Smlouva o dílo

na dodávku IAM souvisejících služeb

uzavřená ve smyslu ustanovení § 2586 a násl. zákona č. 89/2012 Sb.,
občanský zákoník (dále též „občanský zákoník“)

Jihočeský kraj
se sídlem: U Zimního stadionu 1952/2
zastoupený: Mgr. Ivanou Stráskou, hejtmankou kraje
IČO: 70890650
bankovní spojení: 199783021/0300

dále též „objednatel“

a

AUTOCONT a.s.
se sídlem: Hornopolní 3322/34, 702 00, Ostrava
zastoupený/á: Ing. Martin Stejskal, člen představenstva
IČO: 04308697
bankovní spojení: 6563752/0800
zapsaný do obchodního rejstříku vedeného u Krajského soudu v Ostravě, oddíl B, vložka 11012

dále též „zhotovitel“

společně též „smluvní strany“

uzavírají níže uvedeného dne tuto smlouvu o dílo.

1 Předmět smlouvy

1.1 Zhotovitel se touto smlouvou o dílo zavazuje provést na svůj náklad a nebezpečí pro objednatele dílo specifikované v příloze smlouvy č. 1 - Technická specifikace (dále též „dílo“) a objednatel se zavazuje dílo převzít a zaplatit cenu.

2 Doba a místo dodání díla

2.1 Smlouva se uzavírá na dobu neurčitou. Dílo bude předáno najednou, po jeho dokončení. Termín předání díla je **90** kalendářních dnů ode dne účinností smlouvy.

2.2 O předání díla bude sepsán protokol podepsaný oprávněnými zástupci smluvních stran. Budou-li zjištěny vady díla nebo jeho části již při jeho přejímání, je třeba takovou skutečnost uvést do protokolu. Zhotovitel je povinen zjištěné vady odstranit, a to ve lhůtě 10 dnů od jejich zachycení v protokolu. Po dobu odstraňování vad neběží objednateli lhůta k placení. Odstraňování závad nezbavuje zhotovitele povinnosti dokončit další plnění v řádných termínech

2.3 Místem plnění a dodání díla je sídlo objednatele.

2.4 Objednatel nabývá vlastnické právo převzetím bezvadného díla.

3 Cena a platební podmínky

3.1 Cena byla stanovena na základě nabídky zhotovitele, a činí celkem **1 490 000,00** Kč bez DPH. Sazba DPH bude k ceně za dílo připočtena v souladu s příslušnými právními předpisy. Přesný rozpis ceny za jednotlivá plnění je uveden v následující tabulce.

	Cena bez DPH v Kč	Výše DPH v Kč	Cena s DPH v Kč
3.2 Cena za předmět plnění uvedený v bodech 5.1 až 5.8 přílohy č. 1 Smlouvy	1 390 000,00	291 900,00	1 681 900,00
3.3 Cena za předmět plnění uvedený v bodě 5.9 přílohy č. 1 Smlouvy (Školení)	100 000,00	21 000,00	121 000,00
3.4 Celková nabídková cena za dílo v Kč	**1 490 000,00**	**312 900,00**	**1 802 900,00**

3.5 Cena je konečná a zahrnuje veškerá náklady spojené s provedením díla.

3.6 Cena bude uhrazena na základě daňového dokladu (faktury) vystavené zhotovitelem, a to po dokončení díla a jeho převzetí objednatelem. Objednatel nebude poskytovat zálohy. Splatnost faktury je 14 dnů ode dne jejího doručení objednateli.

3.7 Vystavená faktura bude mít náležitosti daňového dokladu dle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, v souladu s § 435 občanského zákoníku. Faktura musí dále obsahovat:

a) číslo smlouvy,
b) předmět plnění a jeho přesnou specifikaci ve slovním vyjádření (nestačí pouze odkaz na číslo uzavřené smlouvy),
c) označení banky a čísla účtu, na který musí být zaplaceno,
d) lhůtu splatnosti faktury,
e) datum uskutečnitelného zdanitelného plnění shodné s datem předání plnění objednateli,
f) název, sídlo, IČO a DIČ příjemce a poskytovatele včetně údajů o zápisu do OR,
g) jméno osoby, která fakturu vystavila, včetně kontaktního telefonu.

3.8 Jestliže nebude faktura obsahovat veškeré údaje, nebo pokud v ní nebudou správně uvedené údaje, je objednatel oprávněn vrátit ji ve lhůtě 5 pracovních dnů od jejího převzetí zhotoviteli s uvedením chybějících náležitostí nebo nesprávných údajů. V takovém případě se přeruší doba splatnosti a nová lhůta splatnosti počne běžet doručením opravené faktury objednateli.

4 Záruka a odpovědnost za vady

4.1 Zhotovitel je povinen provést dílo tak, aby bylo bez vad a nedodělků, a v takovém stavu a kvalitě, která umožňuje jeho řádné převzetí a užívání objednatelem.

4.2 Zhotovitel prohlašuje, že zaručuje dohodnuté vlastnosti díla, a to po dobu 24 měsíců.

4.3 Objednatel není povinen dílo nebo jeho část převzít, pokud dílo obsahuje vady, a to zejména:

- dílo neodpovídá požadované specifikaci,
- dílo obsahuje vady, které ztěžují nebo znemožňují jeho plánované užívání.

4.4 Objednatel je povinen reklamovat zjištěné vady díla písemně u zhotovitele, a to bez zbytečného odkladu poté, co je zjistil. Uplatněním reklamace se staví záruční doba na reklamované dílo či jeho část.

4.5 Zhotovitel je povinen v záruční době rozhodnout o oprávněnosti reklamace nejpozději následující pracovní den po dni nahlášení vady zboží objednatelem. Vada bude odstraněna na místě určeném objednatelem, a to nejpozději do 10 pracovních dnů od uznání oprávněnosti reklamace.

4.6 U reklamovaného díla, u kterého byla reklamace uznána, a které bylo opraveno, běží nová záruční doba ode dne předání díla objednateli.

5 Licenční ujednání

5.1 Zhotovitel poskytuje objednateli oprávnění k výkonu práva užívat dílo (licenci). Licence je nevýhradní, místně, časově a množstevně omezena dle licenčních podmínek příslušného držitele majetkových práv.

5.2 V případě, že zhotovitel bude muset využít k vytvoření a zajištění fungování díla dalšího softwaru, ať již svého nebo od jiné společnosti, zavazuje se převést objednateli nevýhradní licenci k užití tohoto softwaru v takovém rozsahu (místním, časovém i množstevním), aby objednatel mohl dílo řádně užívat.

6 Smluvní pokuta a úrok z prodlení

6.1 Dojde-li k prodlení zhotovitele s řádným a včasným dodáním díla, je objednatel oprávněn účtovat zhotoviteli smluvní pokutu ve výši 10 000,- Kč za každý i započatý den prodlení zhotovitele. Případné odstoupení od smlouvy nemá vliv na povinnost zhotovitele zaplatit smluvní pokutu.

6.2 Je-li zhotovitel v prodlení s odstraněním reklamované vady, je objednatel oprávněn účtovat zhotoviteli úrok z prodlení ve výši 10 000,- Kč za každý i započatý den prodlení.

6.3 Výše uvedenými ustanoveními není dotčeno právo na náhradu škody.

7 Komunikace mezi stranami

7.1 Ve věcech odborných, technických a převzetí díla jsou určeny následující kontaktní osoby.

Na straně objednatele:

Ing. Vítězslav Kubal, kubal@kraj-jihocesky.cz, 386 720 494

Bc. Aleš Velek, velek@kraj-jihocesky.cz, 386 720 508

Ing. František Beránek, beranek@kraj-jihocesky.cz, 386 720 500

Na straně zhotovitele:

Ladislav Kocour, ladislav.kocour@autocont.cz, 602682692

Radim Drgáč, radim.drgac@cleverance.cz, 602768729

8 Ukončení smlouvy

8.1 Tuto smlouvu je možné ukončit dohodou stran.

8.2 Objednatel je oprávněn od smlouvy odstoupit, pokud zhotovitel nedodá řádně a včas plnění dle této smlouvy, anebo bude z jeho postupu zřejmé, že dílo řádně a včas dodáno nebude, a dále v případě, když probíhá insolvenční řízení proti majetku zhotovitele, v němž bylo vydáno rozhodnutí o úpadku, nebo insolvenční návrh byl zamítnut proto, že majetek zhotovitele nepostačuje k úhradě nákladů insolvenčního řízení, nebo byl konkurs zrušen proto, že majetek zhotovitele byl zcela nepostačující.

8.3 Odstoupení musí být písemné, a je účinné okamžikem doručení druhé straně. V takovém případě se smlouva ruší od počátku.

9 Závěrečná ujednání

9.1 Smlouva může být měněna pouze písemnými dodatky.

9.2 Smlouva je vyhotovena ve 2 stejnopisech, kdy každá ze stran obdrží 1 vyhotovení.

9.3 Zhotovitel bere na vědomí, že smlouva bude uveřejněna v registru smluv zřízeného podle zákona č.340/2015 Sb., o registru smluv, ve znění pozdějších předpisů. Zhotovitel prohlašuje, že tato smlouva neobsahuje údaje, které tvoří předmět jeho obchodního tajemství podle § 504 občanského zákoníku.

9.4 Smlouva nabývá platnosti dnem podpisu a účinnosti dnem zveřejnění v registru smluv. Zveřejnění zajistí objednatel.

9.5 Uzavření této smlouvy bylo schváleno usnesením Rady Jihočeského kraje č. 1056/2020/RK-109 ze dne 15.10.2020.

9.6 Strany prohlašují, že si tuto smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují své podpisy.

9.7 Součástí této smlouvy jsou následující přílohy:

- Příloha č. 1 - Technická specifikace
- Příloha č. 2 - Integrované systémy – výčet a stručný popis
- Příloha č. 3 - Podmínky využití Technologického centra Jihočeského kraje
- Příloha č. 4 - Bezpečnostní pravidla objednatele
- Příloha č. 5 - Informace o zpracování osobních údajů

V Českých Budějovicích dne

Za objednatele

Mgr. Ivana Stráská, hejtmanka kraje

Ve Českých Budějovicích dne 20.10.2020

[redacted]

Digitálně podepsal Ing. Martin Stejskal
Datum: 2020.10.20 10:56:46 +02'00'

Za zhotovitele

Ing. Martin Stejskal, člen představenstva

Příloha č. 1 – Technická specifikace

1. PŘEDMĚT ZAKÁZKY

Tato zadávací dokumentace vznikla za účelem realizace projektu IAM (IS integrované s IAM a základními registry, Integrace s dalšími centrálními informačními systémy dle potřeby).

2. ZÁKLADNÍ CÍLE

- Pořízení a implementace IAM, zajištění jednoznačné identifikace, autentifikace, autorizace pro uživatele krajského úřadu (KÚ), příspěvkových organizací, obcí a jejich příspěvkových organizací a dalších uživatelů z komerční oblasti (administrátorů externích SW, „architektů“ a dalších smluvně svázaných subjektů) viz. specifikace jednotlivých implementovaných systémů. IAM bude integrován se systémy uvedenými v příloze č. 2 smlouvy „Integrované systémy“.
- Aplikační brána připojení k ISZR.
- Zajištění všech potřebných sw licencí pro provoz předmětu plnění.
- Vytvoření a implementace centrálního auditního systému včetně napojení na IAM a „Integrované systémy“ – převzetí logů ze současného systému.

3. ÚVOD DO PROBLEMATIKY

V současnosti je na krajském úřadu provozován IAM. Objednatel požaduje zachování současných funkcionalit stávajícího IAM. Objednatel požaduje a zhotovitel se zavazuje realizovat dodávku a implementaci IAM včetně souvisejících služeb dle této smlouvy nejpozději do termínu uvedeného v článku 2 smlouvy.

4. VÝCHOZÍ SW A HW VYBAVENÍ

Pro účely nasazení IAM je počítáno s využitím vybavení TC Jihočeského kraje. Bližší specifikace dle Přílohy č. 3 smlouvy – Podmínky využití Technologického centra Jihočeského kraje.

5. SPECIFIKACE

5.1. Předimplementační analýza

Předimplementační analýza musí vycházet z aktuálního stavu řešení a nasazení stávajícího IAM. Analýza musí obsahovat:

- analýzu procesů a aplikací úřadu se zaměřením na oblast správy uživatelských účtů, přidělování oprávnění a rolí,
- analýzu požadavků vyplývající z připojování IS krajského úřadu (IS KÚ) k centrálním informačním systémům, základním registrům a dalším informačním systémům s požadavkem na autorizaci a autentizaci,
- analýzu možností správy výstupních struktur – evidenční údaje, logy, …,
- analýzu nutných reportů,
- návrh životního cyklu Identity uživatelů,
- analýzu technických a bezpečnostních rizik.

Dodavatel ve spolupráci se zadavatelem zreviduje:

- model struktury úřadu,
- seznam systemizovaných pracovních pozic,
- přiřazení pracovníků úřadu k pracovním pozicím,
- atributy dodávané HR systémem v souladu s potřebami obsluhovaných systémů.

Dodavatel ve spolupráci se zadavatelem vytvoří:

- manažerský souhrn,
- analýzu výchozího stavu informačního systému – technologický popis stávajících technologií,
- detailní popis řešení,
- návrh podrobného postupu implementace nabízeného řešení,
- harmonogram implementace řešení a realizace celého projektu,
- seznam požadavků na součinnost,
- seznam požadavků na HW a SW,
- analýzu technických a bezpečnostních rizik včetně návrhu řešení těchto rizik,

- návrh zabezpečení bezpečného přístupů externích uživatelů,
- návrh akceptačního protokolu.

IAM

- seznam činností podle vykonávaných agend,
- přehled přiřazení informačních systémů a oprávněních v nich k jednotlivým činnostem,
- přehled přiřazení činností k pracovním pozicím v organizační struktuře,
- analýzu a soupis požadavků na navrhované řešení a způsob jejich pokrytí,
- návrh metodiky pro správu identit a jejich oprávnění,
- definici vazeb mezi všemi integrovanými systémy,
- analýzu identifikace a distribuce událostí,
- analýzu vnitřních aplikací určených pro integraci,
- návrh postupu integrace aplikací,
- definici zabezpečení zpráv při předávání mezi aplikacemi a IAM na úrovni zprávy i protokolu,
- definici adres a portů pro komunikaci aplikací a IAM,
- definici autorizace a autentizace při předávání zpráv mezi aplikacemi a IAM.

5.2. Pořízení a implementace IAM

- Pořízení a implementace IAM, zajištění jednoznačné identifikace, autentifikace, autorizace pro uživatele krajského úřadu, příspěvkových organizací, obcí a jejich příspěvkových organizací a dalších uživatelů z komerční oblasti (administrátorů externích SW, „architektů“ a dalších smluvně svázaných subjektů) viz. specifikace jednotlivých implementovaných systémů. IAM bude integrován se systémy uvedenými v příloze č. 2 smlouvy „Integrované systémy“. Součástí bude revize organizační struktury ve vztahu k požadavkům na IAM, blíže popsaná v bodě 5.1.
- Způsob implementace bude vyplývat z předimplementační analýzy.
- Zajištění všech potřebných SW licencí pro provoz předmětu plnění.
- Vytvoření a implementace centrálního auditního systému včetně napojení na IAM a „Integrované systémy“ – převzetí logů ze současného systému.

5.2.1. Obecné vlastnosti IAM

Zadavatel preferuje řešení postavené na standardizovaném SW produktu (open source není Zadavatelem považován za standardizovaný SW produkt), u nějž bude významně menší počet vyvíjených funkcionalit a vývoj tak bude primárně spočívat v přizpůsobení standardizovaného produktu. Za standardizovaný produkt Zadavatel považuje produkt, který je opakovaně implementován (tj. je násobně využíván v rámci autonomních instalací) a existuje síť partnerů výrobce nebo původce SW technologie, kteří produkt technicky podporují. Důvodem uvedené preference je skutečnost, aby Zadavatel nebyl odkázán na jediného dodavatele, který bude autorem příslušného SW. U řešení, které je založeno na standardizovaném řešení lze předpokládat vyšší rychlost nasazení řešení do běžného provozu, významně větší flexibilitu při změnových řízeních iniciovaných změnou legislativy a tento produkt je na trhu násobně ověřen (tj. v jádru/základních strukturách produktu je menší riziko chyb).

5.2.2. Požadované funkce IAM

Implementované řešení musí splňovat především následující požadavky a funkce:

- úplná synchronizace identit mezi personálním systémem a IAM se zachováním možnosti vytvořit identity pouze v IAM s možností zaslání notifikací o nově připravené identitě dopředu.
- identita musí obsahovat jednoznačný a unikátní identifikátor nezávislý na údajích uživatele. Identifikátor musí být zvolen tak, aby vždy byl jednoznačně spojen s konkrétní fyzickou osobou a aby se neměnil v případě změn souvisejících s touto osobou (např. při změně příjmení, pracovního zařazení, …). Sada údajů k identitě bude administrátorsky modifikovatelná v libovolném okamžiku s tím, že některé údaje mohou být nastaveny jako povinné. Údaje k identitě mohou být čerpány z různých integrovaných systémů. K identitě bude možné připojovat soubory.
- možnost uživatele měnit o své identitě některé údaje (např. změna hesla).
- systém musí být schopen evidovat a spravovat certifikáty elektronických podpisů spravovaných identit v souladu s jejich pracovními oprávněními. Spravovat seznam osob a jejich nastavení (pravidel) u dodavatele certifikátů, pokud bude dodavatel certifikátů poskytovat rozhraní pro správu tohoto seznamu. Od dodavatele certifikátů získávat seznam certifikátů a dle tohoto seznamu následně zadávat certifikáty do dalších informačních systémů.

- princip založený na systemizovaných místech, systém musí umožnit systemizaci pracovních míst v souladu se strukturou KÚ. Definovat jednotlivá systematizovaná místa a jejich činnosti a sadu oprávnění a rolí pro jednotlivé IS KÚ vztažené ke konkrétnímu systemizovanému místu.
- přiřazení identit na takto vytvořená systematizovaná místa a to i ve vazbě M:N.
- možnost čerpání rolí z připojovaných systémů a vytvoření katalogu služeb informačních systémů provozovaných v rámci KÚ.
- možnost přidělování a odebírání rolí pro jednotlivé případy.
- možnost přidělení oprávnění nebo role konkrétní identitě nebo systemizovanému místu.
- systém musí umožnit časově omezené přidělení oprávnění konkrétní identitě.
- systém musí umožňovat vytváření dočasných skupin, systematizovaných míst, a identit, které nebudou synchronizovány z personálního IS.
- zastupitelnost interních uživatelů KÚ – systém musí umožnit definovat vztahy zastupitelnosti mezi uživateli. Musí umožnit uživatelům, aby v souladu se strukturou KÚ mohli uživatelé sami delegovat v případě potřeby (dovolená, služební cesta, …) svoje role, nebo jejich část na jiné uživatele KÚ (pověřené osoby) a to i tak, že jeden uživatel může mít pro každou svou činnost nastaveny různé uživatele KÚ jako své zástupce.
- workflow jako proces žádosti o službu, následný schvalovací proces a přiřazení požadované služby.
- řízení celého životního cyklu identit včetně schvalovacího workflow. Toto workflow bude konfigurovatelné pomocí grafického rozhraní. Pro každou roli v IS KÚ musí být možné konfigurovat jiné workflow.
- přiřazení schvalovacího workflow pro každou službu (hromadně i jednotlivě).
- volitelné zasílání e-mailových notifikací v různých částech workflow.
- workflow pro kontrolu a schválení aktuálních oprávnění uživatelů. Toto workflow zajistí v pravidelných intervalech odeslání reportu o přiřazených aplikačních rolích uživatelů a jejich členství ve skupinách vedoucím pracovníkům uživatelů. Vedoucí pracovníci následně v rámci workflow oprávnění schválí nebo upraví a schválí.
- zadávání požadavků uživatelů na změny v přiřazení rolí (aplikační a agendové) a skupin ke schválení nadřízeným.
- průběh workflow bude možné sledovat uživateli v grafické podobě ve formě diagramu, ve kterém bude zřejmý stav probíhajícího workflow. Diagram bude v obvyklém formátu pro zobrazení workflow např. aktivity diagram, BPMN nebo Archimate.
- schvalování či zamítnutí workflow požadavků včetně uvedení zdůvodnění.
- podpora vícekrokového schvalování workflow.
- možnost větvení pro ošetření výjimek vzniklých při schvalování workflow.
- řešení zastupitelnosti workflow.
- eskalace – upozornění při překročení termínu splnění workflow.
- možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů.
- podpora řízení oprávnění pomocí virtuálního konektoru pro nenapojené aplikace.
- obousměrnou, úplnou synchronizaci identit mezi IAM a JIP (výhradně prostřednictvím KAAS).
- propojení se všemi integrovanými systémy uvedenými v příloze č. 2 smlouvy „Integrované systémy“.
- možnost delegace administrátorských práv.
- součástí řešení musí být řízení minimálně dvou fyzicky oddělených AD, (první určené pro zaměstnance KÚ, druhé určeno pro externí subjekty). IAM bude synchronizovat identity do těchto AD.
- uživatelské atributy bude možné modifikovat a odesílat do AD (např fotka, organizační členění, Mac adresa, …).
- možnost řízení i Azure AD.
- bezpečné uložení identit a všech citlivých a vybraných údajů.
- autentizaci (ověření identity), včetně možnosti dvoufaktorové autentizace.
- autorizace (ověření oprávnění) uživatelů při přístupu k Informačním systémům krajského úřadu (IS KÚ).
- možnost exportovat a publikovat informace uložené v IAM a to i historické.
- přístup uživatelů k datům IAM bude zajištěn prostřednictvím webového rozhraní. Řešení musí umožňovat zobrazení přidělených rolí k jednotlivým identitám s rozdělením na role navázané na systemizované místo, na role navázané na identitu, na role vázané na skupinu, na role vázané na organizační jednotku a na role přidělované pro jednotlivé případy.
- po vypršení platnosti přiřazení systém roli přiřazenému objektu automaticky odebere.
- u identity musí být evidován a v systému souhrnně zobrazen seznam všech rolí včetně informace o tom, odkud uživatel roli zdědil nebo mu byla delegována (z organizační jednotky, systematizovaného místa, skupiny apod.). Přístup interních uživatelů krajského úřadu k datům IAM bude zajištěn prostřednictvím webového rozhraní integrovaného do stávajícího intranetového portálu zadavatele.

- správa systému musí být implementována jako webová konzole/aplikace přístupná poslední verze prohlížečů Firefox, Chrome, Internet Explorer, Edge. Tato webová konzole musí být přístupná výhradně protokolem https.
- portál IAM bude implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno).
- zadavatel požaduje vytvoření produkčního a testovacího prostředí IAM.
- řešení musí umožňovat automatizovaný přechod do záložního datového centra v případě nedostupnosti primárního datového centra.
- zálohování bude řešeno jak na úrovni serverů jako celků, tak na úrovni jednotlivých elementů (WS, konektorů, …).
- dodavatel musí systém udržovat vždy v aktualizované podobě bez nároku na další finanční plnění, a to včetně dodání a implementace nových verzí IAM tak, aby systém minimálně odpovídal legislativním a technologickým požadavkům (viz např. GPDR, zákon. č. 110/2019 Sb., o zpracování osobních údajů, zákon č. 111/2009 Sb., o základních registrech, zákon č. 81/2014 Sb., o kybernetické bezpečnosti, zákon č. 365/2000 Sb., o informačních systémech veřejné správy, zákon č. 12/2020 Sb., o právu na digitální služby, zákon č. 250/2017 Sb., o elektronické identifikaci, Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, konec podpory prohlížečů, konec podpory šifrovacích algoritmů, apod.).
- samoobslužný portál pro změnu/obnovení hesla uživatele (ověření SMS/e-mail).
- obsahovat programovatelné konektory na „Integrované systémy“ a dodavatel musí umožnit zadavateli úpravu těchto rozhraní. To znamená že dodavatel předá kompletní dokumentaci a nástroje které jsou třeba pro úpravy tohoto rozhraní.
- portál IAM bude obsahovat možnost vytváření pravidel v grafickém prostředí, tak aby bylo možné automatizovat a zjednodušit postupy pro přidělování skupin, aplikačních rolí, a i dalších atributů osob a uživatelských účtů na základě kombinace libovolných atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo atd.). Provádění vyhodnocení pravidel bude mít stejné vlastnosti jako jiné synchronizační procesy systému. Ruční vs plánované spuštění, historii běhů, simulační režim atd. obsahovat možnosti založení několika účtu jedné osobě.
- systém umožní přidávání a správu dalších typů referenčních objektů, a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity. Systém bude v modulu správy identit u scénáře správy konkrétní identity implementovat v grafickém rozhraní přímý odkaz (proklik) na referenční objekty, na která se daná identita odkazuje včetně toho, aby administrátor mohl po přechodu na tento odkaz vytvářet a editovat další referenční objekty a následně po vrácení zpět na detail identity je v tomto scénáři přiřadil dané spravované identitě. řídit dle údajů z personálního systému životní cyklus osoby včetně všech jejích účtů.
- systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů.
- systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IAM.
- systém umožní kopírovaní aplikačních rolí, mezi jednotlivými systematizovanými místy.
- obsahovat možnosti spuštění skriptů při změnách stavu. (např změna aktivity identity).
- systém bude obsahovat mechanismus zabránění hromadným změnám z důvodu případných chybných vstupních dat (např. z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory apod).
- IAM bude obsahovat možnost exportovat minimálně do následujících formátů: PDF, CSV, HTML, XML a do formátu kompatibilního s MS Word a MS Excel a zahrnuje následující reporty:(historie identity a referenčních objektů, historie identity s ohledem na synchronizace s koncovými systémy, historie přihlášení uživatele do portálu IAM, historie přihlášení uživatele do připojených aplikací, uživatelského účtu a přiřazených rolí uživatele, výsledek rekonciliace, seznam uživatelů v IAM dle stavu, seznam rolí v IAM, seznam systémů v IAM, seznam workflow úloh v IAM, seznam běžících workflow, seznam ukončených workflow, seznam přihlášených uživatelů do portálu IAM, seznam nastavených zástupů uživatele. Pro výběr jednotlivých uživatelů je možné aplikovat vyhledávací kritéria případně filtry.
- export auditního reportu z údajů o identitách uložených v IAM a to i historických. Report bude obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IAM, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti. Report bude možné generovat i do formátu XML.
- report uživatele s přiřazenými aplikačními rolemi a s aplikačními rolemi delegovanými od jiných uživatelů.
- report uživatele obsahující informace o uživateli včetně seznamu rolí, které uživatel má, skupin, certifikátů, atd.
- report uživatelů přiřazených aplikačním rolím.
- report daného běhu synchronizace.

- report daného běhu simulační synchronizace.
- report daného běhu rekonciliační synchronizace.
- report pro ohlášení působnosti k nové agendě.
- IAM bude obsahovat editor pro vyhledávání identit a referenčních objektů v systému IAM pro vytvoření reportu. Do filtru musí být možné zadat libovolné atributy identity, které jsou v systému IAM evidovány včetně přidružených referenčních objektů.
- víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (nebo hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity apod.) umožňovat přes Webové služby řízený přístup k údajům uložených v IAM.
- na úrovní organizační jednotky bude možné pro výběr a přiřazování rolí nastavit sady povolených aplikační rolí, skupiny, systematizovaných míst dostupných pro identity z dané organizační jednotky.
- IAM bude obsahovat centrální dashboard, který bude obsahovat následující údaje (Synchronizační úlohy v chybě, chyby běhu synchronizací, chyby při generování a odesílání notifikací, chyby volaní metod rozhraní webových služeb IAM (např. pokus o přístup k metodě, na kterou nemám oprávnění), chyby plánovaných úloh (agentů), nově vytvořené poznámky, workflow v chybě, neúspěšné akce systému v systému IAM). Záznamy v dashboard se budou načítat za počet dnů definovaných v konfiguraci IAM.
- umožňovat spouštění synchronizací na vyžádání, a to i přes webové služby a přes web rozhraní.
- umožňovat zakládání identit přes webové služby a načítáním xml souborů.
- prezentovat a aplikačně získat organizační strukturu, a to i organizační strukturu dle funkčních míst a i uživatelů.
- systém zajišťuje zprostředkování autentizace formou OTP napojením na SMS bránu. Systém rovněž bude obsahovat modul pro zprostředkování autentizace přes DB systém.

5.2.3. Rozsah implementace IAM

V rámci dodávky a implementace je požadována integrace níže uvedených systémů:
- ISZR,
- RPP – Působnostní,
- systémy uvedené v příloze č.2 smlouvy „Integrované systémy“.
  Primární zdroj identit pro interní uživatele je personální systém. Vlastní způsob implementace a napojení jednotlivých systémů bude stanoven v předimplementační analýze.

IAM musí umožňovat správu všech typů uživatelů informačních systémů:
- zaměstnanci KÚ, (min. 600),
- zaměstnanci příspěvkových organizací zřizovaných krajem, (min. 900),
- zaměstnanci obcí (624 obcí),
- zaměstnanci příspěvkových organizací obcí (min. 827 organizací),
- zaměstnanci externích uživatelů včetně komerčních organizací (min 50 - odhad).
  Pro současné potřeby a budoucí rozvoj je požadován systém s neomezeným množstvím spravovaných identit. A to jak na množství, tak na rozsah.

5.2.3.1. Lokální kopie ISZR-RPP Působnostní s těmito funkcionalitami
- Vytvoření matice práv a rolí dle Informačního systému základních registrů matice RPP (ISZR-RPP) tak, aby vedoucí pracovníci měli možnost zadávat k jednotlivým činnostem konkrétní uživatele (systemizovaná místa) a tyto změny po odsouhlasení odeslat do ISZR-RPP.
- Vytvoření WF přidělování/odebírání agend/činností zaměstnancům vedoucími zaměstnanci s vazbou na systemizovaná místa.
- Potvrzení oprávněným uživatelem úřadu po kompletním zadání každé agendy a následná synchronizace do ISZR-RPP.
- Udržování přehledu oznámené působnosti, jejich stavů, kontrola přeregistrace a změn.
- Vedení přehledu legislativy včetně vazby na jednotlivé činnosti/agendy. Automatická synchronizace všech požadovaných dat mezi lokální RPP, ISZR-RPP, JIP, IAM.
- Vytváření soupisů pověřených úředních osob.
- Vytváření podkladů či aktualizaci pracovních náplní.
- Export dat do XLS (dle stávajícího formátu).
- Inicializace: prvotní synchronizace lokání RPP, ISZR-RPP, IAM, JIP, HR.
- Přístup uživatelů k datům auditního systému musí být zajištěn prostřednictvím webového rozhraní integrovaného do intranetového řešení zadavatele.
- Řešení musí umožňovat automatizovaný přechod do záložního datového centra v případě nedostupnosti primárního datového centra.

5.2.3.2. Integrace Aplikační brány s ISZR

Dodavatel dodá Aplikační bránu na ISZR tak, aby zajistil propojení jednotlivých AIS a dalších systémů, které jsou nezbytné pro připojení na ISZR. Systém musí splňovat ustanovení zákona č. 111/2009 Sb. a souvisejících právních norem.

Systém musí obsahovat přístupový konektor k ISZR a v plném rozsahu musí pokrývat následující funkce:

- vytvoří centrální přístupový bod do ISZR,
- komunikaci do ISZR bude zaznamenávat a ukládat do Auditního systému (viz bod 5.4.),
- vytvoření a aktualizace stejného rozhraní (ISZR) dovnitř IS KÚ v minimálním rozsahu nutném pro pokrytí všech služeb potřebných pro stávající rozsah připojených AIS-ů,
- poskytování seznamu služeb, které je možné využít,
- čtení informačních a referenčních údajů,
- zápis informačních a referenčních údajů,
- ukládání lokální kopie Registru práv a povinností podle článku 5.5 této specifikace, integrace workflow, agendových systémů a spisové služby,
- bude obsahovat mapování vnitřních AIS s agendou ISZR.

5.2.3.2.1. Požadavky na funkcionality centralizovaného komunikačního bodu vůči ISZR

- řešení umožní publikaci eGON rozhraní základních registrů směrem k AISům objednatele,
- řešení umožní definici AISů, které mají oprávnění centrální komunikační bod využívat včetně definování různých rozsahů využívání (jednotlivé webové služby (synchronní, asynchronní, metody push/pull), právo čtení a editace apod.),
- řešení procesu opakovaného volání služby při omezení dat (ISZR omezí výdej dat),
- vypublikovaná rozhraní budou odpovídat rozhraní webových služeb ISZR a to tak, že bude možné jenom na základě změny cíle (serveru, adresy) přemapovat volání jednotlivých AISů z Integrační brány přímo na rozhraní ISZR a opačně,
- možnost definice a správy certifikátů pro komunikaci s ISZR,
- možnost definice a správy oddělených skupin komunikačních kanálů do ISZR a vůči vnitřním informačním systémům pro další subjekty (především ve smyslu hostování celého řešení pro PO a obce),
- systém bude plně respektovat požadavky zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů a zákona č. 365/2000 Sb., o informačních systémech veřejné správy ve znění pozdějších předpisů včetně všech příslušných podzákonných norem a nařízení,
- podpora technik zabezpečení komunikace vůči ISZR proti neoprávněným, nebezpečným, popř. nezdokumentovaným operacím jednotlivých AISů (definice mezních hodnot, hraniční počty dotazů v čase, dotazy na zakázané objekty apod.),
- podpora technik krátkodobého ukládání dat pro urychlení odezvy rozhraní (cachování/ukládání získaných dat z ISZR),
- podpora zpracování pravidelných notifikací a aktualizace uložených (nacachovaných) dat (možnost časování aktualizace např. na noční hodiny),
- podpora zpracování celého procesu reklamace dat v ISZR - využívání reklamačních služeb při procesu zpochybnění referenčního údaje,
- podpora prioritizace AISů - možnost některým AISům dát větší prioritu při využívání služeb proxy řešení a volání ISZR,
- podpora serializace požadavků, která umožní AISům nastavit pořadí zpracování požadavků v ISZR,
- podpora procesu blokování AISů v ISZR - aby dodané řešení bylo schopno tento stav detekovat a upozornit na něj administrátory (mailem, zapsání do logů),
- podpora alertování chybových stavů,
- podpora zpracování osobních údajů v souladu se stanoviskem a metodikou ÚOOÚ,
- podpora ukládání veřejných seznamů z ISZR (např. seznam OVM, seznam právnických osob, seznam existujících adres předpřipravených pro různé účely),
- funkcionalita samostatného nástroje na prohlížení údajů ZR (webové rozhraní, autorizace, zdůvodnění náhledu),
- testovací část dodaného řešení, která bude sloužit k ověření funkčnosti jednotlivých služeb ISZR (eGON rozhraní),
- integrace s IAM ve smyslu autorizace a autentizace (OVM, agenda, agendová činnost. role, uživatel),
- podpora propagace údajů IAM do SOAP hlavičky volání ISZR,
- podpora napojení AISů i pomocí přenosu textových souborů s definovanou strukturou a ODBC, JDBC,
- podpora napojení na ISZR pro příjem aktuálního katalogu rolí pro komunikaci s ISZR,
- uživatelské rozhraní pro přístup ke službám ISZR pro ty agendy, které nemají vlastní AIS.

5.2.3.3. Komunikace a integrace IAM s aplikacemi

- definice standardů komunikace.
- správu aplikačních konektorů mezi integrovanými aplikacemi a IAM.
- databázové konektory pro přímou komunikaci mezi databázemi a IAM.
- identifikaci a distribuci událostí z rozdílných zdrojů.
- redukci integrační logiky v aplikacích.
- možnost modelování procesů pomocí základních prvků (smyčky, odeslání a příjem zprávy, paralelní zpracování, rozhodnutí, korelace, transakce, volání vlastního kódu, pravidla apod.).
- možnost vystavení integračního procesu jako webové služby.
- možnost nabízet transformace dat předávaných mezi jednotlivými systémy.
- podporovat dlouho běžící transakce včetně kompenzace transakce.
- nabízet podporu pro minimálně následující standardní integrační adaptéry:
  - Odeslání/Přijmutí zprávy z disku,
  - Odeslání/Přijmutí zprávy z webové služby – SOAP,
  - Odeslání/Přijmutí zprávy pomocí http(s) protokolu (ne SOAP),
  - Odeslání/Přijmutí zprávy z FTP serveru,
  - Odeslání zprávy pomocí SMTP,
  - Příjem zprávy pomocí POP3,
  - Odesílání/Přijmutí zprávy SMS.
- podpora pro standardizované protokoly (SOAP, REST, MTOM, standardy WS*(WS-Addressing, WS-Enumeration, WS-Policy, WS-MetadataExchange, WS-AtomicTransaction, WS-Eventing, WS-Transfer, WS-Security, WS-Trust, WS-Management, WS-ReliableMessaging).
- podpora pro minimálně následující integrační vzory:
  - synchronní požadavek/odpověď,
  - asynchronní požadavek/odpověď,
  - Publish/Subscribe
  - rozpad dávky na jednotlivé zprávy / Sestavení dávky z několika zpráv,
- nativní podpora XML, ale i jiných formátů (HTTP(S), XML, JSON, Webové služby, csv, txt, MIME, SMIME, zip).
- rozšíření podporované konektivity o aplikační a technologické adaptéry (soubor, JDBC, ODBC, email, FTP atd.) včetně podpory vývoje.
- snadný mechanismus nasazení integračních řešení do neprodukčních prostředí (nejlépe pomocí export/import řešení).
- možnost vizuální tvorby a správy pravidel „Business Rules“, které mohou definovat pravidla ovlivňující další zpracování či chování procesu.

Otevřenost:

- otevřené prostředí s možností dovyvinutí vlastních modulů/adaptérů/komponent v případě potřeby.
- dostupné SDK včetně dokumentace.

Správa:

- v uživatelském rozhraní musí IAM podporovat min.:
  - správu chybových stavů a výjimek při zpracování jednotlivých zpráv a jejich opravu a případné znovuzavedení do zpracování.
  - správu, dohled a dohledatelnost dle kritérií pro jednotlivé zprávy/procesy zpracovávané IAM.
  - redukci času potřebného pro integraci služeb prostřednictvím komfortního nástroje pro vývoj, který umožňuje snadnou integraci bez znalosti konkrétního programovacího jazyka či technologie.
  - zastavení vykonávání vybraného integračního procesu.
  - export zpráv, které nemohly být zpracovány z důvodu výskytu chyby při zpracování.
- skriptovatelné prostředí pro správu.

Spolehlivost/Robustnost:

IAM musí min.:

- zajistit vysokou dostupnost vůči výpadkům jednotlivých komponent řešení a možnost jednoduché obnovy služby v případě výpadku celého řešení.
- nabízet možnost opakovaného doručení zprávy v případě nedostupnosti protistrany (opakovat 3 krát po 3 minutách).
- zajistit spolehlivé zpracování jednotlivých zpráv, díky mechanismu ukládání zpráv při vlastním zpracování.
- podporovat trasování a logování událostí.
- umožnit paralelní zpracování, škálovatelnost, vysokou dostupnost a konfiguračně nastavitelné rozkládání zátěže.

- podporovat širokou škálu komunikačních protokolů, min. TCP/IP, HTTP(s), (s)FTP, SMTP.
- nástroje dodané integrační komponenty musí umožňovat definování konstrukcí pro ošetření výjimek a centrálního logování.
- musí obsahovat vizuální nástroj pro hledání chyb pro správu chybových stavů.
- pro adresování dat ve struktuře datového modelu musí být možné použít jazyk XPath 2.0.
- musí umožňovat definování jak ODBC, tak i JDBC datových zdrojů.
- musí obsahovat prostředky pro vynucení a ověření zabezpečení pomocí: Userid/Password, X.509 token, SAML, Kerberos.
- musí poskytovat otevřené API, pomocí kterého je možné definovat integrační službu, využít API pro nástroje na generování integračních služeb, či jejich migraci.
- zadavatel požaduje vytvoření produkčního a testovacího prostředí.
- řešení musí umožňovat automatizovaný přechod do záložního datového centra v případě nedostupnosti primárního datového centra.
- zálohování bude jak na úrovni serverů jako celků, tak na úrovni jednotlivých elementů (WS, konektorů, …).

5.2.3.4. Funkční požadavky řízení přístupu k aktivům

V rámci systému bude možné spravovat evidenci aktiv s klasifikací dle zákona o kybernetické bezpečnosti. V systému bude možné spravovat evidenci primárních, podpůrných a technických aktiv. Technická aktiva budou dále rozdělena na datová, softwarová, hardwarová aktiva, informační služby. Jednotlivá aktiva je možné členit do hierarchie aktiv.

Minimální rozsah evidovaných dat:

Základní údaje:
- ID Aktiva - identifikátor
- Název aktiva – označení aktiva
- Popis aktiva – popis aktiva
- Typ aktiva – typ aktiva
- Kategorizace aktiva – kategorizace aktiva
- Organizace – označení organizace daného aktiva
- Stav aktiva – stav daného aktiva
- Kód ISVS – číselný kód přidělený informačnímu systému veřejné správy
- Datum identifikace aktiva
- Lokalizace aktiva
- Vazby na jiná aktiva

Analýza rizik
- Požadavky na dostupnost aktiva
- Požadavky na důvěrnost aktiva
- Požadavky na integritu aktiva
- Celkové hodnocení aktiva – číselné hodnocení aktiva
- Popis zabezpečení aktiva – popis způsobu zabezpečení aktiva
- Frekvence přístupu – hodnota frekvence použití aktiva
- Nedostupnost – popis hodnocení maximální doby nedostupnosti a definice náhradních postupů v případě nedostupnosti

Ochrana v rámci zpracování osobních údajů:
- Klasifikace – klasifikace osobních údajů
- Zdroj dat – popis získání osobních údajů
- Aktualizace – popis způsobu aktualizace osobních údajů
- Skartace – popis skartace dat
- Zpracování – popis způsobu zpracování osobních údajů
- Registrace – popis registrace zpracování osobních údajů na Úřad pro ochranu osobních údajů
- Kategorie – kategorie osobních údajů
- Účel zpracování – účel zpracování osobních údajů
- Zpracovatel – informace o zpracovateli osobních údajů
- Příjemce – informaci o příjemci osobních údajů v případě, že jsou předávány
- Legislativa – popis legislativy vztahující se k danému aktivu.

Garanti aktiv:
- Vlastník – vlastník aktiva

- Správce aktiva – správce aktiva (například dané aplikace)
- Zástupce – zástupce správce aktiva
- Uživatelé – seznam uživatelů daného aktiva. Uživatele bude možné slučovat do rolí a skupin

Technické údaje (týkající se technických aktiv):

- Technické prostředky (servery, databáze) – odkaz na technické prostředky, pro provoz a aktiva
- Zálohování – popis způsobu a frekvence zálohování

Systém bude obsahovat správu osob, organizační strukturu, rolí. Tuto evidenci bude možné synchronizovat s personálním systémem a navázat na správu aktiv.

Systém bude obsahovat funkcionalitu pro generování následujících reportů:

- Přehled aktiv s možností filtrování a třídění podle všech dostupných polí
- Karta aktiva se všemi navázanými údaji
- Zobrazení vazeb mezi aktivy
- Možnost definice vlastních sestav
- Přehled žádostí o přidělení aktiva aktivních a dokončených
- Přehled oprávnění a přístupů k danému aktivu

Systém bude obsahovat implementaci následujících workflow:

- Žádost o přístup k aktivu směrovaná na seznam Garantů jako schvalovatele žádosti
- Periodická revize aktiv jednotlivými garanty
- Periodická revize stavu evidence garantem z oblasti řízení bezpečnosti

Funkční požadavky na workflow:

- Zadávání požadavků uživatelů na změny v evidenci
- Možnost sledování stavu svých požadavků uživateli
- E-mailové upozornění schvalovatele na požadavek ke schválení
- Přehled úloh ke schválení pro každého schvalovatele
- Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění
- Podpora vícekrokového schvalování
- Podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů)
- Možnost větvení pro ošetření výjimek vzniklých při schvalování
- Řešení zastupitelnosti
- Eskalace upozornění při překročení termínu splnění
- Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů

Další funkce:

- Průběh workflow bude možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý stav probíhajícího workflow. Diagram bude v obvyklém formátu pro zobrazení workflow např. aktivity diagram, BPMN nebo Archimate.
- Systém bude napojen na systém řízení autentizace uživatelů.
- Systém bude obsahovat webový portál (dále jen Portál), který bude sloužit jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správu a konfiguraci systému.
- Správa systému musí být implementována jako webová konzole/aplikace přístupná poslední verze prohlížečů Firefox, Chrome, Internet Explorer, Edge. Tato webová konzole musí být přístupná výhradně protokolem https.
- Přístup interních uživatelů krajského úřadu k datům systému bude zajištěn prostřednictvím webového Portálu integrovaného do stávajícího intranetového portálu zadavatele.
- Portál bude implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno).
- Systém umožní dodatečné konfigurační rozšiřování evidence o další atributy.
- Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem.
- Systém bude obsahovat editor oprávnění. V rámci editoru bude administrátor definovat oprávnění do systému a následně tato oprávnění přiřazovat konkrétním uživatelům. Oprávnění bude definováno pro jednotlivé části systému (aktiva, uživatelé aktiva, konfigurace notifikací, konfigurace systému, reporty, workflow, správa rozhraní atd.) Oprávnění bude definováno až na konkrétní atributy včetně zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti atributu, pořadí zobrazení atributů ve formuláři. U jednotlivých entit a modulů bude možnost definovat akce, které může uživatel s entitami a v rámci systému provádět.

- Veškeré změny vyvolané požadavky uživatelem systému budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v evidenci. Záznam v logu bude obsahovat původní i novou hodnotu.
- Systém poskytne rozhraní pro pravidelnou synchronizaci softwarových aktiv a jim přidělených uživatelů.

5.3. Auditní systém

Pro potřeby IAM a „Integrovaných systémů“ bude vytvořen zabezpečený auditní a logovací systém, Tento systém bude funkčně nezávislý na IAM. Součástí auditního systému musí být zaznamenání všech událostí systému IAM a všech připojených IS. Dále musí umožňovat:

- vytváření reportů,
- vedení historie jednotlivých přístupů uživatelů a historii jejich přístupových práv včetně sledování toho, kdo změnu provedl,
- v případě využití stávajícího databázového prostředí bude napojení provedeno v součinnosti s pracovníky zadavatele,
- možnost vyhledávání dle všech položek v zadaném časovém intervalu,
- uložení všech položek nutných ke splnění zákonných požadavků ISZR,
- důvěryhodné uložení (lze využít prostředků TCK),
- import dat ze současného auditního systému.

5.4. Bezpečnost

Zadavatel z důvodů maximálního omezení bezpečnostních rizik požaduje vystavení certifikátu jakosti pro dodávané řešení. Analýza technických a bezpečnostních rizik bude zpracována jako samostatná kapitola v předimplementační analýze. Dodavatel řešení navrhne omezení těchto rizik a zajištění bezpečnosti celého řešení. Analýza bezpečnosti by měla pokrýt minimálně tyto oblasti:

- šifrované uložení citlivých dat jako např. přihlašovací údaje,
- zabezpečení použitého databázového serveru (data musí být uložena v šifrované formě),
- zabezpečení bezpečného přístupů externích uživatelů – bude součástí předimplementační analýzy viz.bod 5.1,
- dodavatel musí reagovat na aktuální hrozby a aktivně navrhovat bezpečnostní opatření,
- po obdržení zjištění od objednatele o zjištěných bezpečnostních rizicích musí dodavatel odstranit tyto zjištěná rizika na bez nároku na odměnu včetně instalace a implementace do testovacího a produkčního prostředí.

5.5. Pořízení softwarových licencí

Zadavatel požaduje, aby součástí dodávky byly všechny potřebné licence pro provoz dodávaného řešení. Nabídka musí obsahovat všechny potřebné licence aplikací a další potřebný SW související s provozem dodávaného řešení. Výjimku mohou tvořit licence uvedené v bodě 4 „Výchozí SW a HW vybavení“.

5.6. Dokumentace řešení

Zadavatel požaduje vytvoření kompletní technické a uživatelské dokumentace. Dokumentace bude jednoznačně a detailně popisovat celé implementované řešení včetně popisu všech rozhraní. Umožní uživatelům na všech úrovních bezproblémovou orientaci v implementovaném prostředí. Technická dokumentace bude mimo jiné obsahovat i popis procesu zálohování a obnovy, monitoringu a procedur bezpečného vypnutí a spouštění systému. Součástí bude nejen dokumentace implementovaného řešení ale i dokumentace jednotlivých dodaných systémů.

5.7. Akceptační testy

Předání a převzetí díla bude provedeno na základě protokolu o provedených akceptačních testech. Ukončení akceptačních testů budu stvrzeno podepsáním akceptačního protokolu po ukončení zkušebního provozu. Návrh akceptačních kritérií a obsah a forma akceptačního protokolu bude součástí předimplementační analýzy. Součástí akceptačních testů musí být minimálně:

- ověření funkčnosti řešení v plném rozsahu technické specifikace,
- ověření funkčního řešení v rámci testovacího provozu IAM,
- ověření funkčnosti rozhraní pro jednotlivé připojené systémy,
- úplná technická a uživatelská dokumentace implementovaného řešení včetně popisu rozhraní pro jednotlivé přípojné systémy.

5.8. Zkušební provoz

Uchazeč zajistí zkušební provoz o délce 1 kalendářního měsíce. Termín započetí zkušebního provozu musí být stanoven s ohledem na nutnost dodržení požadavku ukončení zkušebního provozu nejpozději do termínu stanoveného v článku 3. Ukončením zkušebního provozu systém automaticky přechází do provozu ostrého. V rámci zkušebního provozu je požadováno zajištění technické podpory s parametry dostupnosti min. započetí prací na odstranění incidentu nejpozději do 1 hodiny od nahlášení v pracovní době objednatele. V rámci zkušebního provozu bude ověřena funkčnost produktu v nasazení, odpovídajícím finálnímu stavu v ostrém provozu.

5.9. Školení

Dodavatel zajistí proškolení určeného počtu uživatelů min. v níže stanoveném rozsahu:

- správce – 4 osoby, školení v rozsahu minimálně 6 pracovních dnů (8 vyučovacích hodin denně) pro každou osobu zakončené certifikátem pro administraci implementovaných produktů,
- uživatel – školení v rozsahu 2 pracovních dnů v sídle Objednatele.

Uchazeč pro účely školení vytvoří ve spolupráci se zadavatelem osnovu školení a školící dokumentaci pro jednotlivé typy uživatelů. Termíny školení budou stanoveny dodavatelem po konzultaci se zadavatelem. Tyto musí být stanoveny tak, aby proškolení správců a uživatelů bylo dokončeno před započetím zkušebního provozu. Školení bude probíhat v českém jazyce.

5.10. Ostatní požadavky

- Záruka 36 měsíců.
- Další technické požadavky:
  produkt je možné nativně provozovat na všech typech níže uvedeného vybavení:
  - prostředí virtuálních serverů VMWare,
  - typ databáze: Oracle, MS SQL,
  - Internet Explorer, Mozilla Firefox, Google Chrome, Microsoft Edge v aktuálně výrobcem podporovaných verzích.

Součástí nabídky bude položkový rozpočet veškerých potřebných komponent, licencí a prací potřebných pro kompletní implementaci všech navržených technologií.

Všechny části řešení, které budou v interakci s běžným uživatelem musí být plně lokalizovány do českého jazyka. U ostatních částí řešení se kromě českého jazyka připouští i možnost anglického jazyka.

Seznam použitých zkratek

IAM …systém pro správu identit
JIP …jednotný identitní prostor
DC …datové centrum
AD… active directory
KAAS – katalog autentizačních a autorizačních služeb
ISZR – informační systém základních registrů
AIS – agendový informační systém
ODBC – Open Database Connectivity (Jedná se o standardizované rozhraní pro přístup k databázovým systémům)
JDBC - Java Database Connectivity (Jedná se o standardizované rozhraní pro programátory v programovacím jazyku Java, které definuje jednotné rozhraní pro přístup k relačním databázím)
TC – technologické centrum kraje
SeP – service provider
IP – Identity provider
HR – Human resources
BPMN - Business Process Model and Notation
SAML - Security Assertion Markup Language

Příloha č. 2 - Integrované systémy – výčet a stručný popis

1. SKUPINA INFORMAČNÍCH SYSTÉMŮ JIŽ NYNÍ INTEGROVANÝCH.

IS KÚ je v současnosti integrován z jedné části v rámci stávajícího AD. Uživatelé jednotlivých IS se autentizují vůči AD a autorizují členstvím ve skupinách AD. Takto integrovaných IS je v této chvíli větší počet, všechny využívají stejného principu integrace. V rámci integrace je požadováno napojení AD k IAM. Zároveň bude zachována integrace stávajících aplikací na AD. Konfigurace stávajících systémů integrovaných s AD bude probíhat prostřednictvím nástroje IAM odkud budou tyto přenášeny do AD, následně budou tyto úpravy zpropagovány prostřednictvím stávající integrace do cílové aplikace.

Systém	Podřízené systémy	Autor
AD	AD, Exchange, intranet APPs, extranet APPs,(např telefonní seznam) a jiné IS integrované na AD stejným způsobem	Microsoft

2. DALŠÍ SKUPINA INFORMAČNÍCH SYSTÉMŮ

Níže vyjmenované IS jsou převážně dvouvrstvé desktopové aplikace. Tyto aplikace již disponují požadovanými funkčnosti a mají zprovozněné rozhraní definované specifikovanými body:

Specifikace rozhraní společná pro všechny níže vyjmenované systémy

- **Autentizace:** jednotné přihlášení uživatelů napříč IS KÚ, jednotná politika hesel.
- **Autorizace:** Jednotný proces správy uživatelských účtů a rolí, role uživatelů IS budou řízeny externím informačním systémem IAM.
- Synchronizace „referenční údaje“ vedené v IS se **Základními registry** (ISZR).
- **Logování:** zajistit záznam provozních činností.

Je požadováno napojení na již funkční rozhraní těchto systémů.

Systém	Kategorie systému	Dodavatel
Docházkový systém ANeT	Docházkový systém	ANeT, s. r. o.
FLUXPAM a FLUX Personalistika	Personalistika, Mzdy a vzdělávání	Flux, s r.o.
GINIS	Elektronická Spisová služba	GORDIC, s. r.o.
EDA	Evidence dopravních agend	YAMACO Software
EVI9, ESPI9	Evidence rozhodnutí odpadu, synchronizace dat vykázaných obcemi 3	INISOFT, s.r.o.
VITA software	Stavební úřad a přestupky	VITA Software, s. r. o.

iUsnesení	Příprava materiálů pro Zastupitelstvo a Radu kraje	Pilscom spol., s r. o.
Software602 FormFlow Server	Elektronické cestovní příkazy	Software 602, a.s.
SpiritGIS ÚAP	Systém pro správu a vedení územně analytických podkladů	GEOREAL, spol. s r.o.
hostovaná SSL	Hostovaná spisová služba	
KDS, KDR	Krajská digitální spisovna a repozitář	GORDIC, s.r.o.
datový sklad	Datový sklad	GORDIC, s.r.o.
Helpdesk	Helpdesk pro interní a externí uživatele	Tesco SW, a.s.

3. PODROBNÝ POPIS:

3.1. Active directory

IAM bude napojeno na Microsoft Active Directory s následující funkcionalitou:

a) komplexní správa účtů, certifikátů a skupin a organizační struktury (založení, změnu atributů, zrušení, změna hesla, fotografie, vztahy podřízený/nadřízený atd.)

b) založení domovského adresáře včetně nastavení oprávnění

c) správa účtů a jejich certifikátů včetně inicializačního načtení z AD

d) správa skupin a členství ve skupinách včetně inicializačního načtení z AD

e) správa organizačních jednotek včetně inicializačního načtení z AD

3.2. MS Exchange

IAM bude napojeno na Microsoft Exchange s následující funkcionalitou:

a) správa emailových schránek na serveru Microsoft Exchange (vytvoření, zrušení, zneplatnění, opětovná aktivace)

b) řízení životního cyklu emailových schránek v IAM bude prostřednictvím správy odpovídajících aplikačních rolí uživatele

c) při změně role uživatele, na kterou je vázáno umístění schránky v datastore, bude při synchronizaci automaticky přemístěna schránka do odpovídajícího uložiště

d) řízení i dalších objektů a jejich životního cyklu na MS Exchange (např. distribuční seznamy, kontakty,…)

3.3. Telefonní seznam

IAM bude napojeno na telefonní seznam s následující funkcionalitou

a) inicializační načtení dat

b) správa uživatelů

c) správa organizační struktury

3.4. Anet

IAM bude napojeno na Anet s následující funkcionalitou

a) inicializační načtení dat

b) správa lokálních identit

c) správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí

d) správa rolí a středisek

e) přenos údajů z Anet do IAM pro rekonciliační report

3.5. Flux

IAM bude napojeno na personální systém FLUX s následující funkcionalitou:

Z personálního systému budou načítány údaje o organizační struktuře, hierarchii pracovních míst, osobách a tyto údaje budou pro IAM sloužit jako zdrojové. Fotografie zaměstnanců budou předávány v samostatném XML souboru, který bude umístěn ve stejné složce file systému jako hlavní soubor a bude obsahovat fotografie všech zaměstnanců.

IAM bude dále v systému FLUX řídit oprávnění uživatelů FLUX včetně přiřazování odpovídajících rolí. Seznam aplikačních rolí systému FLUXPAM bude do IAM synchronizován prostřednictvím integrační vrstvy. IAM bude dále získávat údaje pro rekonciliační report a údaje o přihlášení uživatelů do aplikace Flux.

3.6. GINIS

IAM bude napojeno na IS Ginis s následující funkcionalitou:

a) inicializační načtení dat

b) správa lokálních identit

c) správa oprávnění pro jednotlivé uživatele na moduly IS (správa konfiguračních skupin)

d) správa funkčních míst a organizačních jednotek včetně vazby na agendové role

e) přenos údajů do IAM z IS Ginis o přihlášení uživatelů do IS Ginis

f) přenos údajů z IS Ginis do IAM pro rekonciliační report

3.7. EDA

IAM bude napojeno na EDA s následující funkcionalitou:

a) inicializační načtení dat

b) správa lokálních identit

c) správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí

d) přenos údajů z EDA do IAM o přihlášení uživatelů do EDA

e) přenos údajů z EDA do IAM pro rekonciliační report

3.8. EVI9

IAM bude napojeno na EVI9 s následující funkcionalitou:

a) inicializační načtení dat

b) správa lokálních identit

c) správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí

d) přenos údajů z EVI9 do IAM o přihlášení uživatelů do EVI9

e) přenos údajů z EVI9 do IAM pro rekonciliační report

3.9. ESPI9

IAM bude napojeno na ESPI9 s následující funkcionalitou:

a) inicializační načtení dat

b) správa lokálních identit

c) správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí

d) přenos údajů z ESPI9 do IAM o přihlášení uživatelů do ESPI9

e) přenos údajů z ESPI9 do IAM pro rekonciliační report

3.10. VITA

IAM bude napojeno na VITA s následující funkcionalitou:

a) inicializační načtení dat
b) správa lokálních identit
c) správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí
d) přenos údajů z VITA do IAM o přihlášení uživatelů do VITA
e) přenos údajů z VITA do IAM pro rekonciliační report

3.11. iUsnesení

IAM bude napojeno na iUsnesení s následující funkcionalitou:

a) inicializační načtení dat
b) správa lokálních identit
c) správa organizační struktury
d) správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí
e) přenos údajů z iUsnesení do IAM o přihlášení uživatelů do iUsnesení
f) přenos údajů z iUsnesení do IAM pro rekonciliační report

3.12. SW602

IAM bude napojeno na SW602 s následující funkcionalitou:

a) inicializační načtení dat
b) správa lokálních identit
c) správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí
d) přenos údajů z SW602 do IAM o přihlášení uživatelů do SW602

3.13. UAP

IAM bude napojeno na Portál UAP a Spirit UAP s následující funkcionalitou:

a) doplnění možnosti basic autentizace při ověření vůči AD v rámci komunikace mezi Spirit UAPa Portál UAP.
b) inicializační načtení dat
c) správa lokálních identit
d) správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí

3.14. Hostovaná spisová služba

IAM bude napojeno na hostovanou spisovou službu s následující funkcionalitou:

Přiřazování rolí a jejich oprávnění se bude řešit přímo v SSL. Z IAM se budou přenášet pouze uživatelé.

3.15. KDS

IAM bude napojeno na KDS s následující funkcionalitou:

a) inicializační načtení dat
b) správa lokálních identit
c) správa oprávnění pro jednotlivé uživatele na moduly IS (správa konfiguračních skupin)
d) správa funkčních míst a organizačních jednotek
e) přenos údajů z KDS do IAM pro rekonciliační report

3.16. KDR

IAM bude napojeno na KDR s následující funkcionalitou:

a) inicializační načtení dat
b) správa lokálních identit
c) správa oprávnění pro jednotlivé uživatele na moduly IS (správa konfiguračních skupin)

d) správa funkčních míst a organizačních jednotek

e) přenos údajů z KDR do IAM pro rekonciliační report

3.17. Datový sklad

IAM bude napojeno na datový sklad s následující funkcionalitou:

a) inicializační načtení dat

b) správa lokálních identit

c) správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí

3.18. Hespldesk

IAM bude napojeno na Helpdesk s následující funkcionalitou:

a) inicializační načtení dat

b) správa lokálních identit

c) správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí

d) správa rolí a středisek

e) přenos údajů z Helpdesk do IAM o přihlášení uživatelů do Helpdesk

f) přenos údajů z Helpdesk do IAM pro rekonciliační report

3.19. JIP

IAM musí obsahovat správu identit, rolí a systémů evidovaných v systému JIP včetně:

a) obousměrné synchronizace s JIP,

b) automatické pravidelné načítání aplikací a rolí z JIP do IAM,

c) automatické předávání identity včetně vazby na jednotlivé aplikační a agendové činnostní role z IAM do JIP,

d) možnosti změny hesla uživatele v JIP prostřednictvím webového portálu IAM.

3.20. Postsignum

IAM bude napojeno na PostSignum s následující funkcionalitou:

a) inicializační načtení dat,

b) správa uživatelů z IAM v Postsignum,

c) správa certifikátů uživatelů v IAM z Postsignum.

3.21. NIA

a) zajišťuje zprostředkování ověření identity vůči externím poskytovatelům identit NIA. Systém bude schopen fungovat v režimu IdP vůči poskytovatelů služeb (SeP). Systém bude dále vystupovat v režimu SeP vůči NIA.

b) obsahuje rozcestník pro výběr vhodného poskytovatele identit a autentizačního prostředku. Pro jednotlivé poskytovatele služeb (SeP) bude možné v platformě konfigurovat seznam povolených poskytovatelů identit (IdP) a úrovní autentizace.

c) bude obsahovat službu autentizace formou jednotného webového přihlášení Single Sign On. Systém bude schopen řídit připojení třetích aplikací pro federovanou autentizaci a autorizaci komunikace mezi poskytovatelem identity (IdP) a poskytovatelem služeb (SeP)) pomocí SAML 2.0 protokolu. Dále zajistí dle nastavení parametru v konfiguraci platnost tokenu pro přihlášení SAML Single Sign On pro napojené aplikace. Po vypršení tohoto časového intervalu bude nutné se opět autentizovat.

Příloha č. 3 - Podmínky využití Technologického centra Jihočeského kraje

Preambule:

- TC JčK je majetkem Jihočeského kraje
- Jihočeský kraj, prostřednictvím OINF, poskytuje prostředky technologického centra dle svých potřeb a možností,

Podmínky využití:

1) TC JčK je provozováno ve dvou geograficky oddělených lokalitách,
2) serverová virtualizace je realizována virtualizační platformou VMware,
3) jsou k dispozici relační databáze Microsoft SQL a Oracle,
4) diskový prostor je poskytován dle možností TC JčK a potřeb IS
5) pro dlouhodobé bezpečné uložení je k dispozici úložiště EMC Centera
6) zálohování je realizováno zálohovacím SW Networker, úložištěm pro ukládání záloh je EMC DataDomain
7) bude umožněn bezpečný, monitorovaný dálkový přístup konkrétním technickým pracovníkům dodavatele IS,
8) pro běh aplikací jsou k dispozici virtuální servery s Windows Server 2019
9) pro aplikační servery je k dispozici internetová konektivita včetně její ochrany firewallem
10) aplikační servery mají přidělována jména v rámci domény kraj-jihocesky.gov.cz včetně zajištění veřejného DNS záznamu
11) aplikačním serverům můžou být vystaveny certifikáty interní CA Jihočeského kraje (tato CA nemá přímou podporu v prohlížečích, nutno doinstalovat root certifikáty mezi důvěryhodné)
12) odbor informatiky KÚ provádí správu celé infrastruktury včetně údržby OS v rozsahu instalace aktualizací dodaných výrobcem OS (instalace aktualizací prostřednictvím Windows Update). Pokud je dodavateli známo, že některá aktualizace s jeho IS nepracuje, musí toto dodavatel dopředu oznámit
13) všechna data, která budou vytvořena v rámci provozu IS budou ve výhradním vlastnictví Objednatele
14) pokud TC JčK nebude obsahovat komponentu, kterou dodavatel vyžaduje, musí tuto komponentu dodavatel dodat v rámci dodávky. Konečné posouzení, zda je komponenta kompatibilní s infrastrukturou TCK a zda bude nainstalována, je plně v kompetenci OINF
15) Zhotovitel se zavazuje, že nezneužije ICT infrastrukturu TC JčK,
16) Jihočeský kraj se nezavazuje poskytnout jiné než aktuálně nainstalované verze jednotlivých technologických komponent
17) OINF poskytuje parametry SLA 8x5 s dobou řešení NBD

Seznam zkratek:

TC JčK	Technologické centrum Jihočeského kraje
IS	informační systém provozovaný v TC JčK
OINF	Odbor informatiky Krajského úřadu Jihočeského kraje

Příloha č. 4- Bezpečnostní pravidla pro dodavatele

Cílem těchto bezpečnostních pravidel je snižování kybernetických rizik a zvyšování účinnosti bezpečnostních opatření chránící Aktiva KÚ JK, ke kterým mají přístup Dodavatelé.

1 Základní odpovědnosti Dodavatele

Dodavatel řešení:

a) Je povinen dodržovat požadavky na bezpečnost informací v souladu s platnými zákony ČR.
b) Odpovídá za své řešení/dodávku/správu tak, aby respektovalo požadavky na bezpečnost KÚ JK, zabránilo bezpečnostním incidentům a stavu kybernetického nebezpečí.
c) Odpovídá za dodávku a implementaci řešení v požadované kvalitě i z pohledu bezpečnosti.
d) Ručí za trvalé zachování mlčenlivosti všech svých pracovníků i po ukončení smluvního vztahu s úřadem.

Dodavatel je povinen akceptovat použití prostředků bezpečnostního auditu, které mohou být útvarem IT využity k sledování aktivit v prostředí ICT/IS či aktivity procházejících přes toto prostředí.

2 Ochrana Aktiv

Dodavatel se před vlastním **přístupem** k datům a informacím KÚ JK musí zavázat mlčenlivostí. Tzn., že platí povinnost Dodavatele se zavázat a také povinnost pracovníků KÚ JK (prioritně ve smlouvě, prohlášením Dodavatele, formulářem, …) zavázat Dodavatele a nezpřístupnit data a informace Dodavateli dříve, než dojde k jeho závazku mlčenlivosti (tj. podpisu NDA – Non Disclosure Agreement či CA – Confidentiality Agreement).

3 Přístup k ICT/IS

Přihlášení Dodavatele do sítě KÚ JK musí podléhat kontrole přístupu na základě autorizace po předchozí autentizaci, včetně autentizace přes VPN v případě užití VPN klienta. Přihlašovací proces do VPN a do Windows domény poskytuje základní bezpečnostní funkce – nikdy se nezobrazuje vkládané heslo a heslo není nikde přenášeno a ukládáno v nezašifrované formě. Přístup ke službám ICT/IS je vždy zajištěn přes proces autentizace, autorizace a bezpečnostního auditu.

4 Ochrana před škodlivým softwarem

Dodavatel je povinen:

a) Centrálně organizovat zabezpečení svých koncových stanic v připojeních do své infrastruktury (např. řízení personálních firewallů, antivirového SW atd.) a to minimálně na úrovni standardů KÚ JK. Standardy KÚ JK se řídí zákonem č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a zejména vyhláškou č. 82/2018 Sb. Vyhláška o kybernetické bezpečnosti a dále bezpečnostními doporučeními NCKB pro administrátory v aktuálně platné verzi. Dodavatel by měl v přiměřené míře splňovat požadavky uvedených dokumentů.
b) Obsahem antivirové ochrany jsou taková opatření technického a administrativního charakteru, která vedou k detekci a následnému odstranění infiltrujícího software u všech prostředků provozovaných v rámci infrastruktury Dodavatele.
c) Dodavatel musí na své straně definovat zásady bezpečného užívání Internetu a s těmito zásadami seznámit veškerý personál užívající ICT prostředky infrastruktury Dodavatele.
d) Dodavatel musí na pracovních stanicích v jeho odpovědnosti zajistit bezpečné nakonfigurování prohlížečů obsahu Internetu (např. www prohlížeče).

5 Řízení bezpečnostních rizik

Dodavatel je povinen zajistit, že:

a) Hesla pracovníků Dodavatele nebudou zaznamenávána v otevřené podobě.
b) Vzájemnou spolupráci a komunikaci mezi Dodavatelem a KÚ JK při řešení ICT bezpečnostní rizik

6 Hlášení

Dodavatel je povinen KÚ JK hlásit:

a) nestandardní situace při práci v ICT/IS;
b) bezpečnostní události nad ICT/IS;
c) bezpečnostní slabiny v ICT/IS Objednatele.

7 Kontrola a audit Dodavatele

KÚ JK má obecné právo auditu prostředí Dodavatele za účelem ověření dodržování Bezpečnostních pravidel Objednatele či za účelem ověření zabezpečení dat a informací na ICT prostředcích Dodavatele, a to minimálně 1x za 12 měsíců.

8 Ošetření výjimek

Ve výjimečných případech je možno vyhlásit výjimku z dodržování bezpečnostních pravidel. Udělení výjimek ze stanovených pravidel se provádí na základě požadavku zaslaného manažerovi kybernetické bezpečnosti, který má právo výjimku udělit.

Schváleno: Bezpečnostní komise – Výbor pro řízení kybernetické bezpečnosti

Příloha č. 5- Ochrana a zpracování osobních údajů

1. Objednatel a zhotovitel se zavazují, v souvislosti s touto smlouvou, postupovat v souladu s platným Obecným nařízením Evropského parlamentu a Rady (EU) 2016/679, ze dne 27. dubna 2016 (dále jen Nařízení).
2. Zhotovitel bere na vědomí, že se ve smyslu všech výše uvedených právních předpisů považuje a bude považovat za zpracovatele osobních údajů, se všemi pro něj vyplývajícími důsledky a povinnostmi. Objednatel je a bude nadále považován za správce osobních údajů, se všemi pro něj vyplývajícími důsledky a povinnostmi.
3. Ustanovení o vzájemných povinnostech správce a zpracovatele při zpracování osobních údajů zajišťuje, že nedojde k nezákonnému použití osobních údajů týkajících se subjektů údajů ani k jejich předání do rukou neoprávněné třetí strany. Smluvní strany se dohodly na podmínkách zajištění odpovídajících opatření k zabezpečení ochrany osobních údajů a základních práv a svobod subjektů údajů při zpracování osobních údajů zpracovatelem.
4. Zpracovatel se zavazuje zpracovávat pouze a výlučně ty osobní údaje, které jsou nutné k výkonu jeho činnosti dle této smlouvy.
5. Zpracovatel je oprávněn zpracovávat osobní údaje dle této smlouvy pouze a výlučně po dobu účinnosti této smlouvy, stanovené v čl. 10 smlouvy „Závěrečná ustanovení“.
6. Zpracovatel je oprávněn zpracovávat osobní údaje pouze za účelem stanoveném v předmětu Servisní smlouvy.
7. Zpracovatel je povinen se při zpracování osobních údajů řídit výslovnými pokyny správce, budou-li mu takové uděleny, ať již ústní či písemnou formou. Za písemnou formu se považuje i elektronická komunikace, včetně emailu. Zpracovatel je povinen neprodleně správce informovat, pokud dle jeho názoru udělený pokyn správce porušuje Nařízení nebo jiné předpisy na ochranu osobních údajů.
8. Zpracovatel je povinen zajistit, že osoby, jimiž bude provádět plnění dle této smlouvy, se zavážou k mlčenlivosti ohledně veškeré činnosti související s touto smlouvou, zejm. pak k mlčenlivosti ve vztahu ke všem osobním údajům, ke kterým budou mít přístup, nebo s kterými přijdou do kontaktu.
9. Zpracovatel je povinen, ve smyslu čl. 32 Nařízení přijmout, s ohledem na stav techniky, náklady na provedení, povahu, rozsah, kontext a účely zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku, zejm. pak osobní údaje zabezpečit vůči náhodnému či nezákonnému zničení, ztrátě, změně, zpřístupnění neoprávněným stranám, zneužití či jinému způsobu zpracování v rozporu s Nařízením.
10. Zpracovatel je povinen písemně seznámit správce s jakýmkoliv podezřením na porušení nebo skutečným porušením bezpečnosti zpracování osobních údajů podle ustanovení této smlouvy, např. jakoukoliv odchylkou od udělených pokynů, odchylkou od sjednaného přístupu pro správce, plánovaným zveřejněním, upgradem, testy apod., kterými může dojít k úpravě nebo změně zabezpečení nebo zpracování osobních údajů, jakýmkoliv podezřením z porušení důvěrnosti, jakýmkoliv podezřením z náhodného či nezákonného zničení, ztráty, změny, zpřístupnění neoprávněným stranám, zneužití či jiného způsobu zpracování osobních údajů v rozporu s Nařízením. Správce bude neprodleně seznámen s jakýmkoliv podstatným porušením těchto ustanovení o zpracování dat.
11. Zpracovatel není oprávněn, ve smyslu čl. 28 Nařízení, zapojit do zpracování osobních údajů dalšího zpracovatele (zákaz řetězení zpracovatelů), bez předchozího schválení a písemného souhlasu správce.
12. Zpracovatel je povinen a zavazuje se k veškeré součinnosti se správcem, o kterou bude požádán v souvislosti se zpracováním osobních údajů nebo která mu přímo vyplývá z Nařízení. Zpracovatel je povinen na vyžádání zpřístupnit správci svá písemná technická a organizační bezpečnostní opatření a umožnit mu případnou kontrolu, audit či inspekci dodržování předložených technických a organizačních bezpečnostních opatření.
13. Po skončení účinnosti této smlouvy nebo v případě předčasného ukončení, je zpracovatel povinen všechny osobní údaje, které má v držení vymazat, a pokud je dosud nepředal správci, předat je správci a dále vymazat všechny existující kopie. Povinnost uvedená v tomto článku neplatí, stanoví-li právní předpis EU, případně vnitrostátní právní předpis zpracovateli osobní údaje ukládat i po skončení účinnosti této smlouvy.