

Green Paper

**Challenges and Recommendations
for a Research Data Ecosystem
to Support Innovations in the FCT Domain**

Table of Contents

03	Foreword
04	The Need for a Research Data Ecosystem in the FCT Domain
06	Methodology
08	Core Challenges for RDEs in the FCT Domain
18	Moving Forward
25	Summative Remarks
26	Bibliography
27	Acknowledgements

Foreword

Conducting reliable, innovative, and impact-driven research in the FCT domain paves the way for better national and European security capabilities, thus supporting improved prevention, detection, and investigation of crime and terrorism.

A significant barrier to FCT research is its highly fragmented nature, as well as a distrust amongst stakeholders about the utilisation or provision of data for research. This fragmentation and propensity for lacking trust have detrimental effects on the efficiency of collaborations amongst stakeholders conducting vital FCT research and innovation activities.

There is an urgent need, therefore, to establish a trusted infrastructure to support robust collaborations and high-quality results. A European FCT Research Data Ecosystem (RDE) is one of the proposals to improve current collaborative practices and opportunities.

The aim of an FCT-specific RDE is to enhance specifically large-scale, cross-border research that leads to new innovations as well as mature tools, solutions, and capabilities for Law Enforcement Agencies (LEAs) to tackle known but also emerging threats in terrorism and crime.

This green paper offers initial findings about the core challenges that may hamper the creation and/or uptake of an FCT-specific RDE, as well as suggestions by subject-matter experts on how to overcome such challenges.

We are grateful for the EU-funded project LAGO to support this work.

Professor Babak Akhgar OBE
Director of CENTRIC

The Need for a Research Data Ecosystem in the FCT Domain

Security research is of utmost interest to the European Commission (EC) due to the constantly evolving and complex threats Europe faces.

Currently, EU-funded research in the security domain contributes to around 50% of the overall funding at the European level and helps to strengthen European security by providing innovations and modern technologies. It further enables vital policy developments in full compliance with ethical requirements and fundamental rights. [1]

Additionally, the Community for European Research and Innovation for Security (CERIS) facilitates collaborations between relevant stakeholders such as policymakers, practitioners, industry, and scientists, which furthers the identification

of needs and gaps in the domain and supports stakeholders to address them.

CERIS is further concerned with the standardisation of research-related needs in the security domain under consideration of citizen views. [2]

Some examples of the benefits of EU civil security research innovations are demonstrated by the deployment of:

decision tools for pandemic management during COVID-19

a pan-European early warning platform for disaster resilience

technical solutions for addressing cybercrime and border control issues. [3]



Data is at the heart of all research and innovation. The European Strategy for Data [4] seeks to initiate a single European market for data by implementing common European dataspaces.

In this context, the strategy seeks to adopt legislative measures on data governance, access, and reuse and to invest in next-generation standards, tools, and infrastructures for data management. [4]

Research and data in the FCT domain require specific regulations and governance due to their often-sensitive nature. In the current list of domain-specific dataspace, a dataspace targeted specifically to FCT research is not mentioned. [5]

An alternative would be the inclusion of FCT data in the European Open Science Cloud (EOSC). However, this solution might lead to compromised security due to the multi-discipline and open characteristics of the EOSC.

A more promising approach is the creation of a dedicated Research Data Ecosystem (RDE) for FCT research.

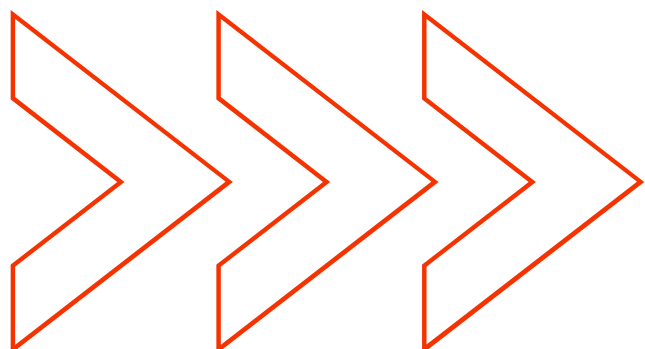
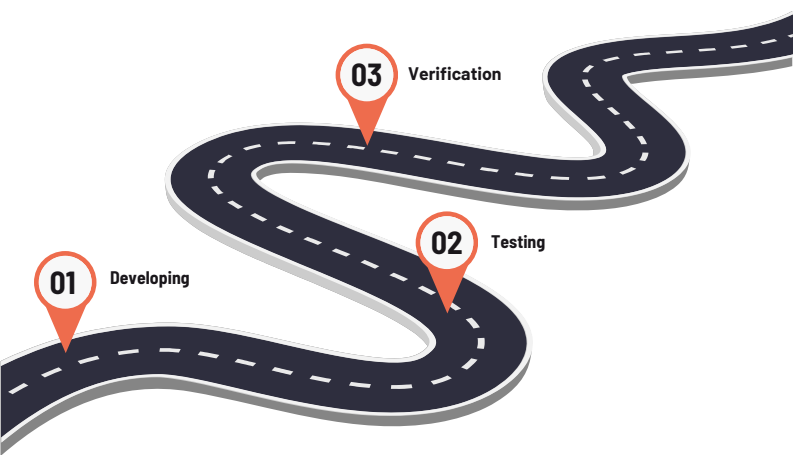
A purpose-built RDE can provide the much-needed infrastructure to address the gaps and frequent fragmentation in FCT research collaborations.

An FCT-specific RDE can further act as support for the development, testing, and verification of tools, solutions, and models for the increasingly important areas of Machine Learning (ML) and Artificial Intelligence (AI).

Effectively implemented, RDEs can enhance trust, which lies at the heart of research efforts, and overall accelerate European efforts to develop innovative approaches to crime fighting.

The creation of effective RDEs is not a trivial task. The following section provides an overview of the frequent challenges FCT researchers and organisations in the FCT research domain encounter in their efforts to share data or create useful products.

This is followed by a summary of suggestions offered by subject-matter experts on how to address these challenges in practical and regulatory terms.



Methodology

The observations presented in this paper combine insights from expert interviews and a review of documentation about existing approaches to data ecosystems and data sharing practices in FCT-related as well as other domains.

The literature review included documentation from European countries, the UK, and the USA. The literature included reports, guidelines, strategies, policies, and other documentation addressing data sharing in applied research. It involved FCT-specific literature but also documentation from other areas with similar complexity (health and defence), equating to over 80 reviewed documents. More specifically, the literature covers regulations and standards at the EU and national level (including Estonia, Bulgaria, Greece, the USA, and the UK), providing a wide overview of current data sharing practices.

Documentation from the USA was incorporated, as the USA is an important source of data suppliers (316,190 as of 2020). [6] In comparison, the cumulative number of data suppliers for the EU and UK was 297,350 in the same year. [7] In 2023, the USA will lead globally with 35.7% of the global information and communication technology (ICT) market share, followed by the EU (11.8%) in second place and the UK (4.5%) in fifth place. [8]




The analysis of US-sourced documentation enabled a comparison of the European landscape and practices in FCT research data sharing with US approaches. UK literature and experts were consulted for the same reason. [8]

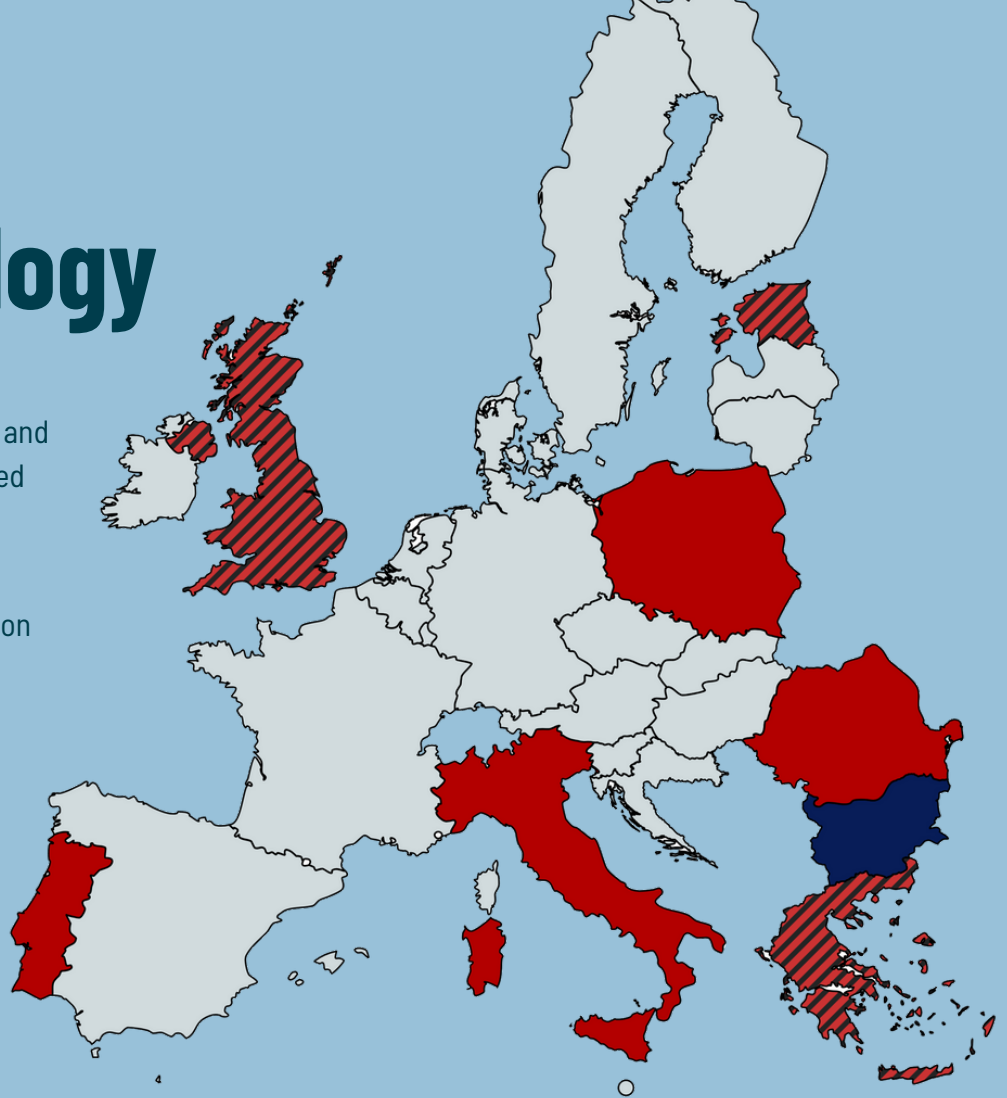
The second step consisted of written expert consultations to obtain the views of 30 subject-matter experts. The experts covered a broad geographical area across Europe, stemming from Estonia, Greece, Italy, Poland, Portugal, Romania, and the UK. The majority (70%) reported moderate to very high experience in FCT research, while 23% reported some FCT research experience, and 7% did not elaborate on their FCT research experience.

The written consultation consisted of four thematic sections: current state of practices; tools, resources, barriers, and enablers; good practices, including risk assessment and management; and mapping future opportunities. The questions were a mix of open-ended and ranking exercises.

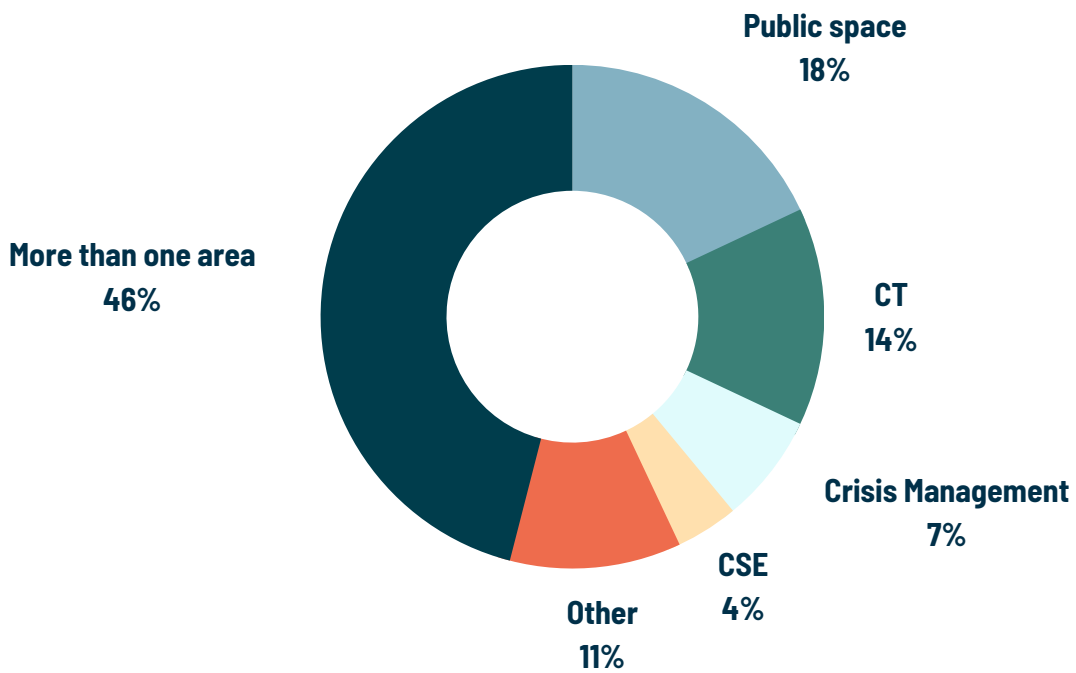
The information from the consultations was analysed thematically to identify common themes, challenges, and suggestions. The analysis aided in the determination of relevant key projects and initiatives, standards, practices, challenges, priorities, and enablers in the FCT research domain.

Methodology

-  Consulted researchers and documentation reviewed
-  Consulted experts
-  Reviewed documentation



Experts' sectors



Core Challenges for RDEs in the FCT Domain

The results of the two-tiered approach identified eight core challenges that may obstruct the development and successful long-term implementation of an FCT-specific RDE.



FCT-Specific Data Standardisation

Dearth of standards specific to FCT and FCT research



Strengthening Cross-Stakeholder Trust and Enabling Transparency

Low trust amongst stakeholders is driven by a lack of transparency



Technological Requirements for FCT Research

High heterogeneity of tools and lack of specialised capabilities



Achieving Appropriate Data Control

Absence of a common data management and governance framework



Importance of an Interoperable Data Infrastructure

Need for the better interoperability of data spaces



Data Quality Assurance

Need for reliable data quality assessment and verification tools, lacking clarity of data ownership



Legal Policies and Regulation

Handling a plethora of EU and national laws with complex application



Intra-Organisational Issues

Need for highly-trained and experienced personnel

Challenge 1: FCT-Specific Data Standardisation

Data standardisation emerged as a central issue. Experts consistently noted the current lack of standardisation in data collection, storage, and analysis, which increases the risks of inconsistencies and errors in the data and, subsequently, in research findings and products.

The first issue is **managing and accommodating the multitude of data formats** that play a role in FCT research.

A vast array of relevant data types, each of which may come in different formats and thus require a different set of tools and solutions for their sharing, processing, and storage were highlighted.

Moreover, the use of different data formats significantly hinders the interoperability of data processing from multiple sources and jurisdictions.

The most relevant data types in FCT research as identified by experts:



A second issue is a lack of common FCT standardisation, which lies at the root of multiple challenges for the development and deployment of a successful FCT RDE.

Most importantly, **different research fields** adhere to different data standards. Experts further reported a **lack of pressure for organisations to comply with relevant standards**—or if entities attempt to comply with standards, they may be unsure how to apply these standards operationally.

This is compounded by the fact that there are often **no FCT-specific standards**. Experts, when asked for recommendations on FCT data standards and policies, often refer to generic data standards rather than FCT-specific ones.

Additionally, different stakeholders involved in FCT research may have **varying professional standards**, which further complicates the sharing and handling of data. This creates a pressing need for establishing shared FCT data standards, regulations, and processes that will enable coherent and regulated data sharing and handling for FCT research.

Accordingly, the majority of the consulted experts also listed the implementation of common standards for data creation and data types as a top-five enabler and priority in FCT data sharing.

However, while standardised FCT data and metadata vocabularies can increase the findability (as referenced by the FAIR Principles) of resources, it may be challenging to achieve due to the **lack of single-source search capabilities** that support metadata fields across domains.

Such search capabilities thus need to be developed alongside standardised practices and processes.

A further challenge facing stakeholders for data sharing emerged from the **multi-level protection present in the shape of EU-wide GDPR and EU countries' individual legislation**, which, although safeguarding personal data, increases the complexity of data sharing for research purposes and creates silos.

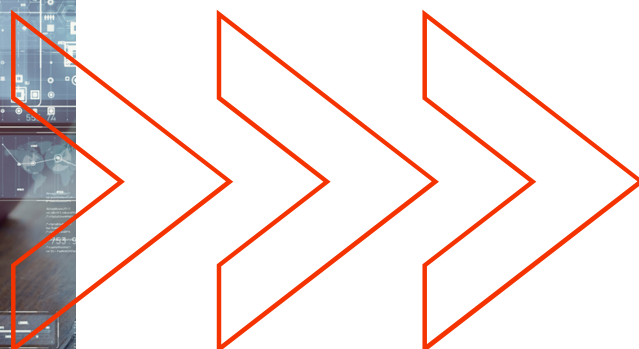
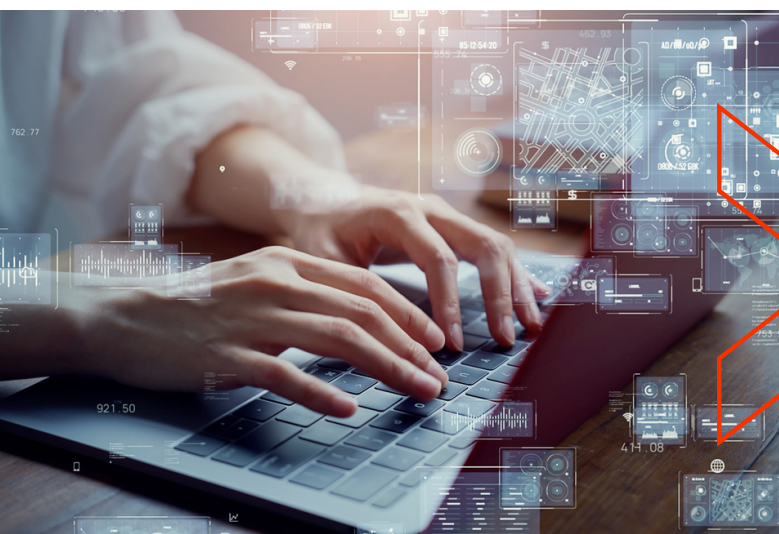
Moreover, the development, implementation, and maintenance of FCT data standards will require reliable and continual funding, either for the entities developing and implementing the standards or the organisations adhering to them.



An FCT-specific RDE may involve various parties with different frameworks, standards, and strategies for sharing, co-creating, and managing data based on their roles and responsibilities within the ecosystem. [...]

To ensure effective collaboration between the different parties in the RDE, it is essential to establish clear policies and standards for data sharing, co-creation, and management within the ecosystem.

Furthermore, interoperability and compatibility between different tools and technologies used within the RDE must be established to enable seamless data exchange and analysis.



Challenge 2:

Technological Requirements for FCT Research

FCT research requires a wide range of technological solutions, including capabilities that enable and support data storage, sharing, processing, and protection. Such **capabilities and solutions** are often costly, especially if they are FCT-specific security considerations. Thus, reliable funding is needed, which may not be equally available for all stakeholders.

FCT research data is often large and complex, with a high diversity of data and data standards—an issue highlighted as part of the standardisation challenges. This diversity can limit data exchange in FCT research to specific sectors or technical capabilities, but it can also create a potentially problematic **heterogeneity in the required tools, technical requirements, and knowledge**.

Additionally, as various experts stated, the present **use of disparate data platforms and formats** severely hinders efficient data sharing, making data analysis from different sources an incredibly difficult endeavour.

The experts therefore highlighted the need for new, user-friendly technologies and tools that can enable the efficient and seamless processing and exchange of large and complex datasets. The experts also expressed the need for the development of automated tools and AI capabilities that would assist in the analysis, visualisation, and interpretation of data, as current

processes can be cumbersome, time-consuming, and inefficient. Answers further illustrate **disparities in preferred storage solutions** within the experts' organisations, with answers referencing on-site storage, cloud storage, data warehouses, own servers, and blended approaches.

As per Article 25 of the GDPR [9], appropriate security measures should be in place in order to provide data protection 'by design and default'. [10] Providing 'privacy by design' means that a system is designed in consideration of privacy and security measures, which effectively become a built-in segment of the system rather than an add-on. [10]

The top three security methods utilised by the experts' organisations were identified as access control, data encryption, and data anonymisation. Especially for data anonymisation, experts indicated that there is an insufficient range of anonymisation tools available.

Advanced technology and tools, like data analysis software, surveillance systems, and network monitoring tools, are necessary for collecting, processing, and analysing large amounts of data, identifying patterns and trends, and supporting investigations.

Challenge 3:

Importance of an Interoperable Data Infrastructure

Ensuring interoperability of infrastructure and processes is a vital prerequisite for the successful implementation of an FCT ecosystem. There are numerous examples where multiple sets of standards, each concerning a limited number of parties, limit data interoperability at the national level, let alone at the EU level.

The experts therefore highlighted the need for interoperability of central data space

components with national systems and cross-border processes.

The interoperability of data infrastructure is critical to enabling FCT data sharing. This includes standardisation of data formats, metadata, and interoperable data platforms, which can facilitate the seamless integration and exchange of data across different systems.

Challenge 4:

Legal Policies and Regulation

FCT research and all data practices within it need to adhere to legal policies and regulations. Experts indicated the **plethora of regulations** as one of the core challenges they face, such as an abundance of personal data protection policies on a national level covering different sectors.

Moreover, the European Union introduced legislation in an attempt to overcome the lack of accessible LEA data by universities and FCT researchers. The regulations intend to create a more robust and accessible network for LEAs and FCT researchers in their efforts against crime and terrorism.

Leading is the General Data Protection Regulation (GDPR, 2016/679), which determines practices for data sharing across the EU. The primary focus of Regulation 2016/679 is to enhance security and 'protect fundamental rights and freedoms of natural persons and, in particular, their right to the protection of personal data'. [11]

However, GDPR is one of the reasons why experts suggest organisations hesitate to share data. **GDPR is complex and open to various interpretations**, which 'could create such rigid restrictions that the initiative becomes ineffective over time'. [12]

And actions are being taken when the GDPR is breached. In Ireland, for instance, the Information Commissioner's Office (ICO) has imposed reprimands and fines against a number of LEAs and officers, while universities in Germany have received fines imposed by the Federal Commissioner for Data Protection and Freedom of Information (BfDI) for non-compliance with data protection principles. [13,14]

In addition, crucial organisations in the FCT domain are required to **adhere to specific regulations**, among them Europol. EUROPOL is involved in a wide range of FCT research activities, including work with the Horizon Europe scheme.

Article 35 of Regulation 2016/794 mitigates the risk of data protection breaches in Europol as it states they are only able to transfer data to Member States, international countries, or organisations that have made an adequacy decision in their respective states.

EUROPOL and their strict data protection policies are a positive example of well-regulated data practices, but they can also introduce complexities for researchers and innovation activities.

Further frameworks aimed at protecting law enforcement officers exist on a national level, such as the Bulgarian Policy of Personal Data Protection regulation of the Ministry of Defence (MOD) and the Bulgarian Army. [15]

The policy outlines the rights of the Bulgarian MOD to process personal data

and to share such for national defence and security reasons, speaking to the difficulty of navigating disparate rules and laws.

A substantial amount of FCT research is conducted in and through third countries. This requires FCT researchers and organisations to be aware of any differences in and changes to specific regulations that impact their area of work relating to their country and possible partnership countries.

For instance, incompatibilities exist between European law and English law on copyright when transferring data that has undergone web scraping. It has further been highlighted that the current legal frameworks do not provide researchers with exemptions from copyright in text and data mining (TDM). [16]



Create policies and procedures that define data management practices, data sharing agreements, data security measures, and guidelines for data access and use. This can help to ensure consistency and transparency in data sharing and can help to build trust among stakeholders.



Challenge 5: Strengthening Cross-Stakeholder Trust and Enabling Transparency

The majority of the consulted experts commented on a **lack of trust between stakeholders** as a significant barrier to data sharing in the FCT domain. This lack of trust was linked to **concerns about the potential misuse of data** and **uncertainties about the reliability and quality of the data provided**.

Furthermore, **security concerns**, such as the risk of data breaches and cyberattacks, can be a cause for reluctance to share sensitive data.

A second trust challenge relates to **citizens as stakeholders** in the FCT domain and their rights and roles in data practices. While citizens should have clarity on how and when their personal data is being processed, this can be problematic to achieve in practice. Experts from Poland proposed a statistical system on criminal and terrorist incidents that is currently being developed on a national level. Here, the data is input by citizens themselves, and a National Threat Map is generated based on the citizens' entries. Such applications, however, rely on trust by citizens (to ensure willingness to share this information) and trust in citizens (e.g., that the provided data is correct, not driven by agendas, etc). It is clear from the expert's feedback that the principle of transparency is a key tenet in gaining and facilitating trust between all participating

actors in the RDE. It is often argued that by providing citizens with a punctual overview of how exactly their data is used, greater trust can be achieved. However, such a level of transparency can be difficult to achieve for practical as well as operational reasons.

Transparency and trust also emerged as challenges within the broader issue of **potential duplication of efforts**. The experts highlighted that often multiple competing EU initiatives or projects exist, which should align to avoid duplications, which may not be efficient due to a lack of mutual awareness or reluctance to share.

Trust is a major concern in FCT research when it comes to data sharing and creation. Since FCT research involves sensitive data, it is crucial to have trustworthy partners involved in sharing and creating data to ensure data quality, accuracy, and privacy. [...] Building trust is critical for successful data sharing and creation in FCT research. Transparency, mutual respect, and open communication channels are essential for establishing trust between partners. Additionally, a clear legal and policy framework that provides guidelines and protocols for data sharing and use can help build trust.

Challenge 6:

Achieving Appropriate Data Control

Thorough data control is paramount in the context of FCT data ecosystems. Data control is a complex issue that encompasses a wide spectrum of aspects, such as levels of data access for different stakeholders, the application of data protection practices (such as anonymisation and encryption), the standardisation of data and metadata formats, the applicability of tools, and the implementation of policies and regulations, to name but a few.

Currently, there is heavy reliance on GDPR as interpreted and applied by each EU state. Experts comment on **severe penalties** and a **lack of knowledge on how GDPR impacts**

data sharing in an FCT context, which can create hesitancy and reinforce silos in this domain. Additionally, EU Member States have their own legislation, which further hinders effective data control. Experts thus highlighted a pressing need for the establishment of effective common data management and governance frameworks.



FCT research involves sensitive data and information, and policies and governance frameworks are required to ensure that data is managed securely and that research is carried out in accordance with ethical, legal, and regulatory requirements.



Challenge 7:

Data Quality Assurance

Poor data quality can lead to erroneous conclusions and wasted resources. Moreover, according to experts, data quality concerns can also **cause a reluctance to share and request data**.

These concerns are also directly linked to the lack of broadly applied and standardised practices and guidelines. Thus, the majority of experts stated the **need for more and more reliable data quality assessment and verification tools**.

Another issue identified in the context of data quality is the lack of clarity of data ownership, which can cause delays in data validation and quality controls.

More specifically, **a lack of clarity regarding the rights and responsibilities of contributing organisations** is not uncommon and can make it difficult to understand which body is responsible for data quality assurance.

Data quality issues may also arise since **research funding is limited**.

Thus, researchers might need to use more readily available data in order to fit into the funding timeline.

Future research in FCT can focus on developing new methods to ensure the quality of the data used in research. Ensuring data quality is critical for producing accurate and reliable research outcomes. Researchers can focus on developing new methods for data cleaning and quality

assurance frameworks to improve data quality. This can include developing new algorithms and tools for detecting and correcting errors in data, as well as new techniques for measuring and validating data quality. By improving data quality, researchers can ensure that their research outcomes are robust and trustworthy, which is critical for informing effective policies and strategies for fighting crime and terrorism.

Challenge 8: Intra-Organisational Issues

Experts also identified a number of organisational barriers within the FCT research domain, most prominently the existence of non-standardised vocabularies, the lack of skilled personnel, and insufficient funding for costly equipment and tools.

Disparate languages and vocabularies across, but also importantly within, organisations can prove barriers to data re-usage and sharing.

Organisations also need sufficient equipment, tools, and access to tools,

infrastructure, services, and personnel. The lack of such resources will have a detrimental effect on the possibilities of participating in FCT research and its outcomes and can lead to loss of trust, compromised security, and wasted data. Continued financing was therefore repeatedly mentioned as one of the biggest challenges.

Experts further mentioned the **need for better education and training** to ensure that those working within FCT research are provided with adequate knowledge and skills.

Experts commented on a **shortage of skilled personnel in regard to data handling** in the FCT domain.

Core training needs identified are: data science, Machine Learning, statistical analysis, cybersecurity, security training, and FCT-specific skills.

In addition, for effective FCT research, generally multidisciplinary teams and personnel are required. Hence, **experience and confidence in interdisciplinary work** are requirements.

However, experts commented on **recurring disbelief in other organisations' trainings** on data practices and security, which can cause a lack of trust and an unwillingness to collaborate and exchange data.

All personnel involved in FCT research should be trained on data security best practices and made aware of their roles and responsibilities in maintaining data security. [...] FCT research requires personnel with specific skills, including expertise in data science, machine learning, statistical analysis, cybersecurity, and domain-specific [skills].

Moving Forward

Supporting the development and maintenance of FCT-specific RDEs requires concrete solutions that address all eight core challenges in a concerted, coordinated effort.

Experts and documentation offered various suggestions on how this might be done. These recommendations will certainly need further elaboration and research, including additional engagements with experts and assessments for more concrete and advanced recommendations. However, these initial recommendations lay a useful foundation to guide upcoming efforts.



01 Recommendations for FCT-Specific Data Standardisation

Creation of common standards and protocols.

The development of common standards and protocols will facilitate data sharing by enabling interoperability and reducing technical barriers.

Implementation of pan-European FCT data standards.

The majority of experts mention common standards' creation and implementation as essential enablers. A key requirement for the implementation of pan-European FCT data standards is taking into consideration the variety of national-level standards, regulations, and legislation in regards to personal data and data processing for research purposes. Such FCT data standards for research, if effective, must further be tailored in compliance with existing regulations on national and EU levels. The ultimate goal should be to develop FCT data standards that will provide common rules and guidelines that encompass all relevant stakeholders in FCT research (from concept to result exploitation) to ensure optimum quality and security.

The creation, introduction, and application of a clear data governance framework.

The development of an FCT-specific data governance framework that addresses issues such as data ownership, privacy, and security is required to support the establishment of clear rules and procedures for data sharing.

FAIRification of FCT data standards.

Efficient FCT data standards must not only clarify data and metadata practices but also ensure standard terminology to reduce barriers to cooperation and collaboration. Infrastructures, procedures, and rules must be created in an aligned way to allow the consistent implementation of FAIR principles so that research data is findable, accessible, interoperable, and reusable, implementing the tenet of "as open as possible, as closed as necessary" to limit any risks related to intellectual property rights, data protection, confidentiality, and security. [17] As per I1 and I2 of the FAIR Principles, the selection or establishment of a widely used machine language for universal representation of (meta)data promises exact identification of the data, both by computer and human agents. The utilised vocabulary needs to provide sufficient machine distinction, which eliminates the chances of false agreements and disagreements. [18]



02 Recommendations for Technological Requirements for FCT-specific RDEs

Central components of the RDE must be interoperable with national systems.

The implementation of standard interoperable central data space components will promote data exchange and international collaboration.

Domain-wide standardisation of data collection, storage, and processing must be implemented.

Standard data practices across the FCT research domain will support more seamless and efficient exchanges and analyses of data.

Tested and accessible standardised tools must be developed and made available on domain-specific platforms.

The development of standardised and user-friendly tools will help decrease the siloed nature of the FCT research domain.

Development of a common European cloud storage infrastructure that is secure and can handle large amounts of data.

Sustainable funding.

Funding streams and organisations need to ensure adequate and sustainable resources for the development, implementation, and maintenance of an FCT RDE. This is needed both for the infrastructure overall and for the organisations that use the RDE.

03 Recommendations for an Interoperable Data Infrastructure

Creation of an interoperable data infrastructure.

The interoperability of data infrastructure is critical to enabling FCT data sharing. This includes standardisation of data formats, metadata, and interoperable data platforms, which will facilitate the seamless integration and exchange of data across the EU.

Learning from or integrating with existing initiatives.

Various initiatives for research data spaces exist, albeit not targeted towards the FCT domain. A prominent example is the non-profit organisation International Data Spaces Association (IDSA), which aims to set a reference architecture model based on open standards and contribute to global standards based on EU values. The IDSA's reference architecture defines the terms and conditions for data economy and promotes maximal adoption due to the open-source nature of the model. [19] Such existing initiatives are helpful to understand possible infrastructures that can be refined and adapted to FCT-specific RDEs.

04 Recommendations for Legal Documentation and Regulations

Clarity on applicable regulations for FCT research.

FCT data sharing must be carried out in compliance with data privacy and security regulations. This includes developing robust data protection and security measures, such as data anonymization and encryption, to protect sensitive data from unauthorised access or misuse. Clarifying the FCT-specific aspects of policy and regulatory frameworks that support data sharing and collaboration while also protecting data privacy and security will be of paramount importance.

Development of standardised FCT-specific data regulations.

FCT research is sophisticated and requires specific security measures. Thus, high-quality legal documents and regulations are required to support national and international research and innovation activities.

Multi-organisational collaboration.

The development of legal and regulatory documentation must take into account not only the existing national legislation but also inter-organisational regulations and legislation. Thus, relevant organisations must be open to collaboration and take part in the development of domain-specific international documentation.

Appointment of an FCT Research International Regulating Body.

An international regulatory entity could help ensure that accredited organisations adhere to the relevant legal, regulatory, and ethical requirements for high-quality research and the exploitation of research results.

Existing regulations and legal documentation should be compiled into a list that is regularly updated to ensure that those working with sensitive data are still working within the regulations as the rules change.

Sustainable funding.

The development, implementation, and compliance with new legislation and regulations require stable and sustainable funding for organisations (e.g., to hire or train skilled staff in the relevant areas). This requires a long-term funding strategy that reaches beyond project timelines.



05 Recommendations for Strengthening Cross-Stakeholder Trust and Transparency

Ensuring transparency between data-handling stakeholders (e.g., researchers, LEAs) and data-providing stakeholders (e.g., LEAs, citizens) helps establish and maintain trust.

Experts proposed the implementation of guidelines and policies that regulate the accessibility and ethical sharing of research data, with specific reference to sector-specific requirements in the FCT domain. Another mechanism proposed were data sharing agreements to further develop transparency and trust between data-handling stakeholders.

Creating a culture of collaboration to facilitate collaborative partnerships between different stakeholders that support the sharing of expertise and resources and assist in the creation of shared goals for data sharing.

Providing citizens with information about when and how their personal data is processed.

Citizens should be provided with information about the operations performed with their data, for instance, by utilising data trackers [20]. Alternatively, some experts preferred to keep data accessible only within the research team but provide publicly available reports and/or data analyses to demonstrate how data is used. This approach is currently employed by the Bulgarian MOD, where individuals are notified that their data will be handled prior to conducting operations. [15] By notifying citizens when and how their data is being used, it is hoped that greater trust and higher levels of collaboration can be achieved.

Improving the ability of citizens to become data providers by adopting systems in which citizens can report criminal or other data directly This could support crime detection and prevention and expand datasets for relevant areas of FCT research.

Engagement with citizens to increase public understanding of FCT research.

Public trust is paramount in the development of an FCT RDE. Estonian experts referred to the Estonian Academy of Security Sciences' Big Data: Nature and Bottlenecks of Use approach, which aims to ensure the safe and ethical handling of data while increasing public understanding, trust, and participation by providing evidence about the benefits of FCT-related research. [21]



06 Recommendations for Appropriate Data Control

Creation of FCT data governance frameworks.

The development of data governance frameworks that address issues such as data ownership, privacy, and security can help establish clear rules and procedures for data sharing.

Implementation of well-defined FCT-specific legal and policy frameworks to regulate data control.

The ethical and secure handling and sharing of data can be achieved by providing well-defined FCT-specific legal and policy frameworks. Multiple experts shared the need for the development of FCT-specific data privacy and protection policies, ethical standards, and guidelines for data anonymisation, sharing, access, and management. A key foundation for adequate data control was seen in the wide dissemination and accessibility of such documentation to all stakeholders in the FCT research domain. The availability of well-defined policy frameworks for data control also serves to strengthen trust amongst FCT stakeholders as well as citizens.



07 Recommendations for Data Quality Assurance

The development of reliable and FCT-specific assessment and verification tools can support effective data quality through all stages of the data management process.

Clarification of the rights and responsibilities of all actors and organisations within the context of FCT research and FCT-specific data ecosystems is needed to ensure resilient data quality processes and, thus, increased data quality.

Give credit and recognition to the entities investing in structured data collection and maintenance.



08 Recommendations for Intra-Organisational Issues

Definition and utilisation of a standardised language.

The findability and, thus, applicability of FCT data can be increased by implementing a standardised and common language. Experts suggested standardisation or at least clarification of vocabularies and terminologies, which will benefit collaborations with other institutions and countries. Furthermore, developing and utilising a more standardised vocabulary can directly support the findability pillar of the FAIR principles.

Availability of sufficient equipment, tools, and services.

FCT research can be costly and require niche and expensive resources, which organisations need to provide in the form of adequate equipment, tools, and access to required services. Researchers and purchase departments in organisations should work more closely together to better understand and forecast ongoing needs.

Established agreed skill and knowledge levels to ensure that individuals working in the FCT research domain are trained to and can be tested against appropriate and agreed standards.

Availability of adequate training along with agreed skill criteria to maintain adequate sectoral knowledge.

Organisations should ensure consistent training in data science, data management, machine learning, statistical analysis, cybersecurity, and FCT-specific research skills (amongst others) to ensure skills follow technical, regulatory, and sector-specific developments in the FCT domain.

Summative Remarks

The issues supporting the successful development and sustainability of a European FCT RDE are complex and interlinked.

Given the intricacies of FCT research and research ecosystems, we are cognisant that this paper can only be the beginning of broader engagements and that further investigations are needed to guide the design of FCT-specific RDEs.

Our intention with this report is to offer a condensed view of the core challenges that need to be addressed to support effective research and innovation within the FCT domain, as seen by the people working in the field. It further offers suggestions, outlined by experts themselves, as pointers for how to address the frequent challenges they encounter.

These observations offer an important starting point for further investigations into the practical and regulatory steps that will help FCT-specific RDEs become successful.



Bibliography

1. [European Commission. \(n.d.\). Innovation and security research. European Commission.](#) Retrieved August 23, 2023.
2. [European Commission. \(n.d.\). CERIS - Community for European Research and Innovation for Security. European Commission.](#) Retrieved August 23, 2023.
3. Directorate-General for Research and Innovation, & European Commission. (2022). [Making EU countries more secure - EU research and innovation tackles challenges to civil security.](#) Publications Office of the European Union.
4. European Commission. (n.d.). [A European Strategy for Data.](#) European Commission. Retrieved August 23, 2023.
5. European Commission, & Joint Research Centre. (2023). [European data spaces.](#) In European Commission.
6. European Commission. (2020). [Number of data suppliers in the United States from 2016 to 2020.](#) statista.com.
7. European Commission. (2020). [Number of data suppliers in the European Union \(EU\) and United Kingdom \(UK\) from 2016 to 2020 and in 2025.](#) statista.com.
8. Bitkom. (2023, January). [Global market share of the information and communication technology \(ICT\) market from 2013 to 2023, by selected country.\[Graph\].](#) statista.com.
9. EU General Data Protection Regulation (GDPR) , (2016).
10. Hansen, M. (2016). Data Protection by Design and by Default à la European General Data Protection Regulation. In Privacy and Identity Management. Facing up to Next Steps (pp. 27-38).
11. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data Article. (n.d.).
12. Greengard, S. (2018). Weighing the impact of GDPR. In Communications of the ACM: Vol. 61(11) (Issues 16-18).
13. [Enforcement action.](#) (n.d.). Retrieved September 15, 2023.
14. [GDPR Enforcement Tracker.](#) (n.d.). Retrieved September 15, 2023.
15. Karakachanov, K. (2018). Политика за защита на личните данни в Министерство на Отбраната, структурите на пряко подчинение на Министъра на Отбраната и Българската Армия (Policy of Personal Data Protection of the Ministry of Defence and the Bulgarian Army). In Ministry of Defence, Republic of Bulgaria.
16. Montagón, R., & Sungmin, C. (2023, 1 March). [UK withdraws plans for broader Text and Data Mining \(TDM\) copyright and database right exception.](#) Herbert Smith Freehills.
17. European Parliament. (2023). [Open data and the reuse of public-sector information.](#) EUR-Lex.
18. GO FAIR. (n.d.). [FAIR Principles.](#) GO FAIR. Retrieved March 7, 2023.
19. International Data Spaces Association. (2020). [Implementing the European Strategy on Data Role of the International Data Spaces \(IDS\).](#)
20. [Data tracker - tool that builds trust in institutions.](#)(2019). e-estonia.com.
21. Puusalu, J. (2020). [SUURANDMED: OLEMUS JA KASUTAMISE KITSASKOHAD.](#)

Acknowledgements

This report is a summary of research conducted in the context of the LAGO project and reported in deliverable D3.1, 'Consensus Report on the FCT Research Landscape and Barriers to Data Sharing'.

The LAGO project, Lessen Data Access and Governance Obstacles, aims to 'address the data issue in the FCT research landscape by building an evidence-based and validated multi-actor reference architecture for a trusted EU FCT Research Data Ecosystem (RDE). The project aims to lay the foundations for a trusted European FCT RDE.

The LAGO consortium is made up of 24 partners across 14 countries. LAGO is funded by the European Union under the grant agreement number 101073951.



LAGO: Lessen Data Access and Governance Obstacles. Funded by the European Union. Grant agreement number 101073951. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

CENTRIC: Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research



centric@shu.ac.uk



research.shu.ac.uk/centric/
