

OBSAH TECHNICKÉHO ZADÁNÍ

1. Úvod k technickému zadání

- Popis vize regionálního datového prostoru
- Strategický význam řešení pro zadavatele a jeho partnery
- Vztah k evropským iniciativám (Data Spaces Support Centre, GAIA-X, IDSA, iSHARE, EDWG)

2. Předmět plnění

- Návrh a realizace technologické architektury datového prostoru.
- Zajištění souladu s referenčním modelem architektury IDSA (IDS-RAM).
- Slanění se společným evropským rámcem důvěryhodnosti datového prostoru (např. GAIA-X, iSHARE, ...)
- Součástí je dodání základních komponent (např. konektory, služba identity, katalogy metadat), jejich konfigurace a provozní podpora včetně dokumentace.

3. Funkční požadavky

- Možnost federovaného a decentralizovaného provozu
- Správa přístupových práv a smluvních podmínek (data usage policies)
- Možnost připojení externích účastníků (např. obce, IZS, soukromí provozovatelé)
- Auditovatelnost a sledovatelnost přenosů dat

4. Technické požadavky

- Kompatibilita s otevřenými standardy (IDS, GAIA-X, W3C, ISO/IEC, EDWG)
- Použitelnost v hybridním (cloud/on-premise) prostředí
- Podpora evropské identity (EUDI Wallet, eIDAS 2.0)
- Prokazatelné zajištění kybernetické bezpečnosti (ENISA, NIS2 ready)

5. Požadavky na interoperabilitu

- Interoperabilita s jinými evropskými datovými prostory (např. mobility, tourism, health)
- Podpora pro standardizované datové modely (např. DCAT-AP, NGSI-LD)
- Export dat do externích analytických nástrojů a BI systémů

6. Organizační a implementační požadavky

- Fáze projektu (analýza, návrh, vývoj, pilotní provoz, dokumentace)

7. Slovník pojmů k datovému prostoru

1. Úvod k technickému zadání

Krajský úřad Královéhradeckého kraje (dále jen „zadavatel“) připravuje zadání veřejné zakázky na výběr dodavatele technologie a služeb nutných pro zprovoznění **datového prostoru** v souladu s referenční architekturou a souborem pravidel IDSA a společnými evropskými rámci důvěryhodnosti datového prostoru (např. GAIA-X, iSHARE, ...). Tento datový prostor bude sloužit jako základ pro **interoperabilní, bezpečné a důvěryhodné sdílení dat** mezi různými aktéry veřejné správy, soukromého sektoru a výzkumných organizací v oblasti cestovního ruchu a s ním spojených problematik.

Tento dokument slouží jako **technické zadání**, které vymezuje rámcové požadavky zadavatele na předmět plnění, a zároveň stanovuje strukturu, ve které budou v dalším průběhu jednání doplněny a upřesněny konkrétní specifikace, harmonogram a požadavky na interoperabilitu, škálovatelnost a bezpečnost.

2. Předmět plnění

Předmětem veřejné zakázky je návrh, dodání a implementace **datového prostoru** (data space), který bude odpovídat technickým a organizačním principům vymezeným ve standardech:

- referenční architektura a soubor pravidel IDSA (**IDS-RAM, IDS Rulebook**) a společnými evropskými rámci důvěryhodnosti datového prostoru (např. GAIA-X, iSHARE, ...).
- specifikace zveřejnění Data Spaces Support Centre (**DSSC**)

Cílem je umožnit **bezpečné, suverénní, auditovatelné a smluvně řízené sdílení dat** mezi různými typy účastníků (např. veřejná správa, samospráva, IZS, výzkumné organizace, firmy) v rámci jednoho federovaného ekosystému.

2.1. Součásti plnění

Plnění se skládá z následujících hlavních prvků:

a. Dodání komponent datového prostoru

Dodavatel navrhne, implementuje a zprovozní níže uvedenou sadu softwarových komponent, tvořících základní infrastrukturu datového prostoru v souladu s referenční architekturou a souborem pravidel IDSA a společnými evropskými rámci důvěryhodnosti datového prostoru (např. GAIA-X, iSHARE, ...):

komponenta	popis funkce
Konektor (např. IDS, EDC, ...)	Umožňuje nahrávání, sdílení a přijímání dat mezi účastníky datového prostoru při dodržení zásad datové suverenity a kontrolovaného přístupu.
Moduly identity a důvěry	Spravuje služby ověřování a identit v souladu se společným evropským rámcem důvěryhodnosti datového prostoru (např. GAIA-X, iSHARE, ...).
Registr účastníků	Udržuje záznamy o registrovaných účastnících datového prostoru, včetně metadat o jejich schopnostech a oprávněních.
Katalog metadat	Uspodňuje přístup k metadatům (datovým katalogům) zveřejněným účastníky.
Auditní a monitorovací komponenty (Clearing House)	Umožňuje nezávislý audit a záznam transakcí v datovém prostoru (např. protokolování datových toků, zajištění důvěryhodnosti).
Správce zásad používání	Spravuje a prosazuje smluvní podmínky používání dat.

b. Integrace datových sad a napojení vybraných účastníků

Zhotovitel provede následující úkoly:

- Integruje nejméně dva poskytovatele pilotních dat (např. veřejný subjekt, výzkumnou instituci).
- Připojit jednoho až dva spotřebitele dat, kteří budou data využívat v konkrétním scénáři aplikace.
- Implementovat katalog dat (např. ve formátu DCAT-AP, NGSI-LD nebo RDF/SPARQL endpoint).

c. Uvedení do pilotního provozu a podpora testování

Dodavatel zajistí:

- Instalaci a konfiguraci komponent v prostředí zadavatele (cloudovém, hybridním nebo on-premise podle dohody).

- Testování interoperability se stávajícími evropskými službami (např. GAIA-X Federation Services, DSSC Sandbox).
- školení správců systému a vybraných uživatelů na obsluhu komponent, správu přístupových práv, publikaci dat a základní správu služeb,
- zajištění přenosu know-how potřebného pro samostatný provoz, administraci a budoucí rozšiřování datového prostoru,

d. Technická a metodická dokumentace

Výstupem bude soubor dokumentů popisujících:

- architekturu řešení (včetně komponent, rozhraní API a integrací)
- bezpečností a provozní konfigurace
- Uživatelské příručky pro správce i účastníky
- Metodiku nástupu nových partnerů.

e. Požadavky na provoz a podporu DSaaS (Data Space jako služba)

Tato část dokumentu popisuje předběžné požadavky a očekávání na službu Data Space jako služba (DSaaS). Tyto požadavky slouží jako základ pro vyjednávání a následné upřesnění zadávací dokumentace. Dodavatelé jsou vyzváni, aby tyto požadavky posoudili z hlediska proveditelnosti, úrovně služeb a navrhli případná vylepšení ve formě všeobecných obchodních podmínek..

1. Dostupnost služby (záruka provozu)

Poskytovatel DSaaS musí zaručit minimální dostupnost služby 99,5 % za kalendářní měsíc, s výjimkou plánovaných odstávek.

- Plánované odstávky musí být oznámeny minimálně 5 pracovních dnů předem.
- Odstávky musí být plánovány mimo pracovní dobu (pondělí–pátek, 08:00–18:00 CET), pokud není dohodnuto jinak.
- V případě nedodržení dostupnosti budou uplatněny kompenzace nebo sankce podle SLA.

2. Helpdesk a technická podpora

Poskytovatel musí zajistit přístup k vícejazyčnému helpdesku (angličtina povinná) s následujícími úrovněmi podpory:

2.1 Řízení incidentů a problémů

Poskytovatel musí:

- Udržovat systém pro správu incidentů přístupný zadavateli.

- Poskytovat pravidelné aktualizace o otevřených incidentech a závěrečnou zprávu pro každý incident úrovně P1
- Zavést řízení problémů včetně analýzy příčin a opatření proti opakování.

2.2 Monitoring a reportování

Bude zajištěn monitoring klíčových služeb v reálném čase s částečným přístupem pro zadavatele (např. status dashboard).

Reporty budou obsahovat:

- Statistiku dostupnosti
- Statistiku reakce na incidenty
- Statistiky podpory
- Plánované a neplánované odstávky

3. Dostupnost a integrita dat

- Data v rámci DSaaS musí být denně zálohována nebo replikována.
- obnovení dat (RPO) do 24 hodin,
- obnova systému (RTO) do 12 hodin.

4. Eskalační postupy

Poskytovatel musí definovat a udržovat eskalační schéma pro nevyřešené incidenty. Kontaktní údaje odpovědných osob musí být aktuální a dostupné po celou dobu trvání smlouvy.

5. Sankce a kompenzace

Při nesplnění SLA budou uplatněny kompenzace nebo finanční sankce (% z měsíční platby):

- 98–99,5 %: 5 % kompenzace
- 95–98 %: 10 % kompenzace
- Pod 95 %: 20 % kompenzace nebo možnost vypovězení smlouvy při opakovaném porušení

6. Integrace podpory koncových uživatelů

Pokud DSaaS zahrnuje komponenty pro koncové uživatele (např. dashboardy nebo API), musí poskytovatel nabídnout možnost jejich podpory nebo integrace systému pro koncové uživatele.

7. Řízení změn a verzování

- Poskytovatel musí informovat minimálně 30 dní předem o každé významné změně nebo nové verzi.
- Zadavatel musí mít možnost nové verze otestovat ve staging prostředí před ostrým nasazením.

8. Exit strategie a přenositelnost dat

- Po ukončení smlouvy musí být umožněn export dat v otevřených standardních formátech (např. CSV, JSON, RDF) a podpora migrace během 30 kalendářních dnů.
- Musí být součástí smlouvy podrobný plán ukončení poskytování služby.

Úrovně podpory Helpdesku

Úroveň podpory	Popis	Reakční doba	Doba vyřešení
Kritická (P1)	Výpadek celé služby, DSaaS nedostupný	1 hodina	4 hodiny
Vysoká (P2)	Závažné omezení funkčnosti, částečný výpadek	4 hodiny	1 pracovní den
Střední (P3)	Nezávažný problém, existuje řešení	1 pracovní den	3 pracovní dny
Nízká (P4)	Drobné problémy nebo dotazy	2 pracovní dny	5 pracovních dnů

f. Technická a metodická dokumentace

Výstupem bude soubor dokumentů popisujících:

- Architekturu řešení (včetně komponent, API a integrací)
- Bezpečnostní a provozní nastavení
- Uživatelskou příručku pro správce i účastníky
- Metodiku onboarding nových partnerů

3. Funkční požadavky

Předmětem plnění je dodání technologického řešení, které zajistí **funkční provoz datového prostoru** s důrazem na **datovou suverenitu, transparentnost, interoperabilitu, škálovatelnost a bezpečnost**. V této kapitole jsou uvedeny klíčové funkční požadavky na dodané řešení.

3.1. Správa a ověřování identit účastníků

Systém musí umožňovat registraci, ověřování a správu všech účastníků datového prostoru v souladu se společným evropským rámcem důvěryhodnosti datového prostoru (např. GAIA-X, iSHARE, ...).

Musí podporovat:

- ověřování totožnosti založené na evropské digitální identitě (EUDI Wallet, eIDAS 2.0 ready),
- důvěryhodného poskytovatele identity s volitelnou integrací s národními nebo odvětvovými registry,
- protokolování certifikátů a atributů účastníků (např. rolí, oprávnění, referencí).

3.2. Publikace a katalogizace dat

Účastníci musí být schopni zveřejnit a popsat své zdroje dat prostřednictvím metadatových záznamů kompatibilních s DCAT-AP nebo podobnými otevřenými standardy.

Metadata musí být zveřejněna prostřednictvím zprostředkovatele metadat, včetně:

- technický popis dat
- obchodní a smluvní podmínky (zásady používání),
- kontakt a identitu poskytovatele,
- klasifikaci a tagování specifické pro danou doménu.

3.3. Vyjednávání a vymáhání podmínek použití dat

Systém musí podporovat mechanismus pro vyjednávání smluv mezi poskytovateli a spotřebiteli údajů.

Musí podporovat:

- specifikaci podmínek používání dat (např. časové limity, účel, geografický rozsah),
- automatizované uzavírání smluv (nabídka a dohoda) mezi poskytovatelem a příjemcem dat

3.4. Prosazování přenosu a přístupu k datům

Výměna dat musí probíhat výhradně prostřednictvím konektorů kompatibilních s protokolem datového prostoru, který zajišťuje:

- šifrovaný přenos dat,
- řízení přístupu na základě dohodnutých smluv,

- přenos strukturovaných i nestrukturovaných dat (např. CSV, JSON, obrázky, videa),
- protokolování každé transakce pro účely auditu.

3.5. Audity, důvěryhodnost a sledovatelnost

Všechny operace musí být:

- musí být auditovatelné prostřednictvím tzv. **Clearing House**, který nezávisle zaznamenává transakce,
- dohledatelné na úrovni jednotlivých žádostí, převodů, porušení smlouvy nebo bezpečnostních incidentů.

3.6. Onboarding a řízení účastníků

Řešení musí správci datového prostoru umožnit:

- posuzovat žádosti o vstupu nových účastníků datového prostoru
- definovat úrovně účasti (např. poskytovatel, spotřebitel, zprostředkovatel),
- ověřovat soulad s požadavky na certifikaci - referenční architekturou a souborem pravidel IDSA a běžnými evropskými rámci důvěryhodnosti datového prostoru (např. GAIA-X, iSHARE, ...),
- monitorovat činnosti účastníků.

3.7. Použití a správa

Administrativní rozhraní musí umožňovat:

- správu služeb a komponent,
- sledování provozu, zátěže a logování incidentů,
- přístup k systémovým statistikám a výstupům z auditních záznamů

Pro koncové uživatele musí být k dispozici:

- uživatelsky přívětivé rozhraní pro publikaci a vyhledávání dat,
- možnost propojení s vlastním systémem pomocí REST API nebo jiné standardizované vrstvy.

4. Technické požadavky

Technologické řešení datového prostoru musí být založeno na otevřených standardech, modulární architektuře a principech důvěry, bezpečnosti a interoperability. Řešení musí být škálovatelné a přenositelné mezi cloudovými a on-premise prostředími a musí umožňovat federované propojení s jinými datovými prostory.

4.1. Architektura systému

Architektura musí vycházet z:

- Modelu referenční architektury IDS (IDS-RAM v4.0 nebo vyšší),
- Společný evropský rámec důvěryhodnosti datového prostoru (např. GAIA-X, iSHARE, ...).
- Stavebních bloků datového prostoru definovaných DSSC.

Dodané řešení musí podporovat následující funkce:

- modulární nasazení jednotlivých komponent (konektor, broker, poskytovatel identit atd.),
- možnost federace s jinými datovými prostory,
- přístup založený na mikroslužbách nebo kontejnerech (např. Docker, Kubernetes).

Infrastruktura může být:

- nasazena v prostorách zadavatele (on-premise), nebo
- provozována v evropském cloudovém prostředí (např. Hetzner, OVHcloud, IONOS, Azure) s důrazem na datovou suverenitu a soulad s GDPR.

4.2. Použité standardy a protokoly

V případě relevance se doporučuje implementace nebo integrace následujících standardů:

Area	Standardy a Technologie
Identita a důvěryhodnost	<i>eIDAS 2.0, W3C Verifiable Credentials, DID (Decentralized Identifiers), GAIA-X Compliance Services</i>
Autentizace a autorizace	<i>OAuth2, OpenID Connect, XACML/ALFA (for policies), Attribute-based Access Control (ABAC)</i>
Metadata a katalogizace	<i>DCAT-AP, NGSI-LD, SHACL, RDF, SPARQL</i>
Správa smluv	<i>IDS Usage Control Language (LUCON / ODRL), Contract Negotiation Protocol (e.g., EDC or Sovity IDS)</i>
Protokoly pro přenos dat	<i>HTTPS/TLS, IDS Message Protocol, IDS Multipart Protocol, RESTful API, GraphQL</i>
Interoperabilita a výměna dat	<i>JSON-LD, XML, CSV, Parquet, GeoJSON, NetCDF, etc., depending on the application domain</i>

4.3. Kybernetická a provozní bezpečnost

Řešení musí splňovat následující požadavky:

- Směrnice NIS2 (2022/2555),
- Doporučení ENISA pro datové prostory,
- Zásady architektury Zero Trust Architecture.

Požadavky zahrnují:

- **end-to-end šifrování dat**
- auditní logy všech přístupů a operací,
- možnost integrace s nástroji SIEM (např. Wazuh, ELK, Splunk),
- dvoufaktorová autentizace a řízení přístupů

Všechny komponenty musí být pravidelně aktualizovány a monitorovány. Dodavatel musí předložit plán reakce na incidenty a zálohování dat.

4.4. Provozní požadavky a škálovatelnost

- Dodané řešení musí podporovat minimálně 10 účastníků a zpracovávat datové toky o velikosti až několik set GB/měsíc (škálovatelné podle potřeby).
- Komponenty musí být možné monitorovat prostřednictvím administrátorského rozhraní (např. Prometheus + Grafana, Zabbix, Kibana).
- Řešení musí podporovat provozní SLA s dostupností alespoň 99,5 % při standardním zatížení.

4.5. Dokumentace a rozhraní

Zhotovitel musí poskytnout:

- Dokumentaci ke všem komponentám (uživatelské, technické a API),
- specifikaci OpenAPI / Swagger pro všechna veřejná rozhraní API,
- ukázková data a testovací scénáře.

Všechny komponenty musí být provozuschopné buď jako varianty s otevřeným zdrojovým kódem, nebo musí být založeny na technologiích dostupných v Evropě. Přednost budou mít řešení založená na:

- Eclipse Dataspace Components (EDC),
- členové IDSA.

5. Požadavky na interoperabilitu

Cílem řešení je zajistit plnou interoperabilitu dodaného datového prostoru s dalšími národními a evropskými datovými prostory a ekosystémy. Interoperabilita je klíčovou podmínkou pro rozšiřitelnost, federaci a připojování různorodých datových zdrojů a spotřebitelů v souladu s principy **Evropského prostoru pro data (European Common European Data Spaces)**.

5.1. Technická interoperabilita

Je požadováno:

- Použití **otevřených a standardizovaných rozhraní API**. Všechny komponenty datového prostoru musí komunikovat pomocí otevřených rozhraní (např. REST, GraphQL, IDS Multipart Protocol).
- **Podpora konektorů EDC/IDS**: Řešení musí být schopno spolupracovat s komponentami založenými na Eclipse Dataspace Components (EDC), i když jsou implementovány různými dodavateli (členy IDSA).

5.2. Sémantická interoperabilita

Podpora standardizovaných datových modelů:

- DCAT-AP (pro publikaci metadat ve veřejné správě),
- NGSI-LD (pro datové entity v reálném čase, např. v Smart Cities),
- INSPIRE / GeoJSON (pro geoprostorová data),
- Další doménově specifické ontologie a schémata (např. SAREF pro energetiku, HL7/FHIR pro zdravotnictví).

Validace a transformace dat:

- Systém musí podporovat transformaci mezi různými datovými schématy a formáty (např. XML ↔ JSON-LD, RDF ↔ CSV) a umožňovat anotaci dat pomocí ontologií (např. OWL, SHACL).

5.3. Organizační interoperabilita

Sdílení zásad a podmínek:

- Dodávané řešení musí umožňovat vyjádření a sdílení smluvních podmínek a zásad (zásad používání dat) ve strojově čitelném formátu (např. ODRL, LUCON).

Výměna identit a mechanismů důvěry:

- Mechanismy identity a certifikace musí být uznávány a kompatibilní se společným evropským rámcem důvěryhodnosti datového prostoru (např. GAIA-X, iSHARE, ...).

- Účastníci musí být schopni používat atributy a certifikáty vydané jinými důvěryhodnými orgány.

5.4. Přenositelnost a otevřenost dat

Export a opakované použití dat:

- Všechna zveřejněná data musí být přístupná prostřednictvím standardních exportních formátů (např. CSV, JSON, XML, RDF).
- Uživatelé musí mít možnost přistupovat ke katalogu dat pomocí standardizovaných dotazovacích rozhraní (např. koncový bod SPARQL).

Podpora principů FAIR (Findable, Accessible, Interoperable, Reusable):

- Metadata a data musí být navržena v souladu s principy FAIR, aby se usnadnilo sdílení a opakované použití v jiných kontextech.

5.5. Kompatibilita s evropskými datovými prostory

Dodané řešení by mělo být technicky a funkčně připraveno na integraci nebo propojení s:

- Datový prostor mobility, datový prostor cestovního ruchu, datový prostor Green Deal). Komunikace v rámci datového prostoru je stále ve vývoji. komunikace s jinými datovými prostory by měla být vyhodnocena podle konkrétního případu použití.
- Sandboxy a federace provozované v rámci Centra pro podporu datových prostorů nebo středisek GAIA-X.

6. Fáze projektu

Zadavatel předpokládá, že realizace datového prostoru proběhne ve strukturovaných etapách, které zajistí funkční, bezpečné a udržitelné zavedení systému do praxe.

Realizace projektu bude probíhat ve fázích, které odpovídají logické struktuře předmětu plnění uvedeného v kapitole 2 tohoto dokumentu. Jednotlivé fáze představují klíčové milníky v procesu návrhu, zavedení, zprovoznění a předání datového prostoru do správy zadavatele. Odhad délky jednotlivých fází slouží jako orientační rámec pro plánování a organizaci prací.

Fáze projektu	Popis činnosti	Odhad trvání
Dodání komponent datového prostoru	Dodání a konfigurace komponent datového prostoru: konektor, katalog, identity & trust moduly, auditní komponenty, správce zásad používání	1–2 měsíce
Uvedení do pilotního provozu a podpora testování	Instalace v prostředí zadavatele, základní funkční testy, ověření interoperability, školení správců a uživatelů	2–3 měsíce
Integrace dat a registrace účastníků	Připojení vybraných partnerů (např. obce, DMO), příprava a katalogizace prvních datových sad, nastavení přístupových práv a rolí	1–2 měsíce
Dodání technické a metodické dokumentace	Komplexní dokumentace komponent, API, architektury, provozních parametrů, onboardingu partnerů a integračních návodů	souběžně s fází 2 a 3
Předání a provozní příprava (DSaaS)	Finalizace dokumentace, nastavení SLA, předání systému do správy, definice provozních procesů, eskalačních schémat a případně exit strategie	1 měsíc

7. Slovník pojmů k datovému prostoru

Pojem	Vysvětlení
Clearing House	Komponenta datového prostoru, která zaznamenává transakce mezi účastníky (např. kdo komu co sdílel). Zajišťuje auditovatelnost, důvěru a někdy i vyúčtování v případě zpoplatněného sdílení dat.
Connector	Softwarová komponenta, která propojuje účastníky v datovém prostoru a umožňuje bezpečné a kontrolované sdílení dat.
CSV (Comma-Separated Values)	Jednoduchý formát pro tabulková data.
DCAT-AP	Evropský profil pro popis metadat katalogů dat (např. ve veřejné správě nebo dataspace). Umožňuje snadné dohledání a sdílení datasetů.
DSaaS (Data Space as a Service)	Model, ve kterém je celý datový prostor nebo jeho komponenty (např. konektor, katalog, správa identity) poskytován jako služba.
DSSC (Data Space Support Centre)	Evropské centrum koordinující vývoj společných evropských datových prostorů. Poskytuje metodiky, blueprinty, standardy a slovník pojmů. Slouží jako zastřešující rámec pro sektorové dataspace iniciativy.
DSSC Sandbox	Testovací prostředí vytvořené DSSC, ve kterém mohou vývojáři a organizace experimentovat s komponentami datového prostoru – např. konektory, katalogy, správa identity.
EDC (Eclipse Dataspace Components)	Open-source framework spravovaný nadací Eclipse pro budování konektorů v datových prostorech.

EDWG (European Data Working Group)	Pracovní skupina na evropské úrovni, která se věnuje rozvoji datových prostorů, datové interoperability a strategických rámců.
eIDAS 2.0	Revidované evropské nařízení o elektronické identifikaci. Zavádí EUDI Wallet a podporuje interoperabilní digitální identitu v EU.
ENISA	Agentura Evropské unie pro kybernetickou bezpečnost. Vydává certifikace a standardy pro bezpečnost v oblasti datových prostorů.
EUDI Wallet	Evropská peněženka digitální identity podle eIDAS 2.0. Občané a firmy si do ní budou moci uložit důvěryhodné digitální doklady a používat je např. při přístupu ke službám či při podepisování transakcí v dataspace.
GAIA-X	Evropská iniciativa usilující o vytvoření federované datové infrastruktury na bázi otevřených standardů.
GAIA-X Federation Services	Sada služeb zajišťující interoperabilitu a důvěru v rámci federace datových prostorů. Jedná se o základní stavební kameny Gaia-X ekosystému.
Identity and Trust modules	Moduly pro správu identit a důvěry v datovém prostoru.
IDS Rulebook	Dokument vydávaný IDSA, který stanovuje pravidla (technická, právní i organizační) pro fungování datových prostorů založených na architektuře IDS.
IDSA (International Data Spaces Association)	Nezisková mezinárodní asociace s cílem umožnit interoperabilní a důvěryhodnou výměnu dat v různých odvětvích.
IDS-RAM (Reference Architecture Model)	Referenční architektonický model vyvinutý IDSA, který definuje komponenty (např. konektor), role, procesy a bezpečnostní zásady pro implementaci datového prostoru.

INSPIRE / GeoJSON	INSPIRE je směrnice EU pro sdílení geografických dat; GeoJSON je formát pro reprezentaci prostorových dat (body, linie, polygony) v JSON podobě.
iSHARE	Nizozemský rámec pro správu identit, přístupových práv a důvěry v decentralizovaných prostředích sdílení dat.
ISO/IEC	Mezinárodní organizace pro standardizaci (ISO) a Mezinárodní elektrotechnická komise (IEC).
JSON-LD (JavaScript Object Notation for Linked Data)	Rozšíření klasického JSON formátu o sémantickou vrstvu. Umožňuje propojení dat pomocí URIs.
LUCON (LUcy CONTRACT enforcement)	Framework pro technické vynucování pravidel použití dat v konektorech (např. logování, blokace, šifrování).
NGSI-LD	Standard FIWARE pro výměnu kontextových informací v reálném čase, založený na principu propojených dat.
NIS2 ready	Označení pro komponenty, infrastruktury nebo organizace, které jsou v souladu s požadavky směrnice NIS2 (o bezpečnosti sítí a informací).
ODRL (Open Digital Rights Language)	Standard pro vyjadřování pravidel přístupu a použití dat (např. pouze pro výzkum).
OWL (Web Ontology Language)	Jazyk pro tvorbu ontologií – popis pojmů a jejich vztahů.
RDF (Resource Description Framework)	Základní model pro sémantická data. Umožňuje vyjádřit trojice (subjekt–predikát–objekt) a vytvářet datové grafy.
RDF/SPARQL endpoint	Webová služba, která zpřístupňuje data v sémantickém formátu RDF a umožňuje jejich dotazování pomocí jazyka SPARQL.

SHACL (Shapes Constraint Language)	Jazyk pro validaci struktury RDF dat. Používá se k ověřování souladu dat s ontologií.
SIEM tools (Security Information and Event Management)	Nástroje pro sledování, analýzu a korelaci bezpečnostních událostí v reálném čase. V dataspace pomáhají detekovat útoky a auditovat bezpečnost.
SPARQL	Dotazovací jazyk pro data uložená ve formátu RDF.
XML (eXtensible Markup Language)	Strukturovaný značkovací jazyk pro výměnu dat.