyslu doplnění či upřesnění požadavku.

Služba HelpDesk musí být pro potřeby hlášení poruch, závad a požadavků ze strany zadavatele dostupná minimálně v pracovní době od 08:00 do 16:00, přičemž reakční čas dodavatele na oprávněné požadavky zadavatele je definován v rámci SLA parametrů.

SLA parametry

Níže uvedené SLA parametry jsou ze strany Zadavatele vnímány jako minimální a zadavatel nebrání dodavateli nabídnout lepší SLA parametry, především v oblasti rychlosti odezvy dodavatele na požadavky zadavatele a rychlosti řešení hlášených závad a poruch systému.

Priorita	Charakteristika problému	Doba vyřešení požadavku od jeho nahlášení
Havárie	• systém nelze spustit nebo dochází ke ztrátě dat, • nebo systém lze spustit, ale nefunguje některá z klíčových funkcí (samotné měření, přijetí měření, validace měření, přijetí podnětu, zobrazení detailu měření či případu, apod.) a neexistuje dočasné náhradní řešení • nebo existují zásadní problémy s výkonem klíčových funkcí systému	24 hodin
Porucha	• nefunguje některá z méně důležitých funkcí systému (úpravy v nastavení, číselnících a organizační struktuře, notifikace, tiskové výstupy, apod.) • problémy s výkonem u důležitých funkcí systému (vyhledávání, hromadné úpravy záznamů, hromadné operace apod.)	72 hodin
Chyba	• Ostatní problémy	120 hodin

Poznámka: Požadavky v rámci SLA parametrů je možné hlásit v rozmezí od 07:00 až 18:00 každého dne. Na požadavek vznesený mimo tuto lhůtu se bude pohlížet jako na požadavek vznesený na začátku nejbližšího pracovního dne.

Za vyřešení se považuje i takový zásah, který způsobí změnu priority problému na menší.

Pokud nastane souběh požadavku s prioritou Havárie s požadavky s prioritou Porucha (resp. Chyba), má řešení požadavku s prioritou Havárie přednost před ostatními požadavky. Doba řešení požadavků s prioritou Porucha a Chyba bude automaticky prodloužena o dobu řešení požadavku s prioritou Havárie.

Požadavky na bezpečnost
Pro identifikaci a autorizaci přístupů uživatelů musí systém podporovat následující metody identifikace a autentizace uživatelů:

- Identifikaci a autorizaci fyzických osob – použití kombinace jméno a heslo
- Definovat přístupová práva daného uživatele k jednotlivým měřením a případům a návazným dokumentům a datům
- Umožnit víceúrovňovou správu systému (nastavení uživatelů, skupin a jejich rolí)
- Identifikaci a autorizaci okolních informačních systémů – například použití kombinace serverový certifikát a IP adresa

Po přihlášení jsou uživateli přidělena přístupová práva na základě předem definovaných pravidel. Identifikace přihlášeného uživatele bude po celou dobu práce uživatele v systému zaznamenána/logována.

Auditovatelnost provedených úkonů

Systém musí zaznamenávat veškeré operace:

- Prováděné uživateli prostřednictvím GUI systému – uživatelé mohou k datům přistupovat pouze tímto způsobem
- Související s činností systému - data mohou být v souladu s touto technickou specifikací měněna také automaticky systémem
- Související s komunikací s případnými okolními IS – tato komunikace může být realizována pouze prostřednictvím webových služeb
- Prováděné následně dodavatelem při zajišťování provozu systému – systém nesmí umožnit jakoukoli modifikaci dat, aniž by došlo k zaznamenání
    - data a času modifikace dat
    - identifikace osoby, která změnu dat provedla
    - původní hodnoty dat
    - nové hodnoty dat.

Systém nesmí umožnit žádné jiné, než výše uvedené, způsoby pro přístup a manipulaci s daty.

Důvěrnost a integrita dat

Systém musí být navržen s ohledem na vysokou míru zabezpečení celého řešení. Systém bude připojen přímo na Internet. Řešení proto musí obsahovat minimálně firewally.

Systém musí zajistit, že:

- Systémem uchovávaná data nesmí být zpřístupněna neautorizovaným osobám, přičemž přístup a veškerá manipulace s daty musí být zaznamenávána
- Data nemohou být během komunikace odposlouchávána či pozměněna neautorizovanou stranou, přičemž pro komunikaci mezi uživatelem a systémem musí být použit zabezpečený komunikační protokol min. SSL verze 3.0, TLS verze 1.1 nebo obdobné.
- Systémem uchovávaná data nesmí být možné změnit nebo poškodit neautorizovanou stranou

Přístup do systému

Přístup k funkcionalitám systému musí být zajištěn minimálně pro standardní PC prostřednictvím běžného webového prohlížeče. Zadavatel vyžaduje minimálně přístupnost systému prostřednictvím PC s OS Windows 7 a vyšším plus odpovídající verzí prohlížeče Internet Explorer a Mozilla Firefox, případně Chrome.
Pro shora pospané PC musí být dostupné funkcionality systému v plné šíři.

Antivirová ochrana

Systém musí obsahovat řešení antivirové kontroly dokumentů, které virem nebo jiným škodlivým kódem mohou být infikovány, pokud to bude z hlediska použitého technického řešení relevantní (zejména pokud pro dané technické řešení budou k dispozici antivirové programy)