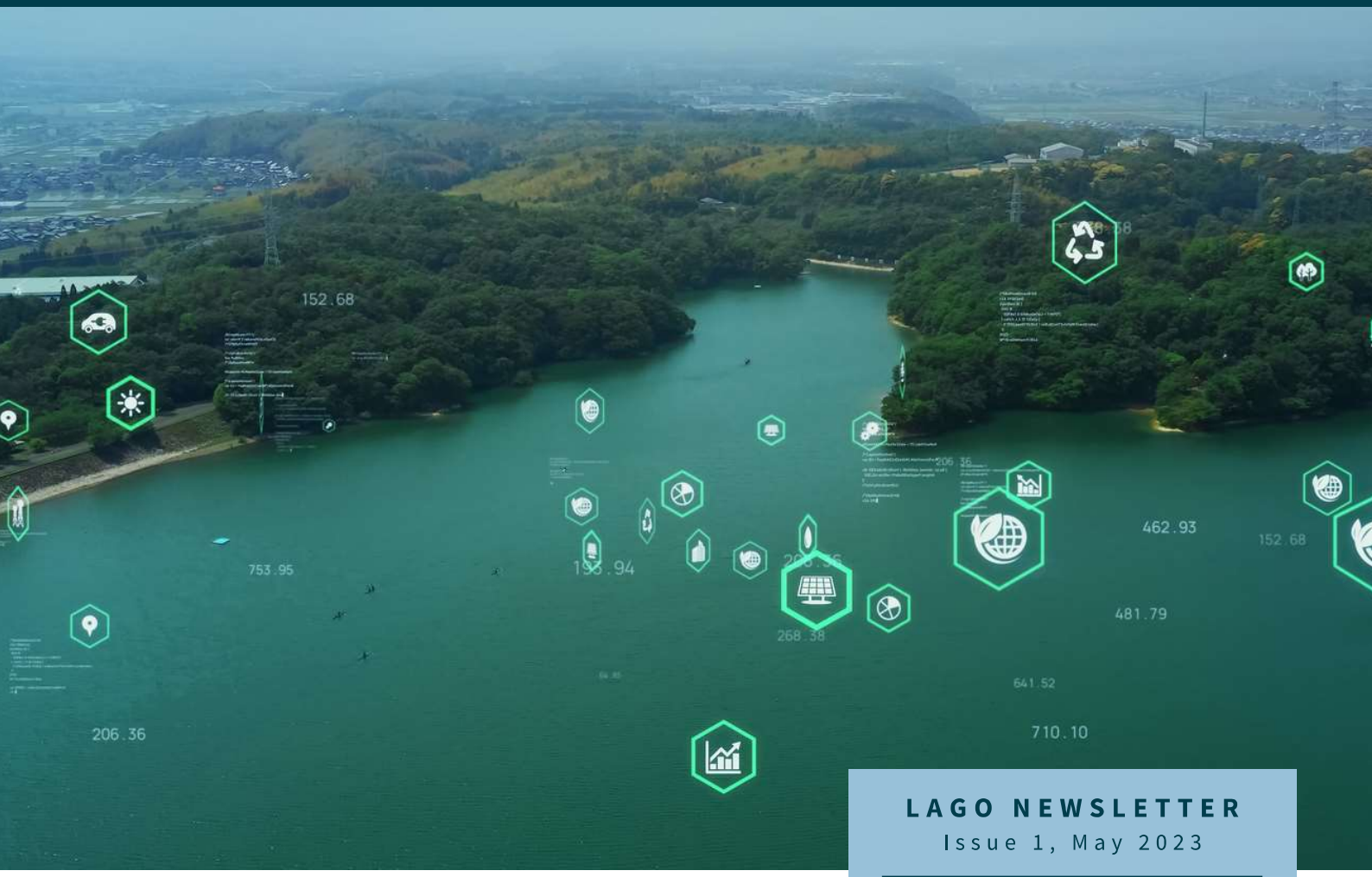
Lessen Data Access and Governance Obstacles

www.lago-europe.eu



LAGO NEWSLETTER
Issue 1, May 2023

TABLE OF CONTENTS

ABOUT LAGO

LAGO, Lessen Data Access and Governance Obstacles, is a European Union-funded security-focused initiative with 25 partners from 14 European countries, including seven law enforcement agencies (LEAs).

LAGO will build an evidence-based and validated multi-actor reference architecture for a trustworthy EU FCT (fight against crime and terrorism) Research Data Ecosystem (RDE) to solve the FCT data issue. FCT-related data can be co-created, shared, and secured in the RDE.

For more information, visit **https://lago-europe.eu/**.

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.

THE PROJECT COORDINATOR'S MESSAGE

ERNESTO LA MATTINA, ENG

Welcome to the first edition of the LAGO newsletter! We are thrilled to see the progress we have made so far, and we are confident that with your help, we will achieve our goals.
This edition will discuss the LAGO project's aims and work package developments, provide updates on past and future events, offer a perspective on the data anonymisation subject, and introduce our consortium partners.
As we move forward with our project, we thank you all for your continued support and input into LAGO. We encourage you to keep providing us with your valuable insights and feedback to ensure the success of this project.

The LAGO project brings together researchers, industries, LEAs, and security practitioners to address pertinent security threats and improve societal resilience. It proposes a reference model and a deployable architecture for a trusted EU Research Data Ecosystem for FCT that complies with European values and principles on data protection, privacy, and ethics. The reference architecture and governance framework will be based on design principles such as decentralisation, data quality, openness, transparency, and trust. Therefore, the results of LAGO will be instrumental in identifying and removing barriers and providing the structural, governance, and technical foundations for the implementation roadmap.

A ROADMAP WILL PROVIDE THE CONSOLIDATED RULES, CONDITIONS AND CONSIDERATIONS FOR THE ACTUAL DEPLOYMENT OF THE EU FCT RDE.

To find out more, please get in touch by email, follow us on social media, or visit the project's website.

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.

WORK PACKAGE (WP) UPDATES

The LAGO consortium is made up of experts with knowledge of data creation, management and governance in security from around the world. This includes European law enforcement agencies with real-world experience, small and medium-sized enterprises (SMEs), and academic partners.

The consortium will carry out extensive research and analysis as well as engage in practical activities such as training sessions and workshops. The involvement of SMEs and academic partners is particularly crucial, as they can bring fresh perspectives and cutting-edge technologies to the table.
In addition, the participation of law enforcement agencies will ensure that the solutions developed are practical and effective in real-world scenarios.

WP2 ETHICAL, SOCIETAL AND LEGAL SCREENING, GUIDANCE AND REVIEW

LAGO recognises the importance of ethics and legal compliance in the sharing of data, and the first two tasks in WP2 are dedicated to assessing the legal and ethical framework for FCT sharing of data. The consortium has recently highlighted the progress of the research during the general assembly and through two blog articles.
The legal expert survey on data sharing law is currently ongoing and will inform national legal framework research by June.
The third task is focusing on fundamental research related to review mechanisms and a self-assessment tool to ensure compliance.

WP3 FRAMEWORK EU FCT TRUSTED RESEARCH DATA ECOSYSTEM (RDE)

WP3 lays the basis for the establishment of an EU-level RDE. During the first six months of the project, the current FCT research landscape and related barriers to the adoption of a research data ecosystem were examined through desk research, a literary review, and many interviews with security experts and stakeholders. This led to the Consensus Report on the FCT Research Landscape and Barriers to Data Sharing, currently in process to be published as a White Paper. Activities are now focusing on the definition of use cases, requirements, and high-level processes that will be part of the Reference Architecture, leveraging best practices, experiences, and lessons learned from initiatives like IDSA and GAIA-X.
A template for the collection of use cases has been prepared with the contribution of all partners. An interactive session among partners was organised during the 2nd LAGO Plenary Meeting in March.
Feedback, ideas, and suggestions have been collected and are now under analysis in strict collaboration with WP and task leaders.
An updated and improved version of these processes will be released before the 3rd Plenary Meeting in June.

WP4 RESEARCH DATA CREATION AND PROVISION

WP4 aims to improve the creation, collection, annotation, and provision of research datasets. All tasks have commenced, and initial steps have been completed successfully.
Progress to date includes investigating novel methods and tools, developing automated annotation capabilities, releasing representative dataset generation tools, enabling privacy preservation, and creating secure techniques for dataset publishing.
The LAGO team will refine and optimize these developments to enhance FCT research capabilities.

WP5 RESEARCH DATA USAGE

WP5 develops techniques and tools for accessing research data within the EU FCT RDE.
During the initial stages of the project, the focus was on the development of methods for verifying the quality and compliance of

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.

research data, as well as establishing the required quality indicators.
Additional activities include the definition of a risk assessment methodology for sharing and accessing research data from multiple perspectives (legal, ethical, privacy, societal, etc.).
The methodology will enable a fine-grained and dynamic risk assessment of a given dataset and a comprehensive evaluation of potential risks.

WP6 RESEARCH DATASET GOVERNANCE

WP6 is focused on setting up a governance model for the FCT RDE to ensure smooth, secure, trusted data sharing, co-production, and exchange among members, taking into consideration that organisations in the RDE will be able to share data only if they are able to: select the data that fits their purpose; select a reliable provider; verify if the organisation that will receive the data is reliable; define and enforce data usage policies; and be able to run their tools over the data that they will receive.
In the short term, the aim is to define the trust policies that will ensure confidence in the identity and capability (in terms of data and services) of participants and foresee mechanisms to protect the integrity and security of data.
These policies should comply with the principles of decentralisation and data sovereignty, where datasets are created and made available in a federated environment and providers keep ownership and control over the data.
The first task the WP6 team undertook was to identify the initial use cases that the WP6 solution and its workflows must address.
A subsequent activity was to assign each of these steps to at least one of the tasks in the WP.
The aforementioned outcomes were the input for a high-level architecture and for the definition of the first set of requirements to be taken into consideration in the first development cycle that is currently being planned.

WP7 VALIDATION AND DEMONSTRATION IN REAL SCENARIOS

WP7 aims at demonstrating the capabilities and potentialities of LAGO concepts, architecture, and solutions in realistic contexts. Activities are currently focused on pilot scenario definition in strict collaboration with use case development in WP3 and will accelerate during the next few months, together with the planning and preparation of the validation and demonstration activities.

WP8 BOOSTING THE CREATION OF EU DATA ECOSYSTEM FOR FCT RESEARCH

WP8 is making significant progress in establishing the necessary visibility and communication for the LAGO project.
The consortium is actively engaging with the community through events and social media channels, and the communication and dissemination plan is being executed effectively. These efforts will help to raise awareness of the project and ensure its success.

WP9 ETHICS REQUIREMENTS

The purpose of WP9 is to ensure compliance with ethical requirements. Three areas to demonstrate compliance and good practice were identified: activities involving work with human beings, processing of personal data, and the development, deployment, and/or use of artificial intelligence (AI)-based systems or techniques. Each of these ethical concerns corresponds to an ethical requirement that the project is addressing.
So far, the first two deliverables have been submitted: a) research policy principles to present in detail the involvement of individuals in the LAGO project activities assuring human rights and personal data protection; b) support of the partners to identify the potential risks related to the data processing activities and to facilitate compliance with the GDPR and the data ethics requirements aimed at safeguarding the fundamental human rights and freedoms of the data subjects.

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.

PAST EVENTS

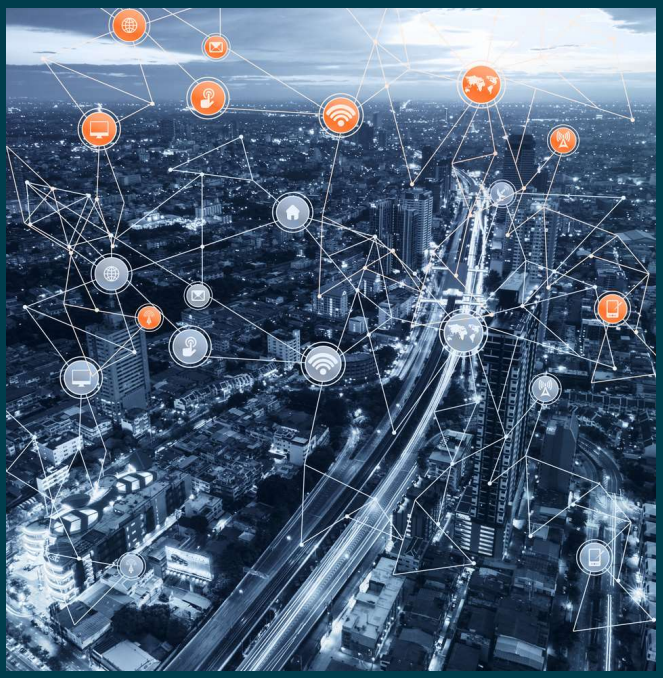
LAGO KICK-OFF MEETING, ROME

On December 7, 2022, the project coordinator, Engineering – Ingegneria Informatica SPA (ENG), convened a kick-off meeting in Rome, to establish the collaboration protocols among the LAGO consortium's 25 members, as well as the project's dates, projected results, and other implementation-related organisational considerations.

LAGO'S 2ND PLENARY MEETING, SAN SEBASTIÁN

Organised by partner VICOMTECH from March 14th to March 15th, 2023.

Two fruitful days which successfully blended project status updates, engaging workshops aimed at boosting technical activity implementation, and a boot camp on the requirements and Reference Architecture of the EU data space for FCT research.



FUTURE EVENTS

3RD PLENARY MEETING

The third plenary meeting will take place in June 2023.
The meeting will provide an opportunity for the project team to discuss any new developments or changes in the project timeline and milestones. Furthermore, it will be a chance for stakeholders to share their feedback and suggestions on the progress of the project so far.

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.

WALKING THE FINE LINE BETWEEN PERSONAL AND ANONYMOUS DATA

BY DR LAURA DRECHSLER
KU LEUVEN CENTRE FOR IT & IP LAW

One core question for anyone handling data within the European Union is whether such data are to be considered personal or non-personal data. This classification matters from a legal perspective, as data that is classified as personal falls within the regime of EU data protection law, such as the General Data Protection Regulation (GDPR), whereas different and often less stringent rules apply for non-personal data.

PERSONAL DATA IS UNDERSTOOD BROADLY IN EU DATA PROTECTION LAW. THE GDPR DEFINES PERSONAL DATA AS 'ANY INFORMATION RELATING TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON' (SEE ARTICLE 4(1)).

Following the guidance of the EU data protection regulator (see for the details of the guidance here), this translates into four partly intertwined building blocks that make data personal, namely (1) the presence of any form of information, objective and subjective, (2) that based on its content, purpose, or result links to ('relates to') (3) an identified or identifiable (4) natural person, whereby identifiability is dependent on the likelihood of the means to do so being available to the entity processing the personal data (called the 'controller' in the GDPR).

The Court of Justice of the European Union (CJEU), the highest court for all questions relating to EU law, has supported a broad understanding of personal data in order to ensure the effective protection of individuals.

For example, the CJEU considered it possible that Google search results on one's own name (Case C-131/12, Google Spain, paragraph 27), corrections on an exam (Case C-434/16, Nowak, paragraph 44), and dynamic IP addresses (Case C-582/14, Breyer, paragraph 49) could be classified as personal data.

The situation is different for non-personal or anonymous data, which are not in the scope of EU data protection law precisely because they do not allow for the identification or identifiability of natural persons.

Anonymous data are not defined in EU data protection, although some legislation regulating data more generally offer a definition of non-personal data. The newly adopted Data Governance Act (DGA), for example, defines non-personal data as any data that is not personal (Article 2(4) DGA). Anonymous data is therefore understood as the opposite of personal data.

The combination of a broad understanding of personal data and the absence of a clear definition of anonymous data has let to difficulties for anyone trying to assess whether data is personal.

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.

These difficulties are heightened by the fact that EU data protection law also introduces the concept of 'pseudonymisation', which describes a process for personal data with which the identifier that links the data to a natural person is removed in order to ensure better protection for individuals (see, for example, Article 4(5) GDPR).
Examples noted by the EU regulator for such processes include encryption processes (see here for further details). The definition already determines that data undergoing this process ('pseudonymous data') are personal data and thereby within the scope of EU data protection law. The wide understanding of personal data, which thus includes pseudonymous data such as encrypted data, has led some data protection scholars to conclude that data protection law will be the 'law of everything' (see, for example, Purtova 2018).
While this is indeed a potential risk as a consequence of the ever-increasing collection of personal data by big tech companies, it does not follow from the legal definitions as such (see also Dalla Corte 2019).
This is because the classification of data as personal depends on the controller undertaking the processing and the means he or she has available to re-identify a natural person.

AT THE END OF THE DAY, DATA ARE ONLY PERSONAL IF THEY CAN SOMEHOW LEAD TO THE IDENTIFICATION OF A NATURAL PERSON.

This has been highlighted in a recent judgement of the General Court of the EU (the first instance court for EU matters) at the end of April 2023.
In the case (Case T-557/20), the General Court was asked, among others, to clarify whether pseudonymous data can be anonymous data for a recipient if there is no possibility to gain the key for re-identification.
The Court suggested that this could be the case and reprimanded the investigating data protection authority for having failed to verify in its investigation how likely such access to the key would be.

The decision therefore appears to open the door for a relative understanding of anonymisation under the GDPR in the context of data sharing. In other words, in a data sharing context, data might be able to change from personal to anonymous if the sharing controller manages to effectively exclude any likelihood of reidentification from the perspective of the recipient.
Since the decision of the General Court can still be appealed in front of the CJEU, such an interpretation is, for now, not quite confirmed.

IN THE ABSENCE OF FURTHER CLARIFICATIONS BY THE EU COURTS, THE LINE BETWEEN PERSONAL AND ANONYMOUS DATA REMAINS DIFFICULT TO WALK.

Given the broad understanding of personal data in EU data protection law, more data are personal than the layperson would probably assume. Anyone dealing with data is therefore well advised to go over the four building blocks of personal data for each datasets in order to understand any potential application of EU data protection law. Finally, it is also worth remembering that EU data protection law is not a prohibitive regime.
If the data are personal, this does not automatically mean they cannot be used, for example in the context of a research project. Rather, the classification translates into a requirement for additional care for legal compliance on the side of the controller using personal data in order to ensure the protection of individuals behind the data.

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.

KEY FACTS

Coordinator: Engineering Ingegneria Informatica S.p.A. (Italy)
Start Date: November 2022
Duration: 24 months
Consortium: 25 partners from 14 countries, including 7 LEAs
Topic: HORIZON-CL3-2021-FCT-01-04, Improved access to fighting crime and terrorism research data
Type: HORIZON Innovation Actions
Total cost: €7.38m

CONSORTIUM

FOLLOW US

lago-europe.eu
info@lago-europe.eu
@lago-europe
@lago_europe

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.