Study to support the technical, legal and financial conceptualisation of a European Security Data Space for Innovation

Summary of the study in support of the
Call for Proposals under the
Internal Security Fund on **Data Sets** for the European Data Space for Innovation
ISF-2022-TF1-AG-DATA

20 February 2023

This document has been prepared by EY and RAND Europe for the European Commission, Directorate-General Migration and Home Affairs.

Table of contents

Table of figures

List of abbreviations

AI	Artificial Intelligence
CFREU	Charter of Fundamental Rights of the European Union
COVID-19	Coronavirus Disease 2019
CRM	Customer-Relationship-Management
DG HOME	Directorate-General for migration and home affairs
ERP	Enterprise Resource Planning
EU	European Union
EU SDSI	European Security Data Space for Innovation
GDPR	General Data Protection Regulation
HPC	High-Performance Computing
IaaS	Infrastructure as a Service
IDSA	International Data Spaces Association
ISF	Internal Security Fund
IT	Information Technology
LEA	Law enforcement agency
LED	Law Enforcement Data Protection Directive
mTLS	mutual Transport Layer Security
OS	Operating System
PaaS	Platform as a Service
SaaS	Software as a Service
SMP	Smart Middleware Platform

1 Introduction

In order to support the European Commission's Call for Proposals under the Internal Security Fund on **data sets for the European Data Space for innovation - ISF-2022-TF1-AG-DATA**, EY and RAND Europe have prepared a tailored, high-level summary of the preliminary results of the explorative "Study to support the technical, legal and financial conceptualisation of a European Security Data Space for Innovation" that is currently being implemented on behalf of the European Commission, DG HOME (RfS 35; HOME/2020/ISFP/FW/EVA2/0068).

The overall objective of the study is to **develop a conceptual framework for the European Security Data Space for Innovation (EU SDSI).** The results will be used to improve the EU-wide sharing of, as well as access to a sufficiently high quantity of high-quality data as an enabler and catalyst for the development and application of Artificial Intelligence (AI) technologies in law enforcement. In the long term, this will support to maintain and increase security levels within the EU and safeguard the EU's technological sovereignty in the fight against crime and terrorism.

The study focuses on the situation at the EU level and in all 27 EU Member States, including their law enforcement agencies (LEAs) and other relevant stakeholders. Major thematic aspects that will be dealt with are the application of AI in law enforcement, the material substance the EU SDSI will be made of (including legal, ethical, financial, and technical aspects). The study has a forward-looking timeframe of five up to ten years and covers current as well as historical dimensions of the topic. The data used to evaluate the current situation has been gathered largely through desk research and stakeholder consultations at the EU and national levels.

This document has been structured as follows: In Chapter 2, the EU SDSI's business case is explained. Chapter 3 will present the high-level vision and draft concept for the EU SDSI. Chapter 4 focuses on data-related and technical features of the EU SDSI. Lastly, Chapter 5 shortly outlines factors that are still to be considered.

2 Business case for the EU SDSI

Criminals and in particular perpetrators of serious and organised crime are not bound by national borders. As for other aspects of life, technology increasingly enables criminal activity. Criminals have become more "innovative" with respect to:

- **Cybercrime**: e.g. compromising business e-mails, identity fraud, ransomware or forging digital vaccination certificates during the COVID-19 pandemic.
- **Financial Crime**: e.g. non-cash payment fraud, closely related to phishing and social engineering through the use of technologies such as voice impersonators.
- **Drug trafficking**: e.g. distribution of illegal drugs through encrypted messaging services/software, social media apps, online sources, post and home delivery services.
- **Other crime areas**: e.g. organised property crime, excise fraud, human trafficking and migrant smuggling, as well as child sexual abuse and exploitation.

This development has called for increased efforts within the EU law enforcement ecosystem for authorities to keep up and themselves become more innovative and to fight crime by **leveraging and reaping the benefits of modern, data-driven technology such as Artificial Intelligence (AI) in full compliance with applicable data protection legislation and the Charter of Fundamental Rights (CFREU).** The application of data-driven technologies such as AI does not only have the potential to address crimes that take place in an online context but can also provide great benefits in the fight against crimes that take place in a "physical" context - but which are monitored via digital means.

In particular the use of data-driven technologies within law enforcement and the improvement of LEAs' general capability to be innovative largely depends on the availability, accessibility, and usability of a high quantity of high-quality data from various sources. However, the use of such data and modern technology appears to not be very advanced on a European level, given the current state of a shared legal framework, technical infrastructure, operational capabilities as well as cross-border cooperation. Given the absence of a comprehensive European framework, Member States are currently developing national solutions or do engage in the area only to a limited extent.

The EU has set itself the objective to become 'a leading role model for a society empowered by data […]'.[1] One of the main corner stones will be the adoption of '**Common European Data Spaces'**, as has been laid out in the European Strategy for Data.[2]

The majority of Member States has already started to invest in data-related innovation in the area of law enforcement. Member States' LEAs collect sensitive and non-sensitive data to solve crimes at hand.

The data collected by LEAs as part of their investigations is often very sensitive and protected through applicable legislation at the EU and Member State levels, e.g. the General Data Protection Regulation (GDPR)[3], the Law Enforcement Data Protection Directive (LED)[4], as well as the Charter of Fundamental Rights of the European Union[5].

While there is a legal framework in place that governs the collection, use, and exchange of sensitive information between Member States' LEAs, a comprehensive framework and technical solutions to enable the access to and exchange of non-sensitive information for innovation purposes – including through a shared technical solution - is absent.

As a consequence, LEAs' innovation efforts with regard to AI (e.g. the development, testing, training, validation, and practical application of AI algorithms) are hampered, including limited access to the necessary quantity and quality of data.

The EU SDSI can facilitate and enable the more effective and efficient fight against serious and organised crime by providing a facility through which, with full respect of applicable data protection and privacy regulations and fundamental rights, LEAs benefit from "better" (i.e. higher quantity and quality) data that can be used for innovation purposes. The aim of the EU SDSI is not the development of an operational system to monitor and mass survey citizens and businesses. Furthermore, the data in the EU SDSI would not be used for operational purposes, but for the purpose of innovation - in particular to **develop, test, and validate innovative solutions to fight serious and organised crime**

3 High-level vision and draft concept for the EU SDSI

This chapter summarises the draft concept for the EU SDSI. At a very high level, it outlines why the EU SDSI is necessary, what it should do, and how it should do that.

3.1 Governance Models for the EU SDSI

The contributions obtained during interviews, focus groups and the workshops broadly point into a common direction, which can be summarised as follows:

Figure 1: Why the EU SDSI is necessary

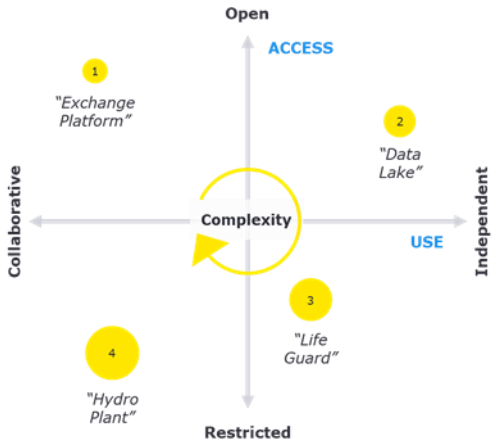
WHY is the EU SDSI necessary?	The EU SDSI would serve to maintain and even increase the high level of security in the European Union for citizens, businesses, and public administrations.
WHAT does the EU SDSI do?	It should facilitate data-driven innovation in the area of law enforcement, both at EU-level and across borders, as well as in the Member States.
HOW does the EU SDSI function?	It would provide an efficient, federated IT-platform through which EU-level and national law enforcement authorities can efficiently collaborate in the area of data-driven innovation based on both specific use cases and shared principles and processes. In full compliance with applicable data protection legislation and the Charter of Fundamental Rights, the EU SDSI builds on and is interoperable with the technical infrastructure available in the Member States in the area of law enforcement, as well as with other EU data spaces.

Source: EY

A matrix of potential governance models has been developed along two axes: **Access** (open vs. restricted) and **Use** (collaborative vs. independent). As a result, four distinct governance

solutions of varying complexity were developed, i.e. the EU SDSI as exchange platform, data lake, lifeguard, and hydro plant (see also the figure below).

Figure 2: Potential governance solutions for EU SDSI exist: Access & Use



Source: EY, based on Stefaan G. Verhuulst and Andrew J Zahuranec (2022).[6]

Based on which governance solution is applied, different implications for the EU SDSI arise. The **exchange platform** as the least complex solution would serve as a virtual, open platform that can be accessed by *all* stakeholders as a collaborative environment. Its purpose is to enable community and capacity building within the law enforcement ecosystem. The **data lake** model is a virtual channel through which non-sensitive data can be accessed by LEAs to develop data-driven innovations and AI algorithms. The **lifeguard** model is comparable to the data lake concept, however, it would be supplemented through a central service (e.g. within the competence of Europol), which will facilitate access and the use of the data while ensuring that quality standards are met. Lastly, within the **hydro plant** model a central body would also be established. In this solution, the central service would also help Member States to extract the desired value from accessible data (in line with applicable legislation and restrictions).

EU-level and national stakeholders have stressed that **all four of these models are relevant** and present a feasible idea of what the EU SDSI should be capable of. Indeed, based on discussions with stakeholders as part of the present study, it was recommended that the EU SDSI's governance solution could depend on the use case at hand.

In addition, stakeholders stressed that the needs of the Member States may change over time, which is why the EU SDSI could show a certain degree of flexibility and changeability. This means that the EU SDSI could develop from a basic version (Minimum Viable Product) as a short-term solution to an advanced version in the long-term, based on the needs of the Member States.

Stakeholder consultations indicated that the EU SDSI should operate within a larger ecosystem of (sandbox) environments, comprising Member States' environments and other EU data spaces. Particularly important would be a central **Europol sandbox environment** based on the AI Act[7] and Europol's strengthened mandate in the field of research and innovation under its revised Regulation[8].

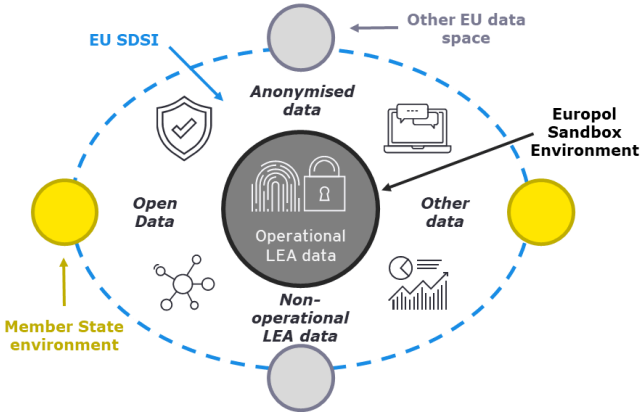
Europol may process personal data for the purpose of research and innovation projects for the development, training, and validation of algorithms (article 18(2)(e) of the Europol Regulation). These research and innovation projects must be carried out in a **separate, isolated and protected data processing environment** within Europol (**Europol sandbox environment** - article 33a(2)(d)(i)). In full compliance with the safeguards established in article 33a, Europol and its Member States will be able to store and process information including personal data in the Europol sandbox environment to train and develop algorithms. In light of the clear and known legal framework for sharing information including personal data within Europol data processing environments, national governments and LEAs are likely to be less sceptical sharing sensitive data in such an environment, as trust levels in Europol are comparably high. The 'surrounding' environment of the EU SDSI could rather be used to for

the 'initial' development of algorithms and tools with non-sensitive data which can later be refined in the Europol sandbox.

It is important to note that a close collaboration between the EU SDSI and Europol is only one of several potential options for the implementation of the EU SDSI. No decisions have been taken in this regard yet.

Keeping this in mind, one can summarise that the EU SDSI could be conceptualised as the shell of a larger ecosystem, whereas Europol's sandbox environment would form the core. The outset consists of other EU data spaces or secure national environments in which Member States' data is stored and can flow in an interoperable manner from one area to another. A proposal for this larger ecosystem is visualised in the figure below.

Figure 3: Larger ecosystem of sandbox environments in the area of law enforcement



Source: EY.

Regarding governance frameworks and best practices, the EU Commission has launched a **Data Spaces Support Centre (DSSC)** that coordinates the actions of all data spaces currently planned under different EU initiatives.[9] The DSSC has been operating since December 2022. A central task of the DSSC will be to co-create blueprints and deliver support for the implementation of various data spaces at the European level. The DSSC will therefore define common requirements and best practices in order to accelerate the formation of independent data spaces. The information provided by the DSSC within this context will comprise technological standards, processes, governance mechanisms and tools that will allow the reuse of data across different sectors and data spaces and will therefore mark a crucial step for the development of a uniform market for data. It should be noted that with regard to this study, the principles of a 'uniform data market' is likely not to be fully applicable to the EU SDSI, due to the sensitive nature of the data shared within it. It must therefore be considered that possible results of liaising with the DSSC must always be carefully assessed for their relevance to the EU SDSI. Nonetheless, the DSSC's activities remain highly relevant for the EU SDSI and should therefore be followed on an ongoing basis.

Examples of potential use cases relevant for the EU SDSI

After being implemented, the purpose of the EU SDSI could be to support Member States in developing innovative solutions to fight crime. It should be noted, however, that the use cases provided here do represent examples mentioned during stakeholder consultations. During and after the implementation, additional use cases might apply.

EU-level stakeholders and Member States are already working on various AI use cases – either on their own, across borders (e.g. in so-called Co-Groups), or together with EU stakeholders such as Europol. As part of the consultations conducted during this assignment, stakeholders raised various examples of potential use cases in law enforcement, including crime suspect profiling (e.g. based on social media), detection of child pornography, fraud detection, anomaly detection in surveillance footage of public spaces, and traffic control (through automated licence plate detection and vehicle identification). Whereas some use cases are still in the conceptualisation phase, others have already been prototyped, tested, or approved for practical application.

There are two main strands identified on how the use of AI technology in the law enforcement sector can benefit authorities: **Administrative** and **operational**. Both are relevant to consider in the context of the EU SDSI. Administrative use cases concern the improvement of inner-organisational efficiency and resource allocation, whereas operational use cases concern the improvement of the LEAs' work on the field. The present study's focus has been on operational use cases and how the EU SDSI could boost the performance of operational duties, however, a widening of the scope towards more administrative options remains a valid option for later use.

In order to support LEAs operations, a specific set of AI technologies must be at the disposal of Member States' data scientists. AI technologies that will be relevant for the further development of above-mentioned use cases comprise:

- Audio processing (speech);
- Visual processing (image and video);
- Resource optimisation; and
- Natural language processing (text).

3.2 EU SDSI Services

As indicated above, the main service of the EU SDSI will be the provision of a data sharing platform, in which relevant authorities can up- and download, as well as share data and train algorithms on the use of AI in law enforcement.

As concerns additional or more detailed services the EU SDSI could offer, national or regional authorities were asked to prioritise smaller services and larger service packages the EU SDSI should offer within a survey distributed between different authorities.

In terms of *larger service packages*, the majority of respondents within LEAs and national Ministries viewed the **facilitation of data sharing between national law enforcement officials** as the most important larger service package.

Noteworthy are in addition:

- Sharing of knowledge and good practices;
- Provision of training and capacity building;
- Enabling the collection, preparation and automated annotation/classfication of data;
- Establishing a common data ontology and common standards for interoperability; and
- Assisting the Member States in the development, testing, validation, training, and optimisation of algorithms and models.

The majority of respondents from the law enforcement and ministry surveys viewed **data storage based on privacy and security design principles** as the most important smaller micro-services. Various additional requested services are: (1) Recognising objects on images of poor quality or language dialect; (2) Safety checks, including compliance with data protection and security concerns; and (3) Assessing data quality and evaluating reference data on bias.

4 Data-related and technical features of the EU SDSI

This chapter summarises main technical and data-related features of the EU SDSI. It focuses on data and data sets in the context of the EU SDSI, the interconnectivity within a federated architecture, as well as on decentralised data collaboration hub Gaia-X.

4.1 Data and data sets

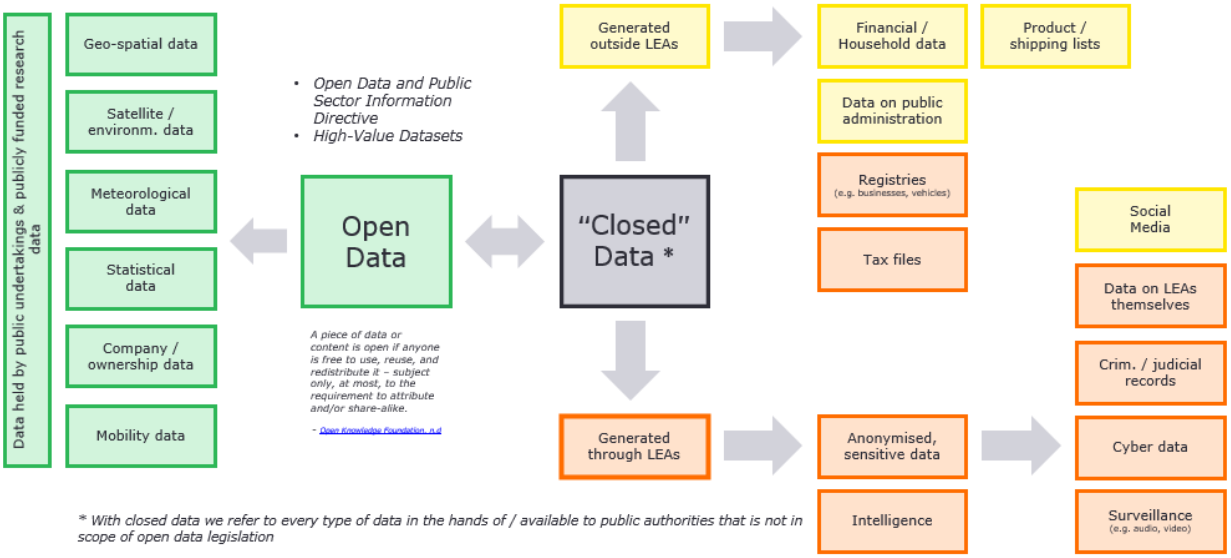
Data and data sets are elementary for the EU SDSI to function properly. It has therefore been one of the main tasks of the study to identify the different kinds of data that could be used in the EU SDSI and also which quality standards such data will need to follow.

An important distinction must be made between the large amounts of **non-sensitive data** and more limited **sensitive, operational law enforcement data**. A high-level overview of the different types of data is given in Figure 4.

Types of data the EU SDSI should not deal with

It is important to note that most of the types of data marked in red should not be accessible or exchanged through the EU SDSI. They are extremely sensitive and, although they may be useful for law enforcement purposes, should not be used for the purpose of innovation in law enforcement.

Figure 4: Basic typology including examples of data



Source: EY.

In order to ensure the EU SDSI will be provided with a sufficient amount of data after its implementation, the Commission has launched a call under the Internal Security Fund (ISF) to carry out preparatory work needed for the creation of large-scale sharable data sets for innovation in law enforcement.[10] In general, the EU SDSI could, inter alia, be served by data corresponding to the High Value Datasets, which have been identified by the Commission as data associated with important benefits for the society and economy.[11] The datasets will comprise a number of main categories, which have been identified in the Commission's Open Data Directive.[12] This will include the following fields: geospatial, earth observation and environment, meteorological, statistics, companies and mobility.[13]

Throughout the stakeholder consultations conducted as part of the present study, it was recommended that the data used in the EU SDSI must adhere to commonly shared quality standards and principles. A common standard that was mentioned and recommended frequently is the FAIR principle for data.

FAIR Principle

Stakeholders should at a minimum consider implementing the FAIR principle within the context of the EU SDSI, but this may also be introduced as a mandatory requirement. The FAIR principle is an internationally recognised standard for data quality. The acronym FAIR stands for data that is: 1. **F**indable, 2. **A**ccessible, 3. **I**nteroperable, and 4. **R**e-usable.

Additionally, stakeholders emphasised the importance of **technical** and **semantic** interoperability of the data used, in order to ensure an efficient cross-border exchange.

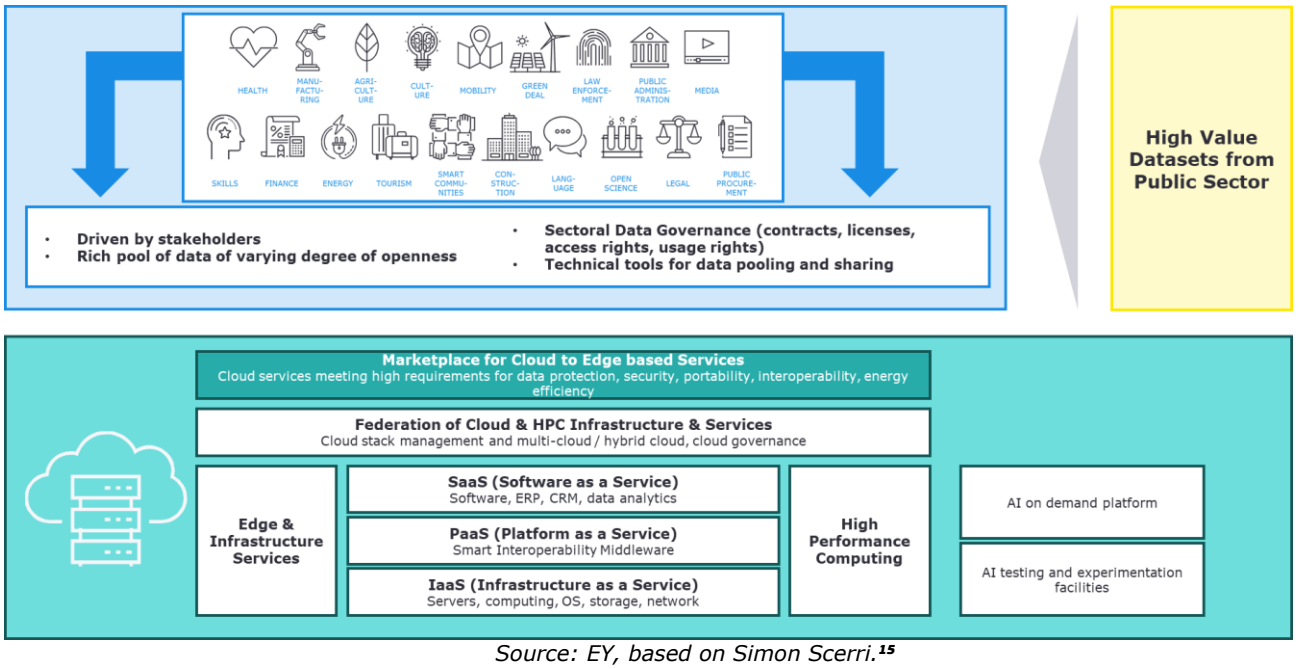
Lastly, desk research and stakeholder consultations indicated the importance of **metadata** for the success of the EU SDSI. Metadata is structured reference data that can help to sort and identify attributes of other data without providing information on the content of respective data.[14] Including AI-readable metadata can therefore be a valuable asset in organising and structuring the EU SDSI.

4.2 Interconnectivity and cloud federation

As shown in section 3.1, the EU SDSI will not operate as an isolated entity, but will be integrated within different environments on Member State and EU levels. As the EU SDSI is not the only

data space currently being developed (the Commission has announced around 20 data spaces across various sectors and areas, including in the areas of health, tourism, energy, mobility, etc.), a connection to other data space environments has been identified as an important success factor. Each of the planned EU data spaces should be built upon a federated cloud infrastructure, leveraging edge and high-performance computing with specific service offerings. An overview of the foreseen, high-level infrastructure and services is provided in the figure below.

Figure 5: Overview of cloud federation, common European Data Spaces and AI



Source: EY, based on Simon Scerri.[15]

In order to ensure the interoperability and connectivity of the different data spaces across all steps of the data sharing process, as well as between the different Member States of the EU, the Commission has launched the development of a **Smart Middleware Platform (SMP) called SIMPL.**[16] SIMPL's main aim is to foster growth and stability through the exchange of data and to ensure that different data sets will be seamlessly interconnectable and interoperable. In essence, SIMPL is necessary to connect different actors and data spaces in a way that ensures a smooth exchange of the different data processed. SIMPL will be freely available without any charges for data providers and data users, as it is conceptualised as an open source software.

SIMPL as a middleware will be used to create a non-centralised federation of cloud-to-edge capacities, which will be at the disposal of all data spaces. When talking about SIMPL, it should be noted that SIMPL is not one product only but consists of three major product strains. Firstly, **SIMPL-open** will form the core product of SIMPL. It will provide an open-source software stack around which the other two main components can be developed. The second component, so-called **"SIMPL Labs"** will be implemented to enable relevant participating actors and stakeholders to experiment the deployment, maintenance, and support of SIMPL in a pre-installed playground environment. Lastly, **SIMPL-live** will provide several instations of SIMPL-open in the form of customised production environments for sectoral data spaces. Therefore, SIMPL-live will be used for the actual deployment of some data spaces.[17]

SIMPL itself will be managed by different service lines, and each of them will be responsible for a different topic. The Data Service itself is only one of three main services responsible for the management of the SIMPL infrastructure, next to the Administration Services and the Infrastructure Connector Services. The different services are all embedded within the IT infrastructure provided by, for instance, a public or private cloud manager. In addition, all services are embedded into relevant EU governance frameworks.

With regard to the EU SDSI, SIMPL might provide a relevant and interoperable framework technology, in which the EU SDSI could be embedded in. However, due to the sensitive nature of the data handled within the Security Data Space, stakeholder consultations underlined that a special solution for the EU SDSI might be needed. How this solution could look like and if intersections with SIMPL will be included is not fully clear at this stage of the study. Nonetheless,

the study team would recommended future contractors to track relevant developments of SIMPL and consider possibilities for cooperation (in accordance with data protection and legislation).

In addition to the main architecture principles of SIMPL, first steps have been made in identifying and mapping the most relevant actors and stakeholders of SIMPL. The focus here is on how SIMPL impacts the different stakeholders and how it helps creating different data spaces and data space environments, which will work according to the main architectural principles listed above. The four most important categories of actors which will use SIMPL are:

- Data providers;
- Infrastructure providers;
- Application providers; and
- End users.

Digression: Gaia-X as a source of inspiration for the EU SDSI

Gaia-X is a private business that facilitates the sharing of data between its member companies through the implementation of a technical infrastructure, mainly developed in Germany and France. SIMPL, at the moment, is a conceptual framework for a technical infrastructure developed by the European Commission aimed at ensuring the interoperability as an enabler of data sharing between EU data spaces. SIMPL and Gaia-X overall pursue similar goals, which include the creation of an interoperable digital ecosystem. While Gaia-X is already operating, SIMPL is still under development. Thus, Gaia-X can serve as a source of inspiration for the technical infrastructure and architecture of the EU SDSI.

Gaia-X, in cooperation with the International Data Spaces Association (IDSA), has not only created a European virtual data share point, but has also developed guidelines on **ensuring interoperability** by creating common framework standards on data spaces. IDSA and Gaia-X have also published a joint document, pointing out the benefits of using a shared digital infrastructure for the realisation of the European Strategy on Data[18]. Moreover, Gaia-X's technical components show similarities to the ones marked as desirable in the EU Strategy on Data, particularly with respect to **cloud federation, data sovereignty** and **portability rights**. Taking a closer look at Gaia-X's infrastructure can therefore provide important learning lessons for the EU SDSI. In addition, other data spaces also provide helpful information on how data can be accessed and which specific security measures are commonly used to ensure the confidentiality of the shared data. **Trusted identities**, **user authentication**, and **secure data transfer methods** (e.g. encryption, mutual Transport Layer Security – mTLS, two-way authentication, CySIMS Certificate Authority) are amongst the most used practices and can be taken into consideration for the construction of the EU SDSI.

However, it should be noted that reportedly, Gaia-X's objective is not to become a Cloud service provider or a Cloud management platform. Instead, its stated aim is to link different elements via open interfaces and standards, in order to connect data and make them available to a broad audience.

5 Examples of factors to be considered for the further development of the EU SDSI

Lastly it should be noted that it is expected that the implementation of the EU SDSI will face a number of challenges. At this stage, nine relevant aspects have been identified.[19] The challenges can be clustered into different areas, comprising the categories governance, legal, technical, and other (as can be seen in Figure 6 in descending order).

In the field of **governance**, it is expected that in particular the definition of a thorough and well-developed governance model will pose a challenge to the implementation of the EU SDSI. This has also been mentioned by various stakeholders during the consultation process. In addition, different readiness levels with regard to data sharing and use might pose significant challenges. It is recommended, to establish an overall governance model that can develop and adapt during and after the final implementation, allowing for the greatest possible flexibility in the process.

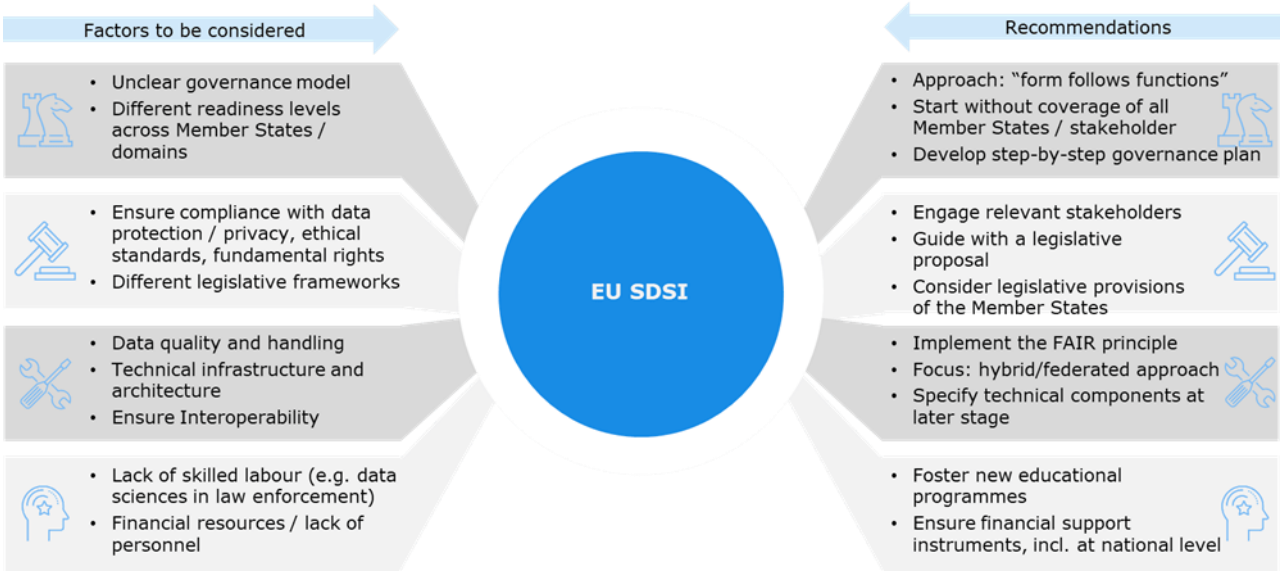
Legal considerations comprise in particular the compliance with data protection and fundamental rights aspects, as well as considering the different legislative frameworks in the Member States. In this regard, recommendations include to engage with relevant stakeholders (such as e.g. the Fundamental Rights Agency, the European Data Protection Supervisor, or

national stakeholders) and consider the legislative provisions and framework in the Member States.

On the **technical** level, the provision of a sufficient amount of high-quality data, the building of a resilient and thorough technical infrastructure as well as interoperability between different formats of data will be crucial factors that will need to be considered. In order to do so, it is recommended to ensure the FAIR data principle will be considered (see section 2.3), that technical components will be specified (e.g. standards), and that hybrid and federated models will be implemented to allow Member States keeping the biggest possible flexibility.

Lastly, **other aspects** that should be considered, comprise the lack of qualified human capital as well as the financial resources. New education programmes as well as establishing financial support instruments can be introduced as counter measures.

Figure 6: Examples of factors to be considered and recommendations



Source: EY

Implementing the EU SDSI will therefore be a major task, requiring finely tuned and well-planned efforts in a number of different fields.

The purpose of this document has been to contribute to these efforts and provide future contractors involved in the EU SDSI's implementation with helpful information on how to proceed and which aspects to take into consideration.

Sources for reference

[1] European Commission (2020). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European Strategy for Data. COM (2020) 66 final, p. 1. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN

[2] European Commission (2020). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European Strategy for Data. COM (2020) 66 final, pp. 5-6. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119/1). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[4] Directive (EU) 2016/680

[5] European Parliament, Council of the European Union & European Commission (2000), Charter of Fundamental Rights of the European Union, 2000/C 364/01, Nice.

[6] Stefaan G. Verhuulst and Andrew J Zahuranec (2022): Governance models of data collaboration. Available at: https://opendatapolicylab.org/articles/event-data-collaboration-for-the-blue-economy-the-govlab-intertidal-agency-and-openscapes-host-studio-on-data-stewardship-and-governance-models-for-data-sharing/index.html

[7] European Commission (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts, COM (2021) 206 final, available: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206

[8] Regulation (EU) 2022/991 of the European Parliament and of the Council on 8 June 2022 amending Regulation 2016/794 as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation (OJ 2022 L 169/1). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0991

[9] Overview available at: https://dssc.eu

[10] International Security Fund (2022). Call for proposals on the European data space for innovation. ISF-2021-TF1-AG-DATA. Available at: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/isf/wp-call/2021-2022/call-fiche_isf-2021-tf1-ag-data_en.pdf

[11] European Commission (2023). Open data. Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12111-Open-data-availability-of-public-datasets_en

[12] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast) (OJ 2019 L172/56). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1024&from=EN

[13] https://digital-strategy.ec.europa.eu/en/news/commission-defines-high-value-datasets-be-made-available-re-use

[14] See: https://egovstandards.gov.in/sites/default/files/Metadata%20Standards%20and%20Metadata%20Registries-An%20Overview.pdf

[15] See: https://link.springer.com/content/pdf/10.1007/978-3-030-98636-0.pdf?pdf=button#page=366&zoom=100,0,0 page 340.

[16] EU Commission (2022), Simpl: cloud-to-edge federations and data spaces made simple, available at: https://digital-strategy.ec.europa.eu/en/news/simpl-cloud-edge-federations-and-data-spaces-made-simple

[17] Additional information on the SIMPL components can be found in: EU Commission (2023), Call for tenders CNECT/2022/OP/0132 – Simpl - Smart Middleware platform for cloud-to-edge federations and data spaces Part 2: Technical specifications, available at: https://etendering.ted.europa.eu/cft/cft-display.html?cftId=12922

[18] International Data Spaces Association (2020), Implementing the European Strategy on Data. Role of the International Data Spaces (IDS), available: https://internationaldataspaces.org/publications/most-important-documents/

[19] The challenges have been identified through different research methods, comprising desk research as well as stakeholder consultations through interviews and workshops. To tackle these challenges in an organised and effective way, recommendations have been worked out based on implications stemming from the stakeholder consultations.