# D3.6 - Mechanisms and Tools for Regulatory Compliance II

| | |
|---|---|
| Title | D3.6 - Mechanisms and Tools for Regulatory Compliance II |
| Revision Number | 1.0 |
| Task reference | T3.5 |
| Lead Beneficiary | NUIG |
| Responsible | Martin Serrano |
| Partners | AL, BPFI, IQB, KM, UNP |
| Deliverable Type | DEM |
| Dissemination Level | PU |
| Due Date | 2025-03-31 [Month 30] |
| Delivered Date | 2025-07-31 |
| Internal Reviewers | NOVA JRC |
| Quality Assurance | UPRC |
| Acceptance | Coordinator Accepted |
| Project Title | FAME - Federated decentralized trusted dAta Marketplace for Embedded finance |
| Grant Agreement No. | 101092639 |
| EC Project Officer | Stefano Bertolo |
| Programme | HORIZON-CL4-2022-DATA-01-04 |

This project has received funding from the European Union's Horizon research and innovation programme under Grant Agreement no 101092639

# Revision History

| Version | Date | Partners | Description |
|---|---|---|---|
| 0.1 | 2025-05-28 | NUIG | TOC |
| 0.2 | 2025-06-14 | NUIG, AL, | Contents updates |
| 0.3 | 2025-07-17 | NUIG, AL | Contents updates |
| 0.9 | 2025-07-30 | NUIG | Version for review |
| 1.0 | 2025-07-31 | NUIG | Version for submission |

# Definitions

| Acronym | Definition |
|---|---|
| 4AML | 4th Anti Money Laundering Directive |
| AI | Artificial Intelligence |
| AML | Anti Money Laundering |
| BPFI | Banking and Payments Federation Ireland |
| DGA | Data Governance Act |
| EBA | European Banking Authority |
| EC | European Commission |
| ECB | European Central Bank |
| ESG | Environmental, Social and Governance |
| EU | European Union |
| FAME | Federated decentralized trusted dAta Marketplace for Embedded finance |
| GDP | Gross Domestic Product |
| GDPR | General Data Protection Regulation |
| HTML | Hypertext Markup Language |
| HW | HardWare |
| ICT | Information Communication Technologies |
| ID | Identity |
| IDS | International Data Spaces |
| IDSA | International Data Spaces Association |
| IP | Internet Protocol |
| IPR | Intellectual Property Right |
| ISP | Internet Service Provider |
| IT | Information Technology |
| NIS | Network and Information Systems |
| NUIG | National University Of Ireland Galway |
| PSD | Payment Services Directive |
| PSD2 | 2nd Payment Services Directive |
| PSDII | Second Payment Service Directive |
| PSPS | Public Safety and Personal Security |
| PSR | Project Security Responsible |
| SA | Solution Architecture |
| SCA | Strong Customer Authentication |
| SW | SoftWare |

Other acronyms and abbreviations not present in the table, are introduced in the text along with their definitions.

# Executive Summary

Recently, some of the most advanced marketplaces have been developed in Europe which provides functionalities for data catalogues, search, analytics, trading, and accounting. Marketplaces such as i3-MARKET, DataVaults, MOSAICrOWN, MUSKETEER provide value-added features for integrating, accessing, and trading data assets, such as data assets monetization, data sovereignty, personal data protection, compliance to regulations (e.g., to GDPR (General Data Protection Regulation)). FAME's ambition is to deliver Europe's first standards-based, secure, regulatory compliant, interoperable, and federated data marketplace platform for Embedded Finance (EmFi) applications. Apart from unique feature of the FAME project, which is federated access control, the project provides a unified access to all related regulations in the field. In that sense, it provides a harmonious ecosystem of the laws and regulations according to the need of different stakeholders.

This Deliverable reports the background study of the related laws and regulations as well as the prototype implementations of the FAME regulatory compliance tool. We also ensure all key achievements and milestones are highlighted to showcase the progress and impact of the project succinctly. The following aspects of the related laws and regulations are highlighted and demonstrated as part of the objective(s) for the regulatory compliance tool reported in this document:

- The possibility of the mapping between FAME and related projects in the field.
- The laws and regulations framework of the similar projects.
- The background study on the related laws and regulations.
- The prototype of the regulatory compliance tool website

In this deliverable we also report on the latest update with task 3.5 asset which is the FAME regulatory compliance tool. The main objective of the regulatory compliance tool is to support unified data policies management in-line with security-by-design and regulatory compliance by design principles, in line with the FAME project functionalities with related laws and regulations that is to comply with the security and regulatory requirements of EmFi applications. In so doing, regulatory compliance tools is set according to the prominent regulations of the sector (i.e., PSD2, MiFIDII, 4AML) in addition to general regulations (e.g., GDPR AI Act). The fundamental aim of FAME's Regulatory Compliance tool is not to designate any sort of legal interpretation or imply that a user should take a certain legal approach. Instead, the aim is to *inform* a user and to facilitating regulatory compliance. The tool does not assume an advisory role, provide legal advice, or insinuate any sort of legal relationship with a user. The intention behind this tool is to provide an initial overview of the legal information, such that a user is informed to know where certain legislation applies in their circumstance.

The tool is up and running and can be access through FAME marketplace portal. The tool provides regulatory compliance information with regards to FAME platform. In close relationship with legal team at FAME we were quite considerate on not to provide legal advisory in any shape or form. Therefore there is a disclaimer in place on this tool that distance FreCo from such activities that may liable FAME.

Final note: This deliverable provides the outcome of design phase of regulatory compliance tool prototype presented in deliverable 3.3 in a concise manner. We strive to maintain this deliverable as stand alone deliverable by providing point of divergence with previous deliverable 3.3. The updated version of the regulatory compliance tool is presented in Chapter 5 of this deliverable in a user friendly manner and walk with user of the tool along the way.

# Table of Contents

# List of Figures

# List of Annexes

# 1 Introduction

FAME is a joint effort of world class experts in data management, data technologies, the data economy and digital finance to develop, deploy and launch to the global market a unique, open, publicly accessible, trustworthy, energy efficient, and secure federated data marketplace for EmFi, which offers novel decentralized programmable pricing and trading of data assets. The FAME data marketplace aims for alleviating the proclaimed limitations of centralized cloud marketplaces towards demonstrating the full potential of the data economy. In this direction, the project enhances a state of the art data marketplace infrastructure (namely the H2020 i3-MARKET marketplace combined with design principles on finance from the H2020 INFINITECH project) with novel functionalities in three complementary directions namely: (i) Secure, interoperable and regulatory compliant data exchange across multiple federated cloud-based data providers in-line with emerging.

The regulatory landscape of the finance sector has been traditionally very dynamic and volatile. Significant changes in regulations and/or the emergence of new regulations has therefore lead to changes in the FAME marketplace implementation. The realization of the project's impacts has been done in phases that were planned at the beginning pf the project. Such a design, implementational and integration, deployment and testing could generate some delays due to the legal implications. However, by providing a thorough review of the related laws and regulations we aim to mitigate the adverse impact of dynamic laws and regulation on the project over the technologies implemented.

We take a systemic approach in reviewing the related laws and regulations. We divide the potential stakeholders into financial institutions, non-financial institutions, public entities, platforms, and individuals. Then we identify three categories of laws and regulations, namely regulations, policy, and standard and guidelines. The related laws and regulations then study in whole by providing detail of each law and regulations. We further provide some information on the mapping between FAME and other related projects name GAIA-X and IDSA.

FAME offers regulatory compliance tools that will ease compliance to applicable regulations. It will also provide support for reliable data provenance, which will ease support for new regulatory rules. In this document we provide an overview of the designed website for regulatory compliance tool. This website summarizes regulatory ecosystem of the Europe in a user friendly way. The users would be able to browse through related laws and regulation and gain access to information regarding regulatory framework. We also suggest an access control for laws and regulation according to the field of their applications.

WP3 is devoted to the implementation of the project's secure, regulatory compliant access to the various federated marketplace, which will lead to the production of the federated catalogue of data assets. Moreover, WP3 will specify the FAME ontologies and will implement the semantic interoperability framework. The WP3 models and ontologies will be used to support the implementation of trusted and efficient analytics in WP5 and the use cases in WP6.

T3.5 Regulatory Compliance Tools (M5-M27); Leader: NUIG; Part.: IQB, KM, UNP, BPFI, AL): This task will specify and implement security policies and data policies that will boost the compliance of data assets to applicable regulations in EmFi UCs (focus on NUIG, IQB). To this end, the security policy management tools of the project will be used to produce various regulatory support and regulatory compliance tools. The work will be driven by the regulatory requirements that will be specified in WP2 and will provide support for regulations like PSDII (focus on BPFI), GDPR (focus of AL), MiFiD (focus of KM), the EU taxonomy for ESG investments (focus of KM), as well as the emerging EU AI Act (focus of AL). In conjunction with the ethical and legal management task of WP1, this task will also specify how the various tools will be used to support the regulation of the FAME marketplace in-line with applicable laws and directives.

This document describes the specifications and the implementation of the regulatory compliance tool for FAME, providing regulatory landscape of the project. D3.3 Mechanisms and Tools for Regulatory Compliance: Prototypes of the regulatory compliance tools (T3.5). The final version of the FAME regulatory compliance tool is the main outcome of the task 3.5 under world package 3 of FAME project is presented here. Feedback from legal advisors of the FAME project, Arthur's Legal, gathered and assimilated in final product in a concise manner. Hence, the final product, regulatory compliance online tool, is user friendly tool that is at the disposal of general public to get familiarized with recent development in related laws and regulations and enjoy comments and suggestions of legal expert and other users in the interactive way.

## 1.1 Objective of the Deliverable

The objective of this deliverable is to document the regulatory compliance tool progress and to present the final version of the FAME Regulatory and Compliance online Tool in the form of a live website. The Online tool relating the relevant laws and regulations is integrated with the FAME reference architecture and the marketplace.

Since deliverable 3.3 we added and updated many aspects of this report in the current document. We added more laws and regulation related to the FAME project and applied consultancy from legal advisors of the project. This document finalizes the report of regulatory compliance tool and present it for the readers.

The FAME regulatory compliance tool objective is to provide a user-centric tool or assistant/wizard that presents related laws and regulations in a user-friendly environment. The related laws and regulations are associated scenarios to identified FAME pilots. To do so, the implemented regulatory framework includes all associated laws and regulations that pilots and the different stakeholders participating in them can use..

## 1.2 Insights from other Tasks and Deliverables

The purpose of this deliverable is to document the outcomes of Task 3.5 Regulatory Compliance Tools. This deliverable aims to present the FAME regulatory compliance tool. This task will specify and implement security policies and data policies that will boost the compliance of data assets to applicable regulations in EmFi UCs (focus on NUIG, IQB). To this end, the security policy management tools of the project will be used to produce various regulatory support and regulatory compliance tools. The work will be driven by the regulatory requirements that will be specified in WP2 and will provide support for regulations like PSDII (focus on BPFI), GDPR (focus of AL), MiFiD (focus of KM), the EU taxonomy for ESG investments (focus of KM), as well as the emerging EU AI Act (focus of AL). In conjunction with the ethical and legal management task of WP1, this task will also specify how the various tools will be used to support the regulation of the FAME marketplace in-line with applicable laws and directives.

As such, this deliverable receives input and refers to work developed as fully open source in other tasks in FAME project and IDSA project. This deliverable primarily serves as first specification and implementation prototype report and as main input for the subsequent deliverables of FAME Work Package 3 (WP3).

## 1.3 Structure

The deliverable is structured as follows:

**Chapter 1 Introduction:**

This section serves as the gateway to the deliverable, detailing the main objectives and goals of the document within the context of the FAME project.

**Chapter 2 Positioning of FAME in the context of similar projects**:

In this section, the deliverable is contextualized within the larger framework of the FAME laws and regulations.

**Chapter 3 Background study on related laws and regulations:**

This crucial section delves into the specifics of laws and regulations within the FAME project. It includes a comprehensive examination of the related laws and regulations. In this sense, each law is study thoroughly by providing details of each regulation.

**Chapter 4 Prototype of the website relating to laws and regulations:**

This section is dedicated to demonstrating the practical application of the key components discussed in previous section. It includes detailed information on the prototype website.

**Chapter 5 The Regulatory Framework Online Tool – Final Version:**

This section provides details of the final product in a user friendly way. This chapter walks with users their journeys embark on the usage of regulatory compliance tool. Each step anointed and described.

**Chapter 6 Conclusions**:

The final section of the deliverable encapsulates the key findings, insights, and outcomes derived from the analysis and demonstrations of the FAME SA and its components. It provides a summary of the deliverable, touching on the significant achievements and the Key Performance Indicators (KPIs) met, as outlined in the document.

**References**

The references considered and most relevant used in this deliverable are included in this chapter.

**Annexes**

The Annexes were introduced to include relevant analysis and also to create a space where large details about regulations can be consulted in case there is further interest by the readers of this document. Thus the Chapter 3 was simplified and reduced to keep the structure of the document. The annexes added are Annex I – Legal Assessment, Annex II – Legal Assessment in Relation to FAME Project and Annex III – Regulations Related to FAME - Deep Analysis.

## 1.4 Table of Changes

The table of changes summarizes the edits and upgrades of this Deliverable D36 in relation to the previous version of this document named Deliverable D3.3. it included new contributions and the latest developments of the FAME Regulatory Compliance Online Tool.

| Section | Status | Description of update/addition |
|---|---|---|
| Executive summary | Added | Paragraph 4 and 5 added to describe the final approach and design concepts of the final FAME regulatory compliance online tool. |
| 1. Introduction | Updated | The introduction was reviewed and updated to represent the current status of regulatory compliance tool as final product and the last paragraph of the Introduction was added to explain the nature of this final document. |
| 1.1 Objective of the Deliverable | Added | Second paragraph added to update descriptions of the objectives in this document related to new and updated features of regulatory compliance tool. |
| 1.3 Structure | Added | Chapter 5: The update version of the Regulatory Framework Online Tool |
| Section 3 | Added/Updated | Thirteen related laws and regulation added to the previous 7 related laws and regulations. Part of the subchapter updated with features legal basis, key definition, and references. |
| Section 5 | Added | This section provides details of the Regulatory Framework Online Tool final version. |
| Annex I | Added | Annex I include a generic list of legislation, both from an end-user and platform perspective. |
| Annex II | Added | Annex II is an overview of additional legislations relevant to the FAME project and included in the Regulatory Framework Online tool. |
| Annex III | Added | Annex II includes the details in relation to the relevant regulations included in chapter 3, this material was moved into an annex to simplify chapter 3 allowing better understanding of the regulations related to the FAME. |
| Overall Structure | Added | Chapter 5 was added, Chapter 3 was simplified and includes more relevant regulations, and 3 annexes are included as listed above. |

# 2 Positioning of FAME in the context of European Initiatives:

## 2.1 FAME versus GAIA-X and IDSA

Figure 1 presents FAME regulatory framework. We divided the potential stakeholders in five groups, namely financial institutions, non-financial institutions, public entities, platforms, and individuals. We also define three main areas in which FAME is located. That is regulations, policy, and standards and guidelines.

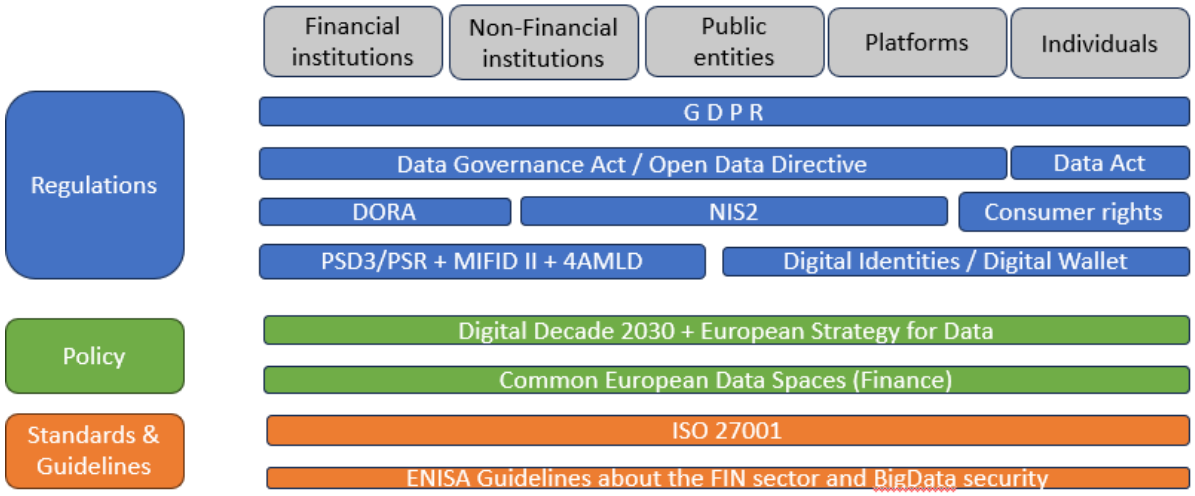



Figure 1. FAME Regulatory Framework

Figure 2 illustrates the FAME regulatory triangle. Accountability, responsibility, and liability are one side of the triangle where transparency, trust, engagement, and success by design is another side of the triangle. Contracts, regulations and legislations, standardisation and guidelines and ethics are the main components of the regulatory triangle.


Figure 2. FAME Regulatory Triangle

While GAIAX provides no specific resolution on the regulatory requirement objectives the IDSA background study on laws and regulation is more comprehensive. The IDSA project complies with GDPR and major regulations in Europe, however they do not provide comprehensive analysis on the related laws and regulations unlike FAME project task 3.5.

IDSA provides a short description of the user-based format while in FAME, we provide a comprehensive study of the related laws and regulations in the systematic manner. For example, we divide the potential users into groups based on their nature and provide related laws and regulations accordingly. We base our analysis on Europe in the same way as what IDSA offers.

Given all these points, we are positive that mapping between IDSA and FAME is possible.

## 2.2 Background study on GAIA-X

Gaia-X is an initiative that develops, based on European values, a digital governance that can be applied to any existing cloud/ edge technology stack to obtain transparency, controllability, portability and interoperability across data and services. Gaia-X is not a market operator, nor will it operate directly or exclusively any of the services required by the governance.

It enables a federated and secure data infrastructure, whereby data are shared, with users retaining control over their data access and usage. It enables the creation of links between many cloud service providers in a wider, transparent and fair ecosystem to drive the European Data economy of tomorrow.

Gaia-X aims to create a federated open data infrastructure based on European values regarding data and cloud sovereignty. The mission of Gaia-X is to design and implement a data sharing architecture that consists of common standards for data sharing, best practices, tools, and governance mechanisms. It also constitutes an EU-anchored federation of cloud infrastructure and data services, to which all 27 EU member states have committed themselves1. This overall mission drives the Gaia-X Architecture.

Gaia-X is:

- A non-profit association in which its members define the Gaia-X architecture & rules
- Gaia-X makes and supports others to make open-source implementations of its specifications
- A qualification authority for the Gaia-X Label, including the Basic Conformity
- GAIA-X project provides no specific resolution on the regulatory requirement objectives.

Gaia-X is Not:

- A formal standardisation body
- A SW or HW product or cloud platform
- A runtime implementation of any Gaia-X service

Data Spaces: What are they?

The term ‘data space’ refers to a type of data relationship between trusted partners who adhere to the same high level standards and guidelines in relation to data storage and sharing within one or many Vertical Ecosystems.A critical aspect of the data space notion is that data are not stored centrally, but rather at the source. Thus, they are only transferred through semantic interoperability as necessary.

A data space is the sum of all its participants, which may be data providers, users and intermediaries. Data spaces can be nested and overlapping. For instance, a data provider can participate in several data spaces all at once. Each Data Space provides specific data. Thereby, it forms a solid ground for one or many ecosystems. The software required to implement data spaces runs on cloud/edge cloud infrastructures.

Data spaces objectives and deliverables within Gaia-X

The main objective of Gaia-X is to create the conditions for an outburst of data within the European market. Key to this is the creation of data spaces, which are the digital representation of existing physical or natural or industrial or social ecosystems. In a data space, several actors belonging to the same value chain (all suppliers and oem in a supply chain, all public and private transportation in a smart city, all hospitals and laboratories in a healthcare, and so forth) federate each other to exchange data. Given the data space create services and insights that can only be achieved through the federation of the multiple actors, every single actor earns a value in participating to the federation that it could not achieve using its data only.

Gaia-X aims to develop data space projects to create an economy of data in several domains, from private to public sector. Through data space projects, Gaia-X will be developed in the market and Gaia-X services will be made available through marketplaces restricted to the federation participants or open to the outside of the federation.

The Gaia-X Association enables the creation of data spaces through the work of the regional hubs. Each hub has the objective to focus on its regional strategic data spaces, and develop concrete business cases creating consortia of member companies around them.

Gaia-X enabled data spaces allow for:

- scaling individual solutions to address new customers
- extending existing solutions with new value propositions
- combine existing solutions to enable collaborations in ecosystems.

Data spaces can be industry-specific or cross-industries, they can involve multiple player within a territory or across territories, and provide for the only way to reduce physical barriers, reduce time to market, leverage the distributed intelligence and create additional value for all, large and small players, users and providers of technology.

Through data space creation, Europe can leverage the most accessible and highest quality raw material that can reinforce our economy by winning the battle of competitivity in the digital era: high quality data. From automotive to healthcare, agriculture to education, transportation, energy or finance, the European processes, legislation, and industrial ecosystem feature by far the highest complexity and quality, and therefore are the way to win the battle to competitivity in the creation of high quality digital products and services.

According to our research, GAIA-X does not provide an stand-alone regulatory compliance framework.

## 2.3 Background study on the International Data Spaces Association

The International Data Spaces Association (IDSA) is on a mission to create the future of the global, digital economy with International Data Spaces (IDS), a secure, sovereign system of data sharing in which all participants can realize the full value of their data.

As an association we are subject to the provisions of the Federal Data Protection Act (BDSG) and the Telemedia Act (TMG). We have taken technical and organisational measures to ensure that the data protection regulations are observed both by us and by external service providers.

Personal data is information that can be used to determine a user's identity. This includes information such as username, address, postal address and telephone number. Information that is not directly associated with the real identity of the user (such as favourite websites or number of users of a site) is not included. Users can use our online offering without disclosing their identity. Personal data is only collected if the user provides it of his or her own accord – for example when registering, making an enquiry via the contact page or submitting an online application.

Access to this data is only possible for a few specially authorised persons who are involved with the technical or editorial support of the servers. In connection with user access, data are stored on our servers for security purposes which may allow identification (for example IP address, date, time and pages viewed). These data are not utilized in a personalised form. We reserve the right to statistically evaluate anonymised data records.

The IP address is stored for data security reasons in order to guarantee the stability and operational security of our system.

1 Name and Address of the controller

Controller for the purposes of the General Data Protection Regulation (GDPR), other data protection laws applicable in Member states of the European Union and other provisions related to data protection is:

International Data Spaces e. V.

Emil-Figge-Str. 80

44227 Dortmund, Germany

Phone: +49 (0) 231 70096 – 501

info@internationaldataspaces.org

Website: www.internationaldataspaces.org

2 Disclosure of personal information to third parties

We do not pass on personal information to third parties without the users' explicit consent. Should data be passed on to service providers within the scope of order data processing, they are bound by the BDSG and other legal regulations. In so far as we are legally obliged to or obliged to do so by court order, we will transfer your data to such bodies that are legally entitled to receive such information.

3 Right of withdrawal

Personal user data can be deleted at any time on request. We set "cookies" (small files with configuration information) in the majority of the internet pages we maintain according to the specifications of the Informationgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e. V. – IVW (German Audit Bureau of Circulation) and for measuring access to advertising media. They

help to determine the frequency of use and the number of users of our websites. We do not collect any personal data via cookies. In some areas of our website we use cookies to implement user functions. Our website can also be used without cookies. Most browsers are set to accept cookies automatically. However, the user can deactivate the storage of cookies or set his or her browser in a way that he or she is informed as soon as cookies are sent.

4 Children

Persons under the age of 18 should not transmit any personal data to us without the consent of their parents or legal guardians.

5 Links

Our website may contain links to other websites. We have no influence over whether their operators comply with the data protection regulations.

6 Reserve the right to change

The rapid development of the internet requires adjustments to the data protection declaration from time to time. We will inform you of any necessary changes.

7 Cookies

Our Internet pages use cookies. Cookies are text files that are stored in a computer system via an Internet browser.

Many Internet sites and servers use cookies. Many cookies contain a so-called cookie ID. A cookie ID is a unique identifier of the cookie. It consists of a character string through which Internet pages and servers can be assigned to the specific Internet browser in which the cookie was stored. This allows visited Internet sites and servers to differentiate the individual browser of the dats subject from other Internet browsers that contain other cookies. A specific Internet browser can be recognized and identified using the unique cookie ID.

Through the use of cookies, the IDSA can provide the users of this website with more user-friendly services that would not be possible without the cookie setting.

By means of a cookie, the information and offers on our website can be optimized with the user in mind. Cookies allow us, as previously mentioned, to recognize our website users. The purpose of this recognition is to make it easier for users to utilize our website. The website user that uses cookies, e.g. does not have to enter access data each time the website is accessed, because this is taken over by the website, and the cookie is thus stored on the user’s computer system. Another example is the cookie of a shopping cart in an online shop. The online store remembers the articles that a customer has placed in the virtual shopping cart via a cookie.

The data subject may, at any time, prevent the setting of cookies through our website by means of a corresponding setting of the Internet browser used, and may thus permanently deny the setting of cookies. Furthermore, already set cookies may be deleted at any time via an Internet browser or other software programs. This is possible in all popular Internet browsers. If the data subject deactivates the setting of cookies in the Internet browser used, not all functions of our website may be entirely usable.

8 Subscription to our newsletters

On our website, users are given the opportunity to subscribe to our enterprise's newsletter. The input mask used for this purpose determines what personal data are transmitted, as well as when the newsletter is ordered from the controller.

The IDSA informs its customers and business partners regularly by means of a newsletter about enterprise offers. The enterprise's newsletter may only be received by the data subject if (1) the data subject has a valid e-mail address and (2) the data subject registers for the newsletter shipping. A confirmation e-mail will be sent to the e-mail address registered by a data subject for the first time for newsletter shipping, for legal reasons, in the double opt-in procedure. This confirmation e-mail is used to prove whether the owner of the e-mail address as the data subject is authorized to receive the newsletter.

During the registration for the newsletter, we also store the IP address of the computer system assigned by the Internet service provider (ISP) and used by the data subject at the time of the registration, as well as the date and time of the registration. The collection of this data is necessary in order to understand the (possible) misuse of the e-mail address of a data subject at a later date, and it therefore serves the aim of the legal protection of the controller.

The personal data collected as part of a registration for the newsletter will only be used to send our newsletter. In addition, subscribers to the newsletter may be informed by e-mail, as long as this is necessary for the operation of the newsletter service or a registration in question, as this could be the case in the event of modifications to the newsletter offer, or in the event of a change in technical circumstances. There will be no transfer of personal data collected by the newsletter service to third parties. The subscription to our newsletter may be terminated by the data subject at any time. The consent to the storage of personal data, which the data subject has given for shipping the newsletter, may be revoked at any time. For the purpose of revocation of consent, a corresponding link is found in each newsletter. It is also possible to unsubscribe from the newsletter at any time directly on the website of the controller, or to communicate this to the controller in a different way.

9 Newsletter-Tracking

The newsletter of the IDSA contains so-called tracking pixels. A tracking pixel is a miniature graphic embedded in such e-mails, which are sent in HTML format to enable log file recording and analysis. This allows a statistical analysis of the success or failure of online marketing campaigns. Based on the embedded tracking pixel, the IDSA may see if and when an e-mail was opened by a data subject, and which links in the e-mail were called up by data subjects.

Such personal data collected in the tracking pixels contained in the newsletters are stored and analyzed by the controller in order to optimize the shipping of the newsletter, as well as to adapt the content of future newsletters even better to the interests of the data subject. These personal data will not be passed on to third parties. Data subjects are at any time entitled to revoke the respective separate declaration of consent issued by means of the double-opt-in procedure. After a revocation, these personal data will be deleted by the controller. The IDSA automatically regards a withdrawal from the receipt of the newsletter as a revocation.

10 Contact possibility via the website

The website of the IDSA contains information that enables a quick electronic contact to our enterprise, as well as direct communication with us, which also includes a general address of the so-called electronic mail (e-mail address). If a data subject contacts the controller by e-mail or via a contact form, the personal data transmitted by the data subject are automatically stored. Such personal

data transmitted on a voluntary basis by a data subject to the data controller are stored for the purpose of processing or contacting the data subject. There is no transfer of this personal data to third parties.

11 Routine erasure and blocking of personal data

The data controller shall process and store the personal data of the data subject only for the period necessary to achieve the purpose of storage, or as far as this is granted by the European legislator or other legislators in laws or regulations to which the controller is subject to.

If the storage purpose is not applicable, or if a storage period prescribed by the European legislator or another competent legislator expires, the personal data are routinely blocked or erased in accordance with legal requirements.

12 Legal basis for the processing

Art. 6(1) lit. a GDPR serves as the legal basis for processing operations for which we obtain consent for a specific processing purpose. If the processing of personal data is necessary for the performance of a contract to which the data subject is party, as is the case, for example, when processing operations are necessary for the supply of goods or to provide any other service, the processing is based on Article 6(1) lit. b GDPR. The same applies to such processing operations which are necessary for carrying out pre-contractual measures, for example in the case of inquiries concerning our products or services. Is our company subject to a legal obligation by which processing of personal data is required, such as for the fulfillment of tax obligations, the processing is based on Art. 6(1) lit. c GDPR. In rare cases, the processing of personal data may be necessary to protect the vital interests of the data subject or of another natural person. This would be the case, for example, if a visitor were injured in our company and his name, age, health insurance data or other vital information would have to be passed on to a doctor, hospital or other third party. Then the processing would be based on Art. 6(1) lit. d GDPR. Finally, processing operations could be based on Article 6(1) lit. f GDPR. This legal basis is used for processing operations which are not covered by any of the abovementioned legal grounds, if processing is necessary for the purposes of the legitimate interests pursued by our company or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. Such processing operations are particularly permissible because they have been specifically mentioned by the European legislator. He considered that a legitimate interest could be assumed if the data subject is a client of the controller (Recital 47 Sentence 2 GDPR).

13 Rights of the data subject

a) Right of confirmation

Each data subject shall have the right granted by the European legislator to obtain from the controller the confirmation as to whether or not personal data concerning him or her are being processed. If a data subject wishes to avail himself of this right of confirmation, he or she may, at any time, contact any employee of the controller.

b) Right of access

Each data subject shall have the right granted by the European legislator to obtain from the controller free information about his or her personal data stored at any time and a copy of this information. Furthermore, the European directives and regulations grant the data subject access to the following information:

the purposes of the processing;

the categories of personal data concerned;

the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

the existence of the right to request from the controller rectification or erasure of personal data, or restriction of processing of personal data concerning the data subject, or to object to such processing;

the existence of the right to lodge a complaint with a supervisory authority;

where the personal data are not collected from the data subject, any available information as to their source;

the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.

Furthermore, the data subject shall have a right to obtain information as to whether personal data are transferred to a third country or to an international organisation. Where this is the case, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

If a data subject wishes to avail himself of this right of access, he or she may, at any time, contact any employee of the controller.

c) Right to rectification

Each data subject shall have the right granted by the European legislator to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

If a data subject wishes to exercise this right to rectification, he or she may, at any time, contact any employee of the controller.

d) Right to erasure (Right to be forgotten)

Each data subject shall have the right granted by the European legislator to obtain from the controller the erasure of personal data concerning him or her without undue delay, and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies, as long as the processing is not necessary:

The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

The data subject withdraws consent to which the processing is based according to point (a) of Article 6(1) of the GDPR, or point (a) of Article 9(2) of the GDPR, and where there is no other legal ground for the processing.

The data subject objects to the processing pursuant to Article 21(1) of the GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) of the GDPR.

The personal data have been unlawfully processed.

The personal data must be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.

The personal data have been collected in relation to the offer of information society services referred to in Article 8(1) of the GDPR.

If one of the aforementioned reasons applies, and a data subject wishes to request the erasure of personal data stored by the IDSA, he or she may, at any time, contact any employee of the controller. An employee of IDSA shall promptly ensure that the erasure request is complied with immediately.

Where the controller has made personal data public and is obliged pursuant to Article 17(1) to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other controllers processing the personal data that the data subject has requested erasure by such controllers of any links to, or copy or replication of, those personal data, as far as processing is not required. An employees of the IDSA will arrange the necessary measures in individual cases.

e) Right of restriction of processing

Each data subject shall have the right granted by the European legislator to obtain from the controller restriction of processing where one of the following applies:

The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.

The processing is unlawful and the data subject opposes the erasure of the personal data and requests instead the restriction of their use instead.

The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims.

The data subject has objected to processing pursuant to Article 21(1) of the GDPR pending the verification whether the legitimate grounds of the controller override those of the data subject.

If one of the aforementioned conditions is met, and a data subject wishes to request the restriction of the processing of personal data stored by the IDSA, he or she may at any time contact any employee of the controller. The employee of the IDSA will arrange the restriction of the processing.

f) Right to data portability

Each data subject shall have the right granted by the European legislator, to receive the personal data concerning him or her, which was provided to a controller, in a structured, commonly used and machine-readable format. He or she shall have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, as long as the processing is based on consent pursuant to point (a) of Article 6(1) of the GDPR or point (a) of Article 9(2) of the GDPR, or on a contract pursuant to point (b) of Article 6(1) of the GDPR, and the

processing is carried out by automated means, as long as the processing is not necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Furthermore, in exercising his or her right to data portability pursuant to Article 20(1) of the GDPR, the data subject shall have the right to have personal data transmitted directly from one controller to another, where technically feasible and when doing so does not adversely affect the rights and freedoms of others.

In order to assert the right to data portability, the data subject may at any time contact any employee of the IDSA.

g) Right to object

Each data subject shall have the right granted by the European legislator to object, on grounds relating to his or her particular situation, at any time, to processing of personal data concerning him or her, which is based on point (e) or (f) of Article 6(1) of the GDPR. This also applies to profiling based on these provisions.

The IDSA shall no longer process the personal data in the event of the objection, unless we can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.

If the IDSA processes personal data for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing. This applies to profiling to the extent that it is related to such direct marketing. If the data subject objects to the IDSA to the processing for direct marketing purposes, the IDSA will no longer process the personal data for these purposes.

In addition, the data subject has the right, on grounds relating to his or her particular situation, to object to processing of personal data concerning him or her by the IDSA for scientific or historical research purposes, or for statistical purposes pursuant to Article 89(1) of the GDPR, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

In order to exercise the right to object, the data subject may contact any employee of the IDSA. In addition, the data subject is free in the context of the use of information society services, and notwithstanding Directive 2002/58/EC, to use his or her right to object by automated means using technical specifications.

h) Automated individual decision-making, including profiling

Each data subject shall have the right granted by the European legislator not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her, or similarly significantly affects him or her, as long as the decision (1) is not is necessary for entering into, or the performance of, a contract between the data subject and a data controller, or (2) is not authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, or (3) is not based on the data subject’s explicit consent.

If the decision (1) is necessary for entering into, or the performance of, a contract between the data subject and a data controller, or (2) it is based on the data subject’s explicit consent, the IDSA shall implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate

interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and contest the decision.

If the data subject wishes to exercise the rights concerning automated individual decision-making, he or she may, at any time, contact any employee of the IDSA.

i) Right to withdraw data protection consent

Each data subject shall have the right granted by the European legislator to withdraw his or her consent to processing of his or her personal data at any time.

If the data subject wishes to exercise the right to withdraw the consent, he or she may, at any time, contact any employee of the IDSA.

14 Web Analytics/Tracking

Our website uses the Matomo open source software by InnoCraft Ltd in New Zealand to analyze the activities of our website users and to optimize our website and its content based on this analysis. In so doing we do not obtain any information that identifies you directly.

The Matomo version we use takes precautions based on DoNotTrack technology (see on this www.donottrack.us) to ensure your website search is not captured if you have set your internet browser to stop tracking.

The use of Matomo involves cookies and tracking pixels which allow statistical analysis of the use of this website based on your visits. The cookie saves information, including personal information, on your visiting behavior on our website, which Matomo then processes under a pseudonym in a user profile for analytical purposes. . Since we host Matomo on our own servers, the analysis does not require data processing by third parties.

Without your specific permission, we neither use the data collected to identify you personally nor will we match the data with personal data pertaining to the pseudonym associated with you.

If IP addresses are collected, they are immediately anonymized after collection by deleting the last number block.

We process statistical data based on our legitimate interest pursuant to Article 6 (1) lit. f GDPR to optimize our online offering and our web presence.

New EU regulatory environment for data spaces

The EU Commission published the “European Strategy for Data” in 2020 to create a single market for data that ensures Europe's global competitiveness and data sovereignty.

As part of this strategy, the Commission proposed different regulations:

- AI Act Proposal (AIA-E)
- Data Act Proposal (DA-E)
- Data Governance Act (DGA)

- Digital Markets Act (DMA)
- Digital Services Act (DSA)

The complexity of the regulatory framework is increasing, but the regulations are not yet aligned, and the interplay with existing legislation such as data protection laws, competition laws, or regulations on intellectual property is not clear. Also, the terminology is not aligned, which causes difficulties in their interpretation and interoperability with existing legislation.

The new regulations differ regarding their subject matter and scope. While the DMA and the DSA are instruments to regulate competition and rights in the digital market, the DA-E and the DGA mainly concern access and use of data. The AI Act can be seen as a separate proposal with little connection to the others. With respect to B2B data spaces, the more general DA-E and DGA will have the greatest impact, while the other regulations are less central in this scope.

Considerations regarding DA-E and DGA

The DA-E concerns the rights to access and use data generated by Internet of Things (IoT) devices. Therefore, it applies to roles related to such data, including manufacturers, data holders, data recipients, and providers of data processing services. As the DA-E covers the whole lifecycle of data processing, it may impact use cases in the data space as the data needs to be handled in compliance (e.g., the grant of access rights).

Due to its broad definitions, the DA-E leaves considerable room for interpretation, creating legal uncertainty. Another uncertainty concerns the interfering with existing contracts and the DA-E impact on the contractual freedom. The freedom to negotiate should be restricted as little as possible to encourage the building of value chains and innovation. Imbalances could instead be addressed through EU competition law or sector-specific legislation. It remains to be seen to what extent the DA-E will undergo adjustments to create legal certainty and practical solutions for data sharing.

The DGA comes also with some concerns, especially regarding the broad definitions for the roles in data sharing (e.g., data holder, data user). Also, how it addresses services provider roles does not cover the complexity of data spaces. The envisioned data governance and the respective roles do not achieve the intended goals of facilitating data sharing. Given the complex roles and services within data spaces, the DGA term “data intermediation services” needs to be aligned with practice as data spaces use different terms for data sharing services.

The DGA defines a number of obligations (such as notification and compliance requirements), especially regarding intermediation service providers, that play a key role in the data economy:

- Obligation for data sharing service providers to notify competent authority.
- Conditions for providing data sharing services, such as neutrality, fair, transparent, and non-discriminatory access to services, adequate technical, legal, and organizational measures to prevent transfer or access to non-personal data that is unlawful under Union law.

The European Commission decided to adopt this approach to ensure that data governance within the Union is based on trustworthy sharing of data. A key element in increasing trust and control of data holders, data subjects, and data users is the neutrality of data intermediation service providers concerning the data shared. It is necessary for these providers to act only as intermediaries and not use the data shared for any other purpose.

The approach and key elements of IDS concepts reflect the DGA's goal of trustworthy data sharing, which involves neutral intermediaries and reliance on reference architecture, connector technology, and certifications.

Challenges and opportunities for EU's DIB in developing common data spaces

The DGA approach comes with several challenges. It only frames general rules, while the details are subject to national laws and need to be translated into practical solutions. The European Data Innovation Board (EDIB), proposed by the DGA, will play a fundamental role. It will support the EU Commission in issuing guidelines to facilitate the development of common European data spaces, as well as identifying standards and interoperability requirements for cross-sector data sharing.

There might be a link between the DGA and other regulations on the topic of interoperability standards. For example, the DA-E defines that the guidelines for "interoperability specifications for the functioning of common European data spaces, such as architectural models and technical standards implementing legal rules and arrangements between parties that foster data sharing, such as regarding rights to access and technical translation of consent or permission" should come from the EU Commission. Therefore, it is likely that such guidelines will come from the EDIB under the DGA. It will be beneficial to link these tasks to achieve harmonized rules in practice between both regulations.

This task will directly relate to the activities of data space initiatives such as IDSA, which will play a major role, as they have already developed frameworks and reference architectures that can act as blueprints for common standards. The EU strategy should build upon existing data sharing initiatives in the quest for interoperability and the specification of future soft infrastructure agreements (see L. Nagel and D. Lycklama in Designing Data Spaces – The Ecosystem Approach to Competitive Advantage, p. 19; https://link.springer.com/content/pdf/10.1007/978-3-030-93975-5.pdf.)

For the future development of data spaces in light of the new EU regulations, the Data Spaces Support Centre (see DSSC – Data Space Support Centre) will also play a significant role in providing aligned support for common EU data spaces.

In the "European Strategy for Data", the Commission proposed five regulations

AI Act Proposal (AIA-E): Proposed April 2021, legislative procedure ongoing. EU framework for regulating AI; Applies to providers and users of AI.

Data Act Proposal (DA-E): Proposed February 2022, legislative procedure ongoing Obligations of developers + manufacturers of products to facilitate the user's access to data generated during the use. Facilitating switching of data processing services, introducing safeguards, and interoperability standards.

Data Governance Act (DGA): Applicable September 24, 2023. Reuse of data by public sector bodies; framework for data intermediation services + voluntary registration of entities that process data made available for altruistic purposes; European Data Innovation Board.

Digital Markets Act (DMA): Entered into force on May 2, 2023. Regulating internet corporations/ gatekeepers (e.g., social media platforms, search engines). Prohibits practices that make it difficult for users to use non-gatekeeper providers.

Digital Services Act (DSA): Will enter into force on February 16, 2024 (some provisions apply earlier). Protection against illegal content + for users' rights. Applies to intermediary services (e.g.,

internet access providers, cloud services). Regulations on liability, handling of illegal content, provision of a notice-and-takedown procedure, and regulation of online platforms.

# 3 Background study on related laws and regulations

In this section we provide thorough details on each related law and regulation in the field. We divide our analysis into seven part, each part representing a related law.

## 3.1 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) [1] is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live and outside of the European Union (EU)1. It was drafted and passed by the European Union (EU) and imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU2. GDPR is designed to give EU citizens more control over their personal data and simplify the regulatory environment for business so both citizens and businesses in the European Union can fully benefit from the digital economy [2].

The General Data Protection Regulation (Regulation (EU) 2016/679, abbreviated GDPR) is a European Union regulation on Information privacy in the European Union (EU) and the European Economic Area (EEA). The GDPR is an important component of EU privacy law and human rights law, in particular Article 8(1) of the Charter of Fundamental Rights of the European Union. It also governs the transfer of personal data outside the EU and EEA. The GDPR's goals are to enhance individuals' control and rights over their personal information and to simplify the regulations for international business. It supersedes the Data Protection Directive 95/46/EC and, among other things, simplifies the terminology.

The European Parliament and Council of the European Union adopted the GDPR on 14 April 2016, to became effective on 25 May 2018. Because the GDPR is a regulation, rather than a European Union directive, it is directly binding and applicable,[clarification needed : On whom? What does 'directly binding and applicable' mean?] and it provides flexibility for individual member states to modify some provisions of the GDPR.

The regulation became a model for many other laws around the world, including in Turkey, Mauritius, Chile, Japan, Brazil, South Korea, South Africa, Argentina and Kenya. As of 6 October 2022, the United Kingdom enacted its own law identical to the GDPR despite no longer being an EU member state. The California Consumer Privacy Act (CCPA), adopted on 28 June 2018, has many similarities with the GDPR.

### 3.1.1 Key Definitions

- Personal data; any information that directly or indirectly identifies a natural person (a data subject) which can include:A name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person
- Processing; Operation or sets of operations conducted on personal data. These activities are considered to be ‘processing’:
- Collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- Controller; determines the purpose and means of processing of personal data. This can be a natural or legal person, public authority, agency, or other body.
- Processor; a natural or legal person, public authority, agency, or other body that processes personal data on behalf of a controller.

### 3.1.2 Reference

- GDPR frequently asked questions

## 3.2 Data Act

The DATA Act [3] is a law that aims to make information on federal expenditures more easily accessible and transparent12. It requires federal agencies to report and track their spending data using government-wide standards established by OMB and Treasury34. The DATA Act covers over $3.7 trillion in annual federal spending and links it to federal program activities32. The DATA Act should not be confused with the Data Act of the European Union, which is a different initiative [4]. Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016.

### 3.2.1 Key Definitions

- Product data: data generated by the use of a connected product that the manufacturer designed to be retrievable, via an electronic communications service, physical connection, or on-device access, by a user, data holder or a third party, including, where relevant, the manufacturer.
- Connected product; an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user.
- Customer; a natural or legal person that has entered into a contractual relationship with a provider of data processing services with the objective of using one or more data processing services.
- Related service; data representing the digitisation of user actions or of events related to the connected product, recorded intentionally by the user, or generated as a by-product of the user's action during the provision of a related service by the provider.
- Data processing service; digital service that is provided to a customer and that enables ubiquitous and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature that can be rapidly provisioned and released with minimal management effort or service provider interaction
- Data intermediary service; a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal, or other means,
- User; a natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services.
- Data holder; a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service
- Data recipient; a natural or legal person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a connected product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation adopted in accordance with Union law.

### 3.2.2 Reference

- Data Act: frequently asked questions

## 3.3 The Data Governance Act & The Open Data Directive

On 25 November 2020, The European Commission published the Data Governance Act (DGA) [5] in response to the public consultation on the European Strategy for Data. The consultation served as a means to gauge stakeholders' opinions on the data strategy (including open data, data sharing and data spaces), and as input for several planned initiatives around access to, and re-use of, data. A legislative framework on common European data spaces and an implementing act on a list of high-value datasets under the Open Data Directive was part of the consultation as well.

This featured highlight will explore what the results of the public consultation are and delve into the Open Data Directive.

Consultation on the European Strategy for Data

The EU Public Consultation on the European Strategy for Data received contributions from various stakeholders, including SMEs, EU citizens, business associations, academia, research institutes, as well as public authorities. Results from the consultation fall into four categories:

1. The data strategy, of which 97.2% of the 806 respondents confirmed that the EU needs an overarching data strategy to enable the digital transformation of society, with 91.5% agreeing to the following statement:

2. "More data should be available for the common good, for example for improving mobility, delivering personalized medicine, reducing energy consumption and making our society greener."

3. Data governance, including data standardisation, secondary use of data, data donation and data intermediaries. 772 of the 806 respondents answered this section. 90% of the 772 consider data governance mechanisms necessary to capture the enormous potential of data, particularly for cross-sector data use.

4. High-value datasets, with some 761 of the 806 respondents contributed to this section. 82.2% of these respondents answered that a list of high value datasets (available free of charge, with no restrictions and accessible via application programme interfaces) are a good way to ensure that public sector data can have a positive impact on the EU economy and society. High-value datasets are those with a high commercial potential and the ability to accelerate the development of value-increasing information products across the EU.

5. The (self-/co-) regulatory context of cloud computing, where 61% of respondents state that the current cloud market offers technological solutions that businesses need to continue growing and innovating. However, 48% of 444 stakeholders answered that at one point they have experienced problems in the functioning of the cloud market, and 68% of 449 stakeholders expect risks for the future. Going forward, 59% of responding users and 64% of responding providers state that self-regulation is appropriate to identify best practices to implement EU legislation around cloud computing.

The Open Data Directive

As part of the European Strategy for Data, the Open Data Directive functions as a common legal framework for government-held data (public sector information) and is geared towards two key concepts in the European market: i.e. transparency and fair competition. This directive will be put in place on the national level over the course of the next years and will ultimately:

- Stimulate the publication of dynamic data and the uptake of Application Programme Interfaces (APIs);

- Reduce the exceptions that now enable public bodies to charge more than marginal costs of dissemination for data re-use;

- Extend the scope of the directive to include data held by public undertakings, under a specific set of rules and research data resulting from public funding; and

- Strengthen the transparency requirements for agreements involving public sector information between public and private parties, thereby avoiding exclusive deals.

Furthermore, the directive includes the adoption of a free-of-charge list of high-value datasets by the Commission. The consultation indicates that the need for these types of datasets is high among stakeholders. They will be labelled within a specific thematic categorisation in the Annex to the directive and act as the building blocks for Artificial Intelligence solutions.

High-value datasets will become a more prevalent topic over the next years and the Digital Governance Act as well as the Open Data Directive provide an initial framework for their arrival and implementation.

The Data Governance Act promotes the re-use of certain categories of data and applies to those held by public authorities but also provides certain organizational rules for data intermediary service providers.

It refers publicly held data that is protected on the following grounds:

- Commercial confidentiality
- Statistical confidentiality
- Third party IPR protection
- Protection of personal data

## 3.4 Digital Operational Resilience Act (DORA)

The Digital Operational Resilience Act (DORA) [6] is a EU regulation that entered into force on 16 January 2023 and will apply as of 17 January 2025.

It aims at strengthening the IT security of financial entities such as banks, insurance companies and investment firms and making sure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption.

DORA brings harmonisation of the rules relating to operational resilience for the financial sector applying to 20 different types of financial entities and ICT third-party service providers.

Why is DORA needed?

The financial sector is increasingly dependent on technology and on tech companies to deliver financial services. This makes financial entities vulnerable to cyber-attacks or incidents.

When not managed properly, ICT risks can lead to disruptions of financial services offered across borders. This in turn, can have an impact on other companies, sectors and even on the rest of the economy, which underlines the importance of the digital operational resilience of the financial sector.

This is where the Digital Operational Resilience Act, or DORA, comes into play.

What does it cover?

- ICT risk management. Principles and requirements on ICT risk management framework
- ICT third-party risk management. Monitoring third-party risk providers. Key contractual provisions
- Digital operational resilience testing. Basic and advanced testing
- ICT-related incidents. General requirements. Reporting of major ICT-related incidents to competent authorities.
- Information sharing. Exchange of information and intelligence on cyber threats.
- Oversight of critical third-party providers Oversight framework for critical ICT third-party providers

Next Steps

The European Supervisory Agencies (ESAs), the European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA) and European Securities and Markets Authority, are jointly leading the development of technical standards as required by the DORA Regulation. These are progressing in two tranches, the first of which is published for public consultation by the ESAs between June and September 2023. The second tranche is expected towards the end of the year. These two tranches of technical standards will:

Tranche 1:

- Further specify required elements of financial entity's risk management framework, and, where applicable, a simplified risk management framework
- Further specify the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats
- Further specify outsourcing policy on contractual arrangements with ICT service providers supporting critical or important functions
- Establish standard templates to be used in the register of information on in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers.

Tranche 2:

- Establish forms and procedures for financial entities to report a major ICT-related incident and to notify significant cyber threats

- Specify further elements for financial entities to determine and assess when sub-contracting ICT services supporting critical or important functions

- Further specify the details of advanced testing of ICT tools, systems and processes based on threat led penetration testing (TLPT) - including criteria to be used to identify those financial entities that are required to perform TLPT

- Harmonise conditions enabling the conduct of oversight of ICT service providers which are

These technical standards are to be developed by the Joint Committee of the ESAs for adoption by the European Commission in January and July 2024.

Pending the adoption of these technical standards, the DORA Regulation itself already contains a lot of useful information on the requirements which financial entities will be required to comply with from January 2025.

Financial entities should be considering steps they will need to take between now and January 2025 to ensure that they can comply with this regulation and support the intended benefits of increased harmonisation of digital operational resilience across the European financial system.

Applies to the following financial entities:

Credit institutions; Payment institutions; Account information service providers; Electronic money institutions; Investment firms; Crypto-asset service providers; Central securities depositories; Central counterparties; Trade venues; Trade repositories; Managers of alternative investment funds; Management companies; Data reporting service providers; Insurance and reinsurance undertakings; Insurance/re-insurance/ancillary intermediaries; Institutions for occupational retirement provision; Credit rating agencies; Administrators of critical benchmarks; Crowdfunding service providers; Securitisation repositories; ICT third-party services providers.

## 3.5 The NIS2 Directive A high common level of cybersecurity in the EU

The Network and Information Security (NIS) Directive [7] is the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States. While it increased the Member States' cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation at different levels across the internal market To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the Commission has submitted a proposal to replace the NIS Directive and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. The proposed expansion of the scope covered by NIS2, by effectively obliging more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term. Within the European Parliament, the file was assigned to the Committee on Industry, Research and Energy. The committee adopted its report on 28 October 2021, while the Council agreed its position on 3 December 2021. The co-legislators reached a provisional agreement on the text on 13 May 2022. The political agreement was formally adopted by the Parliament and then the Council in November 2022. It entered into force on 16 January 2023, and Member States now have 21 months, until 17 October 2024, to transpose its measures into national law.

Cyber-attacks, besides being among the fastest-growing form of crime worldwide, are also growing in scale, cost and sophistication. In 2017, Cybersecurity Ventures forecast that global ransomware damage costs would reach US$20 billion by 2021, 57 times more than the amount in 2015. It alsopredicted that companies would be suffering a ransomware attack every 11 seconds by 2021, up from every 40 seconds in 2016. As a result, businesses have to invest more money to make cyberspace safer for themselves and their customers. Not only companies but also citizens and entire countries have been affected; the first known cyber-attack on a country was mounted on Estonia in April 2007, affecting the online services of banks, media outlets and government bodies for weeks. Since then, many other countries have suffered cyber-attacks, including on critical infrastructure, such as on electric power systems, hospitals or water plants. According to a Eurobarometer survey, about three quarters (76 %) of respondents believe that they are facing an increasing risk of falling victim to cybercrime. In 2019, about 64 % of the US population experienced a data breach and 88 % of organisations worldwide experienced 'spear-phishing' attempts.

### 3.5.1 Key Definitions

Cybersecurity; the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats

Network and information system; can mean:

- An ‘electronic communications network’ as described under article 2(1) of Directive 2018/1972.
- Any device or group of interconnected or related devices, one or more of which, pursuant to a programme, conduct automatic processing of digital data.
- Digital data stored, processed, retrieved, or transmitted by elements covered under the above points, for the purposes of their operation, use, protection, and maintenance.

Security of network and information system; the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems.

Cyber-threat; any potential circumstance, event or action that could damage, disrupt, or otherwise adversely impact network and information systems, the users of such systems and other persons.

### 3.5.2 Reference

- NIS2: Frequently Asked Questions

## 3.6 The PSD3 and PSR in detail

The existing regulatory framework applicable to authorization and supervision of payment institutions and e-money institutions (EMIs) currently anchored in PSD2 and the second E-Money Directive (EMD2) will be merged into a single rule book comprised of PSD3 and PSR [8]. Accordingly, EMIs will become a subcategory of PSPs under the proposed framework with a more harmonized authorization and common supervision process. The Commission also introduces a new

definition of "electronic money services" to include e-money issuance, payment account maintenance and transfer of e-money. PSD2's scope of application and exceptions from the authorization obligation are rehoused to the PSR so as to standardize the EU payment services regulatory framework across the EU.

Summary of key reforms, As for the modernisation of the PSD 2 – which will become PSD 3 – alongside the new PSR, the legislative proposals focus on the following reforms:

Combating and mitigating payment fraud

Allowing PSPs to:

1. voluntarily communicate and share fraud-related information between themselves;

2. increasing consumers' awareness;

3. strengthening customer authentication and SCA rules; and

4. extending refund rights of consumers who fall victim to fraud and making a system for checking alignment of payees' IBAN numbers with their account names mandatory for all credit transfers.

Both the Payment Service Regulation and the Directive apply to Payment service providers (PSPS) operating in the European Economic Area (EEA), including:

- Credit institutions
- Payment institutions
- Post office giro institutions
- the ECB and national central banks when not acting in their capacity as monetary authority or other public authorities
- Member States or their regional or local authorities when not acting in their capacity as public authorities.
- Third-party providers (TPPs) that access customer account data or initiate payments on behalf of users.
- New entrants and FinTechs offering payment-related services under EU jurisdiction.

### 3.6.1 Key Definitions

- Payment service; any business included in Annex I of PSD3 and PSR
- Payment institution; a legal person that has been granted authorisation to provide payment services or electronic money services throughout the Union
- Payment transaction; an act of placing, transferring, or withdrawing funds, based on a payment order placed by the payer, or on his behalf, or by the payee, or on his behalf, irrespective of any underlying obligations between the payer and the payee
- Payer; a natural or legal person who holds a payment account and places a payment order from that payment account, or, where there is no payment account, a person who places a payment order

- Payee; a natural or legal person who is the intended recipient of funds which are the subject of a payment transaction
- Payment service provider; a body as referred to in Article 2(1) of PSD3 or a natural or legal person benefiting from an exemption pursuant to Articles 34, 36 and 38 of PSD3.
- Electronic money services; means the issuance of electronic money, the maintenance of payment accounts storing electronic money units, and the transfer of electronic money units.

### 3.6.2 Reference

- Payment services revised rules

## 3.7 Consumer Rights Directive

The Consumer Rights Directive 2011/83/EU [9] is a consumer protection measure in EU law.[2][3] It was due to be implemented by 13 December 2013. The Directive applies to most contracts between traders and consumers and applied to all contracts concluded after 13 June 2014.[6] Exceptions include financial services, gambling, healthcare by regulated professionals, package travel,[7] property transactions, social services, timeshare[7] and most aspects of passenger transport.

The Consumers Rights Directive 2011/83/EU is applicable to contractual agreements concluded between a trader and a consumer. This includes contracts for the supply of water, gas, electricity, or district heating concluded by both private and public providers.

### 3.7.1 Key Definitions

Consumer; any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession.

Trader; any natural person or any legal person, irrespective of whether privately or publicly owned, who is acting, including through any other person acting in his name or on his behalf, for purposes relating to his trade, business, craft, or profession.

Goods; any tangible movable items, except for items sold by way of execution or otherwise by authority of law; water, gas and electricity shall be considered as goods.

Sales contract; any contract under which the trader transfers or undertakes to transfer the ownership of goods to the consumer and the consumer pays or undertakes to pay the price thereof, including any contract having as its object both goods and services.

Service contract; any contract other than a sales contract under which the trader supplies or undertakes to supply a service to the consumer and the consumer pays or undertakes to pay the price thereof

Distance contract; any contract concluded between the trader and the consumer under an organised distance sales or service-provision scheme without the simultaneous physical presence of the trader and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded.

### 3.7.2 Reference

- Information on the consumer rights directive
- Legislation train: Consumer Rights
- Information on the consumer rights directive
- Consumer Rights Directive text
- Directive 2019/2161

## 3.8 Open Data Directive

The open data directive provides a minimum set of rules concerning the governance of, and practical arrangements for facilitating the re-use of existing documents held by public sector bodies of the Member States, existing documents held by public undertakings, and research data.

### 3.8.1 Key Definitions

Public sector body; the State, regional or local authorities, bodies governed by public law or associations formed by one or more such authorities or one or more such bodies governed by public law

Bodies governed by public law; bodies that possess the following characteristics:

- They are established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character
- They have legal personality
- They are financed, for the most part by the State, regional or local authorities, or by other bodies governed by public law; or are subject to management supervision by those authorities or bodies; or have an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities, or by other bodies governed by public law

Public undertaking; means any undertaking active in the areas set out in point (b) of Article 1(1) of the Open data directive over which the public sector bodies may exercise directly or indirectly a dominant influence by virtue of their ownership of it, their financial participation therein, or the rules which govern it.

### 3.8.2 Reference

- Revision of PSI Directive
- Legislation train: Open data directive
- Open data directive text
- Revision of PSI Directive

## 3.9 Digital Services Act (DSA)

The DSA regulates online intermediaries and platforms such as marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms. Its main goal is to prevent illegal and harmful activities online and the spread of disinformation. It ensures user

safety, protects fundamental rights, and creates a fair and open online platform environment. The DSA introduces new obligations for providers of online marketplaces to counter the spread of illegal goods. Such providers must now ensure that sellers provide verified information on their identity before they can start selling their goods on those online marketplaces. Such providers must also guarantee that users can easily identify the person responsible for the sale. Moreover, if a provider of online marketplace becomes aware of the selling of an illegal product or service by a seller, it must inform the users who purchased the illegal good or product, as well as the identity of the seller and the options for redress.

Subject matter; Intermediary services: focused on providing a set of harmonized rules aimed at facilitating safety, predictability and trust in the context of intermediary services operating within the EU.

Scope; Entities that are offering an intermediary service to recipients who are established in the European Union regardless of where the intermediary service is established. This includes intermediaries that are providing a hosting service, online platforms, and very large online platforms.

### 3.9.1 Key definitions

Information Service Society: a service provided at a distance for remuneration.

i) ‘At a distance’; where parties are not simultaneously present

ii) ‘By electronic means’; where a service is sent and received by means of electronic equipment.

Recipient of Service; means any natural or legal person who uses an intermediary service, in particular for the purposes of seeking information or making it accessible

Intermediary Service: The following information Society Services are considered Intermediary Services:

- a ‘mere conduit’ service, consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network;

- a ‘caching’ service, consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate, and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request;

- a ‘hosting’ service, consisting of the storage of information provided by, and at the request of, a recipient of the service;

Online platform: means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public

Online search engine; an intermediary service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found

Illegal Content: any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law

Dissemination to the public; making information available, at the request of the recipient of the service who provided the information, to a potentially unlimited number of third parties

### 3.9.2 Reference

- Legislative train: DSA
- The Digital Services Act: Ensuring a safe and accountable online environment
- DSA text

## 3.10 MiFiD II

MiFID II aims to improve transparency, fairness, and efficiency in financial markets while strengthening investor protection. The directive covers various financial instruments, including stocks, bonds, derivatives, and structured products, as well as investment services and activities. MiFID II places a strong emphasis on safeguarding investor interests by ensuring firms act in their best interests and provide suitable investment advice. Firms are required to report all transactions in financial instruments to regulators in a timely and accurate manner, promoting market transparency. MiFID II enhances the transparency of trading activities by requiring more pre- and post-trade information to be made publicly available. Investment firms must take all the reasonable steps to achieve the best possible results for their clients when executing orders. To address conflicts of interest, MiFID II requires the separation of research costs from execution services, ensuring transparency in research charges.

This directive applies to the following entities:

- Investment firms,
- Market operators,
- Data reporting services providers,
- Third-country firms providing investment services or performing investment activities.

This Directive establishes requirements in relation to the following:

- authorisation and operating conditions for investment firms
- provision of investment services or activities by third-country firms through the establishment of a branch;
- authorisation and operation of regulated markets;
- authorisation and operation of data reporting services providers; and

- supervision, cooperation, and enforcement by competent authorities.

### 3.10.1 Key definitions

Investment firm;

a) any legal person whose regular occupation or business is the provision of one or more investment services to third parties and/or the performance of one or more investment activities on a professional basis.

b) where a natural person provides services involving the holding of third-party funds or transferable securities, that person may be considered to be an investment firm (as in accordance with MiFiD II & MiFiR) if:

i) the ownership rights of third parties in instruments and funds must be safeguarded, especially in the event of the insolvency of the firm or of its proprietors, seizure, set off or any other action by creditors of the firm or of its proprietors;

ii) the firm must be subject to rules designed to monitor the firm's solvency and that of its proprietors;

iii) the firm's annual accounts must be audited by one or more persons empowered, under national law, to audit accounts;

iv) where the firm has only one proprietor, that person must make provision for the protection of investors in the event of the firm's cessation of business following the proprietor's death or incapacity or any other such event;

Investment services and activities; any of the services and activities listed in Section A of Annex I relating to any of the instruments listed in Section C of Annex I.

Market maker; a person who holds himself out on the financial markets on a continuous basis as being willing to deal on own account by buying and selling financial instruments against that person's proprietary capital at prices defined by that person.

Portfolio management; managing portfolios in accordance with mandates given by clients on a discretionary client-by-client basis where such portfolios include one or more financial instruments.

Financial instrument; Any of the instruments specified in Section C of Annex I

Exchange traded fund; a fund of which at least one unit or share class is traded throughout the day on at least one trading venue and with at least one market maker which takes action to ensure that the price of its units or shares on the trading venue does not vary significantly from its net asset value and, where applicable, from its indicative net asset value.

### 3.10.2 Reference

- Legislation train: MiFiD
- Implementing and delegated acts - MiFiD II
- Implementing and delegated acts - MiFiD
- MiFiD II text

## 3.11 The Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT)

A new legal framework on anti-money laundering and countering the financing of terrorism was proposed on 20 July 2021 by the European Commission, and approved in April 2024 by the EU co-legislators (i.e. EU Parliament and Council of the EU). The new framework introduces three Regulations, a Directive, and a new EU authority to fight money laundering (AMLA) and expands its scope of application to include crypto-asset service providers, residence scheme operators, crowdfunding operators, football clubs and football agents will enter in force in the following months.

Scope, Anti-money laundering legislation in the EU strives to prevention money laundering and applies to the following entities:

- Credit institutions
- Financial institutions
- Auditors, external accountants, and tax advisors, and any other natural or legal person including independent legal professionals such as lawyers.
- Notaries, lawyers, and other independent legal professionals.
- Trust or company service providers.
- Estate agents and other real estate professionals to the extent they function as intermediaries in real estate transactions.
- Persons trading, as a regular or principal professional activity, in precious metals and stones, or in high-value goods.
- Providers of gambling services
- Crowdfunding service providers and crowdfunding intermediaries
- Persons trading or acting as intermediaries in the trade of cultural goods
- Persons storing, trading, or acting as intermediaries in the trade of cultural goods and high-value goods.
- credit intermediaries for mortgage and consumer credits
- investment migration operators permitted to represent or offer intermediation services to third-country nationals seeking to obtain residence rights in a Member State in exchange for any kind of investment.
- non-financial mixed activity holding companies
- football agents.
- Professional football clubs.

### 3.11.1 Key Definitions

Money laundering; conduct discusses under article 3(1) of Directive 2018/1673, including aiding and abetting, inciting, and attempting to commit that conduct, whether the activities which generated the property to be laundered were conducted on the territory of a Member State or on that of a third country.

Criminal activity; any kind of criminal involvement in the commission of any offence punishable, in accordance with national law, by deprivation of liberty or a detention order for a minimum of 6 months, or a maximum of more than one year. This includes any of the criminal activities listed under article 2 (1)(a) to (v) in Directive 2018/1673.

A Credit institution is:

a) an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account within the meaning of article 4 (1)(1) of Directive 575/2013; or b) Any of the undertakings discussed under article 4(1) and 4(1)(17) of Directive 575/2013

Financial institution is any one of the entities discussed under article 2 (1)(6)(a) to (j) of Directive 2024/1624.

### 3.11.2 References

- Legislation train: Sixth AML/CFT Directive (AMLD6)
- AML/CFT Frequently asked questions
- 6th Anti-Money Laundering Directive
- Anti-Money Laundering Regulation
- AMLA Regulation
- Transfer of Funds Regulation

## 3.12 Electronic identification and trust services for electronic transactions in the internal market (eIDaS)

The eIDAS Regulation provides for the interoperability of national eID schemes among EU member states. This requires the development of a technology-neutral framework that does not favour any particular technical solution for eID implementation. Procedural and technical standards have been set to facilitate cooperation among EU countries, aimed at ensuring the seamless exchange of electronic identification data and fostering a cohesive digital ecosystem across the EU. At the same time, eIDAS created a level playing field for a number of trusted services, which have become indispensable in today's digital value chains: Electronic Registered Delivery Services (ERDS). These ensure secure and reliable delivery of electronic messages, data, or documents and provide evidence of the time of sending, receipt, and content integrity.

Subject matter, harmonized rules to provide an adequate level of security for electronic identification and trust services.

Scope, Electronic identification schemes notified by a respective Member State & trust service providers established in the EU.

### 3.12.1 Key definitions

Electronic identification; the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person

Electronic identification scheme; a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons

Trust service; means an electronic service normally provided for remuneration which consists of:

- the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
- the creation, verification, and validation of certificates for website authentication; or;
- the preservation of electronic signatures, seals or certificates related to those services;

Qualified trust service; any trusted service that meets the requirements of eIDAS.

### 3.12.2 Reference

- Legislation train: eIDAS
- eIDAS Regulation
- eIDAS text

## 3.13 AI Act

The general objective of the proposed AI act unveiled in April 2021 is to ensure the proper functioning of the single market by creating the conditions for the development and use of trustworthy AI systems in the Union. It sets out a harmonized legal framework for the development, place on the Union market, and the use of AI products and services. The AI act seeks to achieve a set of specific objectives: (i) ensure that AI systems placed on the EU market are safe and respect existing EU law, (ii) ensure legal certainty to facilitate investment and innovation in AI, (iii) enhance governance and effective enforcement of EU law on fundamental rights and safety requirements applicable to AI systems, and (iv) facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation. The proposal enshrines a technology-neutral definition of AI systems and adopts a risk-based approach, which lays down different requirements and obligations for the development, placing on the market and use of AI systems in the EU. The proposal defines common mandatory requirements applicable to the design and development of AI systems before they are placed on the market and harmonizes the way ex-post controls are conducted.

Scope; as a subject matter, it is focused on the safe development of AI systems that are human centric and trustworthy.

- providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, irrespective of whether those providers are established or located within the Union or in a third country
- deployers of AI systems that have their place of establishment or are located within the Union
- providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union
- importers and distributors of AI systems
- product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark
- authorised representatives of providers, which are not established in the Union
- affected persons that are located in the Union

### 3.13.1 Key definitions

AI system; a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

Provider; a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.

Deployer; a natural or legal person, public authority, agency, or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.

Importer; a natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country.

Distributor; a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market.

Placing on the market; the first making available of an AI system or a general-purpose AI model on the Union market.

Making available on the market; the supply of an AI system or a general-purpose AI model for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge.

### 3.13.2 Reference

- Legislation train: AI Act
- AI Act: Overview
- AI Act text

## 3.14 Framework for Financial Data Access (FiDA)

Applies to the following categories of customer data:

mortgage credit agreements, loans and accounts, savings, investments in financial instruments, insurance-based investment products, crypto-assets, real estate and other related financial assets as well as the economic benefits derived from such assets, pension rights in occupational pension schemes, pension rights on the provision of pan-European personal pension products, non-life insurance products, data which forms part of a creditworthiness assessment of a firm which is collected as part of a loan application process or a request for a credit rating.

Applies to the following financial institutions:

Credit institutions; payment institutions; electronic money institutions; investment firms; crypto-asset service providers; issuers of asset-referenced tokens; managers of alternative investment funds; management companies of undertakings for collective investment in transferable securities; insurance and reinsurance undertakings; insurance intermediaries and ancillary insurance intermediaries; institutions for occupational retirement provision; credit rating agencies; crowdfunding service providers; PEPP providers; financial information service providers.

### 3.14.1 Key definitions

Consumer; a natural person who is acting for purposes other than his or her trade, business, or profession.

Customer; a natural or a legal person who makes use of financial products and services.

Customer data; personal and non-personal data that is collected, stored and otherwise processed by a financial institution as part of their normal course of business with customers which covers both data provided by a customer and data generated as a result of customer interaction with the financial institution.

Data holder; a financial institution other than an account information service provider that collects, stores, and otherwise processes any of the data in the category above.

Data User; anyone of the entities listed above that has lawful access to use any data described in the above categories.

Financial information service provider; a data user authorized to access customer data for the purpose of the provision of financial information services.

### 3.14.2 Reference

- Information on FIDA

## 3.15 Intelligent travel systems (ITS) Directive (2023/2661)

Intelligent Transport Systems help inform, coordinate, and enhance the safety of transport networks, a necessary innovation with the ever increase volume of road transport within the European Union. The ITS Directive was first adopted in July 2010 with the aim of coordinating the implementation of

Intelligent Transport Systems across Europe. Its Initial focused areas were road; traffic and travel information; continuity of traffic and freight management ITS services; ITS road safety road security; and linking vehicles to transport infrastructure. The new directive 2023/2661/EU amended this to adapt to technological developments.

Applies to ITS applications and services in the field of road transport and their interfaces with other modes of transport.

### 3.15.1 Key definitions

Intelligent Transport Systems (ITS); Systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles, and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport.

Interoperability; data on road infrastructure characteristics, including fixed traffic signs and their regulatory safety attributes as well as infrastructure for recharging and for refuelling with alternative fuels

ITS application; an operational instrument for the application of ITS.

ITS service; means the provision of an ITS application through a well-defined organisational and operational framework with the aim of contributing to user safety, efficiency, sustainable mobility, or comfort, or of facilitating or supporting transport and travel operations.

ITS user; any user of ITS applications or services including travellers, vulnerable road users, road transport infrastructure users and operators, fleet managers and operators of emergency services.

ITS provider; any provider of an ITS service, whether public or private.

Road data; data on road infrastructure characteristics, including fixed traffic signs and their regulatory safety attributes as well as infrastructure for recharging and for refuelling with alternative fuels.

Traffic data; historic and real-time data on road traffic characteristics.

Travel data; basic data such as public transport timetables and tariffs, necessary to provide multi-modal travel information before and during the trip to facilitate travel planning, booking and adaptation.

### 3.15.2 Reference

Intelligent Transport Systems Action Plan

## 3.16 Trade Secrets Directive (2016/943)

The trade secrets directive is aimed at protecting trade secrets. It harmonizes national laws that address protecting business know how and information from unlawful acquisition, use and disclosure, and intended to have a deterrent effect on such practices. Amongst some of the key points it addressed are the lawful acquisition of a trade secret; unlawful acquisition, use & disclosure of a trade secret; and exceptions.

This applies to all trade secrets within the EU.

### 3.16.1 Key definitions

Trade secrets; any information which meets the following requirements is considered a trade secret:

a) It is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

b) it has commercial value because it is secret;

c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret;

Trade secret holder; any natural or legal person lawfully controlling a trade secret.

Infringer; any natural or legal person who has unlawfully acquired, used, or disclosed a trade secret.

Infringing goods; goods, the design, characteristics, functioning, production process or marketing of which significantly benefits from trade secrets unlawfully acquired, used, or disclosed.

Reference

- Trade secrets: frequently asked questions

## 3.17 EU Corporate Sustainability Reporting Directive

The EU CSRD introduces certain sustainability reporting obligations. Companies operate within the EU are required by law to disclose information on the various social and environmental risks they face, and how their activities impact the environment & people. This is a fundamental component to the European Green Deal and helps inform investors and other stakeholders on the sustainability performance of a company. This directive is applicable from 2025.

Applies to credit institutions and insurance undertakings (large, medium, and small undertakings).

### 3.17.1 Key definitions

Public interest entities; An entity described in annex I, or annex II where all of the direct or indirect members of the undertaking having otherwise unlimited liability in fact have limited liability by reason of those members being undertakings which are:

i) of the types listed in Annex I; or

ii) not governed by the law of a Member State but which have a legal form comparable to those listed in Annex I

Credit institutions; means an undertaking the business of which is to receive deposits or other repayable funds from the public and to grant credits for its own account.

Insurance undertakings; Those bodies referred to in article 4 (a), (b),(c), (d) and (e) of Council Directive 91/674/EEC (excluding those mentioned in article 3), except where an activity does not wholly or mainly consist of insurance as its business.

### 3.17.2 Reference

- Frequently asked questions on the implementation of the EU corporate sustainability reporting rules

## 3.18 Sustainable Financial Disclosure Regulation

This regulation applies to financial market participants and financial market advisor. It harmonizes the rules for the financial market concerning transparency in the consideration/integration of sustainability risks and the consideration of adverse sustainability impacts in the processes of financial market participants, and financial advisors, and the provision of sustainability - related information in relation to financial products.

### 3.18.1 Key definitions

The following entities are considered Financial Market participants:

a) an insurance undertaking which makes available an insurance-based investment product (IBIP);

b) an investment firm which provides portfolio management;

c) an institution for occupational retirement provision (IORP)

d) an alternative investment fund manager (AIFM);

e) a pan-European personal pension product (PEPP) provider;

f) a pan-European personal pension product (PEPP) provider;

g) a manager of a qualifying venture capital fund registered in accordance with Article 14 of Regulation (EU) No 345/2013

h) a manager of a qualifying social entrepreneurship fund registered in accordance with Article 15 of Regulation (EU) No 346/2013;

The following entities are considered financial advisers:

a) an insurance intermediary which provides insurance advice with regard to IBIPs.

b) an insurance undertaking which provides insurance advice with regard to IBIPs.

c) a credit institution which provides investment advice.

d) an investment firm which provides investment advice.

e) an AIFM which provides investment advice in accordance with point (b)(i) of Article 6(4) of Directive 2011/61/EU.

f) a UCITS management company which provides investment advice in accordance with point (b)(i) of Article 6(3) of Directive 2009/65/EC.

The following are considered financial products:

a) a portfolio managed in accordance with point (6) of this Article;

b) an alternative investment fund (AIF)

c) an IBIP;

d) a pension product;

e) a pension scheme;

f) a UCITS; or

g) a PEPP;

### 3.18.2 Reference

- Q&A for the SDFR (ESMA)

## 3.19 Anti-money Laundering

Anti-money laundering legislation in the EU strives to prevention money laundering and applies to the following entities:

- Credit institutions
- Financial institutions
- auditors, external accountants, and tax advisors, and any other natural or legal person including independent legal professionals such as lawyers.
- Notaries, lawyers, and other independent legal professionals.
- Trust or company service providers.
- Estate agents and other real estate professionals to the extent they function as intermediaries in real estate transactions.
- Persons trading, as a regular or principal professional activity, in precious metals and stones, or in high-value goods.

- Providers of gambling services
- Crowdfunding service providers and crowdfunding intermediaries
- Persons trading or acting as intermediaries in the trade of cultural goods
- Persons storing, trading, or acting as intermediaries in the trade of cultural goods and high-value goods.
- credit intermediaries for mortgage and consumer credits
- investment migration operators permitted to represent or offer intermediation services to third-country nationals seeking to obtain residence rights in a Member State in exchange for any kind of investment.
- non-financial mixed activity holding companies
- football agents.
- Professional football clubs.

### 3.19.1 Key Definitions

Money laundering; conduct discusses under article 3(1) of Directive 2018/1673, including aiding and abetting, inciting and attempting to commit that conduct, whether the activities which generated the property to be laundered were carried out on the territory of a Member State or on that of a third country.

Criminal activity; any kind of criminal involvement in the commission of any offence punishable, in accordance with national law, by deprivation of liberty or a detention order for a minimum of 6 months, or a maximum of more than one year. This includes any of the criminal activities listed under article 2 (1)(a) to (v) in Directive 2018/1673.

Credit institution is:

a) an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account within the meaning of article 4 (1)(1) of Directive 575/2013; or

b) Any of the undertakings discussed under article 4(1) and 4(1)(17) of Directive 575/2013

Financial institution is any one of the entities discussed under article 2 (1)(6)(a) to (j) of Directive 2024/1624.

### 3.19.2 Reference

- AML/CFT Frequently asked questions

# 4 Regulatory Framework Online Tool Prototype

This section introduces the Prototype version of the Regulatory Framework Online Tool addressing laws and regulations for FAME. In this version snapshot of Regulatory Framework Online Tool addressing laws and regulations for FAME is provided as example about the functionalities that are planned to provide as use for the stakeholders and partner on FAME project. The tool is already operationalized with necessary information about background study on laws and regulations. The tool also encompasses an information services section which users can find information related to data protection for the financial sector. The tool also includes a short description on the FAME project, providing related information about the project. Recent news is listed as a subsection of the website which provides update on regulatory ecosystem of FAME for different stakeholders. The tool provides EU data protection regulations which lists the most relevant policies and Regulations on Data Protection and Data Governance.

The FAME website platform, a user-friendly website, is the main entry point for communication to the stakeholders and provide the FAME Regulatory Compliance Online Tool (FReCo). The FAME Regulatory Compliance Online Tool includes an interactive tool for stakeholders to browse into regulatory framework and a download link for retrieving related laws and regulations. The main menu of the FAME Regulatory Compliance Online Tool includes all related laws and regulations. The Figure 3 shows the FAME Regulatory Policy Framework Portal, it acts as the entry point to all related laws and regulation in the FAME ecosystem.

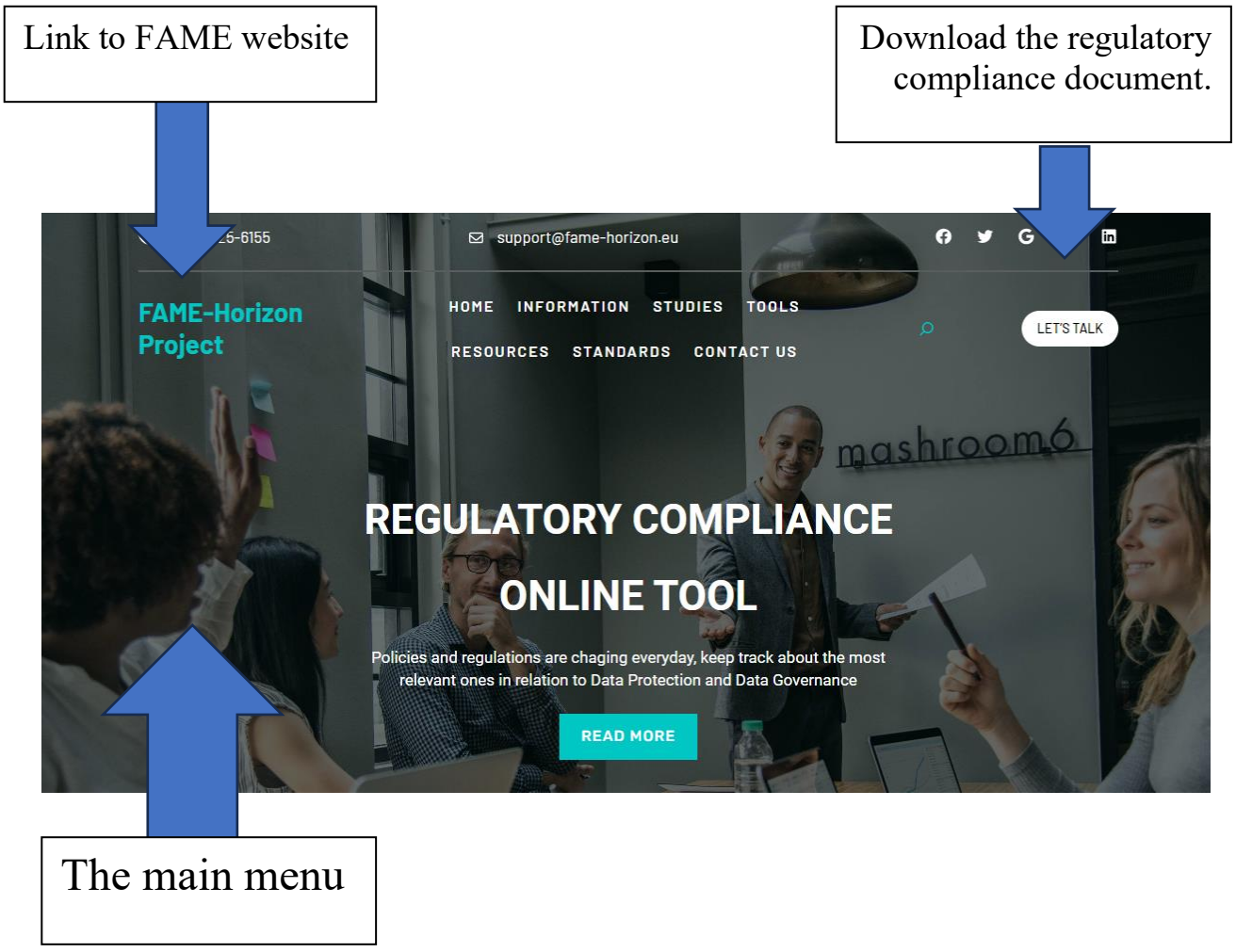



Figure 3. FAME Regulatory Compliance Home - Prototype

The Figure 4 shows the Information Services and Regulation Section. This section of the FAME Regulatory Compliance Online Tool provides information services. Users can extract information related to laws and regulation according to their need. This section categorizes information in an easy-to-use manner for the users. This section include information about laws and regulations, policies, standard and guidelines, best practices and advice, and studies, reports and assessments.

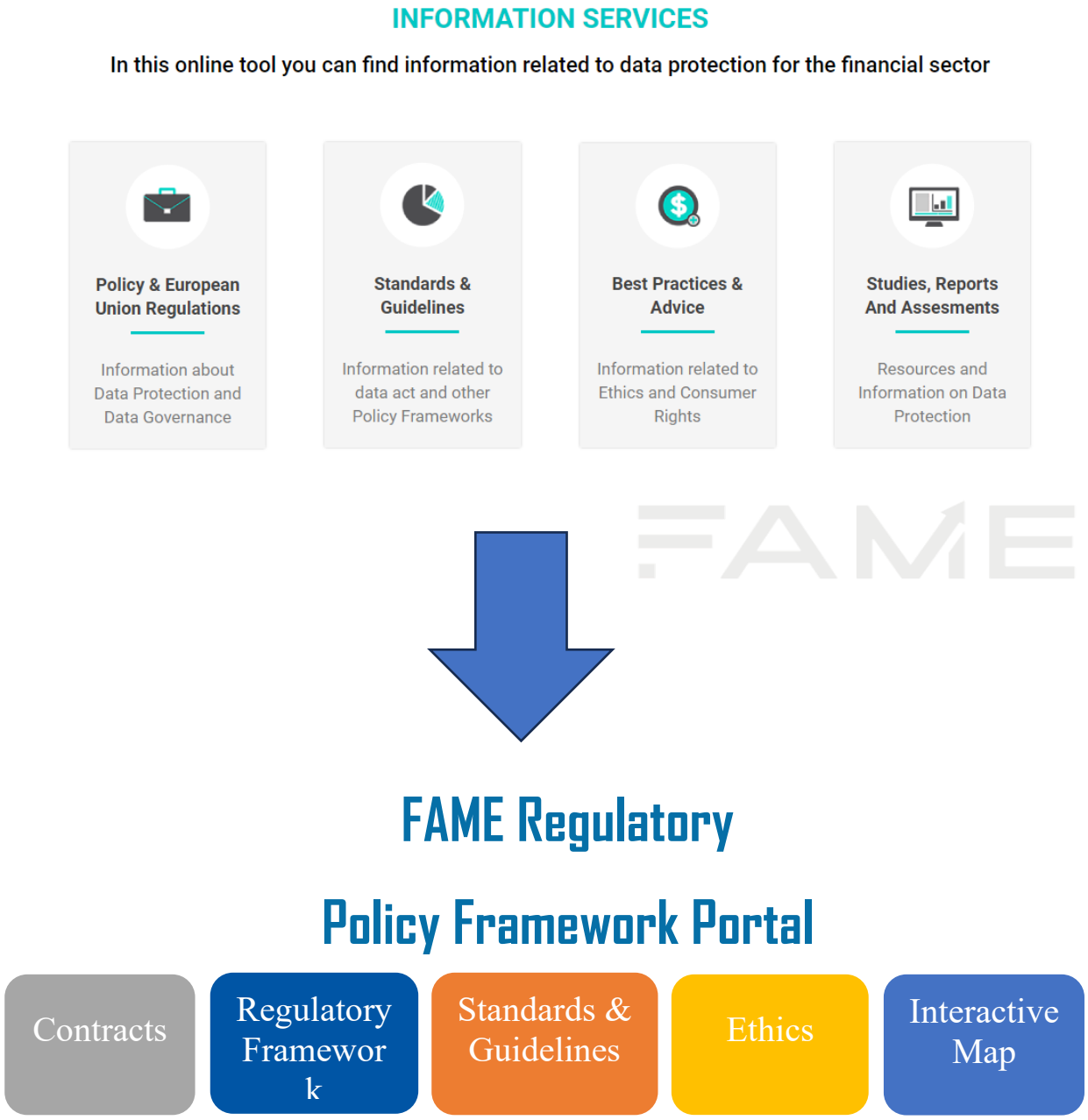
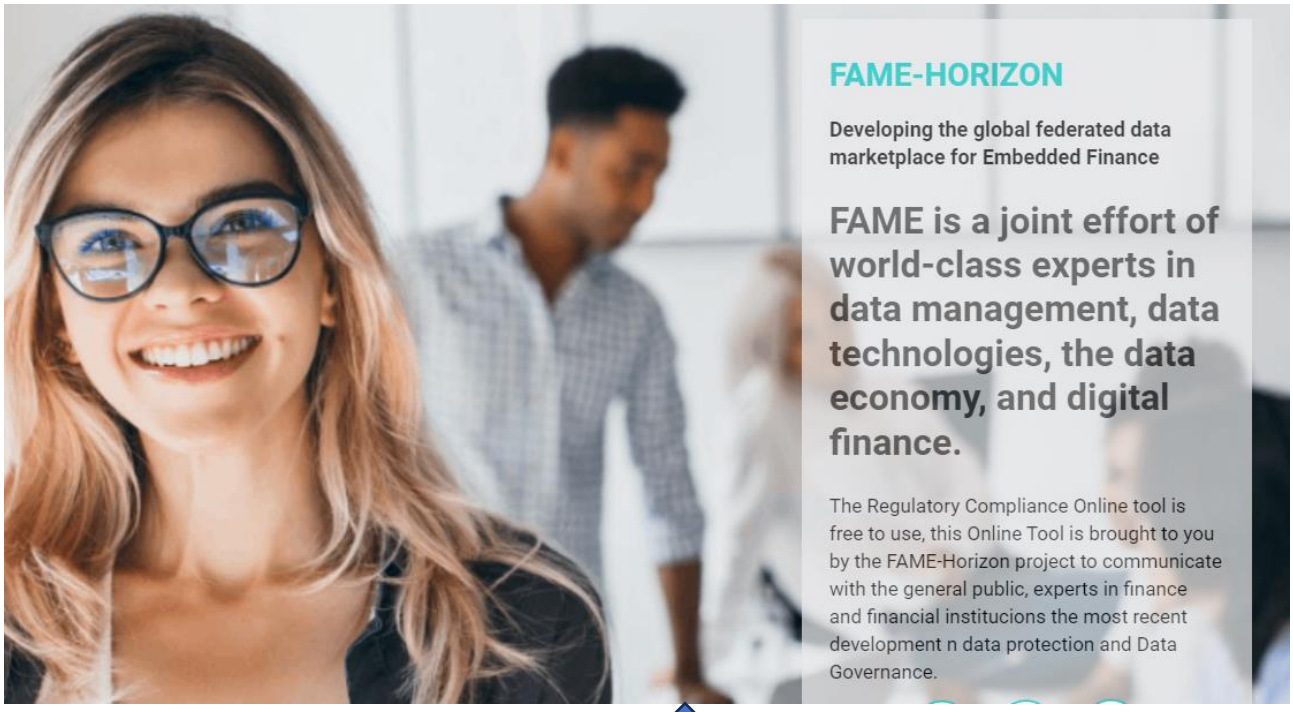



Figure 4. FAME Cluster Areas in the Regulatory Compliance Portal - Prototype

The Figure 5 shows the section were FAME-HORIZON is described briefly. This section of the tool provides general and technical information about FAME. What is FAME, what is its goals and its achievements. There is a link to the main FAME project website for the users to explore more on the topic. The Regulatory Compliance Online tool is free to use, this Online Tool is brought to you by the FAME-Horizon project to communicate with the general public, experts in finance and financial institutions the most recent development n data protection and Data Governance.




General and technical information about FAME

Figure 5. FAME Project References in the Regulatory Compliance Portal - Prototype

The Figure 6 shows a section for summarising some project KPIs. It summarizes the main activities of the FAME project. It provides a snapshot of the number of experts in finance, number of available resources, number of documents studies, and numbers of countries served.

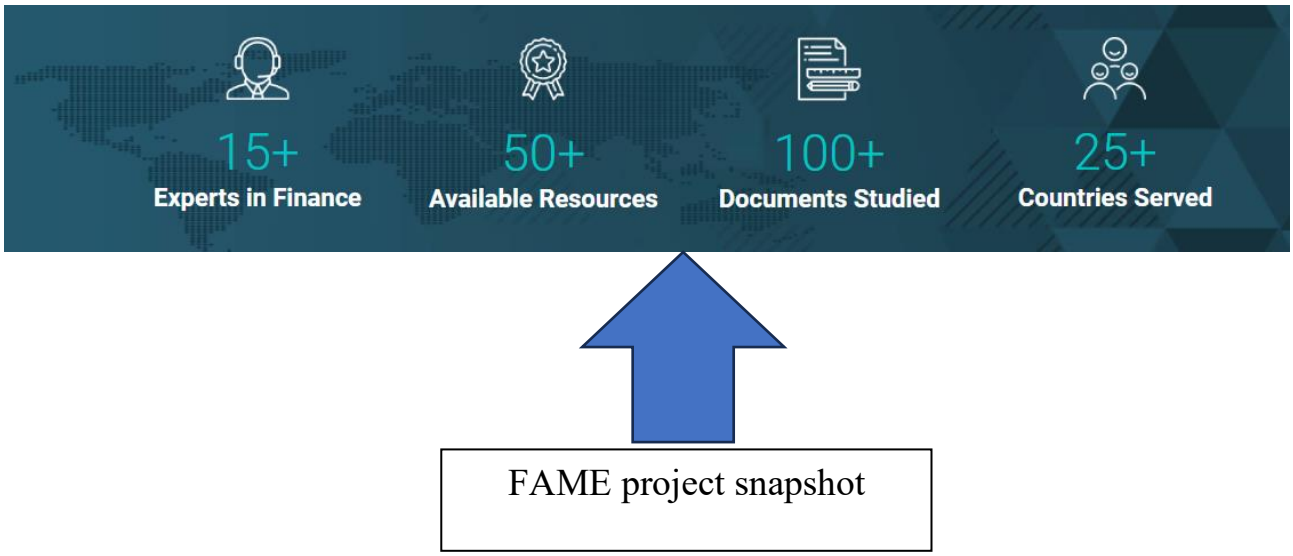



Figure 6. FAME Project KPIs in the Regulatory Compliance Portal - Prototype

The Figure 7 dedicated to the recent news, this section provides information about recent news, and the FAME project public release. It is so vital to provide recent updates about regulatory ecosystem of the FAME project to keep the stakeholders engaged and up to date.


Figure 7. FAME Project Recent News Section in the Regulatory Compliance Portal - Prototype

The Figure 8 Provide the details of the different identified relevant regulations for the FAME project, the pilots and their stakeholders. This section summarizes the EU data protection regulation. All related laws and regulations are listed with proper links to more details of each laws and regulations. The stakeholders can access the whole range of related information in a user-friendly way.

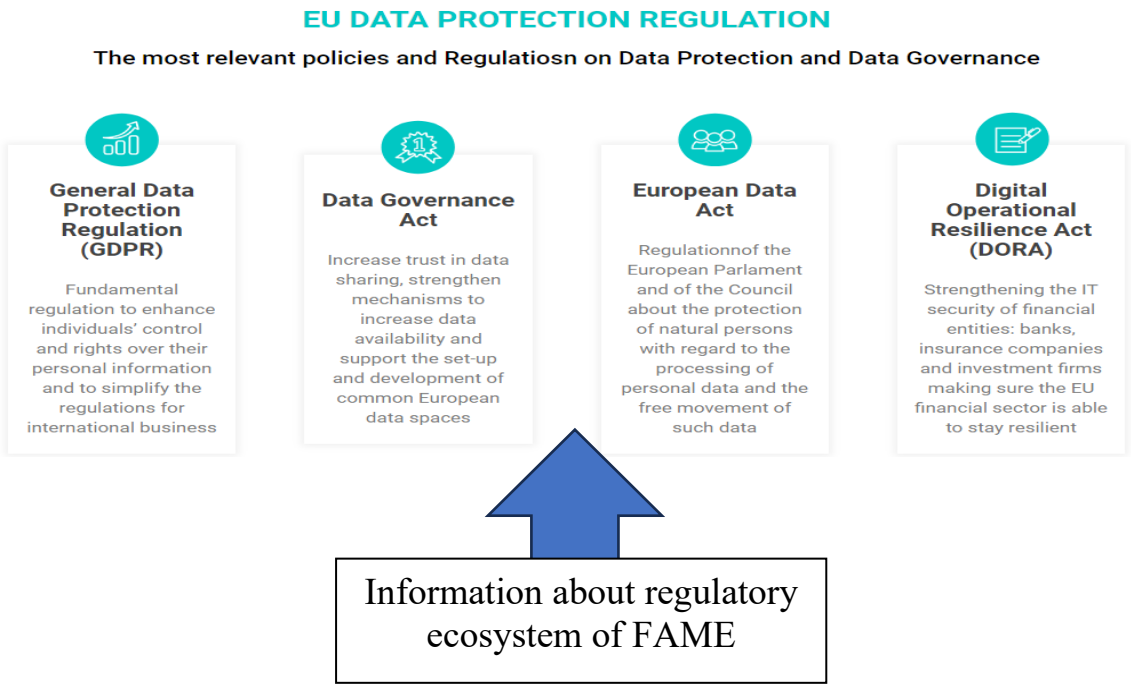



Figure 8. FAME Project Ecosystem in the Regulatory Compliance Portal - Prototype

The Figure 9 shows the polices and regulations that are applicable globally. This section provides information about newly policy and regulations based on location of choice the related laws and regulations are listed with a detail information about related laws and regulations.

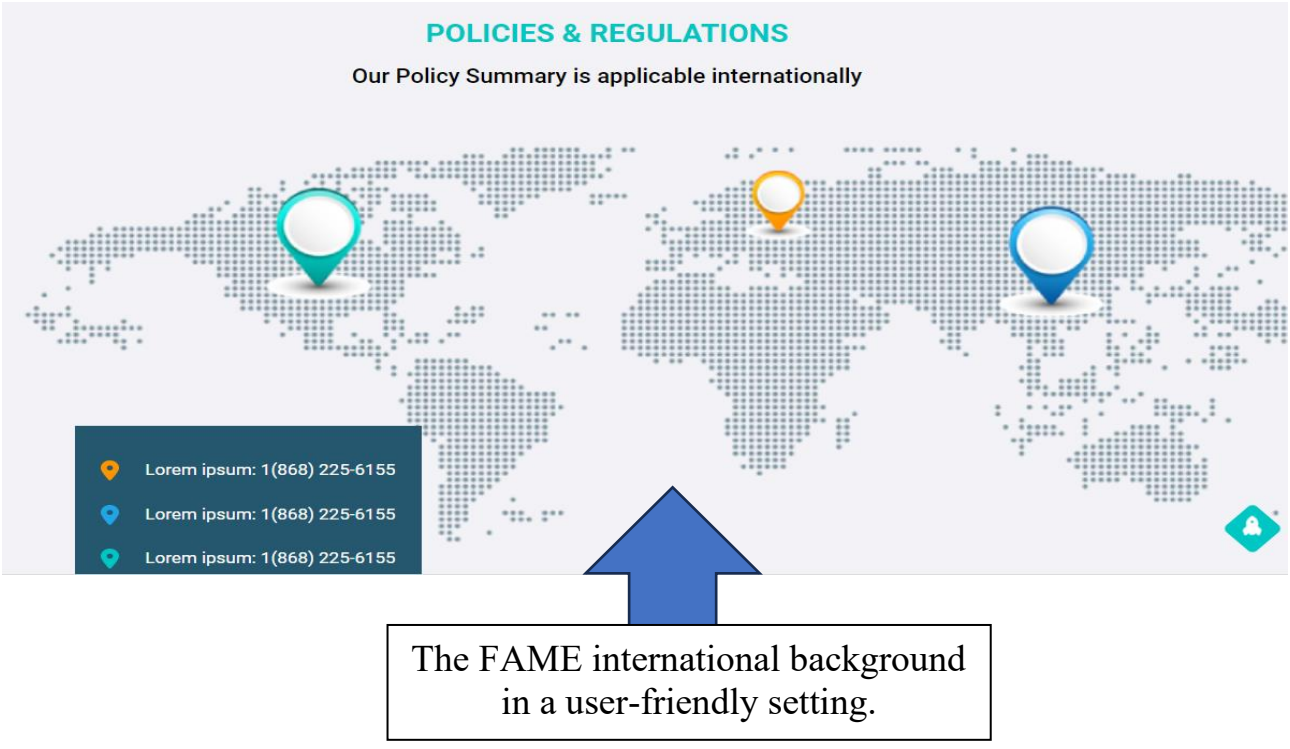



Figure 9. FAME Project Recent News Section in the Regulatory Compliance Portal - Prototype

# 5 The Regulatory Framework Online Tool – Final Version

The Figure 10 shows the FAME Regulatory and Compliance Online Tool Final Version. This section showcase the most recent updates of the regulatory compliance tool. We provide snapshot of the tool with necessary information to navigate through online tool. The regulatory compliance tool is accessible through FAME marketplace access. The home page of the regulatory compliance tool provides necessary tabs to navigate through the tool.

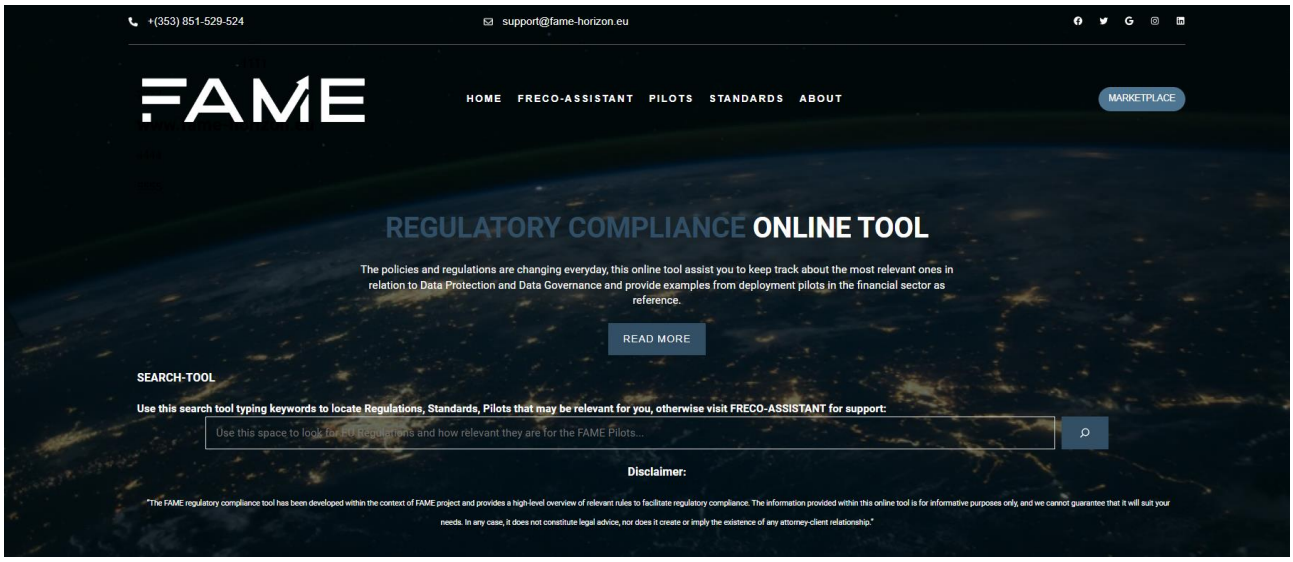



Figure 10. FAME Regulatory Compliance Home – Final Online Version

The Figure 11 shows the FAME Regulatory and Compliance Online Tool how-to-use instructions.. The home page contains the links to both services. The Home also contains a background information on how to use the online tool along with an easy made search bar and compliance examples.

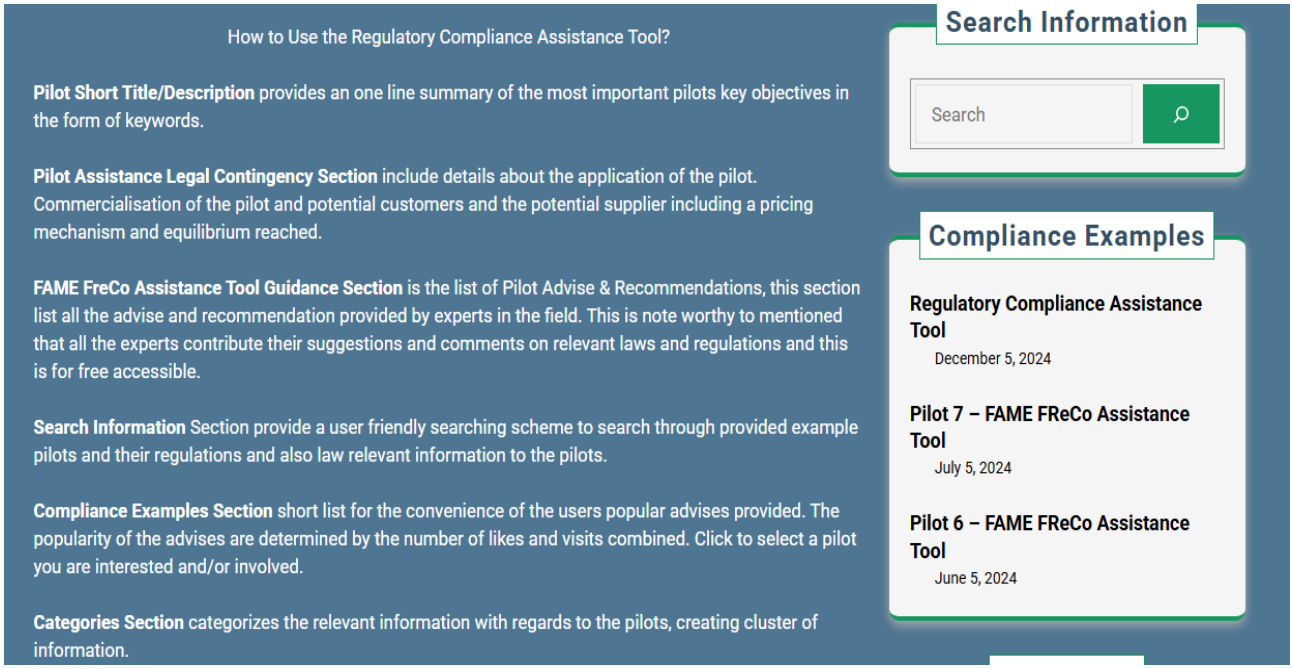



Figure 11. FAME Regulatory Compliance Assistance Tool – Final Online Version

The Figure 12 shows the section where related information can be accessed on-demand and along with tags and social media engagement are all on the assistant page of the regulatory compliance tool.

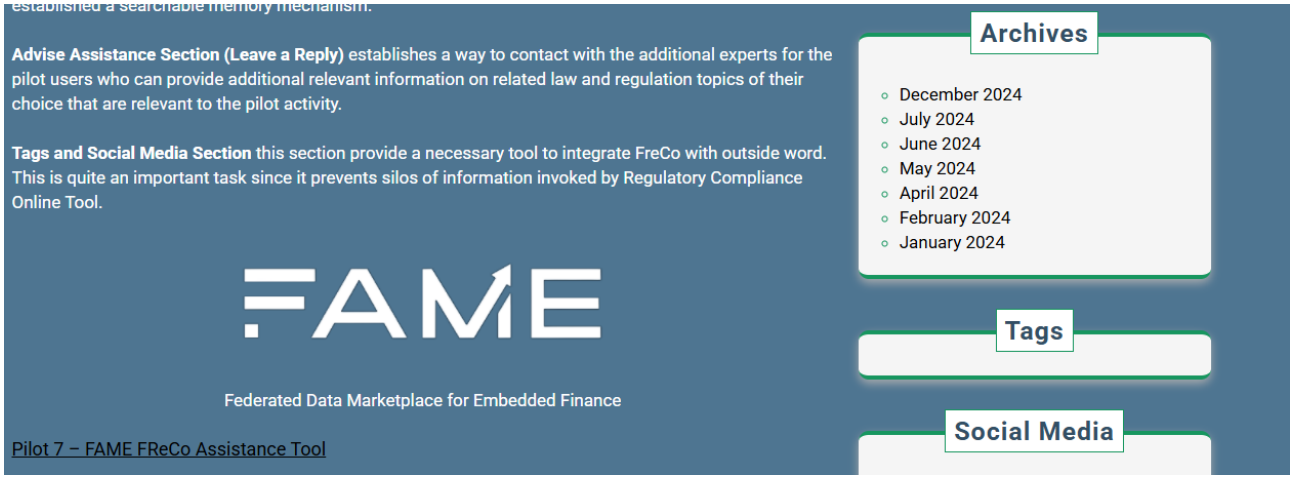



Figure 12. FAME Regulatory Compliance Assistant Tool Archives – Final Online Version

The Figure 13 shows the FAME online assessment tool. The regulatory compliance tool provides an interactive relationship with users through search and comment section as described below. Users can leave a reply pertaining to chosen pilot or in general. They should provide their comments and name email and other optional information to leave a comment.


Figure 13. FAME Regulatory Compliance Assistant Tool Comments – Final Online Version

The Figure 14 shows the section in the home of the FAME Regulatory and Compliance Online Tool, This service offers an easy access to FAME pilot FreCo assistance tool.

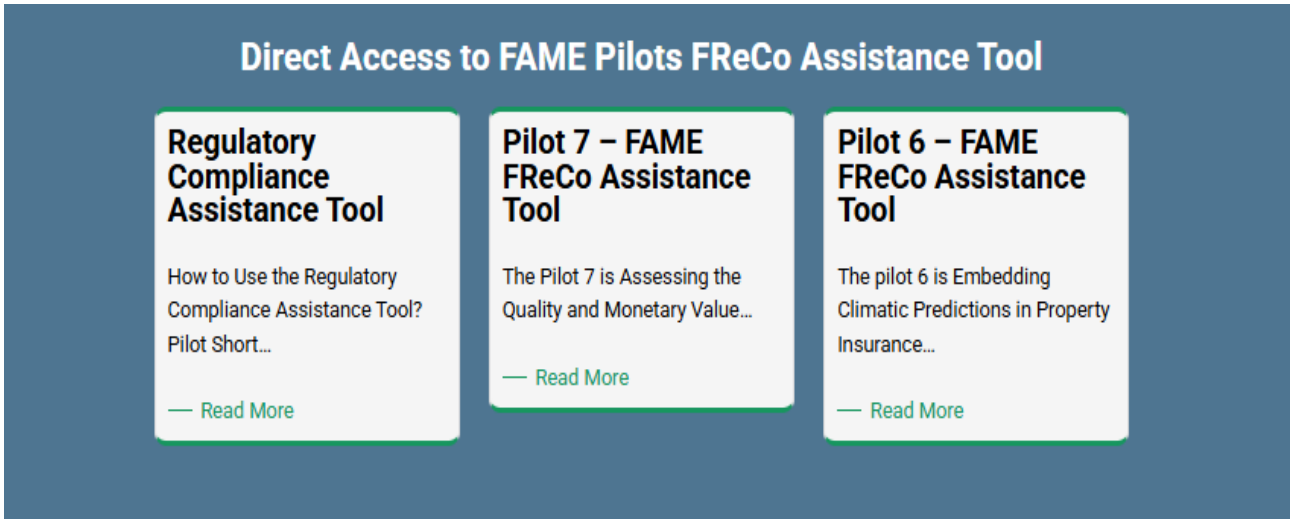



Figure 14. FAME Regulatory Compliance Pilot Direct Access – Final Online Version

The Figure 15 shows the contact details and foot notes section, The home page closes on necessary information to contact and engage with the admin, Regulatory compliance tool provides an easy access to the heart of FreCo functionalities and services.

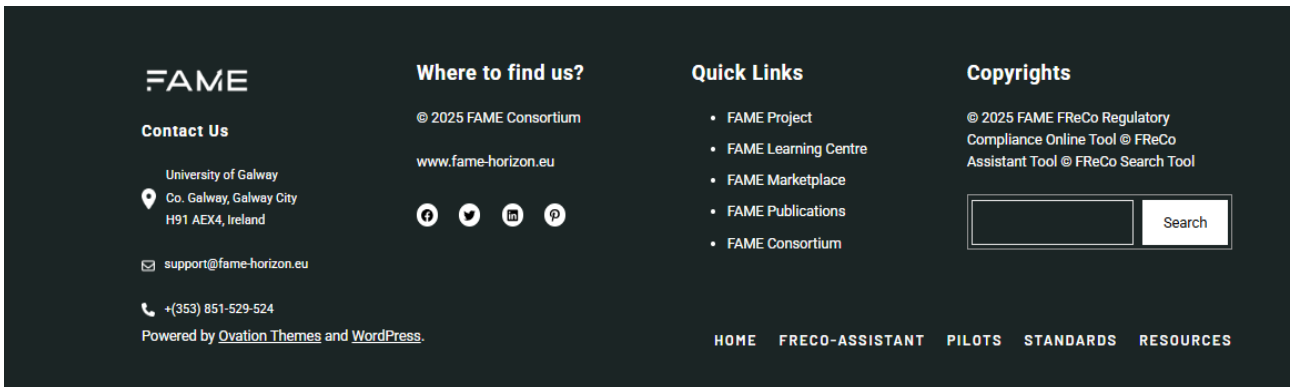



Figure 15. FAME Regulatory Compliance Contact Details – Final Online Version

The Figure 16 shows the FAME Regulatory and Compliance Assistance Online Tool. This sections provide detailed description in how to use and how to operate the different services provided online.

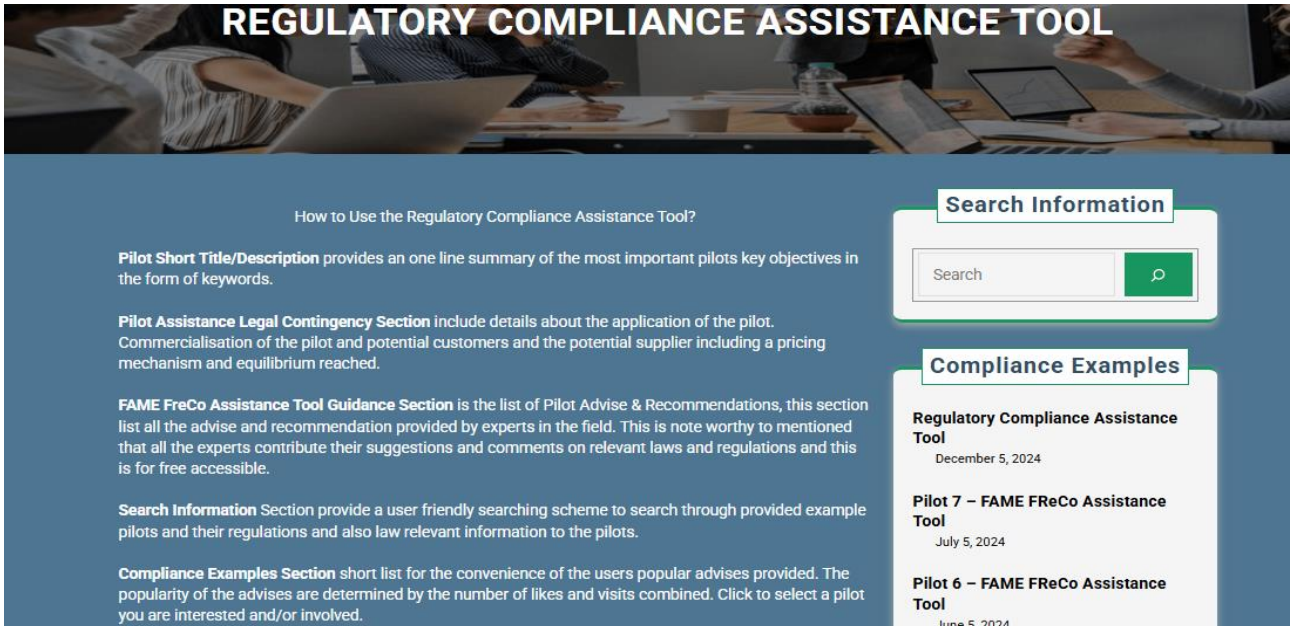



Figure 16. FAME Regulatory Compliance Contact Details – Final Online Version

The Figure 17 shows the FAME different pilots and provide direct access to the relevant pilot legal considerations. The pilots have easy access to snapshot information on each pilot in FAME is made easy through pilots tabs. Here the users can gain access to all pilots at once and update themselves which necessary information on each pilot separately.

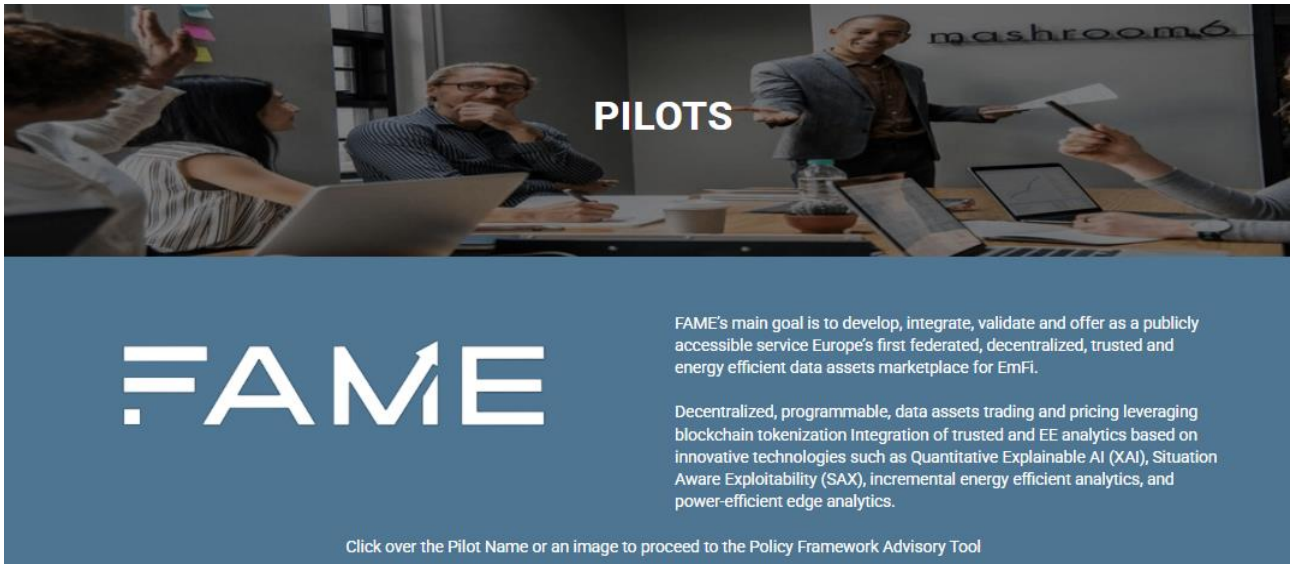



Figure 17. FAME Regulatory Compliance Pilots Section – Final Online Version

The Figure 18 shows the FAME different i.e. Pilots 1 and Pilot 2 as examples. This section in the FAME Regulatory and Compliance Online Tool provide direct access to the relevant pilot legal considerations. The pilots have easy access to snapshot information on each pilot in FAME is made easy through pilots tabs. Here the users can gain access to all pilots at once and update themselves which necessary information on each pilot separately.

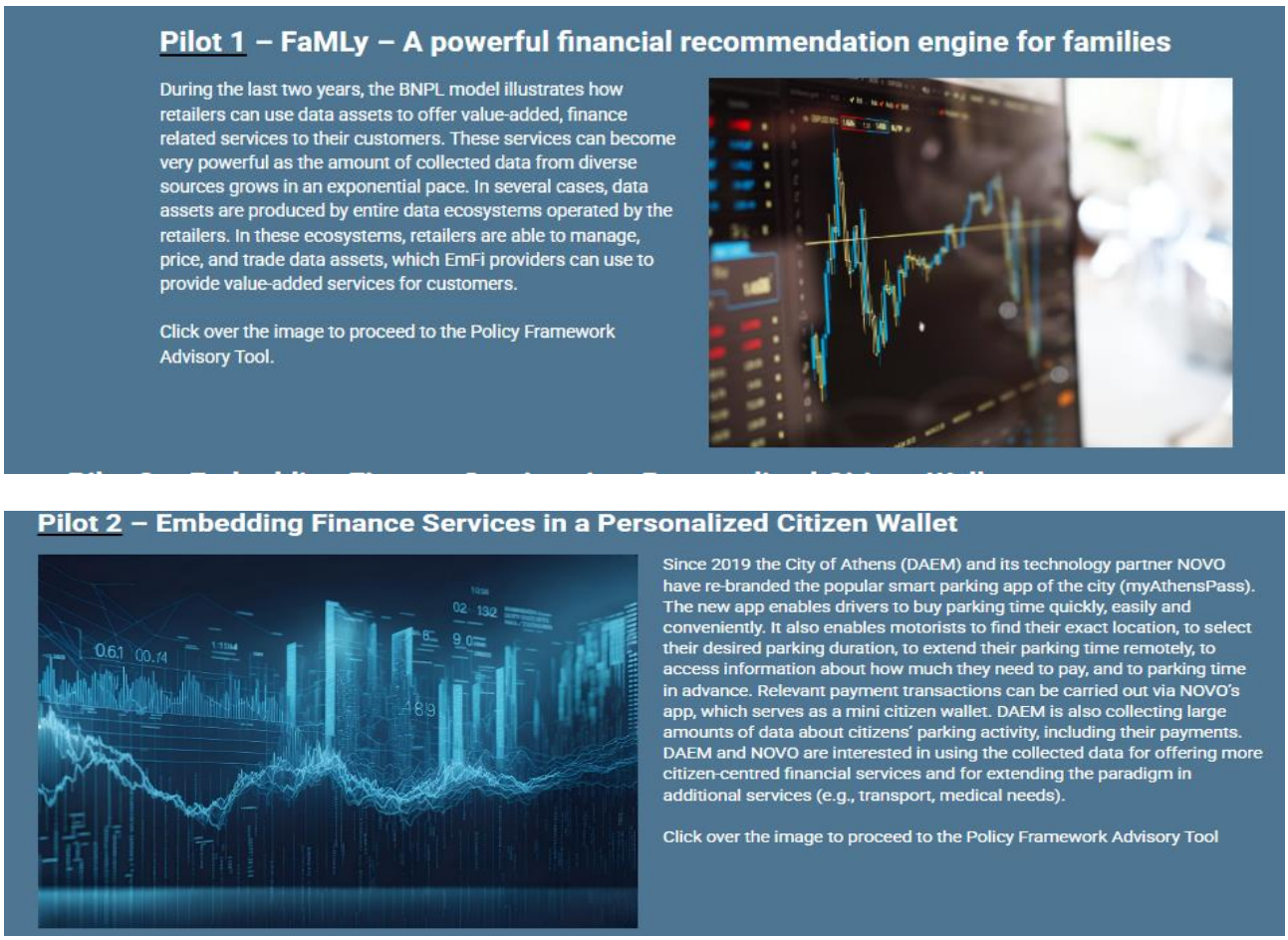



Figure 18. FAME Regulatory Compliance Pilots Section – Final Online Version

The Figure 19 is related to Standards, under different standard tabs, standards pertaining to FAME are listed and provide direct access to shoer descriptions for understanding their use. Users can update themselves with related standard in FAME framework.


Figure 19. FAME Regulatory Compliance Standards Section – Final Online Version

The Figure 20 includes the About section, provide the summary of FreCo and provide users with necessary information related to their search and retrieving of information related to laws and regulations and standards in FAME. This section act as an online handbook about the FAME Regulatory and Compliance Online Tool

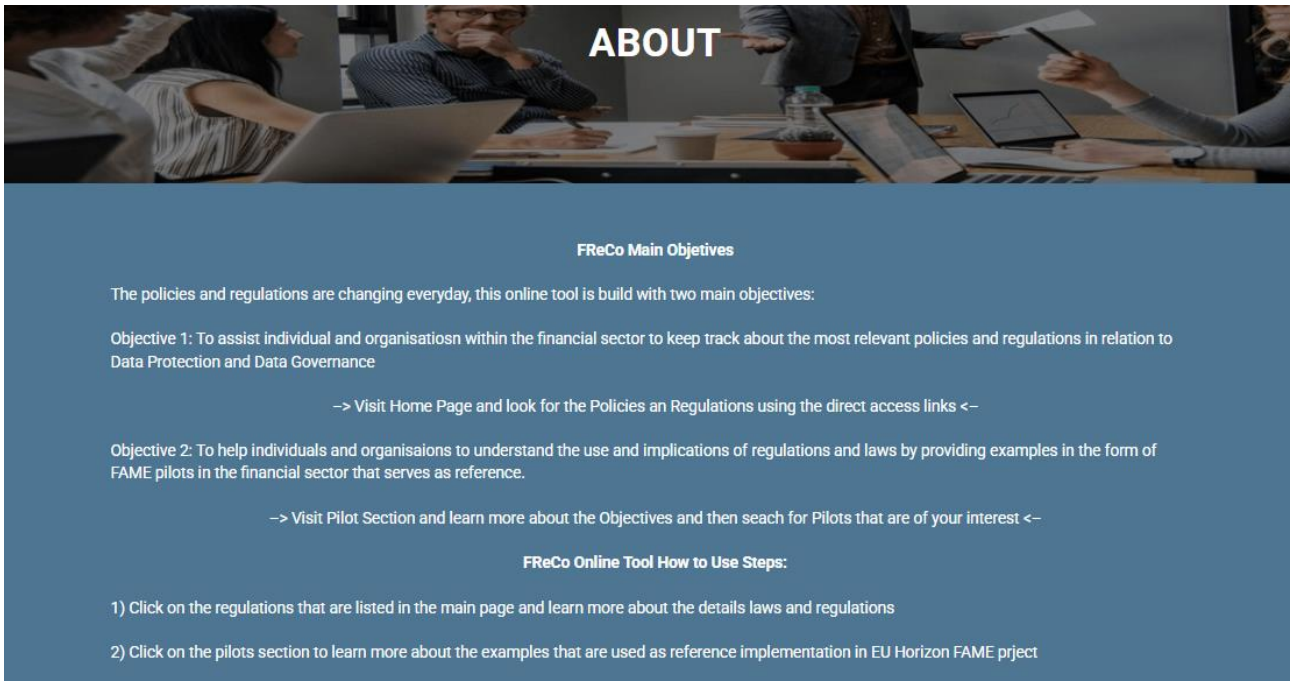



Figure 20. FAME Regulatory Compliance About Section – Final Online Version

## 5.1 Legal Perspective

This chapter addresses certain aspects from a legal perspective in relation to how the FAME Regulatory and Compliance (FReCo) tool can support regulatory compliance. Overall, this chapter clarifies the concept of regulatory compliance, presenting it as a multi-step process, elaborating on the role IT compliance tools can play in it. Furthermore, this chapter points out to the concept of 'legal advice' as a matter regulated by (national) law, which has strict boundaries. Finally, it discusses the added benefit and the limitations of such a compliance tool for the purposes of the FAME Marketplace.

### 5.1.1 Background: IT Tools for compliance

A complex regulatory framework may hinder business activities, and create legal uncertainty for any organisation, and in particular for Small and Medium Enterprises (SMEs). The issue concerns, in particular, the time and cost expended in identifying relevant legislation, their applicable requirements and formulating strategies to satisfy regulatory demands. For at least part of this effort, IT tools for compliance may provide support and sustain regulatory compliance. In particular, IT tools, such as the one provided by FAME, is potentially able to provide a relevant overview of the regulatory framework, which a data operator (either on the providing or receiving end) may be subject to. On the other side, an IT tool may hardly provide the level of nuance or strategic view that an experienced compliance professional would be able to provide. Thus, through the synergy and integration of IT capabilities with human experience, compliance can be simplified and the data sharing activities sustained.

### 5.1.2 Methodology

This chapter provides a legal perspective on how the FReCo tool may support certain aspects of a compliance process. This view should be understood as preliminary and based on the FReCo current prototype, while also taking considering that implementation in a production environment, and testing with additional use cases would be able to trigger additional or different considerations.

Furthermore, it is worth pointing out that the project's legal partner has been involved in certain aspects of the FReCo development, such as through the provision of relevant legal information, (i.e. EU law Directives and Regulations).

In this regard, the collaboration between the legal and technical partners in relation to the pursuit of the completion of the above task has been conducted through the bi-weekly meetings organised by the WP3 leader, as well as through other dedicated meetings and calls. It is worth pointing out, in consideration of the feedback received, that several versions of the FReCo tool have been produced, with the current one under consideration being the latest. 2 Compliance as identification and scoping

Generally, companies and organisations undertaking data processing activities are subject to several regulatory requirements. Within the European Union (EU), and within the context of the FAME Marketplace, the legal framework related to data processing activities, and in particular to the processing of financial data is articulated under D1.3 "Ethical Management and Regulatory Compliance Framework I", submitted in M18, together with certain Ethics-related requirements that were elaborated in Deliverable 8.1 "Ethics Requirement", submitted in M12.

This complex legal framework, which consists of EU Directives and Regulations, as well as national implementations and distinct enforcement mechanisms, presents itself as a maze, which can be difficult to navigate for non-legal experts. In this sense, compliance to regulation requires an initial overview of relevant information within this legal framework, which is the main prerogative of the

FreCO tool. Accordingly, identification of the relevant regulatory frameworks and requirements can be defined as scoping. The latter, namely the identification of the specific legal obligations to which a specific organisation or natural person is subject to, are usually determined for reason of the purpose and object of the (data processing) activity in question. In the context of FAME's use cases, i.e., the making available and sharing of certain datasets, scoping requires addressing certain central questions, such as: what data am I processing? What are the legal entitlements attached to it? And what are the aims related to such data processing activity? Furthermore, this process of discovery and scoping is not a one-time exercise. As the objects and aims of data processing activities may change, and so too will the relevance and the applicability of obligations.

A preliminary analysis, addressing such questions, may determine the relevant laws with which any organisation may be obliged to comply. Nevertheless, determination of the specific legal requirements that an organisation or a natural person may be required to fulfil may depend on national implementations or the specific circumstances of the case at hand, which a general model may not be able to fully capture.

### 5.1.3 Compliance Challenges specific to FAME

The FAME Marketplace will likely face similar challenges in the future, especially as it is promoting the application of novel technology. The compliance requirements for some legislation (e.g. GDPR) are clear, but of course burdensome and requiring close attention, as the consequence of a negligent oversight could result in undesired repercussion (e.g. a fine). The applicability of other legislation depends on the specific nature of FAME's activities, which could change in the future (i.e. it may decide to offer investment opportunities to its users, which would require the satisfaction of additional legislative requirements). Moreover, there are laws that have been proposed (yet to take effect), which can still change, creating uncertainty from a compliance standpoint (i.e. FIDA). The challenges presented in complying with a complex regulatory landscape, and an increase in cross-border operations/interconnectedness, has thus resulted in an increased shift towards the use of tools that assist with compliance.

### 5.1.4 Specific focus point / main challenges

Although this chapter presents legal compliance for the FAME environment as complex and contest specific, there are – at least – three main challenges related to regulatory compliance that are of prominence in the context of FAME:

**1. Processing of personal data**

Although FAME explicitly states that its marketplace is an environment that facilitates the exchange of non-personal data, which are outside the scope of personal data protection law, when it comes to processing of large amount of datasets, excluding the processing of personal data, as defined in Art. 4(1) GDPR, is not so straightforward. The challenge relates to the large datasets made available by their offerors, which despite their best intentions might still be processing personal data. Furthermore, GDPR applies across sectors and establishes some common principles of general relevance, whose value goes beyond personal data protection and privacy. Therefore, the FReCo tool may be able to provide some general information regarding certain GDPR principles, of likely relevance and usefulness for the FAME marketplace users.

**2. Access to financial information (FIDA, perspective)**

Considering FAME's focus on financial services, from a data perspective, given their sensitivity and special regime of protection, access and re-use of financial data represents a prominent regulatory challenge. Furthermore, access and re-use of financial data, the European Commission has proposed new legislation, namely FiDA.1 At present, financial institutions/entities are not obliged to make financial data available, as security and confidentiality interests prevail.

**3. Licensing and re-use (open data)**

The FAME marketplace allows data offerors to connect with entities potentially interested in using their data product. In order for data sharing to take place, both parties would need to establish some form of licensing agreement, which would include, among the other aspects, terms on the responsibilities of the offeror, as well as the use rights and restriction bestowed upon the user. This is an area that is not included in the scope of the FReCo tool, and that the FAME marketplace, through the activities pursued under WP1, supports in the form of "Suggested Transaction Terms", which are non-binding terms which can be used by the parties, notwithstanding that the ultimate decision lies with the parties to the agreement.

## 5.2 The provision of 'Legal Advice' as a regulated matter

Legal advice is the application of legal rules and principles to a specific set of facts, providing guidance on a potential course of action for a particular legal matter. It involves interpreting the law, assessing the client's situation, and offering an opinion on potential outcomes and strategies. This guidance is typically provided by a qualified legal professional, such as a lawyer, and is tailored to the individual's unique circumstances. The provision of legal advice is a right bestowed upon, and limited to, a lawyer who is a part of a national bar association.

In contrast to the provision of legal advice, the fundamental aim of FAME's Regulatory Compliance tool is not to designate any sort of legal interpretation or imply that a user should take a certain legal approach. Instead, the aim is to inform a user and to facilitating regulatory compliance. The tool does not assume an advisory role, provide legal advice, or insinuate any sort of legal relationship with a user. The intention behind this tool is to provide an initial overview of the legal information, such that a user is informed to know where certain legislation applies in their circumstance.

## 5.3 Concluding remarks

From a legal perspective, an IT tool, like the FReCo, that is able to provide some relevant legal information regarding a data processing activity, either in consideration of the type of data processed, or in consideration of the aim of the data processing activity, is of potential legal value. Nevertheless, it should be stressed that the provision of legal advice is a matter regulated by law and reserved to qualified personnel, usually members of a bar associations. Furthermore, analysis of the specific circumstances of the case, or evidence of exceptions or limitations, which are key to understand the actual applicability of a legal norm, and their actual implementation in a national context are also outside the scope of the FReCo tool.

[1] The FIDA proposal is discussed in detail in Deliverable 1.3.

# 6 Conclusions

In this deliverable we outline the mapping of the FAME project's regulatory compliance framework against similar European projects such as GAIA-X and IDSA. Then, we supply information about the related laws and regulations in the field. Finally, we present the prototype of the regulatory compliance tool website.

The regulatory environment of financial technology and embedded finance industry is ever changing. Therefore, it is vital to keep the stakeholder up to date in regards of related laws and regulations. The aim of this deliverable is to provide an overview of the related laws and regulations in full scope. We start by describing the positioning of the FAME project's regulatory framework in relation to similar European projects. Then, we deliver a full review of the seven most related laws and regulations in the field. We also describe a prototype of the regulatory compliance tool website.

Accessing the related laws and regulations in the field of finance in general and embedded finance in particular is easy. There is full access to the related laws and regulations on the European parliament website. However, defining the most relevant laws and regulations is cumbersome. We strive to provide a shprt description of each law and regulation in the regulatory environment follow up by a full description of the laws and regulation for the end users' benefit.

We provide the latest updated version of the regulatory compliance tool which can be accessed through FAME marketplace. We describe its features and functionalities. This tool provides an easy-made all-in-one assistance to users to navigate through FAME while being aware of related laws and regulation and standards. The current version of the tool is a result of searching and designing the most beneficial tool to the users considering their motives and needs. The tool benefits from advisory and team effort of FAME legal team and is designed as such to minimize the liability of FAME in providing advisory legal suggestions. This tool makes searching and retrieving of necessary information quite easy and make the navigation of the users through FAME an aware journey of knowing related laws and regulations and standards.

# 7 References

[1] GDPR General Data Protection Regulation EUR-Lex - 02016R0679-20160504 - EN - EUR-Lex (europa.eu)

[2] https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp

[3] Data Act Data Act | Shaping Europe's digital future (europa.eu)

[4] DATA Act: OMB, Treasury, and Agencies Need to Improve Completeness and Accuracy of Spending Data and Disclose Limitations | U.S. GAO

[5] Data Governance Act / Open Data Directive The Data Governance Act & The Open Data Directive | data.europa.eu

[6] DORA Digital Operational Resilience Act (DORA) (europa.eu)

Publications Office (europa.eu)

[7] NIS2 The NIS2 Directive: A high common level of cybersecurity in the EU | Think Tank | European Parliament (europa.eu)

[8] PSD3/PSR + MIFID II + 4AMLD Introducing the PSD3, PSRs and FIDAR – reshaping the EU's regulatory framework on payment services and e-money - PwC Legal

[9] Consumer rights Consumer Rights Act 2022 (irishstatutebook.ie)

# 8 ANNEXES

## 8.1 ANNEX I – Legal Assessment

The following includes a generic list of legislation, both from an end-user and platform perspective, included for the purposes of the FReCo tool. A more detailed legal analysis of the legislation mentioned below can be found in Deliverable 1.3 and 1.5 ["ETHICAL MANAGEMENT AND REGULATORY COMPLIANCE FRAMEWORK I & II"] submitted in M18 and M36 of the project.

### 8.1.1 General Data Protection Regulation

The General Data Protection Regulation replaces the Data Protection Directive and lays down stringent rules for the protection of an individual's personal data. In upholding a principle-based approach to processing personal data processing activities, it also enumerates the privacy rights of individual persons and designates processing responsibilities to a 'controller' and 'processor' of personal data. The GDPR applies to the automated processing of personal data (wholly or partly), and processing of personal data that is not automated, and intended to form part of a filing system by a person or an entity within the EU. Processing activities conducted outside the EU are included within the scope of the GDPR if they relate to personal data of individuals in the EU.

### 8.1.2 The Data Act

The Data Act seeks to promote access to product data, facilitate B2B and B2C data sharing, and correct imbalances perpetuated by unfair unilaterally imposed contractual terms. In addition, it sets out requirements for the switching of data between processing services, security requirements for the prevention of unlawful access to product data, rules for data interoperability, for data sharing mechanisms and services, and for Common European data spaces.

### 8.1.3 The Data Governance Act

The DGA plays a significant role in the EU's plan to make Europe fit for the digital age and to facilitate Europe's digital transformation by 2030. It aims to improve the conditions for the sharing of data between organisations within the EU to support the use of data research and innovation. Since public entities and organisations generate copious amounts of data daily, the DGA seeks to make use of the combined value of such data to facilitate innovation and economic growth.

### 8.1.4 Framework for Financial Data Access (FiDA)

FiDA is a sector specific piece of legislation aimed at promoting open finance and build on the progress made with respect to payment legislation. It promotes access to financial data held by financial institutions/ entities, permitting the consensual sharing of financial data with third parties interested in its use. These third party's included other financial entities including Financial information service providers (FISPs), and the scope of includes the financial data of consumers and businesses.

### 8.1.5 NIS2 Directive

The Network and Information Security 2 (NIS2) Directive builds on the initial NIS directive, which aimed to achieve a high common level of cybersecurity across the Member States. NIS2 addresses the shortcomings of its predecessor, with a wider scope of application, clearer rules, and stronger supervisory tools. The expanded scope of NIS2 requires Member States to enhance their cybersecurity capabilities, while also requiring entities from an increased number of sectors to make reports and integrate risk management plans. It also obliges Member States to implement rules for cooperation, information sharing, supervision, and enforcement of cybersecurity measures.

### 8.1.6 Digital Operational Resilience Act

The Digital Operational Resilience Act seeks to promote the protection of the financial sector, which has become increasingly dependent on technology and tech companies to deliver their services, making it vulnerable to cyber-attacks and incidents. DORA harmonizes digital operational resilience rules, covering ICT risk and third-party risk management, framework, monitoring, digital operational resilience testing, ICT related incidents reporting, information and intelligence sharing on cyber threats, and an oversight framework for critical ICT Third Party Providers (CTPPs).

### 8.1.7 The Third Payment Service Directive (PSD3) & The Payment Service Regulation (PSR)

PSD3 is a revision of PSD2 (which focuses primarily on payment account data), aimed at regulating newer payment providers and services (internet, mobile, card) and further open access to data in the financial market, while ensuring a high protection level for payment service users across all Member States. The Payment Service Directive and the Payment Service Regulation (PSD3/PSR) contain harmonizing rules on licensing and supervision related to a wider range of providers of payment services, including non-banking Payment institutions (PIs) and Payment Service Providers (PSPs).

### 8.1.8 Open Data Directive

The open data directive replaces the Public Sector Information Directive, and strives to encourage Member States to make as much data available for re-use as possible, with a focus on data held by public sector bodies in the EU, on a local, national, and regional level. This includes material held by ministries, state agencies, municipalities, and organisations that are publicly funded or at least partly under a public authority's control.

### 8.1.9 AI Act

The rules included in the AI Act aim to guarantee the safe development of AI systems with a human-centric approach that respects fundamental rights. The AI Act applies a risk-based approach to regulating Artificial Intelligence, setting out clear rules for developers and deployers of AI in relation to its use. It defines and outrightly bans AI systems that perpetuate an unacceptable level of risk, while developers of high-risk AI systems must comply with strict obligations before a product is placed on the market. Low-risk AI-systems fall outside the scope of the AI Act.

### 8.1.10 Digital Service Act (DSA)

The DSA regulates online intermediaries and platforms such as marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms. Its main goal is to prevent illegal and harmful activities online and the spread of disinformation. It ensures user safety, protects fundamental rights, and creates a fair and open online platform environment. The DSA introduces new obligations for providers of online marketplaces to counter the spread of illegal content.

### 8.1.11 Electronic identification and trust services for electronic transactions in the internal market (eIDaS)

The eIDAS Regulation provides for the interoperability of national eID schemes among EU member states. This requires the development of a technology-neutral framework that does not favour any particular technical solution for eID implementation. Procedural and technical standards have been set to facilitate cooperation among EU countries, aimed at ensuring the seamless exchange of electronic identification data and fostering a cohesive digital ecosystem across the EU. At the same time, eIDAS created a level playing field for a number of trusted services, which have become indispensable in today's digital value chains: Electronic Registered Delivery Services (ERDS). These ensure secure and reliable delivery of electronic messages, data, or documents and provide evidence of the time of sending, receipt, and content integrity.

### 8.1.12 Markets in Financial Instruments Directive (MiFiD II)

MiFID II aims to improve transparency, fairness, and efficiency in financial markets while strengthening investor protection. The directive covers various financial instruments, including stocks, bonds, derivatives, and structured products, as well as investment services and activities. MiFID II places a strong emphasis on safeguarding investor interests by ensuring firms act in their best interests and provide suitable investment advice. Firms are required to report all transactions in financial instruments to regulators in a timely and accurate manner, promoting market transparency. MiFID II enhances the transparency of trading activities by requiring more pre- and post-trade information to be made publicly available. Investment firms must take all the reasonable steps to achieve the best possible results for their clients when executing orders. To address conflicts of interest, MiFID II requires the separation of research costs from execution services, ensuring transparency in research charges.

### 8.1.13 Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT)

A new legal framework on anti-money laundering and countering the financing of terrorism was proposed on 20 July 2021 by the European Commission,1 and approved in April 2024 by the EU co-legislators (i.e. EU Parliament and Council of the EU). The new framework introduces three Regulations, a Directive, and a new EU authority to fight money laundering (AMLA) and expands its scope of application to include crypto-asset service providers, residence scheme operators, crowdfunding operators, football clubs and football agents will enter in force in the following months.

## 8.2 ANNEX II – Legal Assessment in relation to FAME project

The following overview shows a list of additional legislation considered in regard of FAME project pilot and included in the FReCo tool.

### 8.2.1 Consumer Rights Directive

The Consumer Rights Directive promotes the protection of consumer rights across the EU. It addresses internal market barriers to transactions between consumers and traders through the introduction of harmonized rules. This directive applies to contracts concluded between a 'consumer' and a 'trader' and is without prejudice to national legislation in other areas. Established, in this directive, are rules on the information to be provided for 'distance', 'off-premises' and other contracts. In addition, the consumer rights directive also clarifies on the right of withdrawal for both 'distance' and 'off-premises' contracts, while harmonizing rules for performance and B2C contracts.

### 8.2.2 Intelligent travel systems (ITS Directive) 2023/2661

Intelligent Transport Systems help inform, coordinate, and enhance the safety of transport networks, a necessary innovation with the ever increase volume of road transport within the European Union. The ITS Directive was first adopted in July 2010 with the aim of coordinating the implementation of Intelligent Transport Systems across Europe. Its Initial focused areas were road; traffic and travel information; continuity of traffic and freight management ITS services; ITS road safety road security; and linking vehicles to transport infrastructure. The new directive 2023/2661/EU amended this to adapt to technological developments.

### 8.2.3 Trade Secret Directive 2016/943

The trade secrets directive is aimed at protecting trade secrets. It harmonizes national laws that address protecting business know how and information from unlawful acquisition, use and disclosure, and intended to have a deterrent effect on such practices. Amongst some of the key points it addressed are the lawful acquisition of a trade secret; unlawful acquisition, use & disclosure of a trade secret; and exceptions.

### 8.2.4 EU Corporate Sustainability Reporting Directive

The EU CSRD introduces certain sustainability reporting obligations. Companies operate within the EU are required by law to disclose information on the various social and environmental risks they face, and how their activities impact the environment & people. This is a fundamental component to the European Green Deal and helps inform investors and other stakeholders on the sustainability performance of a company. This directive is applicable from 2025.

### 8.2.5 Sustainable Financial Disclosure Regulation

The aim of the SFDR is to promote transparency and clarity for investors on the sustainability aspects of investment funds. It harmonizes sustainability related disclosure rules for financial market participants & advisors, who are required to disclose certain information on their websites, contractual

documents, and reports. The disclosure obligations discussed in this directive have been applicable since March 2021.