Dodatek č. 3
ke Smlouvě o poskytování služeb provozu a rozvoje informačního systému datových schránek na období 2023–2027

ev. č. provozovatele: 2022/06151
ev. č. správce: MV-196653-30/EG-2020

Česká pošta, s.p.

se sídlem:	Politických vězňů 909/4, 225 99, Praha 1
IČO:	47114983
DIČ:	CZ47114983
zastoupen:	Ing. Miroslavem Štěpánem, generálním ředitelem České pošty, s.p. a Mgr. Vlastimilem Hallou, MBA, ředitelem úseku generálního ředitele
zapsán v obchodním rejstříku	Městského soudu v Praze, oddíl A, vložka 7565
bankovní spojení:	Československá obchodní banka, a.s.,
	č. ú.: 102639446/0300

dále jen „**Provozovatel**“

a

Česká republika – Digitální a informační agentura

se sídlem:	Na vápence 915/14, Žižkov, 130 00 Praha 3
IČO:	17651921
zastoupena:	Ing. Martinem Mesršmídem, ředitelem
bankovní spojení:	Česká národní banka
	č. ú.: 6326001/0710

dále jen „**Správce**“

dále jednotlivě jako „**smluvní strana**“, nebo společně jako „**smluvní strany**“ uzavírají tento Dodatek č. 3 (dále jen „**Dodatek**“) ke Smlouvě o poskytování služeb provozu a rozvoje informačního systému datových schránek na období 2023–2027 ze dne 23. 12. 2022 ve znění dodatku č. 1 ze dne 13. 10. 2024 a dodatku č. 2 ze dne 26. 3. 2025 (dále jen „**Smlouva**“).

1. Předmět Dodatku

1.1 Předmětem tohoto Dodatku je dohoda smluvních stran na úpravě znění Přílohy č. 1 (Požadavky kladené na ISDS) Smlouvy (dále jen „Příloha č. 1“).

2. Změna Smlouvy

2.1 Smluvní strany se dohodly, že se stávající znění Přílohy č. 1 Smlouvy ruší a nahrazuje novým zněním, uvedeným v Příloze č. 1 tohoto Dodatku.

3. Závěrečná ustanovení

3.1 Ostatní ustanovení Smlouvy tímto Dodatkem nedotčená zůstávají beze změny.

3.2 Smluvní strany berou na vědomí, že tento Dodatek bude uveřejněn v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále jen „**ZRS**“). Dle dohody Smluvních stran zajistí odeslání tohoto Dodatku správci registru smluv Správce. Správce je oprávněn před odesláním Dodatku správci registru smluv v Dodatku znečitelnit informace, na něž se nevztahuje uveřejňovaní povinnost podle ZRS.

3.3 Tento Dodatek nabývá platnosti dnem jeho podpisu oběma Smluvními stranami a účinnosti dne **19. září 2025**.

3.4 Tento Dodatek je vyhotoven elektronicky.

3.5 Smluvní strany prohlašují, že tento Dodatek je projevem jejich pravé, skutečné a svobodné vůle. Na důkaz toho připojují Smluvní strany níže své podpisy.

3.6 Nedílnou součástí tohoto Dodatku jsou následující přílohy:

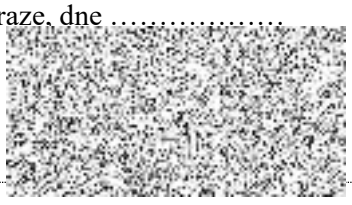
Příloha č. 1	Požadavky kladené na ISDS (nová Příloha č. 1 Smlouvy)

Za Provozovatele:

V Praze, dne ……

Za Správce:

V Praze, dne ……



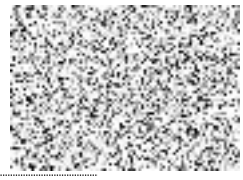
Mgr. Vlastimil Halla, MBA
ředitel úseku generálního ředitele

Česká pošta, s.p.

Ing. Martin Mesršmíd
ředitel

Česká republika – Digitální a informační agentura

V Praze, dne ……



Ing. Miroslav Štěpán

generální ředitel

Česká pošta, s.p.

Požadavky kladené na systém ISDS

1 Obsah

2 Rámcové vymezení požadovaných Služeb a Dodávek

Požadavky vycházejí ze stávajícího stavu a jsou specifikovány zejména:

- Provozními příručkami ISDS (funkčním designem ISDS a architekturou aplikace),
- Provozním řádem ISDS,
- Další Dokumentací, na kterou odkazuje Smlouva o zajištění provozu a rozvoje ISDS (dále jen „Smlouva“) a jejích Příloh,
- Legislativním rámcem uvedeným v kap. 3. této Přílohy.

3 Legislativní rámec – Dotčené právní předpisy

V této části jsou uvedeny právní předpisy a navazující právní akty vztahující se k ISDS, provozu ISDS a požadavkům kladeným na ISDS, které musí ISDS splňovat, a to vždy ve znění pozdějších změn.

3.1 Právní předpisy vztahující se k ISDS:

- Zákon č.110/2019 Sb., o zpracování osobních údajů („ZOOU“)
- Zákon č.111/2009 Sb., o základních registrech
- Zákon č. 297/2016 Sb., o službách vytvářející důvěru pro elektronické transakce
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě
- Zákon č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací a o změně zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů
- Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek
- Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
- Usnesení vlády ze dne 25. 05. 2015 – určení prvků kritické informační infrastruktury (KII)
- Usnesení vlády ČR č. 675 ze dne 26. července 2021 Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025
- Usnesení vlády České republiky č. 390 ze dne 25. května 2015 ke 2. aktualizaci Seznamu prvků kritické infrastruktury, jejichž provozovatelem je organizační složka státu
- Usnesení vlády ČR č. 981-2015 3. aktualizace seznamu KI
- Usnesení vlády ČR č. 889/2015 z 02. 11. 2015 k dalšímu rozvoji informačních a komunikačních technologií služeb veřejné správy
- Nařízení vlády č. 315/2014 Sb., kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určování prvku kritické infrastruktury;
- Nařízení Vlády č. 594/2006 Sb., o přepisu znaků do podoby, ve které se zobrazují v informačních systémech veřejné správy

3.2 Evropské směrnice a Nařízení:

- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářející důvěru pro elektronické transakce na vnitřním trhu
- Směrnice Evropského parlamentu a Rady č. 2016/2102 o přístupnosti webových stránek a mobilních aplikací subjektů veřejného sektoru
- Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů, „GDPR“)

4 Funkční zadání

V případě, že tato kapitola obsahuje i funkční požadavky, které vychází z legislativy, ale příslušný právní předpis dosud nenabyl účinnosti, je Provozovatel povinen zprovoznit v rámci Služeb Rozvoje dotčené funkční požadavky dle Harmonogramu realizace požadavku na Služby rozvoje ISDS. Realizace těchto funkcionalit bude hrazena z Ceny Služeb rozvoje ISDS. Pokud by s ohledem na budoucí změny právní úpravy nebylo možné zajistit soulad ISDS s budoucí právní úpravou prostřednictvím realizace Sužeb Rozvoje, zajistí smluvní strany soulad ISDS s takovou budoucí právní úpravou pomocí uzavření dodatku Smlouvy

4.1 Funkční požadavky na provoz ISDS

Funkční požadavky na provoz ISDS jsou dány mimo níže uvedeného také Provozním řádem ISDS a Provozními příručkami ISDS – Funkčním designem. V případě rozporu mezi jednotlivými dokumenty má přednost Funkční design.

	Činnosti	Zajišťuje	
		Správce	Provozovatel
I	**INTEGRACE SE ZÁKLADNÍMI REGISTRY A DALŠÍMI INFORMAČNÍMI SYSTÉMY VEŘEJNÉ SPRÁVY (ISVS)**		
1	**Údržba a provoz rozhraní pro komunikaci s Informačním systémem základních registrů (ISZR)**		
	Komunikace s ISZR	Zajistí potřebná oprávnění pro Provozovatele	Zajistí komunikaci prostřednictvím komunikačního rozhraní ISDS s ISZR. Zajistí vedení logu ISZR požadavků.
	Údržba rozhraní s ISZR		Zajistí implementaci změn komunikačního rozhraní ISDS s ISZR
2	**Komunikace s registrem obyvatel (ROB)**		
	Získání a ukládání AIFO (Agendový identifikátor fyzické osoby) ROB		V procesu zakládání uživatele ISDS zajistí získání AIFO ROB, pokud bude uživatel ztotožněn vůči ROB a pokud AIFO není již obsaženo v datech, které způsobují založení nebo změnu DS (notifikace z ROS).

	Činnosti	Zajišťuje	
		Správce	Provozovatel
			Zajistí ukládání AIFO ROB v ISDS pro ztotožněné uživatele ISDS.
	Identifikátor datové schránky (DS) FO v ROB		Zajistí zápis nebo vymazání identifikátoru DS FO (fyzické osoby) v ROB (Registr obyvatel) kdykoliv je DS FO zpřístupněna nebo znepřístupněna
	Načítání notifikačních souborů ROB		Zajistí načítání notifikačních souborů ROB
	Automatická synchronizace dat s ROB		Zajistí zpracování notifikačních souborů ROB a automatickou synchronizaci dat ISDS s ROB po notifikaci změn (Změny dat uživatelů ISDS, znepřístupňování DS FO).
	Manuální ztotožnění a synchronizace dat uživatelů a DS FO s ROB	Zadává v servisním modulu požadavky	Zajistí ztotožnění uživatelů a synchronizaci dat uživatelů a DS po přijetí požadavků ze servisního modulu, případně z klientského portálu ISDS po zadání čísla dokladu totožnosti.
	Ztotožňování při změnách údajů		Zajistí vyhledávání a ztotožňování osob v ROB při změnách jména, příjmení, data narození nebo adresy osoby vedené v ISDS pro definované osoby bez AIFO ROB
3	**Komunikace s registrem osob (ROS)**		
	Načítání notifikačních souborů ROS		Zajistí načítání notifikačních souborů ROS
	Iniciace zřizování, znepřístupňování a změn popisu DS na základě údajů z notifikací ROS		Zajistí zpracování notifikačních souborů ROS, automatické zakládání DS určených právních forem OVM (Orgán veřejné moci) a PO (dle příslušných ustanovení ZEU), znepřístupňování a změny popisu DS. Při určených změnách údajů zajistí zneplatňování přístupových údajů a příp. i generování dat pro odeslání nových přístupových údajů uživatelů DS.
	Identifikátor DS v ROS		Zajistí zápis nebo vymazání identifikátoru DS v ROS kdykoliv je DS zpřístupněna nebo znepřístupněna

	Činnosti	Zajišťuje	
		Správce	**Provozovatel**
	Manuální synchronizace dat DS s ROS	Zadává v servisním modulu požadavky	Zajistí synchronizaci dat DS po přijetí požadavků na synchronizaci s ROS ze servisního modulu
	Kukátko do ROS		Zajistí v servisním modulu možnost porovnání dat ROS a ISDS pro IČO náležející k DS
4	**Komunikace s registrem územní identifikace (RUIAN)**		
	Získávání adres z RUIAN		Zajistí pro osoby vedené v ROS získávání adres explicitním dotazem na RUIAN s identifikátorem adresního místa přečteným z ROS.
5	**Komunikace s registrem práv a povinností (RPP)**		
	Vkládání záznamu do RPP		Zajistí vkládání záznamu do RPP při každém zápisu nebo vymazání identifikátoru DS do nebo z ROB nebo ROS.
6	**Komunikace s dalšími systémy a subjekty**		
	Rozhraní na centrálu Czech POINT	Zajistí potřebná oprávnění pro Provozovatele	Vytvoří a bude provozovat rozhraní na centrálu Czech POINT pro předávání dat žádostí jednotlivých agend ISDS na kontaktních místech Czech POINT. Zajistí přebírání těchto dat do ISDS.
	Připojení do Centrálního Místa Služeb (CMS) pro čerpání služeb	Správce zajistí potřebnou součinnost správce CMS	Zajistí potřebné datové propojení ISDS do CMS a nastavení pro konzumaci aplikačních služeb z CMS: ISEO, ISZR, TSA1, TSA3, případně dalších dle požadavků správce ISDS.
	Připojení do Centrálního Místa Služeb (CMS) pro publikaci služeb ISDS	Správce zajistí publikaci služeb ISDS v CMS	Zajistí potřebné potřebnou součinnost pro publikaci služeb ISDS v CMS
	Rozhraní na subjekty s povinností informovat (dle příslušných ustanovení ZEU)	Zajistí součinnost dotyčných subjektů	Vytvoří a bude provozovat rozhraní na subjekty s povinností informovat dle příslušných ustanovení ZEU) pro předávání dat, která nelze předávat prostřednictvím základních registrů. Zajistí přebírání těchto dat do ISDS.

	Činnosti	Zajišťuje	
		Správce	**Provozovatel**
	Rozhraní na ISEO (Informační systém evidence obyvatel)	Zajistí potřebná oprávnění pro Provozovatele	Vytvoří a bude provozovat rozhraní na ISEO pro předávání dat, která nelze předávat prostřednictvím základních registrů. Zajistí přebírání těchto dat do ISDS.
	Komunikace ISDS a ISEO	Zajistí podmínky k využívání této služby	Zajistí funkcionalitu, kdy na zásah uživatele (pracovníci Správce v servisním modulu) se správným pověřením bude umožněna aktualizace osobních údajů majitele Datové schránky vůči ISEO.
	Rozhraní na SOVM (aplikace Seznam OVM), aktualizace dat schránek OVM (u kterých je editorem SOVM)	Zajistí potřebná oprávnění pro Provozovatele	Vytvoří a bude provozovat rozhraní na SOVM pro předávání dat, která nelze předávat prostřednictvím základních registrů. Zajistí přebírání těchto dat do ISDS a aktualizace dat v ISDS.
	Komunikace s ROVM (rejstříkem OVM, součást RPP)	Zajistí potřebná oprávnění pro Provozovatele	Zajistí načítání notifikačních souborů ROVM a jejich zpracování.
	Iniciace zřizování, znepřístupňování a změn popisu DS na základě údajů z notifikací ROVM		Zajistí zpracování notifikačních souborů ROVM, automatické zakládání DS určených právních forem OVM (dle příslušných ustanovení ZEU), znepřístupňování a změny popisu DS. Při určených změnách údajů zajistí zneplatňování přístupových údajů a příp. i generování dat pro odeslání nových přístupových údajů uživatelů DS.
II	**ZŘÍZENÍ, ZNEPŘÍSTUPNĚNÍ, ZRUŠENÍ DS**		
1	**Zřízení DS OVM (běžné) § 6 odst. 1**		
	Získání dat o nově založených OVM		Zajistí zpracování notifikací ROS a ROVM, příp. obdobných elektronicky přístupných evidencí, získání potřebných dat pro založení nových schránek v ISDS.
	Žádost o založení DS		Vygenerování žádosti o zřízení DS

	Činnosti	Zajišťuje	
		Správce	Provozovatel
	Vytvoření DS		ISDS online zpracuje požadavek na vytvoření DS, založí DS, založí přístupové účty a vygeneruje přístupové údaje primárním oprávněným osobám
2	**Zřízení DS právnické osoby (PO) (běžné) § 5 odst. 1.**		
	Získání dat o nově založených PO		Zajistí zpracování notifikací ROS, příp. obdobných elektronicky přístupných evidencí, získání potřebných dat pro založení nových schránek v ISDS.
	Žádost o založení DS		Vygenerování žádosti o zřízení DS
	Vytvoření DS		ISDS online zpracuje požadavek na vytvoření DS, založí DS, založí přístupové účty a vygeneruje přístupové údaje primárním oprávněným osobám
3	**Zřízení DS podnikající fyzické osoby (PFO) advokáta, daň. poradce atd. (běžné)**		
	Získání dat o nově vzniklých subjektech advokátů, daňových poradců a insolvenčních správců, statutárních auditorů, znalců, soudních tlumočníků a soudních překladatelů (dle příslušných ustanovení ZEU)		Zajistí zpracování notifikací ROS, příp. obdobných elektronicky přístupných evidencí, získání potřebných dat pro založení nových schránek v ISDS.
	Žádost o založení DS		Vygenerování žádosti o zřízení DS
	Vytvoření DS		ISDS online zpracuje požadavek na vytvoření DS, založí DS, založí přístupové účty a vygeneruje přístupové údaje primárním oprávněným osobám
4	**Zřízení DS PFO**		

	Činnosti	Zajišťuje	
		Správce	**Provozovatel**
	Příjem žádosti PFO, nebo (dle příslušných ustanovení ZEU) získání dat z notifikací ROS	Zajistí vstupní kanály pro příjem žádosti	
	Předání ke zpracování do systému ISDS	Zajistí vstupní kanály pro příjem žádosti	Zajistí příslušnou funkcionalitu v servisním modulu nebo po úspěšné autentizaci přes NIA (dle příslušných ustanovení ZEU), zajistí komunikační rozhraní pro přebírání dat. Zajistí zpracování notifikací ROS a generování žádostí o zřízení DS
	Kontrola dat v žádosti		Zajistí rozhraní do ROB, ROS, ISEO či do obdobné elektronicky vedené přístupné evidence, pro kontrolu údajů v žádosti, případně pro jejich doplnění
	Kontrola na existenci DS		ISDS, provede kontrolu
	Vytvoření identifikátoru		Přidělí systém ISDS
	Vytvoření DS		ISDS online zpracuje požadavek na vytvoření DS, založí DS, založí přístupové účty a vygeneruje přístupové údaje primárním oprávněným osobám
	Ukládání žádosti PFO	Zajistí vstupní kanály pro příjem žádosti	ISDS zajistí archivaci příslušných záznamů
5	**Zřízení DS fyzické osoby (FO)**		
	Příjem žádosti FO	Zajistí vstupní kanály pro příjem žádosti	Zajistí potřebné funkcionality pro příjem žádostí a dále potřebná komunikační rozhraní
	Předání ke zpracování do systému ISDS	Zajistí vstupní kanály pro příjem žádosti	Zajistí příslušnou funkcionalitu v servisním modulu nebo určeným uživatelům schránek přistupujícím pomocí kvalifikovaného prostředku, dle příslušných ustanovení ZEU

	Činnosti	Zajišťuje	
		Správce	Provozovatel
	Kontrola dat v žádosti		Zajistí rozhraní do ROB, ISEO či do obdobné el. vedené přístupné evidence, pro kontrolu údajů v žádosti, případně pro jejich doplnění
	Kontrola na existenci DS		ISDS, provede kontrolu
	Vytvoření identifikátoru		Přidělí systém ISDS
	Vytvoření DS		ISDS online zpracuje požadavek na vytvoření DS, založí DS, založí přístupové účty a vygeneruje přístupové údaje primárním oprávněným osobám
	Ukládání žádosti FO	Zajistí vstupní kanály pro příjem žádosti	ISDS zajistí archivaci příslušných záznamů
6	**Zřízení DS PO na žádost (§ 5 odst. 2.) a DS OVM na žádost (§ 6 odst. 2.)**		
	Příjem žádosti PO, OVM	Zajistí vstupní kanály pro příjem žádosti	Zajistí příslušnou funkcionalitu v servisním modulu a komunikační rozhraní
	Předání ke zpracování do systému ISDS	Zajistí vstupní kanály pro příjem žádosti	Zajistí příslušnou funkcionalitu v servisním modulu
	Kontrola dat ve formuláři		Zajistí rozhraní do ROB, ROS či do obdobné el. vedené přístupné evidence, pro kontrolu údajů v žádosti, případně pro jejich doplnění
	Kontrola na existenci DS		ISDS, provede kontrolu
	Vytvoření identifikátoru		Přidělí systém ISDS
	Vytvoření DS		ISDS online zpracuje požadavek na vytvoření DS, založí DS, založí přístupové účty a vygeneruje přístupové údaje primárním oprávněným osobám
	Ukládání žádosti PO, OVM	Zajistí vstupní kanály pro příjem žádosti	ISDS zajistí archivaci příslušných záznamů

	Činnosti	Zajišťuje	
		Správce	**Provozovatel**
7	**Znepřístupnění a opětovné zpřístupnění DS FO, PFO na žádost**		
	Příjem žádosti, oznámení	Zajistí vstupní kanály pro příjem žádosti	ISDS zajistí rozhraní a funkcionality pro příjem žádostí
	Kontrola dat		ISDS (funkcionalita servisního modulu a dále dle příslušného ustanovení ZEU ISDS umožní podat žádost určeným uživatelům schránek přistupujícím pomocí kvalifikovaného prostředku předá informace podstatné pro operaci znepřístupnění či opětovného zpřístupnění
	Zpracování žádosti		ISDS online zpracuje požadavek na znepřístupnění či zpřístupnění DS
	Oznámení o znepřístupnění DS dotčeným subjektům		ISDS prostřednictvím určeného rozhraní zašle zprávu o znepřístupnění či opětovném zpřístupnění
	Ukládání		ISDS zajistí archivaci příslušných záznamů
8	**Znepřístupnění a opětovné zpřístupnění DS PO na žádost (§ 5 odst. 2.) a DS OVM na žádost (§ 6 odst. 2.)**		
	Příjem žádosti, oznámení	Zajistí vstupní kanály pro příjem žádosti	
	Kontrola dat		ISDS (funkcionalita servisního modulu) - předá informace podstatné pro operaci znepřístupnění či opětovného zpřístupnění
	Rozhodnutí o znepřístupnění	Zadání žádosti prostřednictvím rozhraní servisního modulu	ISDS online zpracuje požadavek na znepřístupnění či zpřístupnění DS
	Oznámení o znepřístupnění DS dotčeným subjektům		ISDS prostřednictvím určeného rozhraní zašle zprávu o znepřístupnění či opětovném zpřístupnění
	Ukládání		ISDS zajistí archivaci příslušných záznamů

	Činnosti	Zajišťuje	
		Správce	Provozovatel
9	**Znepřístupnění DS PO a OVM (zřízených dle § 5 odst. 1. a § 6 odst. 1.)**		
	Získání dat o Datových schránkách PO a OVM pro znepřístupnění		Zajistí zpracování notifikací ROS, příp. obdobných elektronicky přístupných evidencí, získání potřebných dat pro znepřístupnění schránek PO nebo OVM v ISDS.
	Znepřístupnění		ISDS provede znepřístupnění DS automaticky ve stanovené lhůtě
	Oznámení o znepřístupnění DS dotčeným subjektům		ISDS prostřednictvím určeného rozhraní zašle zprávu o znepřístupnění
	Ukládání		ISDS zajistí archivaci příslušných záznamů
10	**Zrušení DS FO, PFO**		
	Zrušení DS		ISDS provede automaticky ve stanovené lhůtě 3 let po znepřístupnění, dle příslušných ustanovení ZEU
	Likvidace dat – obsah Datové schránky		ISDS zajistí automaticky (výmaz obsahu Datových zpráv, logy zůstávají)
11	**Zrušení DS PO**		
	Zrušení DS		ISDS provede automaticky ve stanovené lhůtě
	Likvidace dat – obsah Datové schránky		ISDS zajistí automaticky (výmaz obsahu Datových zpráv, logy zůstávají)
12	**Zrušení DS OVM**		
	Zrušení DS		ISDS provede automaticky ve stanovené lhůtě

	Činnosti	Zajišťuje	
		Správce	Provozovatel
	Likvidace dat – obsah Datové schránky		ISDS zajistí automaticky (výmaz obsahu Datových zpráv, logy zůstávají)
III	**SPRÁVA PŘÍSTUPU K DS**		
1	**Definice postupu přihlašování**		
	Náležitosti přístupových údajů a elektronické prostředky k přihlášení. Technické podmínky a bezpečnostní zásady přístupu do DS	Vydává a upravuje vyhlášku dle zmocnění v příslušných ustanoveních ZEU	Zpracovává technické podklady pro přípravu vyhlášky
2	**Generování nových přístupových údajů**		
	Při zřízení DS – dle příslušných ustanovení ZEU		ISDS zajistí generování přístupových údajů nebo přístupových účtů (automatický proces při zřízení DS, nebo na základě žádosti)
	Při oznámení dle příslušných ustanovení ZEU	Pro určené právní formy OVM zajišťuje aktualizace dat v SOVM	ISDS zajistí generování přístupových údajů (automatický proces při zpracování notifikací z ROS, ROVM, příp. předání dat z SOVM)
	Při zmocnění pověřených osob – dle příslušných ustanovení ZEU	Zajistí vstupní kanály pro příjem žádosti	ISDS zajistí generování přístupových údajů (na základě přijaté žádosti prostřednictvím servisního modulu). ISDS přijme žádost o zřízení přístupu.
	Ukládání žádostí		ISDS zajistí archivaci příslušných záznamů
	Zavedení účtu osoby do systému		ISDS zavede účet osoby do systému, generuje přístupové údaje a pokud mají být předány, zajistí jejich předání buď formou pro tisk, nebo zasláním elektronické výzvy a využitím virtuální obálky

	Činnosti	Zajišťuje	
		Správce	**Provozovatel**
	Oznámení o zavedení další osoby		Datová zpráva do vlastních rukou
3	**Zneplatňování přístupových údajů**		
	Při změně – dle příslušných ustanovení ZEU	Zajistí vstupní kanály pro příjem žádosti	ISDS zajistí zneplatňování přístupových údajů (automatický proces při zpracování notifikací z ROS, ROVM, příp. předání dat z SOVM). ISDS zajistí zneplatňování přístupových údajů (na základě přijaté žádosti prostřednictvím servisního modulu)
4	**Zneplatnění přístupových údajů a vydání nových**		
	Při ztrátě, odcizení atp. – dle příslušných ustanovení ZEU	Zajistí vstupní kanály pro příjem žádosti	ISDS zajistí proces zneplatňování přístupových údajů a vydání nových (buď na základě přijaté žádosti dle příslušných právních předpisů, nebo prostřednictvím servisního modulu).
	Ztotožnění s osobou vedenou v systému		ISDS (funkcionalita servisního modulu) - zpracuje žádost, ověří údaje a oprávnění osoby
	Kontrola na opětovné vydání PÚ		ISDS (funkcionalita servisního modulu) zjistí interval od předchozího vydání přístupových údajů a vrátí odpověď pro určení, jestli má být vybírán správní poplatek
	Výběr správního poplatku	Správce, kontaktní místo Czech POINT	Po příslušné změně ZEU ISDS umožní výběr správního poplatku
	Zneplatnění starých, vydání nových přístupových údajů		ISDS zajistí zneplatnění starých, generuje nové přístupové údaje a předá je pro tisk, zásilka do vlastních rukou, příp. „virtuální obálka“, nebo zobrazí na obrazovku, pokud jde o přístup pomocí kvalifikovaného prostředku
5	**Předávání údajů pro tisk obálek s přístupovými údaji a dalšími informacemi**		
	Generování údajů pro tisk	Správce určuje typy a pořadí priorit výběru adres pro odesílání obálek s přístupovými údaji a dalšími informacemi. Změny priorit na	ISDS zajistí generování údajů pro tisk obálek s přístupovými údaji a dalšími informacemi, ve struktuře dat dle dokumentu Funkční design.

	Činnosti	Zajišťuje	
		Správce	**Provozovatel**
		základě realizace změnových požadavků. Schvaluje dokumenty procesů pro odesílání obálek s přístupovými údaji (Typy a texty PÚ)	Adresy pro obálky jsou předávány v souladu se Správcem schválenými typy a pořadím priorit výběru adres. ISDS udržuje aktualizované číselníky států a potřebných poskytovaných poštovních služeb, určuje typy obálek k odeslání dle dokumentu schválených procesů pro odesílání obálek s přístupovými údaji (Typy a texty PÚ)
	Předání údajů		ISDS v dohodnutých termínech předá přístupové údaje pro tisk do externího systému hybridní pošty.
	Řazení zásilek s PÚ		Zajistí u zásilek systémem ISDS rozpoznaných jako zásilky do zahraničí a zásilky automaticky rozpoznané jako problémové (např. chybí nebo neznámé PSČ nebo je nestrukturovaná adresa) řazení do speciální fronty zásilek, která bude předávána systému hybridní pošty 1x týdně v samostatné dávce.
IV	**DISTRIBUCE PŘÍSTUPOVÝCH ÚDAJŮ NEBO INFORMACÍ KE ZMĚNÁM PŘÍSTUPOVÝCH ÚČTŮ**		
1	**Hybridní pošta**		
	Převzetí dat připravených pro tisk		Zajistí technický import dat, připravených pro výrobu obálek a tisk, do systému hybridní pošty
	Služba Hybridní pošta		Zajistí službu Hybridní pošta v souladu s definovaným SLA, zejména: tisk obálek s přístupovými údaji a dalšími informacemi (v souladu s aktuálními číselníky států a potřebných poskytovaných poštovních služeb a určenými typy obálek k odeslání dle dokumentu schválených procesů pro odesílání obálek s přístupovými údaji – Typy a texty PÚ), jejich kompletace a výprava do poštovní přepravní sítě.
	Vyhodnocení stavu doručení zásilek		Zajistí vyhodnocování stavu doručení zásilek, tvorbu elektronických sestav s daty stavu doručení zásilek
	Poskytování informací o stavu doručení zásilky		Zajistí načítání souborů s informacemi o stavu doručení zásilek a zpřístupnění informací v servisním modulu

	Činnosti	Zajišťuje	
		Správce	**Provozovatel**
	Archivace doručenek a vrácených dopisů	Schvaluje dokumenty procesů předávání doručenek a vrácených dopisů k archivaci	Zajistí předávání doručenek a vrácených dopisů k archivaci dle dokumentu schválených procesů
2	**Virtuální obálky**		
	Vydání přístupových údajů elektronickým způsobem		Zajistí možnost vydávání nových přístupových údajů formou tzv. „virtuální obálky“ pro osobně podávané žádosti na kontaktním místě Czech POINT – přístupové heslo pro první přihlášení do systému, resp. přístupové heslo při znovu vydávání přístupových údajů. Součástí rozhraní pro aktivační portál (potřebný pro získání přístupových údajů virtuální obálky uživatelem) bude i zpětná vazba do systému ISDS, která bude zaznamenávat informace o „doručení“ přístupových údajů formou virtuální obálky.
	Zobrazení informací o virtuální obálce		Zajistí, aby v rámci servisního modulu byly zobrazeny informace o tom, že přístupové údaje k příslušné Datové schránce byly odeslány na emailovou adresu a o jakou e-mailovou adresu se jedná (identifikace).
	Napojení na aktivační portál Czech POINT		Zajišťuje napojení na aktivační portál pro předávání přístupových údajů formou virtuálních obálek.
3	**Zobrazení Přístupových údajů na obrazovku**		
	Zobrazení Přístupových údajů na obrazovku		Zajistí zobrazení přístupových údajů na obrazovku pro přístup uživatele pomocí kvalifikovaného prostředku, dle příslušných ustanovení ZEU
V	**PROVOZ DS**		
1	**Přístup k DS (portál ISDS, webové služby ISDS)**		
	Přístup k Datové schránce		ISDS umožní přístup prostřednictvím portálu po úspěšném přihlášení do systému ISDS. ISDS umožní přístup prostřednictvím specifického rozhraní (webové služby) po úspěšném přihlášení do systému ISDS.

	Činnosti	Zajišťuje	
		Správce	**Provozovatel**
	Přístup do znepřístupněné Datové schránky		Zajistí uživatelům možnost přístupu do znepřístupněné Datové schránky v režimu „read-only“. T.j. mohou si přečíst a stáhnout doručené zprávy, ale do Datové schránky již nemůže být dodáváno ani nelze zprávy odesílat.
1a	Přepínání schránek v klientském portálu		
	Přepínání schránek v klientském portálu		V případě, že je uživatel přihlášen pomocí Identity občana nebo Mobilního klíče, bude mít možnost v klientském portálu spustit proces přehlášení do jiné schránky (pod jiným svým uživatelským účtem), do které by se v rámci tohoto způsobu přihlášení mohl přímo přihlásit (tj. do schránky, kterou mu při přihlašování nabízí ve výběru předsíň).
2	**Přijetí zprávy**		
	Přijetí Datové zprávy		ISDS zajistí přijetí zprávy systémem a vyrozumění vlastníka DS o dodání určeným způsobem, dle nastavení notifikací u DS.
3	**Náhled Datové zprávy**		
	Funkce "Náhled" Datové zprávy		Zajistí v rámci klientského portálu pro uživatele DS funkci „Náhled“, která dovolí otevřít kompletní obálku Datové zprávy a zpřístupní přílohy obsažené v Datové zprávě. Požadované operace se zprávou: tisk obálky, odeslání ke konverzi; požadované operace s přílohami: stažení jednotlivě, stažení najednou v ZIP, odeslání ke konverzi.
3a	**Náhled vybraných typů příloh v klientském portálu**		
	Náhled vybraných typů příloh v klientském portálu		Zajistí v rámci klientského portálu pro uživatele DS funkci náhled pro následující typy příloh: • PDF, JPG a PNG • HTML – jen pro zprávy ze systémových schránek Správce a Provozovatele • ZFO – podrobněji v kap. 3b níže

	Činnosti	Zajišťuje	
		Správce	**Provozovatel**
	Varovný dialog o možné nepřesnosti náhledu	Definuje text varování o možné nepřesnosti náhledu	Zajistí zobrazování varování uživateli o možné nepřesnosti náhledu.
	Možnost konfiguračního zablokování náhledů		Zajistí novou konfigurační položku klientského portálu pro zablokování funkce náhledů pro určené typy příloh.
3b	**Náhled ZFO přílohy v klientském portálu**		
	Náhled ZFO přílohy v klientském portálu		Zajistí pro přihlášené uživatele DS funkci Náhled ZFO přílohy přímo v klientském portálu. V zobrazení náhledu ZFO bude povolen náhled podporovaných typů příloh.
	Práce s neplatnými soubory v náhledu		Klientský portál zajistí u přílohy typu ZFO, kterou není možné interpretovat jako platnou zprávu či doručenku z tohoto prostředí Datových schránek, zobrazení chybové informace
4	**Zpřístupnění adresáře DS, identifikace vlastníků**		
	Zpřístupnění adresáře DS, identifikace vlastníků DS	Schvaluje podobu adresáře	ISDS poskytne služby, které umožní zjistit, zda zadaný subjekt má DS nebo nemá, zda je DS přístupná či nikoliv, zda lze do DS obecně doručovat či nikoliv
	Vedení veřejného seznamu dle příslušných ustanovení ZEU		Zajistí vedení veřejného seznamu dle příslušných ustanovení ZEU, přístupného způsobem umožňujícím dálkový přístup. Zajistí vytvoření webových stránek seznamu Datových schránek, včetně poskytnutí otevřených dat a příslušných webových služeb pro jejich získávání.
5	**Validace existence DS adresáta**		

	Činnosti	Zajišťuje	
		Správce	**Provozovatel**
	Validace existence DS adresáta		ISDS poskytne službu, která umožní validovat existenci adresáta v ISDS (resp. předá informaci o existenci DS zadaného subjektu)
6	**Odeslání a dodání Datové zprávy**		
	Odeslání a dodání DZ		ISDS zajistí dodání Datové zprávy do DS adresáta, pokud tato existuje a není v daný časový okamžik znepřístupněna
	Garantovaná doba dodání DZ		ISDS zajistí dodání řádně podané Datové zprávy z datové schránky odesílatele do datové schránky adresáta v garantované době dle SLA
7	**Doručení zprávy**		
	Doručení DZ		ISDS zaznamenává informaci, zda zpráva byla doručena přímo (přihlášením uživatele s právy číst zprávu do DS adresáta, dle ZEU) nebo zda vypršela lhůta pro doručení fikcí
8	**Systémová datová zpráva**		
	Odeslání systémové zprávy		Zajistí možnost zasílat systémové zprávy Správce a systémové zprávy Objednatele dle jeho volby, zadávání odesílání zpráv prostřednictvím servisního modulu. Systémová zpráva nemá charakter DZ, systémové zprávy se nebudou objevovat ve statistikách.
9	**Notifikace pro adresáta**		
	Notifikace pro adresáta		ISDS zajistí notifikace předepsané zákonem (a další požadované Správcem) a to prostřednictvím definovaných informačních prostředků (e-mail, SMS, systémové zpráva)
10	**Oznámení o doručení**		
	Oznámení o doručení		ISDS zajistí oznámení o dodání, doručení a změně na nedoručitelnou prostřednictvím DS odesilatele

	Činnosti	Zajišťuje	
		Správce	Provozovatel
11	**Vedení postupu doručení**		
	Vedení postupu doručení		ISDS – automatický proces zajišťující vedení evidence o změnách stavů zpráv – podání, dodání, doručení, způsobu doručení (přímé, uplynutí lhůty), dni a času změn stavů atd.
12	**Dohledání postupu doručení**		
	Dohledání postupu doručení		Prostřednictvím servisního modulu ISDS bude možné získat veškeré informace vztahující se k doručení určité datové zprávy včetně průběhu doručování a příslušných důkazních materiálů
	Doručenka a její formát		Zajistí, aby k informaci o stavu doručení měl přístup odesílatel i adresát. Podoba doručenky ve formě logu, tzn. postupně zaznamenán čas podání, čas dodání, doručení, případně čas znedoručitelnění. Doručenku lze exportovat v PDF (podepsaném a s časovým razítkem) nebo v podepsaném XML (ZFO)
13	**Změna přístupových údajů uživatelem (změna hesla)**		
	Změna přístupových údajů uživatelem		ISDS zajistí uživatelskou možnost změny přístupových údajů prostřednictvím rozhraní portálu a prostřednictvím veřejných webových služeb
14	**Změna přístupových údajů uživatelem (zavedení elektronického prostředku pro přihlašování) dle příslušných ustanovení ZEU**		
	Změna přístupových údajů uživatelem	schvaluje podmínky	ISDS zajistí uživatelskou možnost zavedení či změny přístupových údajů prostřednictvím rozhraní portálu – zavedení elektronického prostředku pro přihlášení.
15	**Třetí autentizační metoda**		
	Autentizace uživatelů pro přístup do DS		Zajistí pro autentizaci uživatelů volitelný způsob přihlašování s využitím jednorázového kódu, zasílaného prostřednictvím SMS nebo vygenerovaného určenou aplikací na zařízení uživatele, nebo prostřednictvím aplikace Mobilní klíč

	Činnosti	Zajišťuje	
		Správce	Provozovatel
16	**Nepovinná změna hesla po 90 dnech (přístupového hesla)**		
	Změna hesla		Zajistí možnost uživatelům v uživatelském rozhraní ISDS zrušit omezení platnosti hesla (90 dnů) na časově neomezenou dobu. Primárně bude periodicita změny hesla po devadesáti dnech nastavena jako „true“. Uživatel bude mít volbu toto nastavení odstranit a zpětně zaktivovat, přičemž bude viditelně upozorněn, že se tím snižuje úroveň bezpečnosti hesla.
17	**Seznamy DZ v portálovém zobrazení**		
	Seznam DZ v Datové schránce		Zajistí přístup k seznamům došlých a odeslaných DZ uložených v Datové schránce, včetně DZ uložených v Datovém trezoru. Umožní filtrování a výběr dle definovaných podmínek.
	Seznamy archivních záznamů o DZ		Zajistí přístup k seznamům archivních záznamů o smazaných DZ, v dělení na došlé a odeslané, včetně exportu seznamu. Zajistí stažení informace o postupu doručování i pro archivní záznamy.
18	**Optimalizace rozhraní pro mobilní zařízení**		
	Optimalizovaný klientský portál ISDS		Zajistí přístup ke službám ISDS prostřednictvím webového rozhraní – klientského portálu ISDS, optimalizovaného pro mobilní zařízení (přístup prohlížečem)
19	**Vytvoření přílohy DZ přímo v klientském portálu**		
	Vytvoření textových příloh na klientském portálu ISDS		Webový klientský portál ISDS umožní při přípravě nové zprávy k odeslání vytvořit přílohu DZ přímo z vepsaného textu (který bude převeden do formátu PDF a připojen jako příloha DZ).
VI	**DALŠÍ FUNKCE**		

	Činnosti	Zajišťuje	
		Správce	**Provozovatel**
1	**Logování informací v bezpečném logu**		
	Logování událostí spojených s provozem ISDS	Definuje události k logování	Zajistit v bezpečném logu vedení informací o událostech provozu ISDS, vyžadovaných ZKB a definovaných ze strany MV. Minimální požadavky na bezpečný log jsou: - Zajistit log proti neoprávněnému přístupu - Zajistit log proti neoprávněnému mazání - Zajistit log proti neoprávněným změnám v záznamech
2	**Řízení a konfigurování ISDS s možností identifikovat původce těchto činností**		
	Blokování konfigurace ISDS bez možnosti jednoznačné identifikace původce		Zajistí, aby uživatelé oprávnění ke vstupu do interní sítě ISDS přes VPN (virtuální privátní síť) nemohli obejít Access Manager při provádění řízení a konfigurování ISDS
3	**V nastavení eDirectory blokovat anonymní přihlášení**		
	Blokování anonymních přihlášení		Zajistí, aby uživatel se síťovým přístupem neměl možnost se přihlásit do eDirectory bez uvedení jména a hesla
4	**Pravidla směrování na síťových prvcích vnitřních sítí ISDS**		
	Blokování anonymních přihlášení		Zajistí, aby uživatel se síťovým přístupem neměl možnost se přihlásit do eDirectory bez uvedení jména a hesla
5	**Report přístupů do datových schránek**		
	Report přístupů do Datových schránek		Zajistí evidenci a výpis informací o tom, kdo měl v daném čase přístup do Datové schránky.
6	**Přidávání časových razítek do DZ - (**datová zpráva)		

	Činnosti	Zajišťuje	
		Správce	**Provozovatel**
	Komunikační rozhraní mezi ISDS a TSA		Zajistí propojení ISDS s primární a záložní lokalitou TSA. Zajistí funkčnost komunikačního rozhraní TSA pro odebírání časových razítek. Zajistí přednostní využití propojení ISDS s primární lokalitou TSA.
	Proxy časového razítka		Zajistí v případě detekování nedostupnosti časového razítka z primární lokality TSA automatické přepnutí na odběr časových razítek ze záložní lokality TSA
	Vložení podacího časového razítka		Zajistí, aby dle příslušných ustanovení ZEU při příjmu DZ do systému bylo do vzniklé Datové zprávy přidáno podací časové razítko, zajišťující integritu DZ a časový údaj o podání.
	Doplňování časového razítka do obálky DZ		Zajistí, aby ve vnější obálce uložené DZ (po aplikaci elektronické pečetě MV) bylo obsaženo časové razítko, které umožní zahájit trvalou archivaci souboru mimo ISDS.
7	**Zajištění dlouhodobé platnosti Datových zpráv a možnosti potvrzení autenticity Datových zpráv**		
	Dlouhodobá platnost Datových zpráv a dodejek/doručenek		Umožní zajištění dlouhodobé platnosti a průkaznosti elektronické pečetě (nebo elektronické značky) a elektronických časových razítek a jejich časové kontinuity v Datových zprávách a dodejkách/doručenkách i pro případy, kdy jsou uživatelem uloženy mimo ISDS, např. aby podle ZEU bylo možné provést konverzi elektronického dokumentu do listinné podoby.
	Potvrzení autenticity Datových zpráv		Umožní prověření autenticity Datových zpráv a dodejek/doručenek – ověření, jestli jakákoliv konkrétní Datová zpráva, vytvořená v ISDS a uložená mimo ISDS, byla vygenerována systémem ISDS a jestli její obsah nebyl po výstupu z ISDS změněn. Ověřující uživatel nemusí být odesílatelem ani adresátem ověřované zprávy.
	Zpřístupnit všem uživatelům ISDS informace, které jsou o nich v ISDS vedeny		Umožní oprávněnému uživateli vidět základní data, která jsou o něm v ISDS vedena.
	Dlouhodobá možnost čtení obsahu Datových zpráv, dodejek a doručenek		Zajistí bezplatnou dostupnost softwarového nástroje pro uživatele ISDS k zobrazení obsahu jakékoliv Datové zprávy, dodejky a doručenky, vytvořené v ISDS a uložené mimo ISDS, a to i

	Činnosti	Zajišťuje	
		Správce	**Provozovatel**
			zpětně pro všechny dostupné verze zpráv, dodejek a doručenek. Součástí nástroje je i kontrola a analýza CAdES úrovně podpisu.
8	**Zabezpečení systému proti ztrátě Datových zpráv a neoprávněnému přístupu k nim**		
	Způsob odeslání Datových zpráv		Zajistí způsob odesílání (tj. podání) zpráv: - uživatel odesílá Datovou zprávu prostřednictvím uživatelského rozhraní (webový klientský portál nebo web services) - při podání je zkontrolována integrita a formát Datové zprávy v souladu s příslušnými ustanoveními ZEU - DZ je synchronně ukládána do trvalého souborového úložiště renomovaného výrobce ve dvou geograficky oddělených replikách, a navíc do dočasného úložiště - dokud není DZ uložena v obou replikách, není potvrzeno uložení - potvrzení o přijetí DZ ke zpracování je vydáno uživateli po dokončení ukládání DZ v obou lokalitách, kontrole integrity a formátu a zápisu popisných informací - úložiště v obou lokalitách jsou nezávisle zálohována - soubor je odstraněn z dočasného úložiště pro příjem zpráv po provedení plné zálohy trvalého úložiště -
	Vyzvednutí DZ		Zajistí pro vyzvedávání DZ: - Uživatel má plný přístup k DZ po stanovený počet dnů pro opětovné stažení - Notifikační zprávy jsou uživatelům odesílány až po bezpečném dokončení procesů. - Všechny operace jsou logovány a logy ukládány bezpečným způsobem - V případě potřeby forenzního dohledávání a dokazování bude poskytnuta součinnost
	Zabezpečení Datových zpráv		Pro naplnění příslušných ustanovení ZEU zabezpečí ochranu Datových zpráv proti neoprávněnému přístupu následujícími opatřeními: - Obsah Datových zpráv je před neoprávněným přístupem zabezpečen šifrováním – šifruje se vlastní obsah Datových zpráv prostřednictvím odpovídajících mechanismů - Datové zprávy jsou v datovém poli uloženy výhradně v šifrované podobě – pokud je nezbytná jakákoliv manipulace s Datovou zprávou, která vyžaduje dešifraci, děje se tak výhradně v rámci přesně definovaných procesů (např. antivirová kontrola) a pouze v operační paměti

	Činnosti	Zajišťuje	
		Správce	**Provozovatel**
			- V procesu přijímání nebo odesílání DZ jsou veškeré komunikační kanály šifrovány (HTTPS, VPN) takže přístup neoprávněné osoby k datům je vyloučen
9	**Velkoobjemové datové zprávy (VODZ)**		
	Zprávy s přílohami souhrnné velikosti od 20 MB do 1 GB	Správce stanoví náležitosti VODZ úpravou vyhlášky ZEU	Systém umožní **od 1.1.2023** přijímat a odesílat VODZ se souhrnnou velikostí příloh od 20 MB do velikosti určené vyhláškou ZEU, maximálně do velikosti 1 GB.
	Umožnění práce s VODZ na klientském portálu ISDS		Klientský portál ISDS umožní uživatelům práci s VODZ a jejich přílohami. Systém sám bude volit úložiště příloh a způsob odeslání – podle souhrnné velikosti příloh DZ
			1)
	Nové webové služby (WS) pro práci s VODZ		Do systému budou zavedeny nové WS pro práci s VODZ: -samostatný upload velkých příloh, včetně kontroly formátu a AV kontroly - odeslání VODZ se zadáním identifikátorů již uložených příloh - stažení jedné přílohy VODZ (zadaného identifikátoru přílohy)
10	**Mazání datových zpráv po 3 letech**		
	Výmaz dodaných zpráv nejdříve 3 roky ode dne, kdy byla datová zpráva dodána do datové schránky		Systém umožní, v souladu s příslušným ustanovením vyhlášky ZEU, vymazat ze systému datové zprávy nejdříve po 3 letech ode dne, kdy byla datová zpráva dodána do datové schránky
11	**Přihlašování s použitím klientského certifikátu**		
	Přihlašování s použitím klientského certifikátu		Systém umožní uživatelům přihlášení s použitím přístupového jména, hesla a osobního přístupového certifikátu, vydaného těmto fyzickým osobám certifikačními autoritami majícími v ČR akreditaci.

	Činnosti	Zajišťuje	
		Správce	Provozovatel
12	**Informovanost uživatelů ISDS o tom, jaké osobní údaje o nich systém DS drží a zpracovává dle článku 15 Nařízení (EU) 2016/679 (GDPR) a výkon práv uživatelů jako subjektů údajů dle GDPR.**		
	Informace o osobních údajích a právo na přístup		Systém umožní zpřístupnit uživateli DS jakožto subjektu údajů přehled zpracovávaných osobních údajů o jeho osobě. Informace o zpracování osobních údajů pro účely poskytování služby datové schránky, poskytuje správce osobních údajů, kterým je Ministerstvo vnitra ČR, na informačním webu ISDS. Informace o osobních údajích, zpracovávaných Informačním systémem datových schránek, získá uživatel po přihlášení do klientského portálu, volbou Nastavení – Osobní údaje. Zde je umožněn i export dat do formátu pdf. U doplňkových služeb datových schránek, a to služeb Datový trezor a Poštovní datová zpráva, je správcem osobních údajů Česká pošta, s.p., která uživatelům poskytuje informace o zpracovávaných osobních údajích v rámci svých vlastních procesů nastavených pro výkon práv subjektů údajů dle GDPR.
	Export dat (právo na přístup)		Systém umožní uživateli export sestavy zpracovávaných osobních údajů pro potřebu uživatele, popř. pro přenos dat mezi informačními systémy. Výstup je ve formátu PDF, elektronicky podepsaný s využitím certifikátu Správce. Každé stažení souboru je zaznamenáno v bezpečném logu.
	Právo na opravu		U ztotožněných uživatelů (vůči ROM) je zaručeno, že jejich osobní údaje jsou shodné s osobními údaji vedenými v základních registrech a denně synchronizovány. Systém ISDS má povinnost aktualizovat svá data podle referenčních dat v ISZR. Pokud fyzická osoba, které byla zřízena datová schránka, a která byla ztotožněna vůči ROB, změnila své osobní údaje (jméno, příjmení, bydliště) a změna nebyla automaticky provedena, může tuto změnu ohlásit správci, nejlépe formou datové zprávy, případně jiným způsobem. Správce následně zajistí opravu údajů po prověření údajů v poskytnutých dokladech.

	Činnosti	Zajišťuje	
		Správce	**Provozovatel**
	Právo na výmaz	Podmínky výmazu dat z ISDS stanoví příslušné právní předpisy a/nebo pokyny Správce.	Systém zajistí realizaci práva na výmaz, za podmínek dle Nařízení a právních předpisů vztahujících se k provozu systému a/nebo dle pokynů Správce. Případné změny v nastavení dosavadních funkcionalit budou předmětem Služeb rozvoje ISDS.
	Právo na omezení zpracování		K přenášení informací o omezení zpracování (zastavení zpracování osobních údajů určitého subjektu údajů) slouží tiketovací systém Dohledového centra eGov. K vlastnímu omezení zpracování slouží servisní modul správce.
	Právo na oznamovací povinnost		Příjemci osobních údajů (Správce, Provozovatel a Poddodavatel v rámci ISDS) se navzájem informují o veškerých opravách nebo výmazech nebo omezení zpracování na základě součinnosti smluvních stran (realizováno automatizovaně prostřednictvím servisního modulu ISDS a komunikační matice v rámci Dohledového centra eGOV).
	Právo na přenositelnost		Neuplatňuje se na základě článku 20 odstavce 3 GDPR.
13	**Přihlašování k ISDS prostřednictvím Národní identitní autority**		
	Přihlášení k systému		Systém umožní přihlášení prostřednictvím autentizační brány Národní identitní autority (dále jen „NIA“)
	Zakázání / Povolení přihlášení prostřednictvím NIA pro celé ISDS		Systém umožní v rámci nastavení zakázat/povolit přihlášení prostřednictvím NIA pro celé ISDS.
	Zakázání / Povolení přihlášení prostřednictvím NIA pro uživatele schránky		Systém umožní, aby přihlášený uživatel pro svůj účet nebo uživatel s oprávněním administrátor pro všechny účty schránky mohl zakázat/povolit přihlašování prostřednictvím NIA
	Zrušení (výmaz) existujících pseudonymů		Systém umožní, aby přihlášený uživatel u svého účtu nebo uživatel s oprávněním administrátor u všech účtů schránky mohl provést výmaz pseudonymů uložených v ISDS, a tím znemožnit jejich použití pro přihlášení.

	Činnosti	Zajišťuje	
		Správce	Provozovatel
14	**Přihlašování k ISDS prostřednictvím Mobilního elektronického prostředku**		
	Přihlášení uživatele ke klientskému portálu ISDS (nebo odesílací bráně, autentizační službě)		Systém umožní přihlášení prostřednictvím elektronického prostředku založeného na použití mobilních zařízení
	Aplikace Mobilní klíč (MK) pro mobilní zařízení	Správce zajistí zveřejnění aplikace	Zajistí vývoj, údržbu a distribuci softwarové aplikace pro mobilní zařízení na platformě Android a iOS, umožňující přihlašování k ISDS a k Národnímu bodu prostřednictvím MK
	Zálohování profilů MK		Uživatel bude mít k dispozici nástroje pro vytvoření bezpečnostně chráněné zálohy dat (profilu) aplikace MK a pro její obnovení v jiném mobilním zařízení.
	Možnost zablokování MK		Systém umožní zablokování prostředku MK vzdáleně, bez nutnosti návštěvy kontaktního místa veřejné správy
	Možnost zákazu přihlašování metodami využívajícími jméno/heslo pro uživatele s aktivovaným MK		Systém umožní, aby si uživatel s aktivovaným MK zakázal/povolil pro svůj uživatelský účet přihlašování metodami využívajícími jméno/heslo
	Přihlášení aplikací třetích stran k uživatelskému účtu		Systém umožní podporu přihlašování prostřednictvím MK i v rámci webových služeb
	Notifikační služby		Systém umožní notifikace na mobilním zařízení alespoň o: - nových DZ - odeslaných DZ, které nelze dodat/doručit - přihlášení pomocí jedné z metod používajících jméno/heslo (bez MK)

	Činnosti	Zajišťuje	
		Správce	**Provozovatel**
			- aktivitách spojených s MK (aktivace dalšího MK, deaktivace MK, provedení zálohy MK, obnovení zálohy atd.)
15	**Autentizační služba ISDS a Odesílací brána**		
	Autentizační služba		Systém poskytuje tzv. Autentizační službu (ExtIS), která umožňuje externí aplikaci Poddodavatele po zadání přístupových údajů do ISDS získat informace o uživateli ISDS a jeho schránce.
	Odesílací brána		Systém poskytuje tzv. Odesílací bránu – službu, která umožňuje externím aplikacím autentizovat uživatele ISDS přihlášením do své schránky. Externí aplikace poté může připravit a odeslat datovou zprávu (např. daňové přiznání) ze schránky přihlášeného uživatele, s prohlédnutím a odsouhlasením konceptu před vlastním odesláním.
	Registrace autentizační služby a Odesílací brány		Registrace Autentizační služby a Odesílací brány je umožněna za stanovených podmínek na klientském portálu ISDS a v Servisním modulu, včetně registrace potřebného certifikátu pro komunikaci externí aplikace s ISDS.
16	**Opatřeni k zamezení nevyžádaných datových zpráv**		
	Možnost zadat oznámení nevyžádaných datových zpráv		Systém umožní prostřednictvím Klientského portálu, Servisního modulu a WS přihlášenému uživateli zadat oznámení nevyžádaných datových zpráv pro dodané zprávy, jejichž odesílatelem není schránka typu OVM. Servisní modul umožní na základě přidělených oprávnění navíc i zadání oznámení nevyžádaných datových zpráv pro dodané zprávy, jejichž odesílatelem je schránka OVM, Klientský portál a WS umožní zadavateli oznámení zadat souhlas s přístupem k obsahu příloh.
	Zpracování oznámení nevyžádaných datových zpráv v Servisním modulu	Správce v Servisním modulu rozhodne o potvrzení zaznamenaného výsledku analýzy oznámených nevyžádaných zpráv.	Systém umožní v Servisním modul na základě přidělených oprávnění: - evidenci oznámení nevyžádaných datových zpráv, - analýzu dokumentů obsažených v oznámených datových zprávách, ke kterým je zadavatelem oznámení předán souhlas s přístupem k obsahu příloh,

	Činnosti	Zajišťuje	
		Správce	Provozovatel
			- zadat rozhodnutí/výsledek analýzy, zda lze oznámené zprávy považovat za nevyžádané, - na základě přiděleného oprávnění zadat potvrzení tohoto rozhodnutí/výsledku analýzy.
	Opatření proti odesílatelům nevyžádaných datových zpráv		Servisní modul na základě přidělených oprávnění umožní: Poslat varování správce do schránek a na u nich evidované notifikační maily Aktivovat a zrušit opatření a nastavit časový limit pro schránky odesílatelů nevyžádaných datových zpráv: - Zákaz odesílání PDZ, nebo VoDZ - Zákaz odesílání multimediálních souborů - Zákaz odesílání zpráv přes WS - Zákaz posílat zprávy s určenou přílohou (se shodným hashem), - Zákaz odesílání zpráv - Označení shodných zpráv příznakem. - Zákaz stahování určených datových zpráv
	Opatření pro adresáty nevyžádaných datových zpráv		Systém umožní označit podezřelé datové zprávy a informovat adresáty, že dodaná zpráva v jejich schránce může být nevyžádaná. Veřejné WS umožní stáhnout seznam ID došlých zpráv takto označených. Klientský portál ISDS umožní v seznamu došlých zpráv a v detailu datové zprávy rozlišit takto označené zprávy. Systém umožní zablokovat stahování určených došlých zpráv z ISDS.

4.1.1 Nové funkcionality

Provozovatel neobdrží od Správce k níže uvedeným funkcionalitám zdrojové kódy, ale je povinen tyto funkcionality zprovoznit od 1.1.2023.

Provozovatel provede před realizací nových funkcionalit návrh potřebných úprav zdrojového kódu a pokud bude nutné i technické infrastruktury ISDS, předloží návrh úprav Správci k projednání, po schválení Správcem provede úpravu zdrojového kódu, pokud bude nutné i změny Technické infrastruktury budovaných prostředí.

1) Bezodstávkový provoz

Provozovatel zajistí Bezodstávkový provoz ISDS za podmínek, které umožní provozovat ISDS bez provádění výluk systému s dopadem na jeho nedostupnost pro uživatele a to především pro následující úkony: aktualizace jeho programového, technického a jiného souvisejícího vybavení včetně aktualizace portálů, formulářů, migrace dat, aktualizace AGW, eDirectory, serverů, firewallů, switchů, datových polí, HCAP nebo ostatních infrastrukturních zařízení a to i při přechodu mezi verzemi, bez provádění výluk systému s dopadem na jeho nedostupnost pro uživatele prostřednictvím webových portálů a služeb, které systém v Řádném a plném provozu (definovaný pojem) poskytuje.

2) Plná podpora lokalizace do cizích jazyků

Všechny uživatelské aplikace (mobilní aplikace, webové aplikace, informační stránky atd.) musí být navrženy tak, aby umožnily spuštění více jazykových verzí bez vynaložení dalších nákladů na úpravy aplikací.

4.1.2 Další nové budoucí funkcionality

Provozovatel neobdrží od Správce k níže uvedeným funkcionalitám zdrojové kódy, ale je povinen tyto funkcionality zprovoznit do 12 měsíců ode dne, kdy od Správce obdrží písemné potvrzení nabídky dle odst. 9.4 Smlouvy, za předpokladu, že Správce realizaci změny vyžádá a poskytne potřebnou součinnost. Některé z uvedených změn mohou mít dopad i do formátu obálky datové zprávy.

Realizace těchto funkcionalit je hrazena z ceny Služeb Rozvoje.

1) Bezplatný archiv pro FO a PFO

Schránky typu FO a PFO zřizované na žádost budou uchovávat dodané datové zprávy na neurčito, bez omezení kapacity. Bude možné zavedení kapacitního limitu pro případy nepřiměřeného využívání, např. v kapacitě 1 GB / schránku.

2) Třívrstvá architektura

Upravit systém dle požadavků Správce tak, aby aplikační rozhraní ISDS nabízelo požadovanou obslužnost pro potřeby uživatelů ISDS, včetně určených konfiguračních a dalších nastavení, která jsou aktuálně dostupná jen v prostředí klientského portálu ISDS.

3) Dekomponovaná architektura – externí autentizace

Upravit systém tak, aby splňoval požadavky Správce ISDS. Cílem Správce je, aby co největší část populace disponovala prostředky pro el. identifikaci dle zákona o el. identifikaci. Přístupové údaje vydané k datové schránce však takovým prostředkem nejsou. Proto Správce ISDS zvažuje potřebné aktivity vedoucí k postupnému utlumení vydávání a používání přístupových údajů ISDS. Pro běžné uživatele bude cestou Národního bodu dostupná celá řada prostředků elektronické identifikace. Národní bod ale řeší jen uživatele zapsané v ROB a umožňuje jen přihlášení do webových aplikací. Provedení uvedeného záměru tedy bude vyžadovat mj. i návrh, jak zajistit:

- Přístup cizinců nezapsaných v ROB (zejména statutárních zástupců firem) do ISDS.
- Autentizaci aplikací třetích stran jménem uživatele, který je schopen se autentizovat cestou Národního bodu.
- Řešení přístupu osob, které zaměstnavatel pověřil ovládáním datové schránky (tedy zda je přípustné, aby byli nuceni zřídit si účet v NIA, když jej soukromě nechtějí, a navíc by jim k tomu byla automaticky zřízena datová schránka FO (ve smyslu nové poslanecké iniciativy).

4) Časový zámek datové zprávy – možnost otevřít až po uplynutí určitého času

Zavedení volitelného časového zámku, který by obsah zprávy zpřístupnil příjemci až po uplynutí konkrétního časového okamžiku.

5) Podpora vícenásobných podpisů u podání právnických osob

Pokud nějaké právní jednání vyžaduje podpis více osob oprávněných jednat za právnickou osobu, nelze jej učinit cestou datových schránek. ISDS umožní záznam projevu vůle více uživatelů postupně a teprve pak umožní odeslat zprávu včetně záznamu o provedení úkonu – záznamu projevu vůle více osob oprávněných jednat za právnickou osobu.

4.2 Funkční požadavky na provoz Aditivních služeb

4.2.1 Datový trezor

Procesy		Zajišťuje	
		Správce	Provozovatel
I	**Zajištění funkcí služby Datový trezor**		
1	Služba Datový trezor		ISDS umožní (dle příslušných ustanovení ZEU) na žádost držitele Datové schránky uložení dodané Datové zprávy v Datové schránce po dobu delší, než je doba stanovená vyhláškou, netýká se uložení příloh VODZ. Za uložení dodané Datové zprávy v Datové schránce po dobu delší, než je doba stanovená vyhláškou, náleží Provozovateli ISDS odměna, která se stanoví dle příslušných ustanovení ZEU – ISDS umožní ČP účtování a inkasování uvedené odměny.
2	Funkce služeb Datových trezorů		Zajistí funkce ISDS pro uložení Datových zpráv v Datové schránce po dobu delší, než je stanovena vyhláškou, tzv. služby Datového trezoru dle specifikací v provozní příručce Funkční design.
3	Neveřejné webové služby ISDS pro službu Datový trezor		Zajistí funkce webových služeb pro službu Datový trezor dle specifikací v provozní příručce Funkční design.
4	Veřejné webové služby ISDS pro službu Datový trezor		Zajistí funkce webových služeb pro službu DT dle specifikací v Provozním řádu, části WS_ISDS_Vyhledavani_datovych_schranek.pdf
II	**Uživatelské rozhraní**		

1	Přístup k DT		ISDS umožní uživatelům přístup k Datovým zprávám uloženým v DT (náležejícím jejich DS) po úspěšném přihlášení do systému ISDS
2	Smazání zprávy		ISDS umožní smazání Datové zprávy, která je umístěna v DT, uživateli s příslušnými oprávněními
III	**Notifikace**		
1	Uživatelské nastavení notifikací		ISDS umožní v nastavení Datových schránek zapnout nebo vypnout určený typ notifikací pro události DT. Provozovatel stanoví podmínky pro notifikace služby DT a texty notifikačních systémových zpráv.
2	Notifikace služby Datový trezor		Zajistí funkce notifikací dle specifikací v provozní příručce Funkční design. Provozovatel stanovuje podmínky pro notifikace služby DT a texty notifikačních systémových zpráv.
IV	**Informování uživatelů služby**		
1	Informování uživatelů služby		ISDS zajistí realizaci dle konkrétní informační akce. Provozovatel rozhodne o způsobu a detailech předávání informací uživatelům ISDS o možnostech a funkcionalitách služby DT. Provozovatel stanoví okruh subjektů, na které se bude informační akce vztahovat.
V	**Stanovení ceny pro koncové zákazníky**		
			Stanovení ceny pro Koncové uživatele je plně v kompetenci Provozovatele.

4.2.2 Poštovní datová zpráva

Procesy		Zajišťuje	
		Správce	Provozovatel
I	**Zajištění funkcí Poštovních datových zpráv (PDZ)**		
1	Služba Poštovní datová zpráva		ISDS umožní dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob dle příslušných ustanovení ZEU. ISDS umožní ČP účtování a inkasování odměny dle příslušných ustanovení ZEU.
2	Funkce služeb Poštovních datových zpráv		Zajistí funkce ISDS pro nakládání s Poštovními datovými zprávami dle specifikací v provozní příručce Funkční design, část Poštovní datové zprávy a související.
3	Povolení příjmu PDZ		ISDS zajistí možnost nastavení zákazu a povolení příjmu PDZ pro datové schránky určené dle ZEU na základě pokynu uživatele, specifikací v provozní příručce Funkční design, část Poštovní datové zprávy.
4	Neveřejné webové služby ISDS pro Poštovní datové zprávy		Zajistí funkce webových služeb pro Poštovní datové zprávy dle specifikací v provozní příručce Funkční design, část Poštovní datové zprávy a související.
5	Veřejné webové služby ISDS pro Poštovní datové zprávy		Zajistí funkce webových služeb pro Poštovní datové zprávy dle specifikací v Provozním řádu, části WS_ISDS_Vyhledavani_datovych_schranek.pdf
II	**Uživatelské rozhraní**		

1	Přístup k PDZ		ISDS umožní přístup k PDZ po úspěšném přihlášení do systému ISDS
2	Odeslání a uložení PDZ		ISDS zajistí odeslání a uložení PDZ po dobu vyplývající ze ZEU
3	Fakturace smluvních PDZ koncovým zákazníkům		ISDS umožní ČP prostřednictvím webových služeb získávání dat pro vyúčtování smluvních PDZ koncovým zákazníkům. Provozovatel zajistí fakturaci smluvním zákazníkům
III	**Informování uživatelů služby**		
1	Informování uživatelů služby		ISDS zajistí realizaci dle konkrétní informační akce. Provozovatel rozhodne o způsobu a detailech předávání informací uživatelům ISDS o možnostech a funkcionalitách služby PDZ. Provozovatel stanoví okruh subjektů, na které se bude informační akce vztahovat.
IV	**Stanovení ceny pro koncové zákazníky**		
			Stanovení ceny pro koncové zákazníky je plně v kompetenci Provozovatele.

4.2.3 SMS notifikace

Procesy		**Zajišťuje**	
		Správce	**Provozovatel**
I	**Zajištění funkcí SMS notifikace**		
1	Služba SMS notifikací		ISDS umožní (dle příslušných ustanovení ZEU) vyrozumění adresáta o dodání datové zprávy do jeho Datové schránky prostřednictvím Premium SMS.

2	Zajištění funkce Notifikačního serveru		Zajistí požadované funkce Notifikačního serveru pro předávání dat potřebných pro odesílání Premium SMS poskytovateli Premium SMS, dle specifikací v provozní příručce Funkční design, část Notifikační server v ISDS a související.
II	**Uživatelské rozhraní**		
1	Nastavení notifikací na klientském portálu ISDS		ISDS zajistí pro uživatele ISDS možnost nastavení funkcionalit služby SMS notifikací.
III	**Stanovení ceny pro koncové zákazníky**		
			Stanovení ceny pro koncové zákazníky je plně v kompetenci Provozovatele.

4.2.4 Kreditní systém datových schránek

Procesy		**Zajišťuje**	
		Správce	**Provozovatel**
I	**Zajištění funkcí kreditního systému ISDS**		
1	Služba kreditní systém		ISDS umožní služby kreditního systému: - Dobíjení kreditu pro konkrétní Datovou schránku - Vedení kreditů k Datovým schránkám - Umožnění čerpání kreditu při aktivaci služby kreditní DT - Umožnění čerpání kreditu při odesílání PDZ hrazených kreditem - Notifikaci při nízkém stavu kreditu a při blížící se expiraci kreditu - Vedení podrobného a bezpečného logu o všech pohybech kreditů

			- Možnost stažení přehledů čerpání kreditu - Umožnit každému uživateli Datové schránky vidět hodnotu kreditu a historii kreditních transakcí - ČP může kredit nabíjet/vybíjet prostřednictvím WS
2	Funkce kreditního systému		Zajistí funkce kreditního systému dle specifikací v provozní příručce Funkční design, část Kreditní systém a související.
3	Neveřejné webové služby ISDS pro kreditní systém		Zajistí funkce webových služeb pro kreditní systém dle specifikací v provozní příručce Funkční design, část Kreditní systém a související.
4	Veřejné webové služby ISDS pro kreditní systém		Zajistí funkce webových služeb pro kreditní systém dle specifikací v Provozním řádu, části WS_ISDS_Vyhledavani_datovych_schranek.pdf
II	**Uživatelské rozhraní**		
1	Změny výše kreditu		Systém ISDS na základě pokynu ČP upraví stav kreditu v DS. ISDS umožní ČP prostřednictvím specifického rozhraní (webové služby) zadávání změn kreditu pro určené Datové schránky, získávání informací o změnách kreditu a získávání potřebných dat pro vyúčtování kreditu. Umožní uživatelům získávání informací o pohybech výše kreditu u vlastní Datové schránky. Provozovatel zajistí možnost nabití kreditu přes externí aplikaci

			napojenou na ISDS přes neveřejné webové služby
2	Notifikace kreditního systému		Zajistí funkce notifikací dle specifikací v provozní příručce Funkční design – upozornění na nízký stav kreditu a na blížící se expiraci kreditu
III	**Informování uživatelů služby**		
1	Informování uživatelů služby		ISDS zajistí realizaci dle konkrétní informační akce. Provozovatel rozhodne o způsobu a detailech předávání informací uživatelům ISDS o možnostech a funkcionalitách služby kreditní systém. Provozovatel stanoví okruh subjektů, na které se bude informační akce vztahovat.
IV	**Stanovení ceny pro koncové zákazníky**		
			Stanovení ceny pro koncové zákazníky je plně v kompetenci Provozovatele.

4.3 Funkční požadavky na provoz podpůrných služeb

	Činnosti	**Zajišťuje**	
		Správce	**Provozovatel**
I	**OBSLUŽNÉ A SERVISNÍ ČINNOSTI**		
1	**Veřejné testovací prostředí pro dodavatele aplikací a širokou veřejnost**		

	Provoz testovacího prostředí pro dodavatele aplikací – veřejné testovací prostředí	Správce schvaluje žádosti o přístup do testovacího prostředí	Zajistí, aby dodavatelům aplikací po schválení požadavku Správcem byl umožněn přístup do veřejného testovacího prostředí ISDS
2	**Napojení Spisových služeb (interface, veřejné testovací prostředí, součinnost Provozovatele)**		
	Napojení na spisové služby (interface, testovací prostředí, součinnost Provozovatele)	Zajistí součinnost dotyčných subjektů	Bude zajištěn přístup prostřednictvím portálu a interface WS (webové služby) pro aplikace třetích stran. Zajistí veřejné testovací prostředí pro testování napojení spisových služeb na interface WS
3	**Rozhraní pro přístup aplikací internetových provozovatelů do ISDS dle příslušných ustanovení ZEU**		
	Rozhraní pro přístup aplikací internetových provozovatelů do DS		Zajistí podklady pro výpočet poplatků za využití přístupového rozhraní.
	Podklady pro výpočet poplatků za využití přístupového rozhraní		Umožní Správci vést seznam Provozovatelů internetových služeb, kteří využívají přístupové rozhraní, a zveřejňovat je dálkovým způsobem.
	Seznam poskytovatelů internetových služeb	Zajistí vedení veřejného seznamu poskytovatelů internetových služeb (dle příslušných ustanovení ZEU).	Umožní Správci vést seznam poskytovatelů internetových služeb, kteří využívají přístupové rozhraní, a zveřejňovat je dálkovým způsobem.
4	**Design rozhraní ISDS**		
	Formát přístupových údajů		Zajistí generování nových přístupových údajů (přístupové heslo pro první přihlášení do systému, resp. přístupové heslo při opakování vydávání přístupových údajů) ve tvaru, který nebude obsahovat speciální znaky, jež se vyskytují mimo rozložení „české“ klávesnice
5	**Servisní modul**		

	Možnosti ukládání dat		Zajistí možnost ukládání dat (provozních statistik systému ISDS) ve formátu CSV a XLS.
	Možnosti exportu tabulek		Zajistí možnost exportu dat (provozních statistik systému ISDS) ve formátu CSV a XLS
	Poskytování informace o datu zpřístupnění a znepřístupnění DS		Zajistí v servisním modulu možnost zobrazení informace o datu zpřístupnění a znepřístupnění Datové schránky
	Poskytování informace o okamžiku znepřístupnění Datové schránky		Zajistí v servisním modulu možnost zobrazení v seznamu žádostí záznamu s datem znepřístupnění Datové schránky na žádost
	Poskytování informace o znepřístupněných a zrušených DS		Zajistí poskytování informace o znepřístupněných a zrušených Datových schránkách v seznamu žádostí Správci ve stejném rozsahu jako informace o aktivních Datových schránkách
	Generování výpisů o dodaných a odeslaných DZ		Zajistí dodatkovou funkci poskytování výpisů z DS o dodaných či odeslaných zprávách za určité období (výpis z logu – základní údaje o DZ).
	Poskytování informací o Datových zprávách uživatelům SM (Servisní modul)		Zajistí uživatelům servisního modulu možnost zjistit podrobné informace o konkrétní Datové zprávě (např. adresát, odesilatel, čas dodání, doručení, stav zprávy apod.)
	Zobrazení informací o počtech zásilek v SM a reportech		Zajistí v Servisním modulu možnost generování reportů o zásilkách předávaných systému hybridní pošty a stavech jejich doručení.
	Zobrazení informací ve „Stavu žádosti“		Zajistí v servisním modulu možnost zobrazení informací ve „Stavu žádosti“, včetně jména a příjmení osoby a data, kdy byla operace provedena, včetně textového popisu.
	Report interních uživatelů		Zajistí uživatelům servisního modulu s nejvyššími právy možnost generovat report interních uživatelů včetně rolí.

	Zpřístupnění informací o odesílajících osobách způsobujících doručení DZ		Dle příslušných ustanovení ZEU umožnit získávat seznamy DZ určité DS pro interní uživatele ISDS. V tabulkách uvnitř ISDS bude uváděna i osoba, která odeslala a osoba, která způsobila doručení.
	Servisní modul pro správu a obsluhu datových schránek	Funkcionality definuje MV. Část Dokumentace je v režimu utajení Důvěrné, část v režimu utajení Vyhrazené.	Zajistí určeným interním uživatelům definované funkce dle Dokumentace. Povede separátní režimovou Dokumentaci pro Servisní modul pro správu a obsluhu datových schránek.
6	**Portál Poskytovatelů dat**		
	Možnosti		Zajistí funkčnost formulářů pro správu Datových schránek pro ty poskytovatele dat, kteří nevyužívají rozhraní webových služeb.
7	**Výstupy forenzní funkcionality**		
	Forenzní vyhledávání		Zajistí funkčnost vyhledávání a výpis událostí bezpečného logu k dané Datové schránce
	Výstupy forenzní funkcionality		Zajistí, aby auditní výpis událostí Datové schránky ze servisního modulu, který je předáván na základě speciálních právních předpisů mimo ISDS ve formátu XLS, neuváděl uživatelské identifikátory jiných uživatelů než z auditované Datové schránky.
	Forenzní šetření	spolupracuje s Provozovatelem na definici procesu	Výstupem je proces přístupů pověřených osob MV k podkladovým informacím ISDS pro potřeby realizace forenzního šetření
8	**Helpdesk (Call centrum – Informační linka) a Service Desk (SD)**		
	Přijetí požadavku		Zajistí funkcionalitu základního Helpdesku a Service Desku pro uživatele na bázi standardních telefonních linek.

	Proces reklamace v SD		V aplikaci TTS pro potřeby evidence incidentů zajistí vedení kategorie „R“, která je určena pro incidenty Koncových uživatelů. Zajistí zpracování ticketů v rámci jednotlivých skupin řešitelů.
9	**Interní správa a auditování systému**		
	Interní správa, monitoring, auditování systému		Zajistí dohled, monitoring a správu systému ISDS včetně bezpečnostní správy, kontrolu monitorovacích zpráv
	Rozšířený monitoring poskytovaných služeb		Zajistí možnost vykazování následujících parametrů: - Počet dodaných Datových zpráv za měřené období dodaných do 4 hodin od podání - Počet Datových zpráv za měřené období nedodaných do 4 hodin od podání - Celkový počet podaných Datových zpráv za měřené období - Počet zřízených DS - Počet přijatých požadavků k vytvoření DS - Počet zrušených DS za měřené období - Počet zrušených DS ve stanovené lhůtě za měřené období - Seznam jednotlivých případů zrušení DS, u kterých nebyla splněna garantovaná doba vyřízení, s uvedením skutečného času zrušení DS - Počet znepřístupněných DS za měřené období - Počet DS znepřístupněných včas za měřené období - Počet přijatých požadavků na znepřístupnění DS za měřené období - Počet zneplatněných přístupových údajů za měřené období - Počet zneplatněných přístupových údajů ve lhůtě do 60 minut, za měřené období - Počet přijatých požadavků na zneplatněných přístupových údajů za měřené období - Počet přijatých požadavků na vytvoření přístupových údajů

			- Počet přístupových údajů vytvořených včas za měřené období - Počet stažených Datových zpráv za měřené období - Počet Datových zpráv za měřené období, připravených včas ke stažení - Počet stažených dodejek a doručenek za měřené období - Počet dodejek a doručenek za měřené období, připravených včas ke stažení - Počet požadavků na Call centrum přijatých v časovém limitu - Počet aktivních Datových schránek na konci měsíce - Počet Datových zpráv podle určených velikostních kategorií, za měřené období
10	**Definování provozních parametrů (identifikátor, formáty, přist. údaje atd.)**		
	Definice provozních parametrů	Schvaluje a vydává vyhlášku	Vypracovává a předkládá návrhy příslušných parametrů (případně jejich struktury) pro vyhlášku
11	**Bezpečnostní monitoring**		
	Bezpečnostní monitoring		Prostřednictvím specializovaného nástroje zaznamenává činnosti systému ISDS, jeho uživatelů a administrátorů v souladu s požadavky Vyhlášky 82/2018 Sb., o kybernetické bezpečnosti
12	**Bezpečnostní audit**		
	Bezpečnostní audit	Iniciace	Připravuje podklady a zajišťuje provedení bezpečnostního auditu. Kontroluje své pracovníky a postupy i pracovníky a postupy Poddodavatele.
II	**PROVOZ INFORMAČNÍHO WEBU DATOVÝCH SCHRÁNEK**		
1	**Hosting webového serveru na Správcem určené doméně**		
	Přesměrování DNS záznamů	Na vyžádání zajistí přesměrování DNS záznamů na adresu určenou Provozovatelem	Sdělí Správci adresu webu pro přesměrování DNS záznamů.

	Hosting web serveru		Hostuje web server v režimu 24x7 s dostupností 99%.
	Sledování návštěvnosti		Technickými prostředky sleduje a ukládá statistiky návštěvnosti webu, jedenkrát měsíčně zpracuje statistiku pro Správce a předá ji ve formátu PDF na e-mailovou adresu udanou Správcem.
2	**Údržba obsahu informačního webu**		
	Správa obsahu	Schvaluje grafické šablony	Spravuje obsah ve vlastním redakčním systému v grafické úpravě dle schválených šablon.
	Publikace nového obsahu z iniciativy Provozovatele		Zpracuje a publikuje nový obsah v grafické úpravě dle schválených šablon.
	Publikace nového obsahu na žádost Správce	Předá Provozovateli požadavky na změnu obsahu informačního webu ve formátu MS Word e-mailem na stanovenou adresu Provozovatele. Správce je oprávněn požadovat změny nejvýše jedenkrát týdně.	Předané podklady zpracuje a publikuje v grafické úpravě dle schválených šablon v termínu do 3 pracovních dnů po obdržení požadavků Správce
	Aktivní údržba obsahu webu		Průběžně udržuje webové stránky tak, aby neobsahovaly zastaralé či neplatné informace.
	Zálohování dat		Provádí pravidelnou zálohu obsahu webu.

4.4 Podpora dodavatelů aplikací třetích stran

Určení služby:	Zajištění podpory Provozovatelem komunitě vývojářů – dodavatelů aplikací třetích stran – využívajících aplikační rozhraní ISDS. Podpora bude poskytována formou diskusního fóra v rámci webové aplikace určené Správcem.
Parametry služby:	Reakční doba 1 pracovní den
Reporting:	Statistika řešení incidentů pro potřeby třetích stran
Režim služby:	9x5

4.5 Zajištění bezpečného provozu a dostupnosti ISDS

Základním cílem zajištění provozu a dostupnosti ISDS je zajištění provozu ISDS a s tím související poskytnutí funkčností tohoto systému oprávněným uživatelům v rozsahu pokrývajícím zákonné požadavky viz. článek 3. Přílohy č. 1 Smlouvy.

Určení služby:	Služba je určena pro zajištění bezpečného, bezporuchového a bezvýpadkového provozu a dostupnosti systému ISDS za předpokladu definované součinnosti v souladu s definovanými SLA uvedenými v Příloze č. 2.
Parametry služby:	Služby provozu ISDS jsou poskytovány na technické infrastruktuře a s garantovanou dostupnost nepřetržitě v režimu 24×7. ▪ Maximální velikost Datové zprávy dodávané do Datové schránky je definována Dotčenými právními předpisy. ▪ Lhůta uchovávání Datových zpráv, u nichž bylo doručení vykonáno přihlášením adresáta do jeho Datové schránky, je dle příslušných ustanovení ZEU. ▪ Lhůta uchovávání Datových zpráv, které byly dodány do datové schránky, ale nedošlo k přístupu do datové schránky, tj. nedošlo k doručení jedním ze způsobů přístupu do datové schránky, je 3 roky ode dne, kdy byla datová zpráva dodána. V systémovém logu budou o těchto událostech uchovávány veškeré záznamy po dobu o tři roky delší než maximální dobu požadovanou právními předpisy.
Reporting:	Součástí služby je i pravidelný měsíční report zahrnující informace o dostupnosti systému.
Režim služby:	24x7

4.6 Tisk a doručování přístupových údajů – služba Hybridní pošta

Určení služby:	Účelem této služby je doručení přístupových údajů nebo opětovné vydání přístupových údajů dle příslušných ustanovení ZEU tak, aby nemohlo dojít k jejich zneužití.
Parametry služby	▪ Služba spočívá v zabezpečení materiálu (obálky, papíru), tisku a dotisku dokumentů z předaných datových souborů, kompletaci zásilek (obálkování, balení) a hromadném podání zkompletovaných zásilek za Správce (dále jen Služby Hybridní pošty). Okamžikem hromadného podání zásilek dochází k uzavření poštovní smlouvy ve smyslu zákona č.29/2000 Sb., o poštovních službách, v platném znění. Zásilka bude podána v souladu s dokumentem schválených procesů pro odesílání obálek s přístupovými údaji – Typy a texty PÚ. Součástí služby Hybridní pošty je předání dodejek

	a tvorba elektronických sestav o doručení. Služba bude poskytována dle potřeb Správce na základě jeho jednotlivých objednávek. ▪ Správce je oprávněn učinit objednávku pouze v pracovní dny v době od 8.00 do 17.00 hodin. V případě, že Správce učiní objednávku mimo tento stanovený termín, je objednávka považována za předanou následující pracovní den v 8.00 hodin. ▪ Provozovatel neprovádí kontrolu adresních údajů z předaných datových souborů, a proto neodpovídá za případnou nedoručitelnost zpracovaných zásilek z důvodu chybných adresních údajů. Za obsahovou správnost tištěných dokumentů odpovídá Správce. ▪ Lhůta pro provedení Služby Hybridní pošty činí: o Pro vnitrostátní zásilky - 1 (jeden) pracovní den ode dne doručení objednávky o Pro mezinárodní zásilky - 5 (pět) pracovních dnů ode dne doručení objednávky o Pro vnitrostátní i mezinárodní zásilky v ISDS automaticky rozpoznané jako problémové (např. chybí nebo je neznámé PSČ nebo je nestrukturovaná adresa, provádí se ruční oprava či doplnění adresních údajů) – 3 (tři) pracovních dny, a to v případě, že jejich počet nepřesáhne 100 (sto) kusů zásilek. Za každých dalších započatých 50 (padesát) kusů zásilek se lhůta pro provedení Služby Hybridní pošty prodlužuje o 1 (jeden) pracovní den ▪ Služba Hybridní pošty je považována za řádně provedenou dnem, kdy jsou zhotovené zásilky předány do poštovní přepravy. ▪ Elektronické sestavy o doručení jsou vyhotovovány dávkově, vždy do 48 hodin po vrácení dodejky. Samotné dodejky jsou Správci předávány hromadně, v souladu s dokumentem schválených procesů pro archivaci doručenek a vrácených dopisů s přístupovými údaji – Přístupové údaje k DS-proces archivace.
Reporting:	Součástí služby je i pravidelný měsíční report zahrnující informace o dostupnosti systému.

Režim služby:	9×5

4.7 Dohledové systémy

4.7.1 Bezpečnostní monitoring

Určení služby:	Předmětem poskytované služby je sběr informací o provozních a bezpečnostních činnostech včetně událostí a incidentů vztahujících se k zabezpečení ochrany osobních údajů, zejména typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa činnosti a úspěšnost nebo neúspěšnost činnosti a ochraně získaných informací před neoprávněným čtením nebo změnou.
Parametry služby:	- Hlášení bezpečnostních událostí a incidentů. Termín pro hlášení: dle reakční doby ve smyslu Bezpečnostní politiky ISDS. - Měsíční report - Organizační a procesní napojení na Dohledové centrum eGovernmentu MV a na kontakty pověřenců pro ochranu osobních údajů správce a provozovatele
Reporting:	Součástí služby je i pravidelný měsíční report
Režim služby:	24x7

-

4.7.2 Služby Service Desku

Určení služby:	Předmětem poskytované služby je poskytnutí jednotného kontaktního místa (SpoC – Single Point of Contact) pro Správce a Provozovatele podle definovaných rolí a oprávnění k přístupu.
Parametry služby:	Služba je poskytována komunikačními kanály. (řazení není podle priority využívaného kanálu): ▪ Telefon ○ standardní telefonní kontakt na Service Desk Provozovatele

	○ eskalační telefonní číslo na manažera Service Desku ○ záložní telefonní kontakt na Service Desk Provozovatele (nezávislý na přenosových trasách standardního telefonického kontaktu). ▪ Elektronická pošta ▪ Trouble Ticket Systém (TTS) - aplikace pro evidenci, správu a řešení Incidentů/požadavků, Slouží pro předávání Incidentů/požadavků od Správce k Provozovateli a zpětnou reakci Provozovatele na řešení, průběh a vyřešení případu. Na základě dohodnutých technických parametrů.
Reporting:	Součástí služby je i pravidelný měsíční report zahrnující počty jednotlivých servisních požadavků dle jejich typu a služeb, kterých se požadavky týkají a stavu, v jakých se řešení požadavků/incidentů nachází
Režim služby:	24x7

4.7.3 Služby Call Centra

Určení služby:	Pracoviště Provozovatele, které slouží pro komunikaci (infolinka, ePoradna, email) s uživateli (včetně potenciálních uživatelů a veřejnosti) Datových schránek a k zajištění technické podpory pro uživatele ISDS. Jedná se zejména o: ○ nastavení prohlížeče u uživatele ○ nastavení zabezpečení na straně uživatele – proxy, firewall, antivir, antispam… ○ propojení ISDS pomocí WS se systémy třetích stran (nejčastěji spisových služeb) ○ problematika formátů dat, příloh, ZFO… spolupracujících s ISDS ○ podpora uživatelů Servisního modulu DS ○ zajištění reportingu statistik ticketů uživatelů
Parametry služby:	▪ webový formulář ▪ standardní telefonní kontakt – jedno společné číslo pro veškerou uživatelskou podporu (954 200 200).
Reporting:	Součástí služby je i pravidelný měsíční report zahrnující počty jednotlivých požadavků dle jejich typu a služeb, kterých se požadavky týkají.
Režim služby:	Webový kontakt 24x7, telefonní kontakt 10x5

4.7.3.1 Řešení provozních incidentů

Určení služby:	Předmětem poskytované služby je řešení Incidentů v provozním prostředí ISDS s garantovanou reakční dobou na straně Provozovatele.
Parametry služby:	Kategorizace Incidentů podle dopadu a naléhavosti. Agenda bude vedena v TTS nástroji Provozovatele tak, aby byly případy dostupné pro náhled určených pracovišť Správce.
Reporting:	Součástí služby je i pravidelný měsíční report zahrnující počty jednotlivých Incidentů dle jejich kategorie. Součástí reportu je přehled počtu nahlášených Incidentů za měsíc, počet vyřešených Incidentů v daném měsíci a celkový přehled otevřených Incidentů na konci měsíce. Pro jednotlivé Incidenty report obsahuje údaje dle bodu 2.5.2 přílohy č. 2 smlouvy.
Režim služby:	24x7

4.7.3.2 Řešení provozních problémů

Určení služby:	Předmětem služby je řešení a správa problémů v provozním prostředí IS. Správa problémů (Problem management) se snaží nalézt neznámou hlavní příčinu Incidentů a následně tuto příčinu odstranit.
Parametry služby:	Určení priority problému na základě dopadu, naléhavosti a existence náhradního řešení. Agenda bude vedena v TTS nástroji Provozovatele tak, aby byly případy dostupné pro náhled určených pracovišť Správce.
Reporting:	Součástí služby je i pravidelný měsíční report zahrnující počty jednotlivých problémů dle jejich klasifikace. Součástí reportu je přehled počtu nahlášených problémů za měsíc, počet vyřešených problémů v daném měsíci a celkový přehled otevřených problémů na konci měsíce. Pro jednotlivé problémy report obsahuje údaje dle bodu 2.6.2 přílohy č. 2 Smlouvy.
Režim služby:	9x5

4.7.4 Provoz informačního webu datových schránek

Určení služby:	Předmětem služby je hosting a správa informačního webu datových schránek

Parametry služby:	Zajištění dostupnosti obsahu webu z internetu v režimu 24×7 Údržba obsahu Publikace obsahu schváleného správcem
Režim služby:	24×7

5 Požadavky na technickou infrastrukturu

5.1 Požadavky na zajištění klíčového hospodářství

Správce požaduje, aby Provozovatel zajistil řádné provádění klíčového hospodářství a technickými a organizačními prostředky zajistil ochranu všech šifrovacích klíčů a případného dalšího kryptografického materiálu použitého pro ochranu Datových zpráv spravovaných v ISDS a při šifrování komunikací KDM (Key distribution management).

5.2 Platnost Datových zpráv, dodejek a doručenek

Provozovatel je povinen zajistit, aby dlouhodobá platnost, prověřování autenticity Datových zpráv a způsob podepisování dodejek a doručenek v ISDS byly v souladu s aktuálně platnými prováděcími rozhodnutími Evropské komise, kterými se stanoví specifikace pro formáty zaručených elektronických podpisů a zaručených pečetí uznávaných subjekty veřejného sektoru a návaznými aktuálně platnými technickými normami ETSI.

5.3 Výkonnostní požadavky

Požadované výkonnostní parametry jsou dány limitními parametry, definovanými tabulkou č. 1 v Příloze č.2.

5.4 Požadavky na rozhraní vůči uživateli

Provozovatel je povinen zajistit, aby při uvedení ISDS do Řádného a plného provozu byly vzhled a funkčnost rozhraní vůči uživatelům ISDS shodné se stávajícím rozhraním a splňovaly grafický manuál státní správy.

5.5 Obecné požadavky na technickou infrastrukturu

Objednatel nepřipouští možnost využití cloudového řešení či použití datových center mimo území ČR.

5.6 Definice prostředí

Definice prostředí, ve kterém probíhá provozovávání ISDS:

a) Produkční prostředí ISDS

b) **Neprodukční prostředí ISDS**

- Prostředí předprodukční (PRED)
- Prostředí veřejný test (VT)
- Prostředí vývojové a interní testovací (VITP)

Datové zprávy zaslané v neprodukčním prostředí nejsou platné Datové zprávy. Tyto zprávy nelze zaměnit ani ověřit na Produkčním prostředí. Neprodukční prostředí mohou být výrazně jednodušší v infrastruktuře, nejsou napojena na produkční externí systémy (pokud externí systémy mají testovací verze, mohou být napojena na ně – např. ISZR, Czech POINT, NIA).

K dalším odlišnostem patří:

- Nekomunikuje se s Hybridní poštou, nevytvářejí se dopisy s přístupovými údaji;
- Odlišné napojení na TSA;
- Při vytvoření uživatele se přístupové údaje vrací do WS nebo do Portálu;

- Při vytváření schránek jsou nastaveny některé vlastnosti (např. posílání PDZ) defaultně;
- Při vytváření DS lze zadat duplicitní IČ – vygeneruje se náhradní;
- Lze si libovolně na Portálu „nabíjet“ kredit;
- Lze si zaregistrovat k přihlašování Testovací certifikát certifikační autority PostSignum;
- Neprobíhá indexování safelogů (na DEV ano, ale jen omezeně a ne zabezpečeně);
- Datové schránky pro prostředí VT si může zakládat přihlášený uživatel v produkčním prostředí z klientského portálu ISDS

c) Dohledové systémy

- Bezpečnostní monitoring
- Provozní monitoring
- Externí monitoring dostupnosti a funkčnosti ISDS (nezávislý monitoring)
- TTS

5.7 Produkční prostředí

Provoz produkčního prostředí ISDS musí být zajištěn jako bezodstávkový ve dvou nezávislých geografických clusterech, které budou umístěny ve dvou datových centrech. Datová centra musí splňovat všechny provozní a bezpečnostní parametry a mít platnou certifikaci Tier III nebo auditní zprávu a čestné prohlášení potvrzující soulad s požadavky na certifikaci Tier III. Fyzické prostředí pro umístění produkčních systémů musí mimo jiné splňovat požadavky ZKB a Vyhlášky o KB.

5.7.1 Služby

Určení služby:	Předmětem služby je: • zprovoznění technické infrastruktury dodané Provozovatelem, • napojení externích systémů • provozování a údržba technologické infrastruktury dodané Provozovatelem, • provozování licencovaného SW • vedení historie Releasů a Patchů. a ostatního SW potřebného pro chod ISDS, pro zajištění bezpečného provozu systému ISDS ve dvou nezávislých geografických clusterech. Toto prostředí slouží pro provoz aplikace, splňuje všechny funkční i nefunkční požadavky, tj. výkon, dostupnost, využití povinných služeb, bezpečnost atd. Do produkčního prostředí je nasazena poslední schválená otestovaná stabilní verze licencovaného SW a ostatního SW potřebného pro chod ISDS. Prostředí pracuje s platnými daty. Předmětem služby je dále ▪ konektivita ISDS do sítě internet s dostatečnou kapacitou, Provozovatel přitom zajistí, aby nemohlo dojít k prostupu mezi CMS a internetovou přípojkou. ▪ příprava rozhraní pro připojení do sítě Centrálního místa služeb (CMS) ▪ služby ISDS budou plnohodnotně dostupné protokolem IPv4 i IPv6 ▪ propojení do CMS protokolem IPv4 a IPv6 podle potřeb správce CMS.

Parametry služby:	▪ Dostupnost technologické infrastruktury v aktivních lokalitách – 99,9 %
Reporting:	Součástí služby je i pravidelný měsíční report zahrnující informace o dostupnosti infrastruktury a o míře využití přípojek systému ISDS do sítě CMS prostřednictvím monitoringu portů
Režim služby:	24x7
Připojení do CMS	Správce požaduje realizovat linkou o kapacitě nejméně 1 Gbps
Připojení do Internetu	Správce požaduje realizovat linkou o kapacitě nejméně 10 Gbps
Připojení k TSA	

5.7.2 Instalace a zprovoznění

Provozovatel provede instalaci prvků technické infrastruktury, jejich konfiguraci, implementaci licencovaného SW, napojení externích systémů a veškeré další kroky nezbytné před provedením migrace dat a zahájením Řádného a plného provozu tak, aby ISDS bylo funkční jako celek včetně všech uvedených náležitostí.

5.8 Předprodukční prostředí

Provoz Předprodukčního prostředí musí být umístěn v jednom ze dvou datových center určených pro produkční prostředí.

5.8.1 Služby

Určení služby:	Předmětem služby je provozování: • zprovoznění technické infrastruktury dodané Provozovatelem, • napojení externích systémů • provozování a údržba technologické infrastruktury dodané Provozovatelem, • provozování licencovaného SW a ostatního SW potřebného pro chod ISDS, • • vedení historie Releasů a Patchů Předprodukční prostředí je provozováno v jednom datovém centru a není vyžadována stejně výkonná technická infrastruktura jako u prostředí produkčního. Předprodukční prostředí slouží pro ověření nových verzí aplikace, splňuje všechny funkční i nefunkční požadavky, tj. využití povinných služeb, bezpečnost atd. Jedná se o prostředí se stejnou HW a SW architekturou, funkčně i bezpečnostně identické s prostředím produkčním. Případné konkrétní odlišnosti od produkčního prostředí musí být definovány nejpozději před zahájením nasazení prostředí a zachyceny v Dokumentaci. Na prostředí je nasazena verze určená ke schválení a následnému nasazení na produkční prostředí. Předprodukční prostředí pracuje s testovacími daty. Předmětem služby je dále

	▪ konektivita ISDS do sítě internet s dostatečnou kapacitou. ▪ napojení na externí systémy, které disponují testovacím prostředím.
Parametry služby:	Dostupnost technologické infrastruktury – není stanovena
Režim služby:	24x7
Připojení do Internetu	Správce požaduje realizovat linkou o kapacitě nejméně 1 Gbps

5.8.2 Instalace a zprovoznění

Provozovatel provede instalaci prvků technické infrastruktury, jejich konfiguraci, implementaci licencovaného SW, napojení externích systémů a veškeré další kroky nezbytné před zahájením Řádného a plného provozu.

5.9 Veřejné testovací prostředí

Provoz veřejného testovacího prostředí musí být umístěn v jednom ze dvou datových centrech určených pro produkční prostředí.

5.9.1 Služby

Určení služby:	Předmětem služby je: • zprovoznění technické infrastruktury dodané Provozovatelem, • provozování a údržba technologické infrastruktury dodané Provozovatelem, • provozování licencovaného SW a ostatního SW potřebného pro chod ISDS, • vedení historie Releasů a Patchů. Slouží pro ověření nové verze aplikace pro SW třetích stran. Veřejné testovací prostředí je umístěno v jednom datovém centru a je dostupné na webové adrese dle požadavku Správce.
Parametry služby:	Dostupnost technologické infrastruktury – 97 % - v souladu s definovanými SLA uvedenými v Příloze č. 2.
Reporting:	Součástí služby je i pravidelný měsíční report zahrnující informace o dostupnosti infrastruktury.
Režim služby:	24x7
Připojení do Internetu	Konektivita ISDS do sítě internet s dostatečnou kapacitou

5.9.2 Instalace a zprovoznění

Provozovatel provede instalaci prvků technické infrastruktury, jejich konfiguraci, implementaci licencovaného SW, napojení externích systémů a veškeré další kroky nezbytné před provedením migrace dat a zahájením Rádného a plného provozu.

5.10 Vývojové a interní testovací prostředí

Provoz vývojového a interního testovacího prostředí bude umístěn v datovém centru určeném Provozovatelem.

5.10.1 Služby

Určení služby:	Předmětem služby je: • zprovoznění technické infrastruktury dodané Provozovatelem, • provozování a údržba technologické infrastruktury dodané Provozovatelem, • implementace zdrojových kódů Licencovaného software, vytvoření vývojového a interního testovacího prostředí pro účely Služeb Rozvoje, které zahrnuje vytvoření prostředí vhodného pro: a. editaci a řízení změn zdrojového kódu včetně systému verzování zdrojového kódu ve vhodném SW nástroji s komentářem kódu po dobu platnosti Smlouvy., b. sestavení binárního kódu, c. testování binárních aplikací. • administrace a správa prostředí, • vedení historie Releasů. Slouží pro zajištění úprav a rozvoje Licencovaného software, programátorského testování a vytvoření binárních kódů určených pro předání do veřejného testovacího, předprodukčního a produkčního prostředí ISDS. Vývojové a interní testovací prostředí je provozováno v datovém centru určeném Provozovatelem. Předmětem služby je dále ▪ příprava bezpečného rozhraní pro konektivitu vývojového prostředí do sítě internet. Zajištění konektivity do Internetu není předmětem služby
Parametry služby:	Dostupnost technologické infrastruktury ve vybrané lokalitě Provozovatele – není stanovena
Režim služby:	24x7

Provozovatel umožní Správci přístup ke kompletní historii Releasů.

Vývojové prostředí musí splňovat požadavky stanovené ZKB na vývojové prostředí systémů kritické infrastruktury.

5.10.2 Instalace a zprovoznění

Provozovatel provede instalaci prvků technické infrastruktury, jejich konfiguraci, příprava bezpečného rozhraní pro konektivitu vývojového prostředí do sítě Internet a veškeré další kroky nezbytné před provedením migrace stávajícího vývojového prostředí a zahájením řádného a plného provozu.

5.11 Dohledové systémy

5.11.1 Bezpečnostní monitoring

5.11.1.1 Instalace a zprovoznění bezpečnostního monitoringu pro ISDS

Provozovatel provede instalaci prvků technické infrastruktury, jejich konfiguraci a veškeré další kroky nezbytné před zahájením Řádného a plného provozu.

5.11.2 Provozní monitoring

5.11.2.1 Instalace a zprovoznění produkčního prostředí ISDS

Provozovatel provede instalaci prvků technické infrastruktury, jejich konfiguraci a veškeré kroky nezbytné před provedením migrace dat a zahájením Řádného a plného provozu.

5.11.2.2 Instalace a zprovoznění produkčního prostředí ISDS

Provozovatel poskytne veškerou nezbytnou technickou infrastrukturu a zajistí umístění nezávislé na požadovaných datových centrech, provede instalaci prvků technické infrastruktury, jejich konfiguraci a veškeré další kroky nezbytné před zahájením Řádného a plného provozu.

6 Požadavky na testování ISDS

6.1 Testy ISDS

Provozovatel navrhne postup testování, který bude obsahovat – Cíle testování, Seznam plánovaných oblastí k testování, Kategorie testů, Požadavky na testovací data, harmonogram plánovaných testů, a předloží jej Správci k projednání. Povinností Provozovatele je zapracovat případné připomínky Správce. Správce schválí postup testování. Provozovatel připraví vše potřebné dle postupu testování, následně ve spolupráci se Správcem provede v plánovaných termínech příslušné testy. Výstupem testování budou průkazné protokoly dokumentující průběh a výsledky testů.

Testování Provozovatel navrhne pro veřejné testovací prostředí a produkční prostředí.

Provozovatel provede testování dle schváleného postupu testování a umožní účast Správce při provádění testů.

6.1.1 Kritéria pro akceptaci testů

Kategorie	Stav akceptace	Popis kritérií
A	Neakceptováno	Kritická vada nebo kombinace níže kategorizovaných vad funkčnosti k termínu provedení Migrace dat do produkčního prostředí – nesplnění zadání dle Smlouvy, nebo vada, která zásadně ovlivňuje klíčovou funkci ISDS, nebo Koncoví uživatelé nemají ke službám ISDS přístup. Ve svých důsledcích může Správci způsobit velké finanční nebo jiné škody.
B	Neakceptováno do doby odstranění vady	Kritická vada nebo kombinace níže kategorizovaných vad funkčnosti – nesplnění zadání dle Smlouvy, nebo vada, která zásadně ovlivňuje klíčovou funkci ISDS, nebo Koncoví uživatelé nemají ke službám ISDS přístup. Ve svých důsledcích může Správci způsobit velké finanční nebo jiné škody.

C	Akceptováno s výhradou, a požadavkem na odstranění	Závažná vada funkčnosti – odstranitelná vada, která zásadně neovlivňuje klíčovou funkci ISDS, neomezuje běžný provoz ISDS, nebo je zasažena nepříliš významná část funkcionality ISDS. Vada, která nebyla zařazena ani mezi vadu kategorie A a B, která nebrání užívání ISDS, anebo má zcela minimální vliv na řádné užívání nebo funkčnost ISDS.
D	Akceptováno bez výhrad	

7 Požadavky v oblasti bezpečnosti

7.1 Legislativní vymezení

Provozovatel realizuje opatření, která vyplývají z požadavků ZEU, Vyhlášky, ZKB, VoKB, ZISVS a ZOOÚ.

7.2 Požadavky na soulad se Zákonem o kybernetické bezpečnosti

Provozovatel je povinen realizovat opatření nutná k zajištění souladu ISDS s požadavky ZKB a ostatních právních předpisů o kybernetické bezpečnosti. Jedná se především o:

1. **Technická opatření** požadovaná ZKB, která musí být zvolena a implementována s ohledem na architekturu a požadované technické provedení ISDS:
    - fyzická bezpečnost dle §17 vyhlášky č. 82/2018,
    - nástroj pro ochranu integrity komunikačních sítí dle §18 vyhlášky č.82/2018,
    - nástroj pro ověřování identity uživatelů dle §19 vyhlášky č. 82/2018,
    - nástroj pro řízení přístupových oprávnění dle §20 vyhlášky č.82/2018,
    - nástroj pro ochranu před škodlivým kódem dle §21 vyhlášky č. 82/2018,
    - nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů dle §22 vyhlášky č. 82/2018,
    - nástroj pro detekci kybernetických bezpečnostních událostí dle §23 vyhlášky č. 82/2018,
    - nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí dle §24 vyhlášky č. 82/2018,
    - aplikační bezpečnost dle §25 vyhlášky č. 82/2018,
    - kryptografické prostředky dle §26 vyhlášky č. 82/2018,
    - nástroj pro zajišťování úrovně dostupnosti dle §27 vyhlášky č. 82/2018.
2. **Organizační opatření** požadovaná ZKB, která musí být navržena, zavedena a prováděna s ohledem na model provozování ISDS:
    - systém řízení bezpečnosti informací dle §3 vyhlášky č. 82/2018,
    - řízení aktiv dle §4 vyhlášky č. 82/2018,

- řízení rizik dle §5 vyhlášky č. 82/2018,
- organizační bezpečnost dle §6 vyhlášky č. 82/2018, určení manažera a architekta kybernetické bezpečnosti,
- bezpečnostní role dle §7 vyhlášky č. 82/2018
- řízení dodavatelů dle §8 vyhlášky č. 82/2018,
- bezpečnosti lidských zdrojů dle §9 vyhlášky č. 82/2018,
- řízení provozu a komunikací dle §10 vyhlášky č. 82/2018,
- řízení změn dle §11 vyhlášky č. 82/2018,
- řízení přístupu dle §12 vyhlášky č. 82/2018
- akvizice, vývoj a údržba dle §13 vyhlášky č. 82/2018,
- zvládání kybernetických bezpečnostních událostí a incidentů dle §14 vyhlášky č. 82/2018,
- řízení kontinuity činností dle §15 vyhlášky č. 82/2018
- audit kybernetické bezpečnosti dle §16 vyhlášky č. 82/2018.

V případě změny právních předpisů či jiné závazné dokumentace v oblasti kybernetické bezpečnosti je Provozovatel povinen navrhnout a po schválení Správcem realizovat potřebná opatření v souladu s příslušnými právními předpisy a oprávněnými požadavky Správce. Pokud budou tato opatření znamenat změny ISDS definované touto Smlouvou v části Služeb Rozvoje, budou řešeny v rámci Služeb Rozvoje.

7.3 Bezpečnostní pravidla nakládání s informacemi

Obě strany jsou povinny při nakládání s **Dokumentací vytvořenou v souvislosti s ISDS, zdrojovými kódy Licencovaného software** a **zdrojovými kódy Software vytvořeného Poddodavatelem** (dále jen „informace“) dodržovat bezpečnostní pravidla, která odpovídají klasifikaci dokumentace dle předložené tabulky Klasifikace informací.

V případě, že některá část Dokumentace ISDS podléhá klasifikaci stupně utajení dle Zákona 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, postupuje se v tomto případě v souladu se zněním ustanovení tohoto zákona v platném znění.

7.3.1 Klasifikace informací

Na základě významu a povahy je informace zařazena (klasifikována) do jedné z následujících kategorií, které mohou být dále členěny dle platné bezpečnostní politiky. Zařazení do odpovídající kategorie navrhuje zpracovatel předávaných informací.

	Kategorie	**Označení informace** (kategorizační znak)	**Základní popis** (Zpracování a manipulace s informací příslušné kategorie se řídí níže uvedenými předpisy.)

CHRÁNĚNÉ INFORMACE	Citlivá informace	CITLIVÉ („CI“)	**Definice:** jsou určeny pouze pro omezený okruh osob. Jedná se např. o informace obsahující osobní údaje nebo jiné údaje definované ZOOÚ. Dále se může jednat o informace určené výhradně pro adresáta, kde okruh osob stanovuje vlastník informace. Jedná se o informace, jejichž zneužití může vést k poškození nebo ohrožení zájmů Objednatele.
	Obchodní tajemství	OBCHODNÍ TAJEMSTVÍ („OBT“)	**Definice:** Jedná se zejména o strategické informace a rozhodnutí, koncepce, údaje o zaměstnancích, obchodních vztazích (smlouvy), cenová ujednání, ekonomické, obchodní a marketingové analýzy, souhrnné přehledy a zprávy, speciální know-how, auditní a obdobné zprávy, projekty, bezpečnostní údaje.
VEŘEJNÁ INFORMACE	Veřejná informace	Bez označení	Kategorie veřejná informace je určená pro pracovníky Objednatele.

7.3.2 Zpracovávání informací

1) Na základě klasifikace dané informace, tj. důležitosti její ochrany před nepovolanými osobami, jsou dokumenty označovány podle výše uvedené tabulky Klasifikace informací a zpracovávány podle následujících pravidel.
2) Ústní informace je považována za dokumentaci pouze v případě, je-li o něm na místě pořízen písemný záznam. Záznam obsahuje datum a místo podání, obsah podání a je podepsán jak osobou, která tento záznam pořídila, tak podávající osobou. S tímto záznamem je dále nakládáno jako s dokumentem, který je povinně evidován v projektové knihovně.
3) Manipulace s chráněnými informacemi kategorie „OBT” (Obchodní tajemství) a „CI“ (Citlivé informace) je prováděna dle následujících pravidel:
    - Informace jsou zpracovávány na prostřednictvím Objednatelem schválených prostředků.
    - Informace jsou distribuovány prostřednictvím zabezpečených Objednatelem schválených prostředků.
    - Informace jsou zpřístupněny pouze osobám uvedeným v Objednatelem schváleném distribučním seznamu a jejich převzetí je potvrzeno podpisem přejímající a předávající osoby. Informace nesmí být dále poskytovány mimo tento seznam zpřístupněny.
    - Podrobná pravidla zpracování, označování, ukládání a nakládání s dokumentací budou uvedena v Základním dokumentu projektu.
4) Manipulace s dokumenty obsahujícími osobní údaje se vedle stanovených postupů pro nakládání s chráněnými informacemi řídí dále požadavky dle ZOOU a GDPR.
5) Manipulace s obyčejnými dokumenty bez označení se řídí pravidly stanovenými projektovou dokumentací.

7.3.3 Ukládání informací

1) Ukládání dokumentů se řídí následujícími pravidly:
    - Projektová dokumentace je ukládána v projektové knihovně určené Objednatelem.

- Ostatní dokumentace vzniklá v rámci plnění Smlouvy je ukládána v projektové knihovně určené Objednatelem.

7.3.4 Přístup k informacím

1) Přístup k Chráněným informacím může být umožněn vždy pouze oprávněným osobám.
2) Přístup k Veřejným informacím není omezen.
3) Přístup k Chráněným informacím – má vždy vlastník informace. Další konkrétní přístupová oprávnění k Chráněným informacím jsou stanovována vlastníkem informace.

7.4 Zajištění podmínek a součinnosti při auditu kybernetické bezpečnosti

1. Provozovatel zajistí, aby testovací (auditní) Datové schránky nastavené a spravované v produkčním prostředí pro potřeby auditu byly:
    a. typu FO, PFO, PO, OVM,
    b. přístupné po dobu provádění auditu auditorovi, kterého určí Správce a za tímto účelem mu předá bezpečným způsobem příslušné přihlašovací údaje,
    c. po ukončení auditu budou příslušné přihlašovací údaje k testovacím (auditním) Datovým schránkám změněny.
2. Provozovatel zřídí ve veřejném testovacím prostředí Datové schrány základních typů (FO, PFO, PO, OVM) a nastaví příslušné přístupová údaje pro držitele těchto DS, které předá auditorovi.
3. Provozovatel zajistí, aby v době provádění auditu byly ve veřejném testovacím prostředí ISDS implementovány a řádně nastaveny všechny bezpečnostní funkce stejně, jako ve verzi produkčního prostředí, ke které je prováděn bezpečnostní audit.
4. Provozovatel umožní auditorovi v době provádění auditu provést prověrku konfigurací HW, základního a generického SW, síťových prvků, datových linek, Licencovaného software a Software vytvořeného Provozovatelem (dále jen prověrky konfigurací), které tvoří produkční prostředí ISDS a při tom mu poskytl potřebnou součinnost, která spočívá v následujícím:
    a. poskytnutí veškeré interní Dokumentace skutečného provedení ISDS.
    b. ověření, že nástroje, postupy a procedury navržené auditorem k provedení prověrek konfigurací nemohou narušit bezpečnost produkčního prostředí ISDS a způsobit jeho nedostupnost na dobu delší, než je plánovaná doba na provedení prověrky konfigurací.
    c. schválení, že je možné použít nástroje, postupy a procedury navržené k provedení prověrek konfigurací.
    d. za asistence auditora spustí nástroje a provede postupy a procedury navržené a schválené k provedení prověrek konfigurací.
    e. zabezpečí data, která vznikla během nástrojů a provedením postupů a procedur navržených a schválených k provedení prověrek konfigurací. Zabezpečení dat spočívá v
        i. vytvoření otisků pomocí kryptografických hash funkcí ke každému vzniklému datovému souboru,
        ii. ověření, že vzniklé datové soubory mají obsah, který odpovídá vytvořeným otiskům,
        iii. uložení datových souboru a jejich otisků na výměnné datové medium (DVD),
        iv. předání otisků auditorovi.
    f. provede sanitaci dat, která vznikla během nástrojů a provedením postupů a procedur navržených a schválených k provedení prověrek konfigurací. Sanitizace spočívá v odstranění všech osobních údajů z těchto dat. Dále vytvoří otisky pomocí kryptografických hash funkcí ke každému vzniklému sanitizovanému datovému

souboru. Soubory společně s otisky umístí na výměnné datové medium (DVD) a jeho kopii předají auditorovi.

g. Pokud auditor v průběhu vyhodnocení předaných dat vyjádří odůvodněnou pochybnost o provedené sanitizaci dat, provede pověřený zástupce Provozovatele a auditora v prostředí Provozovatele zkoušku, ve které použijí příslušné původní datové soubory, příslušné sanitizované soubory, jejich integritu ověří pomocí dříve vytvořených otisků. Zkouška prověří, zda sanitizace byla provedena řádně či nikoliv. V případě negativního výsledku se provede nová vytvoření sanitizovaných dat a jejich předání auditorovi.
h. Provozovatel je povinen se seznámit s vybranými výsledky prověrky konfigurací a vyjádřit se k nim.
i. Provozovatel je povinen na pokyn Správce navrhnout, jakým způsobem odstraní prověrkou zjištěné nedostatky v konfiguraci ISDS.

- Provozovatel umožní auditorovi provést externí a interní penetrační testy produkčního prostředí ISDS a při tom mu poskytne potřebnou součinnost, která spočívá v následujícím:
  a. poskytnutí aktuální Dokumentaci vnitřní sítě ISDS
  b. zajištění účasti na připomínkování plánu provedení externích a interních penetračních testů
  c. předání auditorovi aktuálních a úplných informací o adresách (rozsazích adres) vstupních bodů bezpečnostního perimetru ISDS, přes které budou vedeny externí penetrační testy
  d. předání auditorovi kompletních informací o adresách (rozsazích adres) ve vnitřních sítích, přes které budou vedeny interní penetrační testy, a o fyzických portech na zařízeních interní sítě, kde mohou být zapojena zařízení, ze kterých budou prováděny interní penetrační testy.
  e. Provozovatel zajistí v průběhu penetračních testů zvýšené monitorování kybernetických bezpečnostních událostí a incidentů a v případě, že zjistí vznik závažného nebo velmi závažného kybernetického incidentu, tak informuje neprodleně Správce a auditora. Auditor neprodleně pozastaví provádění penetračních testů do doby, kdy se rozhodne o jejich pokračování.
  f. Provozovatel zajistí v průběhu penetračních testů zvýšené monitorování provozních událostí a mezních stavů a v případě, že zjistí překročení nastavených mezních hodnot, informuje Správce a auditora. Auditor neprodleně pozastaví provádění penetračních testů do doby, kdy se rozhodne o jejich pokračování.
  g. Provozovatel je povinen se seznámit s vybranými výsledky penetračních testů a vyjádřit se k nim.
  h. Provozovatel je povinen na pokyn Správce navrhnout, jakým způsobem odstraní penetračním testováním zjištěné nedostatky v zabezpečení ISDS a na vlastní náklady je odstranit.

8 Požadavky v oblasti ochrany osobních údajů

8.1 Postupy sloužící k ochraně osobních údajů a informací

Správce je správcem osobních údajů a Provozovatel je zpracovatelem osobních údajů ve smyslu Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně údajů „GDPR“) a Zákona č.110/2019 Sb., o zpracování

osobních údajů („ZOOU“). Smluvní strany na základě uzavřené Smlouvy nastavily níže uvedené postupy sloužící k ochraně osobních údajů a informací, které jsou v bližších podrobnostech specifikovány touto přílohou Smlouvy.

1) Kontrola osobních údajů při založení datové schránky včetně autentizačních služeb
2) Správa přístupu k datové schránce, zabezpečený tisk a doručování přístupových údajů k datové schránce
3) Logování informací v bezpečném logu
4) Zajištění informovanosti uživatelů ISDS o zpracování osobních údajů ve smyslu čl. 15 GDPR pomocí exportu dat a zajištění výkonu práv uživatelů jako subjektů údajů dle GDPR
5) Ochrana osobních údajů prostřednictvím bezpečnostního monitoringu
6) Ochrana osobních údajů v rámci nastavených bezpečnostních pravidel pro nakládání s chráněnými informacemi

8.2 Záznamy o činnostech zpracování ve smyslu čl. 30 GDPR

Správce vede záznamy o zpracování osobních údajů v rámci ISDS v souladu s čl. 30 odst. 1 GDPR

Provozovatel vede záznamy o zpracování osobních údajů v rámci ISDS v souladu s čl. 30 odst. 2 GDPR

8.3 Postupy sloužící ke zjištění, zda nedošlo ke kompromitaci informací (například ke ztrátě nebo modifikaci dat) a Systém hlášení, upozorňování a vyšetřování mimořádných událostí a případů prolomení bezpečnosti.

Pro oblast zajištění ochrany osobních údajů se použijí postupy nastavené pro komunikaci bezpečnostních událostí a incidentů v rámci postupů Dohledového centra eGovermentu MV. V případě událostí a incidentů spočívajících v porušení zabezpečení ochrany osobních údajů bude o takových událostech či incidentech předána neprodleně informace pověřencům pro ochranu osobních údajů obou smluvních stran.

Ohlášení adresované pověřencům pro ochranu osobních údajů musí mít písemnou formu a musí obsahovat:

a) Popis povahy daného porušení zabezpečení osobních údajů. A to včetně kategorií a počtu dotčených subjektů údajů a kategorií a počtu dotčených záznamů subjektů údajů, pokud je to možné.;
b) Popis pravděpodobných důsledků, které porušení zabezpečení osobních údajů představuje, včetně předběžného posouzení, zda může mít za následek riziko pro práva a svobody fyzických osob;
c) Popis nápravných opatření, která byla přijata nebo navržena k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.;

V rámci řešení porušení ochrany osobních údajů musí být vždy provedeno řešení, navržena opatření pro eliminaci dopadu porušení ochrany osobních údajů a přijata organizačně technická opatření zamezující vzniku identických nebo podobných porušení ochrany osobních údajů (pokud je to možné).

Pokud ze zjištěných skutečností vyplývá, že s vysokou pravděpodobností došlo k porušení zabezpečení osobních údajů, které má za následek riziko pro práva a svobody fyzických osob, ohlásí pověřenec správce tuto skutečnost do 72 hodin Úřadu pro ochranu osobních údajů.

Podle míry závažnosti takového případu, resp. je-li pravděpodobné, že porušení bude mít za následek vysoké riziko pro práva a svobody fyzických osob, je vyžadováno ohlášení tohoto případu též dotčeným subjektům údajů ze strany správce.

8.4 Integrita a dostupnost informací

Integrita a dostupnost informací je zajišťována prostřednictvím bezpečnostních pravidel dle této přílohy Smlouvy a dle schválené Bezpečnostní politiky ISDS.

8.5 Konkrétní smluvní závazky externích subjektů

Pravidla pro využití dalších zpracovatelů osobních údajů stanoví Smlouva. Provozovatel je povinen zajistit, aby byl každý jím využívaný subzpracovatel osobních údajů vázán požadavky vyplývajícími ze Smlouvy a související smluvní dokumentace a aby zajišťoval nezbytnou součinnost k výkonu činností souvisejících s ochranou a zpracováním osobních údajů.

Za smluvní závazky případných externích subjektů zasmluvněných ze strany správce je odpovědný správce.

8.6 Právo monitorovat a zakázat aktivity uživatele

Právo monitorovat a zakázat aktivity uživatele je zajišťováno prostřednictvím bezpečnostních pravidel dle této přílohy Smlouvy a dle schválené Bezpečnostní politiky ISDS.

8.7 Školení uživatelů a správců v metodách, postupech a v bezpečnosti

Smluvní strany zajistí, aby pracovníci zapojení do zpracování osobních údajů byli v potřebné míře proškolení v metodách, postupech a v bezpečnosti dle požadavků vyplývajících ze smluvní dokumentace a právních předpisů vztahujících se k ochraně osobních údajů a k zajištění kybernetické bezpečnosti.

8.8 Opatření k zajištění ochrany před škodlivým programovým vybavením

Opatření k zajištění ochrany před škodlivým programovým vybavením je zajišťováno prostřednictvím bezpečnostních pravidel dle této přílohy Smlouvy a dle schválené Bezpečnostní politiky ISDS.

9 Náležitosti měsíční zprávy o provozu

Provozovatel předkládá vždy do 15. dne v měsíci pravidelnou měsíční zprávu o provozu za uplynulý měsíc (měřené období), která obsahuje požadované údaje reportingu uvedené v Příloze č. 2 a dále následující informace:

- Limitní parametry (dle Přílohy č. 2) – časový průběh hodnot limitních parametrů (mimo vyhrazenou dobu), průběh maximálních, průměrných a minimálních hodnot.
- Časové průběhy počtu stahování Datových zpráv (DZ/min, průběh maximálních, průměrných a minimálních hodnot)
- Výsledky získávání časového razítka – přehled dostupnosti služby zajištění časových razítek

- Seznam jednotlivých případů zrušení DS, u kterých nebyla splněna garantovaná doba vyřízení s uvedením skutečného času zrušení DS
- Informace Change managementu a Release managementu
- Rozvoj ISDS – rozpis počtu MD vynaložených v daném měsíci a vztažených ke konkrétním změnovým požadavkům Služeb rozvoje ISDS
- Plánované výluky
    - časový plán výluk měsíc dopředu
    - požadavky na součinnost Správce
    - naplnění časového plánu výluk za uplynulý měsíc
    - odstranění chyb a problémů z minulého období,
- Bezpečnostní incidenty – Informace o průběžném bezpečnostním dohledu a prověřovaných bezpečnostních událostech, rekapitulaci řešených bezpečnostních událostí a požadavků, informaci o dalších provedených kontrolách.
- Provozní statistiky pro Správce a Provozovatele ISDS – podoba statistik bude formou tabulky, která bude upřesněna dohodou mezi Provozovatelem a Správcem
- Systémové požadavky – Podporované operační systémy a prohlížeče, testované prohlížeče

10 Požadavky na Dokumentaci

Dokumentací se rozumí veškeré písemnosti, ať v listinné nebo elektronické podobě, včetně podkladových materiálů, předané Správcem nebo vytvořené či užívané Provozovatelem pro poskytování Služeb nebo realizace Dodávek dle této Smlouvy, obsahující popis ISDS, jeho fungování, administrace, provozu, funkcionalit a jednotlivých komponent včetně jejich vzájemných vztahů.

Povinností Provozovatele je při jakýchkoli změnách ISDS nebo na výzvu Správce Dokumentaci **aktualizovat v celé její struktuře** a v souladu požadavky uvedenými ve Smlouvě.

Povinností Provozovatele je zpřístupnit Správci Dokumentaci v souladu s požadavky uvedenými ve Smlouvě.

Jedná se zejména nikoliv však výlučně o následující typy Dokumentace:

Neveřejná dokumentace

1. Projektová Dokumentace

- Dokumentace o nastavení projektu a jeho průběžná kontrola a doplňování;
- harmonogram projektu a jeho fází, průběžná kontrola a revize;
- registr rizik a jejich řízení;
- Dokumentace rolí v projektu a jejich obsazení, průběžná kontrola a revize;
- další součásti projektové Dokumentace související s převzetím a rozvojem ISDS;

  Povinností Provozovatele je, vytvořit a udržovat projektovou Dokumentaci ve struktuře, která je běžně doporučována uznávanými metodikami např. Prince2 respektive PMBOK 5th edition po celou dobu trvání smluvního vztahu.

2. Technická Dokumentace

- Dokumentaci obsahující funkční popis systému popisující procesní a logické vztahy jednotlivých částí ISDS a jejich napojení na externí systémy, architekturu aplikace ISDS popisující jednotlivé vrstvy systému ISDS, technické napojení na externí systémy, technickou architekturu popisující ISDS na úrovni hardware a infrastruktury a bezpečnostní architekturu popisující zabezpečení systému a jeho nastavení jako celku; doplněnou základní Dokumentací, která musí odpovídat architektonickým principům Archimate dle metodiky MV (hlavní komponenty technologického celku, vazby mezi komponentami technologického celku na úrovni fyzické, logické, datové, propojení na externí systémy a popis komunikace s externími systémy);
- Dokumentaci potřebnou pro vybudování, sestavení a zprovoznění jednotlivých částí systému ISDS i systému ISDS jako funkčního celku, zahrnující všechna prostředí ISDS, včetně Migrace dat;
- administrátorskou Dokumentaci (konfigurace jednotlivých prvků TI, komplexní popis všech užitých analytických a monitorovacích nástrojů a jejich konfigurace),
- datový popis infrastruktury – CMDB
- provozní deník, popisu logické a fyzické architektury);
- zálohovací plány a postupy
- Dokumentaci k zajištění kontinuity provozu vč. plánů obnovy ISDS (postupy pro obnovení dat včetně konfigurací do původního provozního stavu)
- katalog periodických činnosti daných jednotlivými KL.

3. Programátorská Dokumentace
    - popis datových struktur a návrh databází
    - Dokumentaci všech zdrojových kódů Licencovaného software a Software vytvořeného Provozovatelem, včetně seznamu všech předávaných aplikací, obsahujícího m.j. odkazy na zdrojové kódy a na předpisy pro sestavení aplikací a jejich částí, -
    - seznamu, popisu a verzí Software třetích stran,
    - seznamu veškerých licencí, použitých v ISDS, v členění dle čl. 6.19 Smlouvy na:
        - zdrojový kód všech pro ISDS vyvinutých částí a komponent systému a použité Open source aplikace a knihovny
        - použitý komerční Software, který zajistí Provozovatel
    - seznamy použitých softwarových komponent a standardního SW včetně jejich verzí (zejména operační systémy, aplikace, frameworky, runtime prostředí),
    - všechny programové kódy, vzniklé jako předmět dodávky, kromě Standardního SW
    - všechny programové kódy, vzniklé nebo změněné v průběhu platnosti Smlouvy
    - konfigurace a artefakty, nezbytné pro sestavení programových komponent z programových kódů

4. Dokumentace sloužící k testování systému obsahující metodiku testování pro funkční, integrační zátěžové, performance a bezpečnostní testy, testovací scénáře a testovací data;
5. Bezpečnostní Dokumentaci odpovídající požadavkům ZKB na bezpečnostní Dokumentaci systému kritické infrastruktury. Výstupy budou ve formátu kompatibilním se standardními formáty MS Office.

6. Uživatelská Dokumentace k servisnímu modulu a dalším částem systému

Veřejná Dokumentace:

1. Provozní řád ISDS
2. Veřejné formuláře žádostí o zřízení Datové schránky případně další uživatelské formuláře, které mohou být nedílnou součástí provozu ISDS
3. Veřejná uživatelská Dokumentace nebo Dokumentace určená ke školení uživatelů.

Režimová Dokumentace

Povinností Stran je, vytvořit a udržovat režimovou Dokumentaci, která podléhá ochraně dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, se stupněm utajení Vyhrazené a Důvěrné.