D5.2 DATA MANAGEMENT PLAN

AUGUST 2024

έξιGence

DELIVERABLE INFORMATION	
Author(s)/Organisation(s)	F6S
Document type	Deliverable
Document code	D5.2
Document name	Data Management Plan
Work Package / Task	WP5 Project Management
Dissemination Level	PU – Public
Status	Final
Delivery Date (GA)	M6
Actual Delivery Date	8 August 2024

DELIVERABLE HISTORY

Date	Version	Author	Summary of main changes
	0.1	F6S	Creation of the document, structure
27-Jun-2024	0.8	F6S	Complete version ready for internal review
5-Jul-2024	0.9	TNO	Revision
08-Aug-2024	1.0	F6S	Final version

Co-funded by the European Union

Funded by the European Union.

The project is supported by the Smart Networks and Services Joint Undertaking and its members.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Smart Networks and Services Joint Undertaking (SNS JU). Neither the European Union nor the granting authority can be held responsible for them.

Table of Contents

1 INTRODUCTION

This document was developed as part of the EXIGENCE project. It corresponds to deliverable D5.2 Data Management Plan, as refereed in the Description of Action (DoA) – Annex 1 of the Grant Agreement (GA). It is included in the work package 5 Project Management.

The Data Management Plan (DMP) will support the management life cycle for all data that will be collected, processed or generated by EXIGENCE. It covers how to make data findable, accessible, interoperable and reusable (FAIR), including the handling of data during and after the project, what data will be collected, processed or generated, what methodology and standards will be applied, whether data will be shared/made open access (and how) and, if any, what data will not be shared/made open access (and why), how data will be curated and preserved.

In addition, the DMP describes the responsibilities regarding data management and security.

EXIGENCE is funded by the European Union under the Smart Networks and Services Joint Undertaking, referred to in this document as granting authority.

The EU General Data Protection Regulation 2016/679 (GDPR) will be enshrined in the practices of the EXIGENCE project. As described in this deliverable, and presented in the GA, the EXIGENCE consortium is committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. The EXIGENCE consortium is dedicated to safeguarding the personal information under our remit and providing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the GDPR.

Whilst a Data Protection Officer (DPO) has been appointed by F6S generally, and such DPO will assist with the oversight of the project's DMP and implementation, data protection is the responsibility of the various partners generating data, and should be monitored by each institution's DPO or designated person responsible for compliance. Each institution notes that the role of the DPO is to ensure compliance with data protection regulations, such as the General Data Protection Regulation (GDPR), and that personal data is collected, processed, and stored in a secure manner. The GDPR requires that the DPO is allowed to perform their functions independently and is provided the resources to carry out those tasks and access to personal data and processing operations. The designated DPO representing each institution involved in this project will have the following tasks and responsibilities:

- Cooperate in the establishment of common rules and requirements for the consortium data protection policy;
- Advise on the coordination of data protection processes and information among the partners involved, representing each institution;
- As applicable to their institution with guidance on how to implement the privacy principles;
- Monitor compliance of their own institution with national data protection laws;

- Provide advice to their own institution regarding data protection impact assessments and monitoring;
- Cooperate with the supervisory authority for prior consultation when required by law pertaining to their own institution.

The EXIGENCE project will follow the Open science: research data management principles established in the Horizon Europe Grant Agreement. The protection of data extends to Intellectual Property Rights (IPR) of the external participants which are kept exclusively by them. The protection of personal and privacy data is taken seriously by all consortium members, who shall follow this DMP during the project.

Relation with other project documents:

The Data Management Plan is related to the following documents:

- Grant Agreement (GA): Contract between the consortium and the granting authority describing the description of action (DoA).
- Consortium Agreement (CA): Contract between the consortium members defining internal provisions not mentioned in the Grant Agreement.
- D5.1 Project Handbook: Living document specifying operation procedures such as internal communication channels, repository structure and access management, naming conventions, quality assurance procedures, and responsibilities.

1.1 STRUCTURE OF THE DELIVERABLE

This report is divided into five main sections. This deliverable will first introduce the initial datasets identified at this project stage. It is important to underline the nature of the deliverable as a living document, meaning that it will be regularly updated by the end of the project as it is developing and adding more features that will deal with data as well as the actions related to data exploitation post-project. Sections 3, 4, 5 and 6 will each deal with additional details on handling the data from the point of openness, ethics, legal compliance, and other issues that may appear.

2 DATA SUMMARY

The processing of personal data that may occur under EXIGENCE will be related to its use in project activities (and without prejudice to the fact that in many cases, the relevant entities will be legal persons and, as such, the corresponding data used for such purposes will not constitute personal data):

- Promotion: sending communications by email to the professional contacts of the potential interested entities related to the relevant events.
- Identity and external platforms: enrollment in platforms involved in delivering the project.
- Implementation of activities: involving the participating entities (partners, ICT technology providers and consumers, policy makers and other stakeholders) in the EXIGENCE activities and contacting them for this purpose.
- Impact assessment: conducting feedback and impact assessment activities with the participating entities.
- Dissemination of results: producing media content, including with relation to the EXIGENCE events.
- Logistics and administration: putting in place the necessary means for the organisation of project activities, such as identification needed for security purposes or dietary requirements.
- Reporting: complying with any reporting obligations in relation to the granting authority under the project.

Relevant data for the project delivery will be collected, including personal data, as required to execute project activities. The GDPR sets out the legal framework for processing personal data. This will be incorporated into the project's policies and procedures to ensure data protection compliance. Personal data collected will be processed based on the legal basis of consent and legitimate interests. All personal data processed throughout the project's lifetime will be done in line with the principles of the GDPR. Policies will be developed to ensure clear procedures are in place for the collection, storage, accuracy, security, retention and destruction of personal data.

No special category data (defined by Article 9 of the GDPR as "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, (…) genetic data, biometric data to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation") will be collected by the EXIGENCE project.

Data will be collected, depending on the purpose and method of collection, in machine-readable, physical, and other formats.

Data will originate from multiple platforms, with different project partners responsible for the various platforms used in the project's delivery. The project will map the platforms used in the project's delivery to maintain a data management plan mapping. The project will not reuse any existing data unless the terms under which such data was originally supplied provide for such re-use.

The project is expected to generate data covering individuals and organisations, such as ecosystem organisations, investors, corporations, event attendees, etc.

The data might be useful to researchers and other entities regarding mapping activities to growth outcomes, understanding the project's area of focus and those seeking to understand public funds' impact on ecosystem growth.

Overall description of EXIGENCE

At the moment, the project already identified it will generate the following datasets:

- Event registration and participation
- Consent to use images and audio in dissemination actions
- Webinars and other video-recorded meetings
- Website and social media

During the project, the consortium may generate data sets associated with the research and development. The consortium will work on continuously updating this document during the project, identifying the data sets produced.

Repository and access management

Repository structure, naming conventions, and access policies are defined in the D5.1 Project Handbook.

Sections used to describe each dataset:

Section	Content
X Name of dataset	General description of the dataset.
x.1 Data capture	Describes how the data will be collected.
x.2 Data storage	Describes procedures and persons responsible for archiving data in the repository.
x.3 Data quality assurance	Describes procedures and persons responsible to assure that data is accurate and complete.
x.4 Utility and re-use	Describe the purpose and usage of the data and eventual reuse inside the project
x.5 Data sharing	Describes how and if the data will be shared outside of the project.
x.6 Archiving and preservation	Describes the timeframe and requirements for the archiving and preservation of the dataset.

x.7 Snapshot	Moments in time when snapshots of the dataset are archived, typically linked to milestones or project reports.

2.1 EVENT REGISTRATION AND PARTICIPATION DATASETS

The project will organise and run a series of events where it will be necessary for participants to register.

2.1.1 DATA CAPTURE

Participant registration for an event will be done using an online registration form or in-person at the event. The information collected will be the same independently of the registration being on or offline. Information collected will be the minimum needed to generate statistics regarding participation at the event. When relevant, consent for usage of participants' image and audio in dissemination actions will also be collected. Participant registration will be collected for every event run in the project.

In physical events, attendees will be requested to sign attendance sheets or similar documents. Attendance sheets will include a column that allows participants to mark their consent preference in relation to their image and information being publicly displayed.

2.1.2 DATA STORAGE

Information related to participants' registration will be stored on the project's documentation repository to enable the long-term storage and access to data by consortium members. Information will be stored according to each event organised in the project. Information will be stored as it is received by the project team.

All files sent to the repository must comply with the locations, names and permissions defined in D5.1 Project Handbook.

2.1.3 DATA QUALITY ASSURANCE

The task leader is responsible for verifying that participants provide all required information, that it is stored, and that the instructions in the informed consent forms are enforced.

2.1.4 UTILITY AND RE-USE

The registration dataset will be used by consortium members to increase participants' engagement in the project. It will also serve to generate aggregated or anonymised statistics and reports about the participants.

Upon specific consent by the registrants, the dataset may be used to communicate other events or initiatives organised by the EXIGENCE or other projects that pursue a similar objective.

2.1.5 DATA SHARING

Upon specific consent by the registrants, names and emails may be shared with other funded projects that pursue a similar objective to that of EXIGENCE.

The granting authority may be informed of the number and general characterisation of the participants in official reports.

2.1.6 ARCHIVING AND PRESERVATION

The EXIGENCE consortium must retain generated data until five years after the balance of the project is paid or longer if there are ongoing procedures (such as audits, investigations or litigation). In this case, the data must be kept until they end.

2.1.7 SNAPSHOTS

The dataset will have the following cumulative snapshots archived in the project repository.

Month	ID	Name / Purpose
Mxx	<yyy>	<Name of the snapshot n and purpose>
Mxx	<yyy>	<Name of the snapshot n and purpose>

2.2 OTHER EVENTS PARTICIPATION DATASETS

The project will organise activities for which there will be no registration form, and where it may be useful to collect images and audio recordings of participants for dissemination actions. Examples of activities are: interviews, focus groups, and round tables.

2.2.1 DATA CAPTURE

Consent for usage of participants' images and audio recordings in the project will be requested via a dedicated form collected through an F6S form or via email by another partner in charge of the activity. The partner in charge of the event collects the consent forms. The consent forms describe the purposes of the data collection and how the data will be used, and contain checkboxes for the participant to mark their preferences. Participants are informed that they can withdraw their consent by emailing the project explicitly stating this, or in the case of a newsletter subscription, they can unsubscribe. Consent will be stored in the project repository.

For physical events, attendees may be requested to sign attendance sheets or similar documents. This includes a column asking participants their consent preferences in relation to the publication and use of their image.

2.2.2 DATA STORAGE

Information related to participants will be stored on the project's repository to enable the long-term storage and access to data by consortium members. Information will be stored according to each event organised in the project. Information will be stored as it is received by the project team.

All files sent to the repository must comply with the locations, names and permissions as defined in the D5.1 Project Handbook.

2.2.3 DATA QUALITY ASSURANCE

The task leader is responsible for verifying that all required information is provided by participants, that it is stored and that instructions in the informed consents are enforced.

2.2.4 UTILITY AND RE-USE

The dataset generated will be used by consortium members to increase participants' engagement in the project. It will also serve to generate statistics and reports about the participants, which will be aggregated or anonymised data that will not compromise personal details of the participants nor any other confidential information.

This information will not be re-used outside of the project.

2.2.5 DATA SHARING

Data sharing is not applicable for this dataset. The granting authority may be informed of the number of participants that provided consent/ non-consent in official reports.

2.2.6 ARCHIVING AND PRESERVATION

The EXIGENCE consortium must retain generated data until five years after the balance of the project is paid or longer if there are ongoing procedures (such as audits, investigations or litigation). In this case, the data must be kept until they end.

2.2.7 SNAPSHOTS

The dataset will have the following cumulative snapshots archived in the project repository.

Month	ID	Name / Purpose
Mxx	<yyy>	<Name of the snapshot n and purpose>
Mxx	<yyy>	<Name of the snapshot n and purpose>

2.3 WEBINARS AND OTHER VIDEO RECORDINGS DATASETS

The project will organise and run one or more webinars that may be recorded for and manage a project website and social media channels to raise awareness about the project, engage stakeholders, and disseminate information and results.

2.3.1 DATA CAPTURE

Webinars and other activities will be recorded with video in the following cases:

- Participants have been informed and able to withdraw consent to be recorded for the purpose of the webinar/ activity.
- Recording is necessary to fulfil the objectives of the project.
- Recording is in the public interest or is in the interests of the recorder, unless those interests are overridden by the interests of the participants that require protection of personal data.

If one of the above mentioned cases is applicable, all participants of the webinar or activity that will be recorded will be informed at the start that such recording will take place. The following information will be disclosed to the participants:

- Confirmation the webinar/ activity will be recorded.
- Justification of the reason for the recording.
- Request consent for the recording: individuals who do not consent to the recording can still participate in the webinar/ activity. They can do this by turning off their camera and hiding/removing their name from the recording session so they can remain anonymous.

In the process of recording, the following will be considered:

- If at any time there is a need to protect sensitive data, the recording will be paused/ stopped.
- Any part of the recording that contains sensitive data will be erased.
- Recordings with sensitive data will be marked as such.

2.3.2 DATA STORAGE

Webinars and other video recordings will be stored on the project's repository and/or public platforms.

All files sent to the repository must comply with the locations, names and permissions as defined in the D5.1 Project Handbook.

2.3.3 DATA QUALITY ASSURANCE

The task leader will verify the appropriateness of the convention applied and the organisation within the repository. Any recording uploaded to a public platform will also be verified by another consortium member to confirm an adequate characterisation of the recording.

2.3.4 UTILITY AND RE-USE

Webinars and other video recordings may be used by the consortium members for dissemination purposes or to increase external engagement in the project.

2.3.5 DATA SHARING

Webinars and other video recordings may be shared and made publicly available through the project website or a public platform.

2.3.6 ARCHIVING AND PRESERVATION

For files stored in the repository, the EXIGENCE consortium must retain generated data until five years after the balance of the project is paid or longer if there are ongoing procedures (such as audits, investigations or litigation). In this case, the data must be kept until they end.

For files stored in public platforms the project has no control in archiving and preservation.

2.3.7 SNAPSHOTS

The dataset will have the following cumulative snapshots archived in the project repository.

Month	ID	Name / Purpose
Mxx	<yyy>	<Name of the snapshot n and purpose>
Mxx	<yyy>	<Name of the snapshot n and purpose>

2.4 PROJECT WEBSITE AND SOCIAL MEDIA DATASETS

The project partners will run and manage a project website and social media platforms to raise awareness about the project, engage stakeholders, and disseminate information and results. Anonymous statistical information about the visitors to the website and users' engagement with social media will be collected.

2.4.1 DATA CAPTURE

The project website will be set up to provide statistics that will be collected using a web analytics service. Only anonymised data will be collected that can not be tracked back to a specific individual. Social media platforms include their own analytics services that will be used to collect and provide information about user engagement on these platforms.

2.4.2 DATA STORAGE

In order to allow for a more thorough and varied analysis, data will remain stored on the analytics platforms. If relevant, data may be exported to the project's documentation repository to enable access by consortium members. Data will be stored separately, divided into the website and relevant social media platforms.

2.4.3 DATA QUALITY ASSURANCE

Data exported to the project's documentation repository will be stored using a common naming convention to ensure easy access by consortium members. Whenever possible, data will be exported regularly (e.g. fortnightly, monthly) and consistently in terms of indicators. The task leader will verify that the dataset is exported regularly and that it is consistent in terms of indicators.

2.4.4 UTILITY AND RE-USE

The dataset generated will be used by consortium members to analyse visitors and users' engagement with the project via the website and social media, and to adjust the existing strategy to improve engagement. The dataset will also be used to generate statistics and reports about visitors and users, which will be aggregated or anonymized data that will not compromise personal details of the participants nor any other confidential information. This information will not be re-used outside of the project.

2.4.5 DATA SHARING

Data sharing is not applicable for this dataset. Information extracted from the dataset will be made available via official reports.

2.4.6 ARCHIVING AND PRESERVATION

The EXIGENCE consortium must retain generated data until five years after the end of the project.

2.4.7 SNAPSHOTS

The dataset will have the following cumulative snapshots archived in the project repository.

Month	ID	Name / Purpose
M3	001	Website statistics
M3	002	LinkedIn statistics
M6	003	Website statistics
M6	004	LinkedIn statistics

2.5 (TEMPLATE FOR) EXTERNAL COMMUNICATION WITH THIRD PARTIES DATASETS

The project partners will engage and communicate with third parties throughout the project on one or more of the planned activities.

2.5.1 DATA CAPTURE

Communication and Information exchange between the partners and third parties will be carried out through one or more different platforms and may include e-mail, the F6S platform, or other communication platforms.

2.5.2 DATA STORAGE

The communications and information exchanged will primarily be stored on the platforms used for this purpose. Specific information and documentation that is relevant to all partners may be exported and saved on the project repository to enable access by consortium members.

Information will be stored separately according to the type of activity that the communication is related to. Such information will be exported as soon as it is available.

2.5.3 DATA QUALITY ASSURANCE

Information and documentation of interest that is exported to the project's documentation repository will be stored using a common naming convention to ensure easy access by consortium members. The task leader will verify that the information and documentation is consistent in terms of its naming and organisation within the repository.

2.5.4 UTILITY AND RE-USE

The dataset will be used primarily to enable access to information and documentation by consortium members involved in activities. With exemption to the third parties involved, no other third parties will use the information and documentation contained in the data set.

2.5.5 DATA SHARING

Data sharing is not applicable for this dataset.

2.5.6 ARCHIVING AND PRESERVATION

The EXIGENCE consortium must retain generated data until five years after the end of the project.

2.5.7 SNAPSHOTS

The dataset will have the following cumulative snapshots archived in the project repository.

Month	ID	Name / Purpose
Mxx	<yyy>	<Name of the snapshot n and purpose>
Mxx	<yyy>	<Name of the snapshot n and purpose>

3 FAIR DATA

3.1 MAKING DATA FINDABLE, INCLUDING PROVISIONS FOR METADATA

The data produced and used by the project will be largely discoverable with metadata, identifiable by participant name and/or organisation and in some cases, be indexable/findable using a persistent and unique actor key. The project will evaluate using the unique actor key across the multiple platforms that will be used in delivery of the project to enhance findability.

Some of the data, such as applicant and evaluation data, will be organised as structured data. One example is the use of a taxonomy of markets/industries or skill sets present with project applicants. As another example, project data, such as applicant and evaluation data, will be indexable chronologically with change and version control parameters.

Metadata used from the project will include (depending on the capabilities of each of the project's platforms):

- How data was created
- Time and date of creation or modification
- Source of data
- Who created data
- Expected quality of data

Naming conventions will vary by platform used in the delivery of the project. Each platform typically maintains its own conventions, with such conventions not under the control of the project.

3.2 MAKING DATA OPENLY ACCESSIBLE

Although some of the data used in the project will be personal, confidential, or proprietary, the project will work to make data openly accessible as possible. There are two specific categories of data where the project will endeavour to deliver on this goal:

- **Dissemination:** Information that is relevant to promote the project, such as data on the EXIGENCE Alumni and community, as well as testimonials and pictures/videos of the project activities, will be published on the EXIGENCE communication channels. The channels include websites and social media platforms, and will be made available for the public for dissemination purposes. Of course, consent will be secured before any publication and this data may be shared based on such consent.
- **Participant Profile:** The project will compile anonymised profile reports on specific project aspects (where such data is not subject to deanonymisation), such as the industries, funding stages or national origin of projects applicants and/or participants. This dataset may be shared without restriction as anonymised data.

No special tools other than standard web browsers, desktop text editors, spreadsheets and presentation software will be required for access to the data above. There is no source code that will be provided as part of the project.

EXIGENCE does not expect to need a data access committee.

3.3 MAKING DATA INTEROPERABLE

The project will endeavour to make data produced by the project interoperable to encourage any reuse and data exchange between external stakeholders. Data used in the project will be available on-line (browser), using standard spreadsheet formats (Open Office, Excel, Google Sheets, etc.), using standard text editors (Open Office, Word, Google format) and using standard encoding and formatting to reduce the likelihood of incompatibility.

Many of the metadata and structured data types used by the project's platforms have become de facto standards. Wherever possible and within the control of the project, the project will choose to adopt open, free, and commonly used metadata and structured data types. If required, the project will consider providing mapping to commonly used structures that are not already supported by the project.

EXIGENCE deliverables in Public dissemination level will use standard vocabulary and methodologies to facilitate interoperability and exchange among other business support organisations and start-up ecosystems.

The sustainability plan and the respective activities will ensure that it is possible to use the relevant EXIGENCE results and information after the project ends, while continuing to ensure data privacy.

3.4 INCREASE DATA RE-USE (THROUGH CLARIFYING LICENSES)

The project will make data related to dissemination available for re-use, if requested. Other datasets collected will not be made available due to EXIGENCE's commitments to its applicants and sub-grantees in relation to personal information and business private information.

The information made available on the project website and other communication channels will be free for third parties to use. If files or datasets are produced, they will be shared to eligible third parties.

Data retention periods in EXIGENCE will be determined in line with the GDPR principles of 'data minimisation' and 'storage limitation'. Regarding the use of each platform employed in delivery of the project, the application of these principles will be determined by policies of each respective platform.

Personal data collected by the project will be stored on Microsoft Sharepoint as well as on each platform used, until the end of the project. The project is currently set to end in 30 June 2026, with extension of retention through the conclusion of granting authority review. The project will retain data including, personal data processed by the EXIGENCE consortium members, if strictly needed, in accordance with the current terms needed to answer potential audits by the granting authority services, such as data that enables the assessment of EXIGENCE activities' impact.

The EXIGENCE must retain generated data for five years after the balance of the project is paid or longer if there are ongoing procedures (such as audits, investigations or litigation). In this case, the data must be kept until they end), and to the extent applicable, the potential processing of the relevant personal data for such purpose would be supported on the necessity of the consortium parties to comply with an applicable legal obligation to which such entities are subject to hereunder.

Notwithstanding the foregoing, any personal data may be deleted earlier if a data subject explicitly requests their records to be deleted and the applicable requirements to the exercise and execution of the right to erasure are fulfilled. In order to follow the principle of data minimisation, personal data will be deleted/destroyed in accordance with the applicable criteria and requirements resulting from the applicable personal data protection laws, namely, the GDPR.

4 ALLOCATION OF RESOURCES

Each partner in EXIGENCE is responsible for the application of the DMP for the data it contributes to the project repository and data that is received, stored, modified or deleted on a platform the project uses that is such partner's responsibility.

The project partners will maintain mapping on the platforms each partner uses in the project. The 10 consortium members have a responsibility towards ensuring a correct use of and management of data, in particular in the tasks and WPs which they lead.

There are no additional costs to make data FAIR in the project, as the costs to operate each platform used in the project are already integrated into the project costs. The personnel costs described in the GA and related with WP5 Project Management and T5.3 Data management take into account data management activities.

5 DATA SECURITY

All consortium members must understand their data security obligations and responsibilities. Such procedures are defined in the present deliverable. There is a dedicated focus on privacy by design and the rights of individuals engaged in the project. Each partner organisation will take responsibility for the platforms which they contract and/or operate for the project. As mentioned, the project will maintain records on each platform that each organisation carries responsibility for under the project.

Each partner will review each of the platforms they use to deliver the project with regards to data security, data encryption, data retention, secure access, secure transfer, and the security of storage.

In sum, the EXIGENCE project will maintain protection of personal data and compliance with Data Regulations as per national and European legislation regarding the protection of personal data. Procedures will be in place for applicable technical means to avoid the loss, misuse, alteration, access by unauthorised persons and/or theft of the data provided to this entity. Notwithstanding, security measures (particularly for Internet accessible data) are not impregnable. To mitigate risk of unauthorised access, access controls will be applied to data sources. As an example, applications to the EXIGENCE project and feedback forms will be made accessible to a limited number of team members using user-level security and permissions.

EXIGENCE participants (data owners) will be able to exercise their right to be forgotten.

Breach procedures will be put in place by the consortium members to ensure that the partners are able to identify, assess, investigate, and report any reported or detected data breach at the earliest possible time.

Additionally, all consortium members will be asked to adopt security measures to protect computers, laptops, mobile phones, and similar tools to prevent unauthorised access in case of leaving the tool unattended or in case of loss or theft.

6 ETHICAL ASPECTS

While no ethics issues apply to the EXIGENCE project, as stated in the DoA and GA, ethics will be taken into consideration in the way data is collected, stored and regarding who can visualise and use it. The project will work to ensure that management of personal data is compliant with GDPR and other applicable legal frameworks related to personal data protection. During the project, each partner will consider the standards, treaties and laws regarding data protection and privacy in both EU and national level legislation.

Prior to joining EXIGENCE activities, participants need to sign a "Commitment Agreement", where they consent to their involvement in the project activities and disclosure of their (public) profile and image, and confirm they understand and approve of how their personal data will be used. Informed consent for data sharing and preservation is not only included in the Commitment Agreement, but it is also requested at the open call stage. Consent documents are stored on the project repository and are only available to the consortium.

In addition to the consortia validating of platforms used in the project, this Commitment Agreement will increase transparency through an additional consent mechanism where participants can define additional preferences on data disclosure. When participants wish to remain anonymous in project dissemination materials, their identity will be anonymised for purposes of these materials in line with their wishes.

EXIGENCE has committed to be inclusive and to respect gender balance and will seek to present gender-related data in line with legal requirements.

As part of the open call for start-ups, EXIGENCE has requested the applicants to answer to the following question in the application form: "What steps has your company taken to be socially and environmentally responsible (e.g., gender diversity, social impact, carbon footprint)?". Although this question is part of the eligibility criteria that the start-ups need to meet in order to get to the second phase of the evaluation process, the project will ensure that special category data is not collected as part of the responses.

7 OTHER ISSUES

There are no relevant other issues at this time. We would expect to update this DMP if any other national, funder, sectoral or departmental factors affect project procedures for data management.

8 SUMMARY

This DMP aims to present the principles and measures the consortium will adopt to ensure the compliance of EXIGENCE's prospective data flows.

Each partner in the project will be responsible for platforms that are used to carry out the project work. The partners will collaborate to ensure that correct and compliant data, privacy, security and other procedures are followed.

This document will be updated in months 12 and 30 as part of the project's periodic report.