Specifikace požadavků na zadávané řešení elektronického systému spisové služby (ESSL)

1. FUNKČNÍ POŽADAVKY NA ZADÁVANÉ ŘEŠENÍ

1.1. Požadavky na funkčnost dané legislativou

Požadavky na funkčnost ESSL sestávají ze souborů dílčích požadavků rozdělených mezi požadavky na funkčnost ESSL dané legislativou a požadavky na konfiguraci ESSL v prostředí Zadavatele. Tyto požadavky jsou chápány jako celek mandatorních požadavků na ESSL.

ESSL musí splňovat všechny požadavky dané příslušnou legislativou, v aktuálním znění, a to zejména:

a) Národní standard pro elektronické systémy spisové služby, který stanovuje základní požadavky na funkce těchto systémů a vytváří sjednocující parametry pro výkon spisové služby vztahující se k dokumentům v digitální podobě (dále jen **„Národní standard“**)[1].
b) zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů **(dále jen „zákon č. 499/2004 Sb.“)**,
c) vyhláška č. 259/2012 Sb. o podrobnostech výkonu spisové služby, ve znění pozdějších předpisů (dále jen **„vyhláška č. 259/2012 Sb.“**),
d) zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů **(dále jen „zákon č. 300/2008 Sb.“)**,
e) vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů (dále jen **„vyhláška č. 193/2009 Sb.“**),
f) vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, ve znění pozdějších předpisů (dále jen **„vyhláška č. 194/2009 Sb.“**),
g) zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (dále jen **„zákon č. 297/2016 Sb.“**),
h) zákon č. 298/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, **(dále jen „zákon č. 298/2016 Sb.“**),

[1] Oznámení Ministerstva vnitra č. V-74291-3/AS-2012, kterým se zveřejňuje národní standard pro elektronické systémy spisové služby (uveřejněno ve Věstníku Ministerstva vnitra č. 64/2012 ze dne 11. 7. 2012)

i) Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. 7. 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále jen **„Nařízení č. 910/2014“**),
j) Nařízení Evropského parlamentu a Rady (EU) 2016/679 z 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále jen **„GDPR“**),
k) zákon č. 110/2019 Sb., o zpracování osobních údajů,
l) zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů,
m) zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů,
n) zákon č. 365/2000 Sb., o informačních systémech veřejné správy,
o) zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů,
p) zákon č. 111/2009 Sb., o základních registrech,
q) zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích),
r) zákon č. 106/1999 Sb., o svobodném přístupu k informacím,
s) zákon č. 218/2000 Sb., rozpočtová pravidla,
t) zákon č. 130/2002 Sb., o podpoře výzkumu, experimentálního vývoje a inovací,
u) Metodický návod k tvorbě jmenných rejstříků (Ministerstvo vnitra, č.j. MV-134140-1/AS-2019),
v) a další právní normy související s předmětem ESSL.

Řešení ESSL musí respektovat, v souladu s výše uvedenými legislativními normami, požadovaná technická opatření na informační systém typu ESSL a jeho budoucí interakce s ostatními informačními systémy spravujícími dokumenty (ISSD), nebo jinými elektronickými evidencemi, a to zejména: EIS JASU CZ (MÚZO Praha s r. o.); OK Base (OK System a. s.); Office 365 (CZC.CZ); IS CEDR-resorty.

Zadavatel požaduje servisní a technickou podporu ESSL v souladu s plánovaným vývojem a požadavky legislativy po celou dobu trvání smluvního vztahu na dodávku díla a poskytování služeb údržby a podpory.

Zadavatel dále stanovuje, že podmínkou je získání atestace dle § 69b - § 69e zákona č. 499/2004 Sb. nejpozději do 31. prosince 2025, přičemž proces atestace musí být zahájen (podaná žádost o atestaci systému) nejpozději do 1. července 2025, pokud nebude zákonnou úpravou stanoveno jinak.

1.2. Komponenty ESSL

Systém musí obsahovat minimálně tyto komponenty:

1.2.A. Elektronická podatelna;

1.2.B. Uživatelské prostředí zajišťující klíčové úkony dané zejména: § 63–70 zákona č. 499/2004 Sb.; vyhláškou č. 259/2012 Sb.; správním řádem č. 500/2004 Sb. a dalšími souvisejícími normami (viz výše);

1.2.C. Elektronická spisovna a skartace dokumentů;

1.2.D. Funkční rozhraní k propojení ESSL s ostatními informačními systémy Zadavatele v souladu s kapitolou 8 Národního standardu pro elektronické systémy spisové služby (zejména EIS JASU CZ (MÚZO Praha s r. o.); OK Base (OK System a. s.);

1.2.E. Automatizované zpracování dokumentů a spisů na základě definovaných atributů

1.2.F. Funkcionalitu umožňující anonymizaci dat v dokumentech;

1.2.G. Funkcionalitu umožňující autorizovanou konverzi dokumentů z moci úřední;

1.2.H. Jmenný rejstřík s propojením na základní registry – registr osob, registr obyvatel a RÚIAN;

1.3.I. Dlouhodobé důvěryhodné úložiště.

Výše uvedené součásti musí tvořit funkční a integrovaný celek.

1.2.A.1. Elektronická podatelna

Podatelna musí zajišťovat všechny úkony Zadavatele v souladu s platnou legislativou a Národním standardem, Jedná se zejména o:

a) příjem elektronického podání;
b) digitalizace analogového dokumentu a jeho export včetně metadat do jádra ESSL;
c) uložení obsahu dokumentu do ESSL a vytvoření vazby s jádrem ESSL prostřednictvím Jednotného identifikátoru a čísla jednacího;
d) předávání dokumentu na další spisové uzly nebo jednotlivé referenty a rozesílání notifikací na e-mailové adresy uživatelů u každého předání nebo přidělení dokumentu;
e) zpracování dodejek (potvrzení o doručení) a jejich provázání s odeslanými dokumenty;
f) ověřování elektronických podpisů, elektronických pečetí, elektronických časových razítek;
g) kontrola tzv. škodlivého kódu, čitelnosti dokumentu a jeho datového formátu;
h) automatické odeslání potvrzení o příjmu dokumentu podatelnou;

E-podatelna musí být schopná vypravovat jak analogové, tak elektronické dokumenty na jednu nebo více adres prostřednictvím datové schránky, emailu, klasické pošty.

1.2.A.2. Napojení na datovou schránku

Zprávy z datové schránky musí automatizovaně vstupovat přímo do e-podatelny v definovaných časových intervalech a v daném časovém rozmezí, a to spolu s metadaty. Analogický postup je nutný též u odesílaných zpráv prostřednictvím datové schránky. Musí být zajištěna možnost synchronizace manuálním spuštěním procesu.

Systém musí přijímat a ukládat zprávy z datové schránky ve formátu ZFO.

1.2.A.3. Příjem emailové pošty:

E-podatelna Zadavatele bude přijímat emailovou poštu z centrální sběrné emailové adresy, popř. dalších určených emailových adres Kanceláře AV ČR v definovaných časových intervalech a v daném časovém rozmezí. Musí být zajištěna možnost synchronizace manuálním spuštěním procesu. Odesílatel obdrží informaci o příjmu a zaevidování dokumentu podatelnou.

E-podatelna zpracuje zprávu tak, aby zůstala zachována pevná a neměnná vazba mezi tělem a přílohami.

1.2.B.1. Uživatelské rozhraní elektronického systému spisové služby

ESSL musí obsahovat následující funkcionality v souladu s Národním standardem: Administrace systému; Adresář; Příjem evidenčních záznamů, včetně připojených dokumentů z e-podatelny; Evidence dokumentů; Rozdělování a oběh dokumentů; Zpracování; Termínování; Verzování při revizích; Opravy a úpravy metadat, změny elektronických příloh; Hromadné operace; Propojování dokumentů/záznamů; Vyřízení; Správa spisů; Transakční protokol; Správa elektronické spisovny (vyhledávání, zápůjčky); Skartační řízení (vytvoření SIP balíčku); Vyhledávání dokumentů dle fulltextu nebo metadat; Filtrování dokumentů; Tisky seznamů (podacího deníku, apod.). ***1.2.B.1. Organizační struktura a počet uživatelů ESSL***

Předpokládaný maximální počet uživatelů ESSL je 100 pracovníků, kteří mohou mít více pozic nebo rolí.

1.2.B.2. Evidence a označování dokumentů v ESSL

Jednoznačný identifikátor dokumentu (JID) a čísla jednacího:

Pro účely jednoznačné identifikace dokumentu musí v ESSL existovat jedna souvislá řada pro každý kalendářní rok. Je požadováno zachování stávající struktury JID Zadavatele.

Struktura čísla jednacího je tvořena zkratkou Kanceláře AV ČR, pořadovým číslem dokumentu v daném kalendářním roce, zkratkou příslušného útvaru a označením kalendářního roku, ve kterém byl dokument zaevidován v elektronickém systému spisové služby.

1.2.B.3. Vytváření spisů

ESSL musí umožnit vytváření spisů formou sběrného archu, případně též priorací. Dále musí umožňovat vedení hybridních spisů. Součástí sběrného archu musí být spisový přehled.

1.*2.B.4. Životní cyklus dokumentů*

ESSL by měla zajistit kompletní životní cyklus včetně jejich workflow. Systém by měl umožnovat tyto stavy dokumentu:

Doručené a vlastní dokumenty: (dodaný, doručený, přijatý, vytvořený, předaný, převzatý, vrácený, ve zpracování, k připomínkování, ke schválení, schválení, vyřízený, k odeslání, k vypravení, vypravený, odeslaný, ve spisovně, převedený do výstupního formátu, připravený ke skartačnímu řízení (zařazen do SIP), archivován, skartován, anonymizován, konvertován).

V případě dokumentů odeslaných v listinné podobě prostřednictvím pošty je požadována tzv. fikce doručení, tedy že se dokument automaticky přesune do stavu Dodaný a označí se „fikcí“.

1.*2.B.5. Tvorba a vyřizování dokumentů*

ESSL musí umožnit tvorbu a vyřizování dokumentů ve smyslu Národního standardu a příslušné legislativy.

Kancelář AV ČR požaduje splnění zejména následujících funkcí:

a) vygenerování dokumentu ze šablony ESSL v napojením editorů formátu Microsoft Office (word, excel apod.);
b) automatizovaný převod do PDF/A všech typů dokumentů, tj. aby bylo zajištěno, že každý dokument před svým vyřízením bude obsahovat všechna aktuální legislativou vyžadovaná metadata a všechny komponenty dokumentu budou ve výstupních datových formátech. Ve výstupních datových formátech je nutné mít komponenty dokumentu, nebo jejich verze, které v těchto formátech musí být pro potřeby skartačního řízení;
c) připojení verifikačních prvků (elektronického podpisu, elektronické pečeti, elektronického časového razítka);
d) nastavení upozornění na nedostatky dokumentu (chybějící příloha, nepodepsaný dokument apod.);

e) zajištění automatizované urgence a eskalace termínu vyřízení dle nastavení a nastavitelné parametry;
f) filtrování a náhled na dokumenty dle termínů vyřízení;
g) převod záznamů o dokumentech a dokumenty na nástupce při změně pracovního poměru zaměstnance, zrušení role apod.;
h) zajištění zastupitelnosti a jejího nastavení (nemoc, dovolená);
i) funkce pro záznam ztráty, poškození dokumentu nebo tzv. škodlivého kódu;
j) funkce pro nastavení systému tak, aby spis a jednotlivé dokumenty v něm zařazené přejímaly skartační lhůtu podle dokumentu s nejdelší skartační lhůtou a nejvyšším skartačním znakem;
k) automatické zasílání notifikace na e-mailové adresy uživatelů o předání, nebo přidělení dokumentu ke zpracování mezi uzly a v rámci uzlu;
l) automatizovanou kontrolu všech přijímaných i odesílaných souborů antivirovým programem.

1.2.B.6: Vypravování a odesílání dokumentů

Funkci výpravny budou plnit pověřené osoby.

1.2.B.7. Skartační řízení a výběr archiválií

Proces musí odpovídat platné legislativě. Zejména je požadována funkce exportu dat do NDA nebo MÚA-DA (SIP balíček). Musí být zajištěn kompletní proces skartačního řízení – od zaslání návrhu ke skartaci, přes výběr archiválií po vyřízení procesu včetně výmazu skartovaných dokumentů.

1.2.B.8. Transakční protokol

ESSL denní obsah transakčního protokolu automaticky uloží na konci kalendářního dne v datovém formátu XML a umožní náhled a tisk v systému. Transakční protokol opatří elektronickým podpisem nebo elektronickou pečetí a časovým razítkem a uloží jej do příslušného spisu a dokument uzavře.

1.2.C. Elektronická spisovna

E-spisovna musí splnit požadavky Národního standardu a ostatních norem, které podporují a prokazují tzv. autenticitu a integritu dokumentu.

1.2.D. Rozhraní pro externí systémy

Je požadováno funkční rozhraní dle Národního standardu. Cílem této komponenty je přístup k funkcím ESSL.

Rozhraní má poskytnout též univerzální technické prostředky pro získávání dat ze systému a jeho modulů a zajistit přístup k vybraným objektům systému.
Toto rozhraní musí být součástí ceny licence.
Do doby před zajištěním povinné atestace je možné zpřístupnit alternativní funkční řešení pro systémy OKBase a MÚZO.

1.2.E. Automatizované zpracování

ESSL musí umožnovat automatizované vyřízení dokumentů a spisů na základě uživatelsky definovaných atributů, např. přidělení č.j., předání do vybraného uzlu, vložení do spisu, přidělení osoby k vyřízení dokumentu, uzavření dokumentu atd.

1.2.F. Anonymizace dokumentů

ESSL musí obsahovat nástroj pro anonymizaci dokumentu uživatelem.

1.2.G. Autorizovaná konverze dokumentů z moci úřední

1.2.G.1. ESSL musí umožňovat úplné převedení dokumentu v listinné podobě do elektronické podoby, nebo úplné převedení elektronického dokumentu do dokumentu v listinné podobě v souladu se zákonem.

1.2.G.2. ESSL musí vést evidenci konvertovaných dokumentů v souladu se zákonem

1.2.H. Jmenný rejstřík

ESSL musí umožňovat vedení jmenného rejstříku v souladu se zákonem, zejména automatizované získání bezvýznamového identifikátoru ze základních registrů a ISDS.

1.3.I. Důvěryhodné úložiště (archiv)

1.3.I.1. ESSL musí disponovat úložištěm, které zajistí platnost bezpečnostních prvků (elektronických podpisů a pečetí) souborů v něm uložených.

1.3.I.2. Požaduje se takový způsob ukládání dokumentů, který umožní dokladovat původ, pravost a neměnnost po celou dobu životního cyklu dokumentu.

1.3.I.3. Úložiště by mělo být možné integrovat s informačními systémy a úložišti jiných výrobců.

2. TECHNICKÉ, PROVOZNÍ A DALŠÍ POŽADAVKY

2.1. Rozsah užití software

ESSL bude užíván v následujícím rozsahu a počtu příslušných uživatelů:

a) rozmezí 50-100 uživatelů
b) 3 administrátoři

2.2. Rozsah zpracovávaných informací

Objem zpracovávaných dokumentů ve spisové službě je aktuálně cca 10 000 ročně.

2.3. Požadavky na způsob nasazení software

Pro účely kompletního nasazení software ESSL do provozního prostředí zadavatele je požadováno v rámci implementačních prací zajištění instalace software ESSL do následujících prostředí:

a) testovací prostředí – za účelem seznámení s funkčností základního software ESSL, školení obsluhy a správy systému, testování aktualizací a akceptačního testování,
b) produkční prostředí – za účelem ostrého provozu systému v reálném prostředí zadavatele.

Je požadováno, aby testovací prostředí bylo přístupné po celou dobu provozu produkčního (ostrého) prostředí.

2.4. Výpočetní prostředí zadavatele

Zadavatel požaduje kompatibilitu, nasazení a integraci systému dodavatele do prostředí stávající infrastruktury zadavatele:

- koncová zařízení: operační systém Windows 10 a vyšší, Microsoft Office 365+;
- servery potřebné pro chod aplikační vrstvy ESSL budou realizovány jako virtuální servery v rámci virtualizační technologie VMware;
- Databázový server bude realizován jako virtuální server (VMware, Hyper-V apod.).

Zadavatel dále požaduje, aby licence k platformě, na které budou provozovány databáze, byly součástí nabídkové ceny.

2.5. Bezpečnost

Požadujeme splnění následujících charakteristik, vlastností a parametrů bezpečnosti systému:

a. centrální správa ESSL;
b. synchronizace uživatelských profilů LDAP kompatibilního serveru do ESSL alespoň v rozsahu: jméno, příjmení, login, útvar;

c. systém přístupových práv s možností delegování na osoby, role či organizační jednotky a řešení zastupitelnosti, včetně neplánované;
d. systém přístupových práv umožní nastavení v souladu s Národním standardem omezení přístupu k dokumentům obsahujícím citlivé nebo osobní údaje pro určité role nebo skupiny;
e. využívání kvalifikovaného e-podpisu, kvalifikované e-pečetě, kvalifikovaného časového e-razítka a ověřování platnosti certifikátů;
f. podpora ověření PDF souborů, které mají e-podpis, včetně správy kořenových certifikátů;
g. možnost šifrování a anonymizace uložených dokumentů a jejich názvů;
h. zaznamenání všech pokusů o narušení systému neoprávněných přístupem do transakčního protokolu;
i. logování činnosti ESSL po dobu minimálně 6 měsíců, přístup k logům pro administrátory.

Komunikace mezi klienty a servery musí být šifrována šifrovacím algoritmem, který je obecně považován za bezpečný, důvěryhodný a není znám případ jeho prolomení.

2.6. Ostatní požadavky

a. Řešení pomocí třívrstvé architektury (klient – aplikační server – databázový server). Preferujeme řešení tenkého, ideálně webového klienta na straně uživatelů.
b. Pravidla a chování uživatelského rozhraní ESSL jsou konzistentní v celém systému.
c. Často prováděné operace (např. otevření dokumentu) musí být navrženy tak, aby mohly být provedeny malým počtem interakcí.
d. Dokumentace životního cyklu ESSL musí být zpracována formou typového spisu v souladu s Národním standardem.

3. PILOTNÍ PROVOZ A ŠKOLENÍ (administrátorů, uživatelů)

a) Pilotní provoz by měl trvat nejméně 90 kalendářních dní. Dodavatel zajistí v předstihu dostatečné zaškolení administrátorů a uživatelů ESSL. Po ukončení pilotního provozu bude Dodavatelem vytvořena zpráva o jeho průběhu. Akceptační protokol může být vyhotoven v jedné ze tří variant:
    i. Pilotní provoz ukončen s neakceptovatelnými vadami – v případě, že zadavatel nalezl vady, které brání realizaci následného plnění nebo užití ESSL. V takovém případě je Dodavatel povinen neprodleně zjištěné vady odstranit jak v testovacím, tak produkčním prostředí. Tento proces započne po vzájemné dohodě obou stran, nejpozději do 14 kalendářních dnů.

ii. Pilotní provoz ukončen s akceptovatelnými vadami – v případě, že zadavatel nalezl vady, které nebrání realizaci následného dílčího plnění nebo užití ESSL. Tyto vady je Dodavatel povinen odstranit bez zbytečného prodlení a v termínech uvedených v akceptačním protokolu.

iii. Pilotní provoz ukončen bez zjevných vad.

b) Dodavatel zajistí, zejména prvních 10 pracovních dní, přítomnost svého odborníka/odborníků v sídle zadavatele.

Požadavky mohou být upraveny Zadavatelem na základě jeho reálných potřeb. Pro účely této VZ se jedná o maximální požadavky.

4. POIMPLEMENTAČNÍ SERVISNÍ A TECHNICKÁ PODPORA

4.1. Nedílnou součástí implementace ESSL bude dokumentace o ESSL v souladu s Národním standardem, včetně předávacích a akceptačních protokolů.

4.2. V případě budoucího přechodu na jiné řešení ESSL zajistí Dodavatel patřičnou součinnost, včetně případné migrace dat.

4.3. Zadavatel požaduje, aby dodavatel zajistil také údržbu, resp. rozvoj systému v souladu s vývojem a požadavky legislativy po celou dobu trvání smluvního vztahu na dodávku díla a poskytování služeb údržby a podpory.

4.4. HELPDESK

Dodavatel zajistí, aby po dobu trvání smluvního vztahu byl k dispozici ucelený manuál pro práci s ESSL a helpdesk pro administrátory a uživatele ESSL.

4.5. Specifikace služeb SLA

PODROBNÁ SPECIFIKACE SLUŽEB SLA	
Dostupnost (v provozním čase)	99,5 % Dostupnost = ((požadovaná doba dostupnosti – suma (doby nedostupnosti podle měření) / (doba dostupnosti)) * 100
Technologická podpora	Po-Pá 8:00 – 16:00
Zadávání požadavků ServiceDesk (email, web)	7 x 24
Odezva (Response time)	Dle detailu priorit v následující tabulce
Řešení (Fix time)	Dle detailu priorit v následující tabulce
Plánovaná údržba	Mimo provozní čas, souvislá délka odstávky max. 2 hodiny – servisní okno
KATEGORIE VAD A JEJICH PRIORITIZACE	

Priorita/kategorie vady	Popis	Odezva (Response time)	Řešení do (Fix time)
1 – kritická Kategorie vady A	• Systém nefunguje vůbec nebo jeho nefunkčnost je omezena tak, že tento stav má významný dopad na klíčové procesy Zadavatele • Aplikaci nebo některou její klíčovou funkci není možné používat • Dochází k narušení uživatelských dat závažným způsobem • Dochází ke zhroucení systému jednou nebo několikrát za den	1 hod.	6 hod.
2 – vysoká Kategorie vady B	• Funkce systému je narušena tak, že dochází k významnému zpomalení výkonu klíčových procesů Zadavatele.	4 hod.	8 hod.
3 – střední Kategorie vady C	• Funkce systému je omezena, ale toto omezení má minimální vliv na zpracování klíčových procesů Zadavatele • Závada narušuje, avšak neznemožňuje využití systému • Blokuje dokončení určitých úkolů, které nejsou časově kritické • Působí dílčí závadu nebo nepohodlí uživatele • Procesní závada (vyřeší se změnou procesu) Tuto závadu lze jiným náhradním dočasným způsobem (např. ruční úpravou dat) nebo dočasnou změnou pracovního postupu obejít (workround). Uživatel však musí vykonat vícepráce na	8 hod.	24 hod.

4 – nízká Kategorie vady D	• Systém je funkční. Závada způsobuje jen minimální obtíže při jeho používání. Jde o situace, kdy: o vznikne malý problém nebo nepohodlí obsluhy o kosmetická chyba ve vizuálním rozhraní (chybné popisy, řazení dat, překreslování) • Uživatel nemusí vykonat vícepráce na obejití závady. Způsobuje mu nepohodlí při práci (např. pohyb myší navíc, klik myší navíc, stisk několika kláves navíc atp.).	8 hod.	120 hod.

5. DOKUMENTACE

5.1. Zadavatel požaduje kompletní dokumentaci ESSL v souladu s Národním standardem (typový spis) a zákonem o informačních systémech veřejné správy. Dokumentace bude průběžně aktualizována v případě provedení změn v ESSL znamenajících změnu postupů, funkcionalit systému atd, nejpozději však k okamžiku nasazení takové změny do ostrého provozu.

5.2. Zadavatel požaduje dokumentaci k implementaci ESSL (harmonogram, požadavky na součinnost Dodavatele se Zadavatelem, komunikační matice atd.) v prostředí Zadavatele.

5.3. Uživatelská dokumentace

Uživatelská dokumentace bude obsahovat popis veškerých funkcí aplikace. Dokumentace bude členěna dle jednotlivých modulů a uživatelských rolí.

Součástí dokumentace bude kontextová nápověda integrovaná v řešení.

5.4. Administrátorská dokumentace

Dokumentace bude obsahovat:

- popis architektury aplikace,
- administrátorské funkce,
- postup instalace,
- postup konfigurace systémových souborů,
- a další informace určené pro systémové administrátory.

5.5. Bezpečnostní dokumentace

Bezpečnostní dokumentace bude obsahovat veškeré informace týkající se provozní bezpečnosti a kybernetické bezpečnosti, zejména:

- plán zálohování a obnovy,
- popis aplikačních logů, jejich ochrany a vytěžování,
- další relevantní informace dle Prováděcího projektu.

5.6. Dokumentace vývojáře

Dokumentace pro vývojáře bude obsahovat dokumentaci API, popis veškerých použitých knihoven, frameworků a dalších komponent, které jsou nutné pro integraci, a rozvoj služeb třetích stran.

6. DALŠÍ POŽADAVKY

6.1. Dodavatel bere na vědomí požadavky vyplývající ze ZZVZ, GDPR, ZoKB, ZoISVS a souvisejících předpisů. Zejména se jedná o:

- Povinnost řídit se těmi právními předpisy a souvisejícími vnitřními předpisy Zadavatele.
- Povinnost poučit a zaškolit všechny svoje pracovníky přidělené na projekt v rozsahu odpovídajícím interním školením Zadavatele – bezpečnost práce, kybernetická bezpečnost, ochrana osobních údajů a jiné relevantní.
- Povinnost hlásit případné zjištěné události a incidenty, bezpečnostní události a incidenty a porušení ochrany osobních údajů, včetně neprodlené přípravy podkladů k incidentům a povinnosti spolupracovat na vyšetření a vyřešení těchto incidentů.
- Povinnost spolupracovat s kontrolními orgány Zadavatele a veřejné správy v případně jejich žádosti.