Horizon HLTH 2022 Project MISTRAL
"A toolkit for dynaMic health Impact analysiS to predicT disability-Related costs in the Aging population based on three case studies of steeL-industry exposed areas in Europe".

Research and Innovation Action
Topic: HORIZON-HLTH-2022-ENVHLTH-04-01
GA n. 101095119

Duration: 48 months from 01/01/2023
Coordinator: ISTITUTO SUPERIORE DI SANITÀ

Deliverable ID.:	**D2.3**	
Deliverable title:	**Data Protection Impact Assessment**	
Planned delivery date:	31/12/2023	
Actual delivery date:	31/12/2023 (M12)	
Deliverable leader:	PLANET (Giuseppe Campanile, Ilaria Bortone)	
Contributing partners:	ASL TA (Rodolfo Sardone)	
Dissemination Level:	X	PU = Public;
		CO = Confidential
		Cl = Classified

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101095119.

Document information and history

Deliverable description (from DoA)
Development of a report of data protection impact assessment

Please refer to the Project Quality Handbook for guidance on the review process and the release numbering scheme to be used in the project.

Version N.	Date	Author [Person and Organisation]	Reviewer [Person and Organisation]	Milestone*	Notes
01	**29/10/2023**	**Giuseppe Campanile (PLANET)**	**Ilaria Bortone (PLANET)**	**Intermediate**	
02	**29/12/2023**	**Giuseppe Campanile (PLANET)**	**Ilaria Bortone (PLANET)**	**Proposed**	
03	**30/12/2023**	**Giuseppe Campanile (PLANET)**	**Rodolfo Sardone (ASL TA), Ilaria Bortone (PLANET)**	**Revised**	

** The project uses a multi-stage internal review and release process, with defined milestones. Milestone names include abbreviations/terms as follows:*

- *TOC = "Table of Contents" (describes planned contents of different sections);*
- *Intermediate: Document is approximately 50% complete – review checkpoint;*
- *ER = "External Release" (i.e. to commission and reviewers);*
- *Proposed: document authors submit for internal review;*
- *Revised: document authors produce new version in response to internal reviewer comments approved: Internal project reviewers accept the document.*

Table of Contents

Table of Figures

List of Tables

1 Executive Summary

Regulation 2016/6791 (GDPR) will apply from 25 May 2018. Article 35 of the GDPR introduces the concept of a Data Protection Impact Assessment (DPIA), as does Directive 2016/680.

A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with the requirements of the GDPR but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation (see also article 24). In other words, a DPIA is a process for building and demonstrating compliance.

In line with the risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. A DPIA is only required when the processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1)).

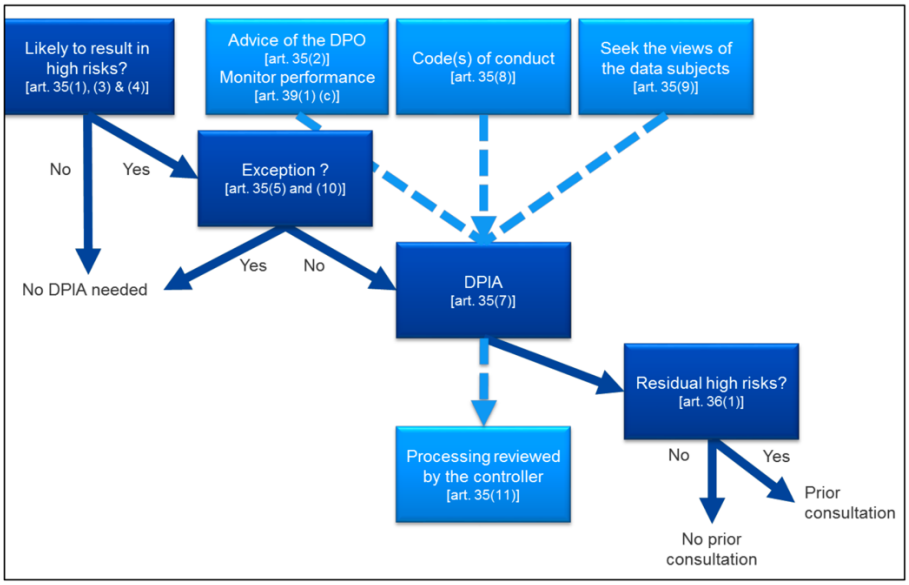

Figure 1. Illustration of the basic principles related to the DPIA in the GDPR

PLANET evaluated the necessity of a DPIA to comply with the requirement of 'data protection by design' since MISTRAL met at least two of the nine criteria reported in the *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*.

The present document represents the first assessment carried out by PLANET on MISTRAL started as early as is practicable in the design of the processing operation even if some of the processing operations are still unknown, thus being carried out "prior to the processing" (Articles 35(1) and 35(10), recitals 90 and 93)23. This is consistent with data protection by design and by default principles (Article 25 and recital 78).

As a matter of good practice, a DPIA should be continuously reviewed and regularly re-assessed. Therefore, PLANET will update the DPIA throughout the lifecycle project to ensure that data protection and privacy.

1.1 Role of deliverable

The DPIA should be seen as a tool for helping decision-making concerning the processing. PLANET carried out a first assessment of the MISTRAL Project with the existing limitations:

- Ethical Approvals of ZEPHYR studies are still ongoing (Italian Local Ethical Committee has already approved the study; Poland has submitted the study to their Bioethical Committee; Belgium will do it next month);
- The concept design and the definition of the requirements of the MISTRAL web app have started at M12 due to delays in subcontracting;
- The design of the virtual architecture is still ongoing.

1.2 Relationship to other deliverables

The present deliverable is linked to the Data Management Plan (DMP) we have already submitted. The present document will be updated at M24, along with the update of the DMP. Updating the DPIA throughout the lifecycle project will ensure that data protection and privacy are considered and will encourage the creation of solutions which promote compliance. It can also be necessary to repeat individual steps of the assessment as the development process progresses because the selection of certain technical or organizational measures may affect the severity or likelihood of the risks posed by the processing.

1.3 Structure of the document

The GDPR does not specify which DPIA process must be followed but instead allows for data controllers to introduce a framework which complements their existing working practices provided it takes account of the components described in Article 35(7). The GDPR sets out the minimum features of a DPIA (Article 35(7), and recitals 84 and 90):

- “a description of the envisaged processing operations and the purposes of the processing”;
- “an assessment of the necessity and proportionality of the processing”;
- “an assessment of the risks to the rights and freedoms of data subjects”;
- “the measures envisaged to:
    - “address the risks”;
    - “demonstrate compliance with this Regulation”.

The document stems from the FR Framework (FR: Privacy Impact Assessment (PIA), Commission nationale de l’informatique et des libertés (CNIL)) by using the PIA software (https://www.cnil.fr/en/privacy-impact-assessment-pia) aimed to help data controllers build and demonstrate compliance with the GDPR.

2 Data Protection Impact Assessment (DPIA)

2.1 Context

This section gives a clear view of the treatment(s) of personal data in question.

2.1.1 OVERVIEW

This part allows us to identify and present the object of the study.

What is the processing under consideration?

The process under consideration is the Project MISTRAL “” (GA 101095119).

The MISTRAL project aims to develop a technological toolkit for dynamic, intelligent HIA toolkit to predict the health impact of health-related features, forecasting the trajectories of disability and quality of life reduction. This method will use environmental, socio-economic, geographical, and clinical characteristics, managed, and elaborated with a federated learning architecture. The generated models will be adjusted for lifestyle and individual conditions data sourced from large population-based digital surveys. The models will be trained and validated on three different exposures to the steel plants' pollution: Taranto in southern Italy, Rybnik in Poland, and Hasselt in Belgium.

In detail, the technological platform will operate geographical, and mathematical health impact assessment based on solid exposure-response functions (ERF) using metanalytic and local data. The local exposure-response data will be collected through two observational studies foreseen within MISTRAL:

1. ZEPHYR: a cross-sectional multi-centre observational study that aims to derive precise exposure-response functions considering black carbon concentration in urine as exposure and quality of life as the outcome, in different subpopulations distinguished by age group and residence (Primary Data Collection).
2. TRAMONTANA: a multi-centre retrospective observational study to define the ERF of health, environmental, economic, and social determinants and QALY and DALY measures through deterministic and stochastic models from 30,000 citizens distributed in the three European countries (Secondary Data Collection).

Thus, the processing of the data in question, which concerns individuals, in individual and aggregate form, constitutes the "processing of special categories of personal data," according to Article 9(j) of the GDPR, for scientific research purposes, with the legal basis being Regulation (EU) 2021/695 of the European Parliament and the Council.

What are the responsibilities linked to the processing?

The data controller should be identified according to the study under consideration. In fact, for ZEPHYR, each health data collection centre about the study is a data controller in itself:

- for Italy: National Institute of Health (ISS) and the affiliated entity Local Healthcare Authority of Taranto (ASL TA), in the person of their respective legal representatives;
- for the University of Hasselt, Prof. Tim Nawrot;
- for the AGH - the University of Krakòw, Prof. Agnieszka Gruszecka-Kosowska, as controller, and the Independent Public Health Care Provincial Specialist Hospital No. 3 in Rybnik (WSS3), in the person

of the Local Study Coordinator: Katarzyna Musioł, PhD, MD Head of the Pediatrics Department, as processor.

Also concerning the TRAMONTANA study, the data controller appears to be the legal representative of the entity accessing the national social and health database. As set out in the project, each partner institution involved in the Tramontana study, i.e. (as in the ZEPHYR) ASL TA for Italy, University of Hasselt for Belgium and AGH - the University of Kraków for Poland, will appoint a data controller within the institution, with the qualification of health professional (as required by the GDPR), expressly authorised to download from the respective databases (Local Electronic Health Record of Taranto, MyHealth for Belgium and P1 for Poland) the data from time to time necessary for the data analyses of the study. In this regard, the University of Krakow had specific contractual safeguards in place to ensure a level of data processing by the data controller (Independent Public Health Care Provincial Specialist Hospital No. 3 in Rybnik (WSS3), in the person of the Local Study Coordinator: Katarzyna Musioł, PhD, MD Head of the Paediatrics Department). Within this framework, PLANET will carry out a special assessment in Poland in April 2024.

Are there standards applicable to the processing?

From the point of view of data processing rules and standards, the whole project and its implementation were designed and imagined from the beginning according to principles of privacy by design and by default, under the GDPR, as well as the Guidelines on Data Protection Impact Assessment adopted by the "Article 29 data protection working party."

Based on this, each data processing partner is in any case obliged to structure a data processing flow that is compliant with the GDPR rules, concerning the register of data processing, appointments of data processors, and the assessment of the respective DPOs in charge of the measures put in place. From this point of view, Planet will carry out at least an annual assessment of each data processing partner, starting with the TRAMONTANA and ZEPHYR studies.

2.1.2 DATA, PROCESSES AND SUPPORTING ASSETS

This part allows us to define and describe the scope of the processing in detail.

What are the data processed?

Data collected for ZEPHYR:

a) type of data: personal, socio-health and health data, concerning urine samples collected from patients and delivered at the healthcare operators employed by ASL TA, AGH University of Krakow, University of Hasselt, involved in the study, formally indicated by the data controller as responsible.
b) storage time: from collection until the conclusion of the MISTRAL-related activities and not more than 25 years after the end of MISTRAL.
c) recipients: the healthcare operators who physically collect the data during the observational study.

Data extracted from the health records of each country of the 3 partners involved in the TRAMONTANA;

a) type of data: personal, socio-health and health data;
b) storage time: from collection until the conclusion of the MISTRAL project activities;

c) recipients: the study coordinators appointed by the data controller (Prof. Rodolfo Sardone for ASL TA; Prof. Tim Nawrot for Hasselt University; Katarzyna Musioł, PhD, MD Head of the Paediatrics Department, Independent Public Health Care Provincial Specialist Hospital No. 3 in Rybnik (WSS3)).

How does the life cycle of data and processes work?

ZEPHYR Data Flow

In ZEPHYR (primary data collection), data on clinical, social and environmental pressure will be collected by healthcare providers along with biological samples (non-invasive, urine). After collection by the physician, the data will be anonymized with a random number that will become the project code. Special categories (children aged 5 to 15 years) will also be enrolled, and clinical characteristics and urine samples will be collected. The data will be kept for the duration of the after the end of the MISTRAL project. Thereafter, the pseudo anonymized data will be retained and entered an "open" dataset without any direct or indirect relationship with either the data owner or the data controller. All personal data collected will be deleted when the project code (ID) is generated, therefore, it will be impossible to trace the origin of the data. The project will contain a total sample of 4000 subjects recorded as primary data (thus collected because of new recruitment) and 60000 secondary data from electronic health records in the 3 study cities. Primary data will be collected directly from subjects enrolled by physicians and will also include a population of children aged 5-15 years. All subjects will be aware of the processing and sign an informed consent on data protection. Secondary data (data collected from electronic health records, without the involvement of census individuals) will be obtained from local health records in the three study cities. Recruitment subjects will be selected by a physician and immediately anonymized by assigning a random project identification code (ID) using anonymization software. The physician will be "blinded" to the match between personal data and the project code. Data related to the physical address (georeferenced) of the recruited individual will also be present. In the case of secondary data, such data will be processed with software that will generate an ordinal score according to the geographic area of interest (calculated with the address), to avoid the precise location of the same, and "noise" and geographic masking techniques (i.e. 200 m residence aggregate buffering on geographic grid) will be implemented to ensure that the data collected cannot be traced back to individuals. The privacy policy, drafted following the GDPR, will be included in the informed consent signed by subjects enrolled in the survey.

TRAMONTANA Data Flow

The Tramontana study is aimed at collecting data from the 3 research units (Taranto for Italy, Genk/Hasselt for Belgium and Rybnik for Poland), to structure a database that can be used to carry out a retrospective longitudinal observation of the incidence of chronic diseases and relative disabilities with the highest impact on the population. Exposure data, collected as of 1 January 2012 and the most important incident cases after 10 years, will be selected as of 1 January 2022.

Objectives of the Study:

- To assess the frequency and determinants of specific causes of death for four different major chronic diseases (dementia, stroke, chronic heart disease and chronic obstructive pulmonary disease) in the three study populations, using a case-cohort approach.
- Assess longitudinal determinants for the QALYs of the adults and elderly cohort evaluated in the Zephyr cross-sectional survey.

- Assess the QALYs, YYLs, and YYDs on a longitudinal cohort for the different age groups, using the different adverse health outcomes.
- Test and calibrate QALY-Proxy scores on a longitudinal cohort.
- To feed and validate the health impact assessment toolkit using local (from cohort studies) and metanalytic (existing literature) derived exposure-response functions developed by MISTRAL's technology partners.

Treatment Flow

Secondary data will be extracted from the medical records of each participating country (Local Electronic Health Records of Taranto in Italy, MyHealth in Belgium and System Informacji Medycznej (SIM P1) in Poland). The variables of interest will be initially selected in a test sample of 200 subjects observed in the datasets of each country to verify the interoperability and functionality of the system. Once the variables have been verified by the medical researchers involved in the study, the master data frame will be created to extrapolate the complete datasets according to the study design. The entire sampling frame will be 20,000 from each country involved and 50% (10,000) will be sampled using probability sampling by age group (10 years) and biological sex. The allocation proportion of cases to the cohort will be based on the European mortality rate for chronic heart disease (as the most common mortality related to the main disease considered), i.e. 64% mortality as a proportion of cases and 12% cause-specific proportional mortality. Therefore, a number between 1,000 and 1,200 cases will be considered as the target sample for each country. The total target sample for the entire study will be 33,600 subjects.

The data analysed will be:

- Individual secondary clinical data: reported anthropometric data, smoking habits and eating habits (including the amount of food), vaccination coverage, functional limitations, substance dependence, diagnosis and mortality.
- Individual and aggregated secondary socio-health data: Social deprivation indicators, education levels, labour force and employment, health services and resources, poverty.

All first extractions from the data repositories will be carried out in original by specially authorised health personnel delegated by the respective data controllers. The extracted data sets will be pseudo-anonymized with a random number and any other copy of the original personal data frame connected to the random sample will be destroyed. All the data will be processed exclusively in healthcare facilities dedicated to the specific partners of MISTRAL in a federated privacy-by-design approach.

What are the data supporting assets?

Table 1. List of the data supporting assets for the entire life cycle.

Study	Data	Country	Operating System	Server	Software	Network	People	Print media
ZEPHYR	Survey	Italy	Ubuntu	DELL PowerEdge R940	MISTRAL Web-App	VPN	Healthcare personnel (GPs, Pediatricians, Working Group ASL TA, Researchers UNIBA)	Printed questionnaires Informed Consent
ZEPHYR	Survey	Belgium	Windows 11	Google Cloud	MISTRAL Web-App	Belnet	Researchers UHASS	Printed questionnaires Informed Consent
ZEPHYR	Survey	Poland	NA	NA	MISTRAL Web-App	NA	Healthcare personnels (WSS3)	Printed questionnaires Informed Consent
ZEPHYR	Urine Sample	Italy	-	-	-	-	Healthcare personnel (Working Group ASL TA)	Printed results Informed Consent
ZEPHYR	Urine Sample	Belgium	-	-	-	-	Researchers UHASS	Printed results Informed Consent
ZEPHYR	Urine Sample	Poland	-	-	-	-	Healthcare personnel (WSS3)	Printed results Informed Consent
TRAMONTANA	Healthcare Data	Italy	Ubuntu	DELL PowerEdge R940	CALLIOPE Web -App	VPN	Healthcare personnel (Working Group ASL TA)	-
TRAMONTANA	Healthcare Data	Belgium	NA	NA	MyHealth	NA	NA	

Study	Data	Country	Operating System	Server	Software	Network	People	Print media
TRAMONTANA	Healthcare Data	Poland	NA	NA	System Informacji Medycznej (SIM P1)	NA	Healthcare personnel (WSS3)	-
TRAMONTANA	Socio-Economic Data	Italy	Ubuntu	DELL PowerEdge R940	CALLIOPE Web -App	VPN	Healthcare personnel (Working Group ASL TA)	-
TRAMONTANA	Socio-Economic Data	Belgium	NA	Google Cloud	ENVIRONAGE	Belnet	Researchers UHASS	Informed Consent
TRAMONTANA	Socio-Economic Data	Poland	NA	NA	System Informacji Medycznej (SIM P1)	NA	Healthcare personnel (WSS3)	-

NA Not yet Available

2.2 Fundamental principles

This section allows us to build the compliance framework for privacy principles.

2.2.1 PROPORZIONALITY AND NECESSITY

This part allows us to demonstrate that you are implementing the necessary means to enable the persons concerned to exercise their rights.

Are the processing purposes specified, explicit and legitimate?

Data processing for both ZEPHYR and TRAMONTANA is carried out in strict compliance with the principles set out in Articles 5 and 6 of the GDPR.

The purposes of the processing are:

- specific, because they are aimed at the concrete realisation of the MISTRAL project, approved and financed by the European Union, using HORIZON EUROPE Framework, Cluster Health Work Programme 2021-22;
- explicit, since the data collected through the ZEPHYR are subject to the consent given by the recruiting doctors to the recruited subjects, and the TRAMONTANA (like ZEPHYR) will also be subject to specific authorisation by the Ethics Committees of the individual countries of reference of the partners involved in the activities.

What are the legal basis making the processing lawful?

- For ZEPHYR, the legal basis is the specific consent given by the recruited subjects to the doctors and health professionals involved by the partners in the Studio's activities, as well as the clearance of the relevant national ethics committees.
- For TRAMONTANA, the legal basis is under article 9, j, of the GDPR [processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes following Article 89based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject], in conjunction with Regulation (EU) 2021/695 of the European Parliament and of the European Council of 28 April 2021.

Are the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?

The entire project and its implementation are informed by the principles of the GDPR, with reference to the minimisation of processing.

The approach of privacy by design, through federated learning, on which the entire project is built, guarantees minimisation of the risks of possible breaches or misuse of data by third parties, avoiding data copies and multiplications. In addition, the data, as regards both ZEPHYR and TRAMONTANA, will be extracted in the original (the first time) exclusively by healthcare personnel, specially trained on privacy and GDPR issues. Furthermore, after the first access (for TRAMONTANA) or the first collection (for ZEPHYR), the data will be completely anonymised and encrypted, to make the processing as secure as possible, and the origin of the data de-identifiable.

Are the data accurate and kept up to date?

Measures to ensure the quality of the data differ depending on the reference studies.

For ZEPHYR, each recruiting partner will have to ensure alignment between the data held by the recruiting general practitioners and paediatricians and any discrepancies emerging from the questionnaires and analyses administered to the patients involved.

For TRAMONTANA and ZEPHYR, a data quality plan is being implemented, which includes - among others - the following main points:

1. data cleaning:
   a) develop and implement automated algorithms for identifying outliers and inconsistencies;
   b) conduct systematic checks for missing or illogical data values;
   c) document and justify any data cleaning or transformation procedures applied.
2. data analysis:
   a) confirm that statistical analyses adhere to predefined methodologies;
   b) verify that software tools used for analysis are up-to-date and validated;
   c) perform sensitivity analyses to assess the impact of potential outliers or missing data.
3. quality assurance audits:
   a) conduct periodic internal audits of study procedures and data management processes;
   b) engage external auditors to perform independent assessments of data quality;
   c) document findings and implement corrective actions in response to identified issues.

In both cases, the advisory board appointed by the project Steering Committee will have the task of performing a quality check of the data collection and analysis methodologies.

What are the storage duration of the data?

The data retention period is equal to the duration of the project.

2.2.2 CONTROLS TO PROTECT THE PERSONAL RIGHTS OF DATA SUBJECTS

This part allows us to demonstrate that you are implementing the necessary means to enable the persons concerned to exercise their rights.

How are the data subjects informed on the processing? If applicable, how is the consent of data subjects obtained?

In ZEPHYR, data subjects are informed through a data processing notice, under Article 13 of the GDPR.

Furthermore, PLANET, together with the University of Oxford and partners directly involved in the recruitment of patients, is taking steps to organise territorial meetings to raise awareness among the population concerned, also from the point of view of the rights inherent to data processing.

The first of these meetings was held on 22.12.2023 in Taranto at Tamburi neighbourhood (one of the two areas involved in recruitment in Italy), and others will be scheduled in Italy as well as in Poland and Belgium.

With reference, on the other hand, to the Tramontana Study, Article 13, paragraph 5, letters b and c), of Regulation (EU) 2016/679 will apply, but at the same time all partners involved in the study will ensure an

adequate level of information to the communities involved in the analyses, through their respective websites, the MISTRAL project website and the METEOR Cluster website, as well as through the territorial awareness events mentioned above.

How can data subjects exercise their rights of access and to data portability?

Concerning the right to data portability referred to in Art. 20 of the GDPR, in ZEPHYR, as clarified in the specific information notice issued to the data subjects when signing the recruitment consent, it is expressly guaranteed and taken care of by the responsible partner institution (ISS - ASL TA for Italy, AGH – University of Krakow for Poland and University of Hasselt for Belgium), and can be exercised using an email request by the data subject to the data controller.

How can data subjects exercise their rights to rectification and erasure?

All project partners that process personal data are obliged to allow data subjects to exercise their rights under Articles 18 and 21 of the GDPR, where the legal requirements are met, since both provisions are also applicable to processing with a legal basis such as the one in question (scientific research), upon simple request made by email to the data controller.

How can data subjects exercise their rights to restriction and to object?

Without prejudice to the need to analyse concrete cases case by case, the right to be forgotten in the present case may not apply, under Article 17(3)(d) of the GDPR.

Are the obligations of the processors clearly identified and governed by a contract?

The data controllers in question are all researchers incardinated in public institutions/universities, so they are obliged ex se to process the data in a manner that complies with the GDPR and sector regulations. Moreover, they are bound to the same rules by MISTRAL's GRANT AGREEMENT and the Project's CONSORTIUM AGREEMENT, which contain precise obligations concerning the protection of personal data and compliance processing with the GDPR.

In the case of data transfer outside the European Union, are the data adequately protected?

Data will not be processed or stored outside the EU, as the only non-EU project partner, Oxford University, is not involved in the data analysis. However, as is well known, England ensures a level of processing that is not inferior to the GDPR, by the EU adequacy decision, approved on 28 June 2021 the EU adopted two adequacy decisions for the UK, one under the General Data Protection Regulation (EU GDPR) and the other under the Law Enforcement Directive (LED). This adequacy decision allows the continued free flow of personal data between the EU and the UK for four years, at which point the European Commission will review the adequacy decision.

2.3 Risks

This section allows us to assess the privacy risks, taking into account existing or planned controls.

2.3.1 PLANNED OR EXISTING MEASURES

This section allows us to identify controls (existing or planned) that contribute to data security. This measure aims to prevent and mitigate the risk of a data breach on the private cloud used for the MISTRAL

project, especially when dealing with sensitive data, implementing a combination of technical, organizational, and procedural measures. The data breach prevention plan will follow NIS directives.

Measures

Table 2. List of all planned measures.

Measure	Implementation
Encryption	- For data in transit, implement Transport Layer Security (TLS) or Secure Sockets Layer (SSL) protocols. - For data at rest, utilize strong encryption algorithms such as AES (Advanced Encryption Standard) to protect stored data.
Access Controls	- Deploy Identity and Access Management (IAM) solutions to enforce strict access controls. - Utilize Privileged Access Management (PAM) tools to implement the principle of least privilege
Authentication and Authorization	- Implement multi-factor authentication (MFA) solutions, combining passwords with additional authentication factors. - Employ Role-Based Access Control (RBAC) to enforce authorisation policies and control user actions.
Network Security	- Utilize next-generation firewalls to monitor and filter network traffic. - Implement Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to detect and respond to network threats. - Integrate Network Access Control (NAC) solutions to ensure only authorized devices connect to the network.
Regular Audits and Monitoring	- Implement Security Information and Event Management (SIEM) solutions for centralized log management and real-time monitoring. - Leverage Managed Detection and Response (MDR) services for continuous monitoring and threat detection. - Utilize vulnerability scanning tools and Endpoint Detection and Response (EDR) solutions for regular security audits.
Data Backup and Recovery	- Implement backup solutions with encryption, such as cloud-based backup services. - Utilise disaster recovery tools and technologies to ensure data availability in case of breaches.
Security Patching and Updates	- Employ Patch Management tools to automate the process of applying security patches. - Use vulnerability scanning tools to identify and remediate potential security weaknesses.
Employee Training	- Provide cybersecurity awareness training using interactive platforms and simulated phishing exercises.

Measure	Implementation
	- Utilize Security Awareness and Training tools to reinforce security protocols.
Incident Response Plan	- Implement Incident Response Platforms (IRPs) for automated incident detection, analysis, and response. - Leverage MDR services to enhance incident detection and response capabilities. - Conduct tabletop exercises using simulation tools to test the incident response plan.
Privacy Impact Assessment (PIA)	- Utilise PIA tools to systematically assess and manage privacy risks associated with data processing activities. - Implement Data Loss Prevention (DLP) solutions, including EDR, to prevent unauthorized access and disclosure of sensitive data.

By integrating MDR, EDR, SIEM, and NAC into the cybersecurity framework, MISTRAL organization will enhance threat detection, incident response capabilities, and network access controls, thereby further reducing the risk of data breaches in a private cloud environment, particularly one hosting sensitive data like that from the MISTRAL observational studies.

Data Breach Intervention Protocol

Responding to a data breach in the Mistral network/database requires a well-prepared and coordinated approach to minimize the impact, identify the cause, and implement corrective actions. Here's a step-by-step intervention plan that will be adopted for each partner of MISTRAL involved in the treatment of personal data.

1. Activate Incident Response Team
    - Immediately activate the incident response team, which should include representatives from IT, security, legal, and communications departments.
2. Isolate and Contain
    - Isolate affected systems or segments of the Mistral network to prevent further unauthorized access and data exfiltration.
    - Contain the breach to limit its impact on other parts of the network.
3. Notify Relevant Parties
    - Notify key stakeholders, including senior management, legal, and compliance teams, about the data breach.
    - Comply with legal and regulatory requirements for data breach notifications, considering the jurisdiction of affected individuals.
4. Communication Plan

- Develop a communication plan to manage both internal and external communications. Transparency is crucial for maintaining trust.
- Designate a spokesperson to provide updates to employees, customers, and the public as necessary.

5. Forensic Investigation

   - Conduct a thorough forensic investigation to determine the scope of the breach, identify the compromised data, and understand the methods used by the attackers.
   - Preserve evidence for potential legal or law enforcement actions.

6. Data Recovery and Restoration

   - Restore affected systems and databases from clean backups to ensure data integrity.
   - Implement additional security measures to prevent a recurrence.

7. Password Resets and Access Reviews

   - Reset passwords for affected accounts and conduct access reviews to identify any unauthorized account access.
   - Enforce stronger authentication mechanisms for affected users.

8. Patch and Update Systems

   - Identify and remediate vulnerabilities that contributed to the breach.
   - Apply patches and updates to secure systems and prevent further exploitation.

9. Enhance Security Measures

   - Strengthen security controls based on the lessons learned from the breach.
   - Implement additional security measures such as intrusion detection and prevention systems.

10. Incident Documentation

    - Document all actions taken during the incident response process for post-incident analysis and regulatory compliance.
    - Identify areas for improvement in the incident response plan.

11. Collaborate with Authorities

    - Cooperate with law enforcement agencies, regulatory bodies, and other relevant authorities.
    - Share information necessary for investigations while ensuring legal compliance.

12. Post-Incident Review

    - Conduct a comprehensive post-incident review to understand the root causes of the breach and identify areas for improvement.
    - Update policies, procedures, and security controls based on the findings.

13. Training and Awareness

    - Provide additional training and awareness programs for employees to prevent similar incidents in the future.

- Reinforce the importance of security best practices and reporting suspicious activities.

14. Legal and Public Relations Support

- Engage legal counsel to assess the legal implications of the breach and ensure compliance with relevant regulations.
- Work with public relations professionals to manage the public perception and protect the organization's reputation.

15. Continuous Monitoring

- Implement continuous monitoring of the Mistral network to detect any signs of ongoing or future attacks.
- Regularly review and update incident response plans based on evolving threat landscapes.