Let the dialogue begin

Firelogue

D7.4 DATA MANAGEMENT AND IPR PROTECTION STRATEGY

Project: Cross-sector dialogue for Wildfire Risk Management

Acronym: Firelogue

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

Document Information

Grant Agreement Number	**101036534**	**Acronym**		**Firelogue**
Full Title	Cross-sector dialogue for Wildfire Risk Management			
Start Date	01/11/2021	**Duration**		48 months
Project URL	https://Firelogue.eu/			
Deliverable	D7.4 Data management and IPR protection strategy			
Work Package	WP7 Stakeholder Management, CSA Coordination and Consortium Management			
Date of Delivery	**Contractual**	30/04/2022	**Actual**	30/04/2022
Nature	Report	**Dissemination Level**		Public
Lead Beneficiary	FhG			
Responsible Author	Sebastian Wagner (FhG), Claudia Berchtold (FhG)			
Contributions from	Mariza Kaskara (NOA), Katrina Petersen (TRI), Mistale Taylor (TRI)			

Document History

Version	Issue Date	Stage	Description	Contributor
v_0.1	24.03.2022	Draft	Initial contributions	FhG + partners
v_0.2	05.04.2022	Draft	Draft for internal review	TRI + NOA
v_0.3	07.04.22	Draft	Draft for internal review	TRI
v_1.0	29.04.22	Final	Final Version	FhG

Disclaimer

This document and its content reflect only the author's view, therefore the European Commission is not responsible for any use that may be made of the information it contains.

Citation

Wagner, S.; Berchtold, C.; Kaskara, M.; Petersen, K.; Taylor, M. (2022). Data Management and IPR Protection Strategy. Deliverable D7.4. FIRELOGUE.

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

CONTENT

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020
RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

LIST OF TABLES

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020
RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

Glossary

Abbreviation	Meaning
AB	Advisory Board
AP	Associated Partner
BFSI	Banking, Financial Services and Insurance
CB	Communication Booster
CO	Data restricted to the Firelogue consortium
EAB	Ethics Advisory Board
EWE	Extrema Wildfire Events
IA	Innovation Actions
GA	Grant Agreement
GDPR	General Data Protection Regulation
IR	Data to be stored in institutional repositories
IPR	Intellectual Property Rights
PU	Data available to the public
RIA	Research and Innovation Action
TRL	Technology Readiness Level
WFRM	Wildfire Risk Management
WGs	Working Groups
Consortium partners	
ADAI	Association for the Development of Industrial Aerodynamics
CMCC	Centro Euro-Mediterraneo sui Cambiamenti Climatici
CTFC	Consorci Centre de Ciència i Tecnologia Forestal de Catalunya
EDGE	EDGE in Earth Observation sciences Monoprosopi IKE
FhG	Fraunhofer Gesellschaft für Angewandte Forschung e.V. (FhG)
IIASA	International Institute of Applied System Analysis
INESTEC	Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência
KEMEA	Centre for Security Studies
NOA	National Observatory of Athens
PCF	Pau Costa Foundation
SAFE	SAFE Cluster
TIEMS	The International Emergency Management Society
TRI	Trilateral Research
UAH	Universidad de Alcalá
VOST	Virtual Operations Support Team from Portugal

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

Executive Summary

Deliverable, D7.4 provides an initial data management plan for Firelogue and details what will be done going forward. The plan will set out the consortium's strategy to improve and maximise access to and re-use of research data generated or collected under the project, while ensuring data protection as well as the consortium's intellectual property rights (IPR). This document details the expected types of data to be collected by the consortium partners (Chapter 1), the storage of data and deliverables, the protection of data (Chapter 2), and states the role of the Data Protection Officer as the contact person for consortium members. The deliverable further focuses on the FAIR data requirements set out by the European Commission as well as data protection and data security measures that will be undertaken by the consortium. Chapter 3 deals with the questions of intellectual property and outlines the requirements as well as supportive measures. The concluding section (Chapter 4) provides a description of the future course of action in an effort to continuously adapt the plan, to expand it if necessary and to render it more precise. The data management plan is a living document in which information will be made available on a more detailed level as the implementation of the Firelogue project progresses and when significant changes occur. This document is the initial of the two versions to be produced for the data management plan throughout the Firelogue project's duration with a second official version to be released at the end of the project.

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020
RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

1 Data summary

2.1 Types of data the project will generate/collect

This section contains the main types of data that can be obtained, as well as a list of those that each partner plans to collect.

Firelogue is a Horizon 2020 Coordination and Support Action (CSA) under the Green Deal that brings together expertise from across Europe in wildfire risk management (WRFM). Firelogue focuses on creating spaces for dialogue, enabling the WFRM community to address the current and future challenges of wildfires. In doing so, Firelogue acts as a facilitator of knowledge by bringing together the experiences and best practices of a variety of stakeholders from within and outside the WFRM community, with a specific focus on supporting the Innovation Actions (IAs) funded under the same call, namely DRYADS, FIRE-RES and SILVANUS as well as the FirEUrisk project (funded via H2020 call LC-CLA-15). In order to fulfil this main objective, it is indispensable for the project to gather and disseminate known and new data on stakeholders, WFRM research results, experiences, and existing and planned products, among others.

The expected "data utility" is as diverse as the group of addressees. As an example, publications derived from the collected and disseminated data are addressed to a wide range of stakeholders active in the field of WFRM. These include first responders, IT technicians, farmers, researchers, policy and decision makers, asset managers, firefighter associations, forest and landowners, civil protection, environmental educators, to name but a few (for a more detailed preliminary enumeration of stakeholders, see D7.2 "Stakeholder Clustering").

In principle, the project is expected to generate 3 types of data: (i) human participant data in relation to research and dissemination, (ii) data on those on the Firelogue mailing list, (iii) qualitative data on synergies and conflicts between different sectors and stakeholders in managing WFRM.

2.2 Data collected by each partner

Data collection began at the start of the Firelogue project and will continue for much of the duration of the study. Participants were asked to indicate their needs by means of a data collection form. It is crucial to emphasise that the data given in the Table 1 is only a first estimation of the data sources and thus cannot be claimed to be complete for the entire duration of the project. The summary of the estimated types and formats of data to be collected by the respective project members can be found below:

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

Table 1: data to be collected by each partner

Organisation name	Data to be collected
FhG	- Contact information of research participants - Photographs, video and audio recordings, transcripts - Consent forms and signatures - Personal and professional experiences and opinions
PCF	- Survey data (survey records, survey results) - Contact information for login/register to the Platform (full name, organisation, contact, password)
NOA	- Contact information of research participants (in the TechMall) - Statistics (from EFFIS report and national databases regarding impact assessment) - Personal and professional experiences and opinions for communication purposes
SAFE Cluster	- Movement data
TRI	- Personal and professional experiences and opinions - Consent forms and signatures - Contact information of research participants (e.g. contact points from IA and other projects)
EDGE	- User logins (name, surname, contact information) - Contact information of research participants and service providers (TechMall) - Photographs and videos in news portal - Metadata (for connection with other platforms) - Contact information of stakeholders and IA+FireEURisk partners
IIASA	- Contact information of stakeholders participating in the insurance working group - Qualitative, anonymised/pseudonymised data: Professional experiences and opinions from stakeholders involved in the insurance- and the cross-WG workshops
INESCTEC	- Mailing lists
TIEMS	- Newsletter/webinars subscription (email address)
VOST	- Survey data (survey records, survey results), metadata, movement data, personal and professional experiences and opinions
CMCC	- Personal and professional experiences and opinions
CTFC	- Contact information of stakeholders and IA+FireEURisk partners participating in Environmental/Ecology Working Groups and Cross-WG workshops - Personal and professional experiences and opinions
ADAI	- Mailing lists; contact information of research participants (e.g. contact points from IA and other projects)

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

KEMEA	- Contact information of research participants (e.g. contact points from IA and other projects), contact information of external stakeholders (CI operators), personal and professional experiences and opinions
UAH	- Topographical/geographical data

As a CSA, Firelogue aims at establishing networks between the project partners, the Innovation Actions (IA) and various stakeholders, e.g. through conferences, seminars, studies, policy dialogues or joint initiatives. It can be seen from Table 1 that the data that inherently arises from these measures is reflected in the entries submitted by the project partners. The dissemination, awareness-raising and communication activities, as well as complementary actions to network and coordinate programmes between different countries, creates a spectrum of data ranging from publicly-available information (such as topographical data) to confidential data (e.g. movement profiles, signatures, video and audio recordings). In order to handle this data in a trustworthy manner, the partners of the Firelogue project commit themselves to comply with a series of standards that lead to protection of the data in a systematic manner. The project partners will adhere to the standards included in:

- the General Data Protection Regulation (GDPR)[1]
    - The GDPR is the main EU/EEA personal data protection and privacy regulation, however it can also apply to entities that transfer or store personal data outside the EU/EEA.
- ISO/IEC 29100:2011
    - ISO/IEC 29100:2011 applies to individuals and organisations involved in the specification, acquisition, architecture, design, development, testing, maintenance, management and operation of information and communication technology systems or services where privacy controls are required for the processing of personally identifiable information.
- ISO/IEC 27001:2005
    - SO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system in the context of the organisation's overall business risks. It specifies requirements for the implementation of security controls tailored to the needs of individual organisations or parts thereof. It is designed to ensure the selection of appropriate and proportionate security controls that protect information assets and provide confidence to interested parties.
- the EU Charter of Fundamental Rights 2009
- the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1980
- the FAIR data management guidelines in Horizon 2020 (FAIR guiding principles: Findability, Accessibility, Interoperability, Reusability)[2]

[1] Furthermore, the deployment of a systematic data protection impact assessment will also be considered in the long term: For this purpose, ISO/IEC 29134:2017 could be beneficial as it details the process of a data protection impact assessment from the preparation phase through the implementation phase to the follow-up and reporting phase. The privacy impact assessment is a process that aims to identify the privacy risks associated with a processing system for stakeholders, partners or other data subjects and to ensure the protection of their information and compliance with applicable regulations.

[2] For a more in-depth academic discussion of the guidelines, see Wilkinson, Dumontier, Aalbersberg et al. (2016).

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

2.3 The Fair Data Management Guidelines

Given their increasing relevance among the scientific community and their importance for the project, the ideals of the Fair Data Management Guidelines are presented in Table 2 below. These guidelines are supposed to help researchers to make their research data Findable, Accessible, Interoperable and Reusable (FAIR) to ensure that data is properly managed. Adhering to the greater part of these principles, it is believed that the integration and reuse of shared data and knowledge subsequently leads to knowledge generation and ultimately to innovation. These are ideals that are considered fundamental by the Firelogue consortium.

Table 2: The FAIR Data Principles

Data has…	Criteria
…to be Findable:	> F1. (meta)data are assigned a globally unique and eternally persistent identifier. > F2. data are described with rich metadata. > F3. (meta)data are registered or indexed in a searchable resource. > F4. metadata specify the data identifier.
…to be Accessible:	> A1 (meta)data are retrievable by their identifier using a standardised communications protocol. > A1.1 the protocol is open, free, and universally implementable. > A1.2 the protocol allows for an authentication and authorisation procedure, where necessary. > A2 metadata are accessible, even when the data are no longer available.
…to be Interoperable:	> I1. (meta)data use a formal, accessible, shared and broadly applicable language for knowledge representation. > I2. (meta)data use vocabularies that follow FAIR principles. > I3. (meta)data include qualified references to other (meta)data.
…to be Re-usable:	> R1. (meta)data have a plurality of accurate and relevant attributes. > R1.1. (meta)data are released with a clear and accessible data usage license. > R1.2. (meta)data are associated with their provenance. > R1.3. (meta)data meet domain-relevant community standards.

(cf. https://force11.org/info/the-fair-data-principles/)

The following paragraphs briefly outline the way in which these ideals are reflected in the Firelogue project and suggestions on how their realisation can be implemented.

2.3.1 Making data *Findable*

The consortium aims to make the data created and/or used in the project discoverable and identifiable by means of metadata. This is particularly necessary at the interface with the general public and external researchers. This gateway function is assumed, for example, by the envisioned Firelogue platform, which is intended to enable stakeholders to share knowledge, information, resources and technologies. For this purpose, the data made available on the platform are tagged accordingly by the supervising working group and provided with metadata. The same applies to the envisaged joint

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

publications. The repositories provide open access to the bibliographic metadata that identifies the deposited publication. This bibliographic metadata will be in a standard format and will include all of the following:

- the terms “European Union (EU)” and “Horizon 2020”;
- the name of the action, the acronym and the grant number;
- the publication date and, where applicable, the duration of the closure period;
- and a persistent identifier.

2.3.2 Making data openly *Accessible*

First of all, it is first important to distinguish between two types of openly accessible scientific data in “Open Science”, namely *open access research data* and *open access publications*. Open access to research data means that data collected and/or created during the course of research is published freely accessible on digital repositories. The data and the information required for access and use, i.e. metadata and tools/instruments, are deposited in a data repository. Data repositories make it possible to tag datasets with persistent identifiers so that they can be cited, linked and tracked (cf. 1.3.1 above). If these data can be used and reused with no conditions other than stating the source, they are defined as ‘open access research data’. When research data is published openly, other researchers are enabled to validate and continue building on previous results. Further advantages are the amplification of the impact and the avoidance of duplication of efforts. Therefore, Firelogue encourages the sharing of datasets beyond publication.

Since Firelogue, as a CSA, does not collect much of its own raw research data, the project rather contributes to identifying and communicating a good overview of the landscape in relation to the work on open access to research data in the field of WFRM. Furthermore, Firelogue will foster the implementation of the FAIR principles by the IAs to facilitate access to research data beyond the boundary of research groups.

As far as open access publications are concerned, open access (OA) journals typically offer immediate access to articles free of charge, without the need for a subscription. Some OA journals charge authors a fee for OA publication, known as Article Processing Charges (APC). Researchers of European projects can also publish free of charge on the Open Research Europe platform such as, for instance, Open Research Europe (ORE). ORE is a scientific publishing platform available to Horizon 2020 and Horizon Europe beneficiaries which is free of charge, has a rigorous and open peer-review process, and the open access model allows everyone to access the results. Similar to other repositories, ORE calls for open access to research data in support of the article in line with the principle of "as open as possible, as closed as necessary" and the mandate of Horizon 2020 and Horizon Europe. The ORE platform uses an open model for publishing research results: Publications are published within a few days of submission, followed by transparent, open peer review. However, it is important to note that an article published in the ORE repository cannot be published a second time in another journal or platform.

Open access is a consideration when publication is chosen as a means of dissemination. However, it is important to emphasise that open access does not influence the decision to exploit research results

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

commercially, e.g. through patenting or licencing. This is especially relevant for publications that relate to data published on planned platforms such as the TechMall (cf. below). The decision on whether to pursue publication via open access must be made after the consortium has established whether the results are to be published directly or protected first.

As stipulated in the Firelogue Grant Agreement (GA), Article 29.3, regarding the digital research data generated in the action ('data'), the beneficiaries must:

a) deposit in a research data repository and take measures to make it possible for third parties to access, mine, exploit, reproduce and disseminate - free of charge for any user - the following:
   i. the data, including associated metadata, needed to validate the results presented in scientific publications, as soon as possible;
   ii. not applicable;
   iii. other data, including associated metadata, as specified and within the deadlines laid down in the 'data management plan';

b) provide information — via the repository — about tools and instruments at the disposal of the beneficiaries and necessary for validating the results (and — where possible — provide the tools and instruments themselves).

This does not change the obligation to protect results in Article 27, the confidentiality obligations in Article 36, the security obligations in Article 37 or the obligations to protect personal data in Article 39, all of which still apply.

As an exception, the beneficiaries do not have to ensure open access to specific parts of their research data under point (a) (i) and (iii), if the achievement of the action's main objective would be jeopardised by making those specific parts of the research data openly accessible. In this case, the data management plan must contain the reasons for not giving access.

As a rule, the Firelogue project recommends the use of repositories that support open data principles (e.g. Zenodo by OpenAIRE). Zenodo is particularly well suited as it has no requirements in terms of format, size, access restrictions or licence. The online storage service's code is itself open source and based on the digital library Invenio, which is also open source. Furthermore, all metadata is freely available under a CC0 licence and all open content is accessible via open APIs. For open access publications, Firelogue recommends the Open Research Europe (ORE) publishing platform as a default. However, if a specific OA repository is found that is more suitable for a WFRM topic, this may be used as well. Each publication and the choice of publication platform must be coordinated with the Firelogue Consortium to ensure compliance with the FAIR Data Principles.

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

2.3.3 Making data *Interoperable*

When publishing results, e.g. in scientific journals, the Firelogue project prefers self-archiving (also known as "green open access"), which means that the published article or final peer-reviewed manuscript is archived in an online repository by the researcher - or a representative - before, after or in parallel with its publication.[3] In addition, partners will inform each other of planned publications well in advance of publication to see if other partners with relevant expertise are interested in participating or to allow partners to raise any questions regarding ownership of the results included in the publication. In this way, the project will enable the exchange and reuse of data between researchers, institutions, organisations, countries, etc. For this to be successful, it is crucial to adhere to standards for formats that are compatible as far as possible with available (open) software applications as well as adherence to a labelling standard (in terms of making transparent e.g. coherent bibliographic metadata, glossaries, acronyms, project-specific ontologies etc.) with the aim to enable interdisciplinary interoperability. Especially with regard to the large number of diverse stakeholders as potential recipients of this data, such a consistent measure is imperative. While the project will mainly focus on its proprietary data, Firelogue, acting as a CSA, will be in direct exchange with the IAs to stimulate a desired long-term interoperability of data across project boundaries. It is therefore envisaged to continually discuss the achievement of cross-disciplinary interoperability and the establishment of standards, for example, within the Research Integration Board.

2.3.4 Increase data *Re-use*

The project aims at the widest possible re-use of the data obtained and stored. Both via the platform and via targeted publications, data should be made available quickly for further use. Moreover, it is a central part of the Firelogue project to take up existing strands and "traditions" of discontinued WFRM projects and to transfer them into current and future projects. This means that data can be reused as a matter of course right from the start of the project. Consequently, the ongoing project will continue to aim at sharing data with the research community and all stakeholders as quickly as possible. Ideally, most of the data obtained is released for sharing and can be made immediately available for access (after an anonymisation process, where necessary). The desired, thorough (meta)categorisation of the data will help prospective users to obtain the appropriate type of data. As Firelogue considers itself to be part of a WFRM research tradition, the aim is that the data produced and/or used in the project will be usable by third parties even after the project has been completed. Thus, the information on the platform is to remain available and re-usable for at least five years after completion of the project.

While the encouragement to maximise access to and re-use of the (research) data generated in the project is an important issue, the consortium is also addressing the need to balance openness and protection of scientific information and not to neglect commercialisation and intellectual property rights (IPR). The latter is particularly necessary as the Firelogue project aims to establish a so-called TechMall. This platform will contain descriptions of specific services and products that can be used by

[3] The consortium is aware that if costs related to open access to research data under Horizon 2020 are incurred on the "gold open access" pathway (i.e. the research paper is freely available immediately after a processing charged has been paid to the publisher), they are eligible during the project lifetime under the conditions set out in the H2020 Grant Agreement, in particular in Article 6 and Article 6.2.D.3.

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

stakeholders throughout the WFRM value chain. Interested stakeholders will be able to discover what is being offered by different Innovation Actions (IA). It is envisaged that the TechMall will assist in discovering which services are available and can be purchased, and will enable comparison of services offered by different providers and provide access to the respective technology providers. It should be pointed out that the data deposited is essentially metadata on the services and does not constitute background data or information.

Especially for subprojects and platforms such as the TechMall, a clear strategy on data security is needed to protect commercialisation and intellectual property rights (IPR), as well as, of course, the protection of personal data. This is explained in more detail in the next section.

2 Data security

The subsequent section outlines the basic classifications and dissemination levels of the data collected and the extensive measures taken by the project to ensure the highest level of data protection and security.

2.1 Data type classification

Depending on the purpose of the data and data protection concerns, data processed within the project may be made **public** (category **PU**), shared only within the **consortium** (category **CO**/sensitive data), or kept in **institutional repositories** (category **IR**/highly sensitive data). The main types of data (including personal data) that will be collected, processed and/or produced during the project include:

- Academic (PU) and grey literature (CO) on relevant topics, including reports from similar/related projects
- Relevant ethics codes, guidelines, policies, and legal texts (PU)
- Results of interviews, surveys, and workshops with experts and stakeholders in the forms of video recordings (IR), audio recordings (IR), transcripts (CO or PU), qualitative summaries (CO or PU), and quantitative data sets (CO or PU)
- Views on selected technologies derived from such interviews, surveys, and workshops (CO or PU)
- Contact lists (of relevant stakeholders and for the mailing list) (IR)
- Signed information sheet and consent forms (RO)
- Media articles (PU)
- Project work plans and internal notes (IR or CO)
- Deliverables, articles, virtual whiteboards and PowerPoint presentations (IR, CO, or PU)
- Dissemination materials, including the website, newsletters, videos, etc. (PU)

These dissemination levels are provisional, and subject to change throughout the project depending on the actual data included, the needs of the partners, and relevant privacy rules.

2.2 Data security and protection

The Firelogue project takes comprehensive measures to ensure that the project complies with EU regulations on privacy and data protection, as well as ethical standards in research and society. According to the Firelogue working plan, the Fraunhofer-Gesellschaft (represented by the Fraunhofer

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

INT team) serves as consortium leader. The partner Trilateral Research serves as Ethics Manager and is the task leader for D7.3 “Ethics and quality protocol and monitoring” (with contribution from FhG). Fraunhofer-Gesellschaft as the consortium lead partner i.e. host institution provides the main Data Protection Officer (DPO) in accordance with GDPR Art. 37:

Ralph Harter
Data Protection Officer
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.
Hansastrasse 27c
80686 Munich
(hereinafter "Fraunhofer")
Email: datenschutz@zv.fraunhofer.de
Phone: +49 89 1205-2045
Fax: +49 (0)89 1205-7531

Within the Fraunhofer-Gesellschaft, the in-house DPO and the data protection coordinator support the specialist departments on data protection aspects. The task of the DPO is to monitor compliance with data protection requirements within the Fraunhofer-Gesellschaft and to provide advice on data protection questions. The DPO generally acts as a point of contact for data protection matters and is the interface with the national supervisory authority. Fraunhofer-Gesellschaft has appointed a Corporate DPO pursuant to the requirements of Art. 37 GDPR. Said officer performs the advisory and supervisory duties assigned by law and performs them in independent application of his expertise. The institutes and departments at the headquarters provide the information, records, etc., that are required for this purpose. Customers, research participants and employees of Fraunhofer-Gesellschaft may contact the DPO directly with any comments, suggestions or complaints. Confidentiality is guaranteed.

The consortium ensures data security (including data recovery, secure storage and transmission) and secure storage of data in certified repositories (e.g. Microsoft Sharepoint (CO/PU), Fraunhofer OwnCloud (IR)) for long-term preservation and curation.

Art. 32 GDPR contains requirements on how personal data must be handled from a technical and organisational point of view. This is done in order to achieve data security. Data security is thus a further and complementary aspect of data protection. The regulations and guidelines provided for the handling of information technology systems and information security within the Fraunhofer-Gesellschaft implement and guarantee this data security (Fraunhofer-Gesellschaft e.V., p. 5).

The Firelogue consortium, its consortium leader and its partners use appropriate technical and organisational security measures to protect data against accidental or intentional manipulation, partial or complete loss, destruction or against unauthorised access by third parties. The security measures are continuously improved in line with technological developments. Special attention is paid to the confidentiality of data storage. Access to the collected data is password-protected and is only granted to partners authorised to process the data.

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020
RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

In addition, access to information or input of data (including changes) will only be allowed to authorised users to ensure their confidentiality and will only be reserved for partners collecting and providing data.

In general, the following principles will be followed:

- Participants' personal data will be kept strictly confidential during the entire period of data collection and processing
- All participants taking part in workshops, interviews or other participatory activities will be asked to read and sign a consent form
- In line with Art. 12 GDPR, participants will be informed that their personal data is being collected and why. They will be told how the data will be processed, who will have access to it and how it will be kept secure. This information must be included in the privacy notice of the consent form and provided to data subjects at the time of data collection

Where possible, personal data will be anonymised or pseudonymised.[4] Data will be encrypted where possible and abstracted and/or anonymised in a way that does not affect the final project outcome; any data collected will not be used in any way outside the Firelogue project or for other secondary purposes. The project coordinator will ensure that all personal data is successfully and permanently deleted after the completion of the project and after the completion of the audit. As set out in the Grant Agreement, a retention period of five years is foreseen after the end of the project due to audits by the European Commission. The personal data will be deleted immediately after this purpose has been achieved. The Firelogue project includes different levels of security, with the most confidential information having the highest level of security and only selected persons, such as the data controller, will have access. The project will not download data to remote devices (USBs, external hard drives) even if they are encrypted or password protected.

All files are stored on secure servers with restricted access. All sensitive personal data are processed on a legal basis under Art. 6 GDPR and a separate condition for processing under Art. 9 GDPR and are subject to additional safeguards. All sensitive (restricted) or highly sensitive (confidential) data will only be stored and transferred via a secure repository. For this repository, the Firelogue consortium will use the Fraunhofer OwnCloud (https://owncloud.fraunhofer.de/), which provides the required data protection measures. Fraunhofer OwnCloud also uses appropriate technical and organisational security measures to protect the data against accidental or intentional manipulation, partial or complete loss, destruction or against unauthorised access by third parties. The security measures are continuously improved in line with technological developments. Access will only be granted to the partners of the consortium and will be password protected.
From the moment a prospective platform is activated on which classified, hence highly sensitive information, is stored, the data sharing principles must be re-defined as to which data will be accessible and visible to whom. For this purpose, each partner appoints a data manager (and a deputy data

[4] It is suggested to use the tool *Amnesia* for this purpose: According to the developers, Amnesia allows the user to replace unique values or unique combinations of values with more abstract ones and further to create rules for generalising these values semi-automatically, save them and reuse them or import them from other sources (https://amnesia.openaire.eu/index.html).

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

manager) who reports to the consortium lead and is responsible for data management and protection of intellectual property within their organisation.

Whenever possible, data transmitted by users (e.g. telephone, video conference, website) is encrypted using the generally recognised and secure standard Transport Layer Security (TLS). A secure TLS connection can be recognised by the appended s to http (e.g. https://..) in the address line of the browser or by the lock symbol in the lower area of the browser.

The same standards apply, for instance, for the use of virtual whiteboards. Due to the pandemic, hybrid working has become inevitable. The Firelogue consortium has decided to exchange information via virtual whiteboards. The company RealtimeBoard, Inc. dba Miro stores all production data within the EU (Ireland) and the USA (Virginia). In addition, all personal data transfers to non-EU/EEA countries without adequacy decisions, where necessary, comply with the requirements of the GDPR by using Standard Contractual Clauses (SCCs).

Furthermore, as a member of the Fraunhofer Group for Defence and Security and as a reliable partner of the Federal Ministry of Defence, the consortium leader Fraunhofer Gesellschaft (in this case in particular Fraunhofer INT as the institute coordinating the project) has high requirements for ensuring security. This means that all Fraunhofer INT employees are subject to a security clearance in accordance with Art. 36(2) SÜG of the German Security Clearance Act (*Sicherheitsüberprüfungsgesetz*). Therefore, the highest security standards apply to the use of information and communication technology (ICT) used by the consortium leader's team members.

Upon completion of the Firelogue project and at the end of the five-year review period, all information constituting personal data will be deleted. In this case, the term “completion” refers to the time when the Firelogue project is completed and submitted to the European Commission. Data that has been depersonalised will be kept secure and accessible for up to five years after the end of the project. Whenever data is deleted prior to the completion of the project, such action must be documented within the project’s data management plan and confirmed as such to the data controllers/owners.

The collection and use of personal data for research purposes will be limited to information that is lawful and necessary solely for the performance of the specified task. Partners will limit the collection of sensitive personal data to that which is generally accepted to influence the adoption of DRM measures. The partners will ensure that any sensitive personal data collected is anonymised and cannot be linked to the data subject in order to protect their rights. Therefore, the consortium will not publish in the project reports and other published documents any personal information that could directly or indirectly identify the participant, unless the participant requests otherwise. To ensure this, partners will adhere to the principle and methodology of anonymisation and follow the recommendations, best practices and anonymisation techniques described in the Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques[5]. Participants are asked if their answers can be

[5] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020
RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

directly quoted. Interview participants will be asked to consent to the research interview itself and to the collection, storage, retention and sharing of the data.

The consortium grants participants the "right to be forgotten", i.e. personal data will be deleted immediately when a data subject (ordinarily a participant) requests its erasure.

It is understood that participants will be notified of data breaches by the consortium if there is a serious risk to them.

3 Management of knowledge and intellectual property

Shared ownership often arises in the context of collaborative innovation and is of particular importance for EU-funded projects such as Firelogue, which involve joint development of intellectual property (IP). In these situations, it is the task of the consortium to provide a clear allocation of ownership of the jointly developed IP for the collaborative partners involved in order to prevent disputes and even litigation.

The new elements concerning the IP strategy for projects within the scope of Article 39 of the Horizon Europe legislation include a "Mandatory Results Ownership List (ROL)". It states that beneficiaries must now inform on the owner(s) of the results (results ownership list) in the reporting. This includes whether the ownership is single or joint, the name of the owner(s), the country of establishment of the owner(s) and whether the results will be exploited by the owner(s)". The apparent aim of this is to clarify the ownership of the results in order to support, promote, accelerate and simplify the exploitation of the results. This illustrates the need for clear identification of both the intellectual property and the owner(s) of that very property. According the Grant Agreement Article 2.2.3.2 "Management of knowledge and intellectual property", Firelogue will handle IPR as set out in the Consortium Agreement that was signed by all members. In the following, the most relevant aspects concerning IPR are singled out:

Section 8 of the Consortium Agreement covers the main issues of (joint) ownership, the transfer and the dissemination of results. Here it is stated that, in general, "results are owned by the Party that generates them." In case of a joint ownership, parties either "establish a written separate joint ownership agreement regarding the allocation of ownership and terms of exercising, protecting, disseminating, the division of related costs and exploiting such jointly owned Results on a case by case basis" or, in the absence of such an agreement, "each of the joint owners shall be entitled to use their jointly owned Results for non-commercial research and education activities on a royalty-free basis, and without requiring the prior consent of the other joint owner(s), and each of the joint owners shall be entitled to otherwise Exploit the jointly owned Results and to grant non-exclusive licenses to third parties (without any right to sub-license), if the other joint owners are given: (a) at least forty-five (45) calendar days advance notice; and (b) Fair and Reasonable compensation." (8.2). Each Party may transfer ownership of its own results. It may designate specific third parties to whom it intends to transfer ownership of its results. The other Parties hereby waive their right to prior notice and their right to object to any transfer to the listed third Parties. However, the transferring Party shall, at the

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020
RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

time of the transfer, notify the other Parties of such transfer and shall ensure that the rights of the other Parties are not prejudiced by such transfer (cf. 8.3).

Section 9 addresses, access rights, the ownership of results obtained from the execution of the project, the know-how and information related to the use of knowledge owned by one of the partners, resulting from work carried out prior to the agreement. It is stated here that "Each Party shall implement its tasks in accordance with the Consortium Plan and shall bear sole responsibility for ensuring that its acts within the Project do not knowingly infringe third party property rights."(9.2.1). The following passage regulates the provision of information within the parties: "Access Rights to Results if Needed for Exploitation of a Party's own Results shall be granted on Fair and Reasonable conditions. Access rights to Results for internal research and education activities shall be granted on a royalty-free basis." (9.4.1)

Section 10 covers the non-disclosure of information. In 10.1 it is stated that "[a]ll information in whatever form or mode of communication, which is disclosed by a Party (the "Disclosing Party") to any other Party (the "Recipient") in connection with the Project during its implementation and which has been explicitly marked as "confidential" at the time of disclosure, or when disclosed orally has been identified as confidential at the time of disclosure and has been confirmed and designated in writing within fifteen (15) calendar days from oral disclosure at the latest as confidential information by the Disclosing Party, is "Confidential Information". Any obligations, such as not using confidential information other than for the purpose for which it was disclosed or ensuring that internal disclosure of confidential information by a recipient is only made on a need-to-know basis, must be fulfilled by CA signatories.

To ensure that these rules are adhered to, the descriptions will be updated and concretised as needed in the course of the project as part of the data management plan. The above regulations give rise to the intellectual property rules agreed upon by the Firelogue partners. Generally, they are as follows:

- Pre-existing partners' knowledge (background) are specified in the Consortium Agreement; Knowledge that is generated within the framework of Firelogue (foreground) shall remain the property of the partner that generated it. If more than one Partner generates that knowledge and it is not possible to separate their contributions, the knowledge will be jointly owned.
- Access rights to knowledge that is needed by a partner for the execution of its part in Firelogue shall be granted to the partner on a royalty-free non-transferable basis, unless otherwise agreed in the Consortium Agreement.
- A partner will not publish any knowledge provided by another partner and identified as confidential, without the other partner's prior written approval. However, if open source software licenses apply, the open source software license rules will apply for publishing knowledge.
- Dissemination assets will be submitted to the project coordinator and the dissemination leader and distributed to the other relevant partners who may object within a small-time period (no more than a month) which is agreed upon in the Consortium Agreement. Otherwise, the dissemination may proceed.

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020
RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

Partners will inform one another of planned publications well in advance of writing the publication to identify whether any additional partners with relevant insight are interested in being involved or to enable partners to raise any issues regarding the ownership of results included in the publication. Firelogue has also allocated a budget for covering the Article Processing Charge (APC) for publishing along the "gold open access" route. In this type of publishing, the version of the research paper is freely available immediately after publication without embargo.

Background IPR (pre-existing know-how) will be made accessible provided that the partner concerned is free to grant it and that this background is needed to carry out the activities foreseen. The consortium agreement will identify any background that partners will make freely available to partners for access and use, and any that is subject to commercial restrictions or payment of license fees. A partner may explicitly exclude specific background from its obligation before the start of the project. The other partners may only withhold their agreement if they demonstrate that the implementation of the project will be significantly impaired thereby.

Foreground IPR will be the property of the partner carrying out the work. Where several partners have jointly carried out work and where their respective share of work cannot be ascertained, they will have joint ownership of such foreground. Unless otherwise agreed, each of the joint owners shall be entitled to use their jointly owned results for non-commercial research activities on a royalty-free basis, and without requiring the prior consent of the other joint owner(s). Each of the joint owners shall be entitled to otherwise exploit the jointly owned results and to grant non-exclusive licenses to third parties (without any right to sub-license), if the other joint owners are given at least 45 calendar days advance notice.[6] Where relevant, repositories supporting open data principles (e.g. OpenAIRE's Zenodo) will be used.

Confidential information may not be disclosed, copied, reproduced or otherwise made available to third parties without the consent of the other parties. Each party agrees to use its best efforts to maintain confidentiality and to treat data and research materials as confidential until publication, licensing or until the filing of appropriate patent applications.

The Firelogue project's consortium will, in case of doubt, turn to the European Helpdesk for intellectual property (IP), which "helps European SMEs and beneficiaries of EU-funded research projects to manage their IP in the context of transnational companies or EU research and innovation programmes, free of charge."[7]

[6] The other party may request in writing to extend the examination period, due to the importance of the information disclosed.

[7] The European IP Helpdesk also provides support in identifying possible intellectual property (IP) infringement (https://intellectual-property-helpdesk.ec.europa.eu/regional-helpdesks/european-ip-helpdesk_en).

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

4 Data Management Plan

These considerations eventually feed into a data management plan (DMP). The outline detailed in Table 3 below presents an initial data management plan (which is based on Article 2.2.3.1 of the Firelogue Grant Agreement). It has been mentioned above that the DMP is considered as a dynamic document that will be uploaded and accessed through the collaboration tools set up under the project and will be regularly updated by the task leader, collecting contributions and suggestions from all partners. The DMP will be continuously enriched with data from the research activities.

Table 3: Firelogue Data Management Plan (DMP) V1.0

Types of data the project will generate / collect	Firelogue is expected to generate 3 types of data: (i) human participant data in relation to research and dissemination, (ii) data on those on the Firelogue mailing list, (iii) (qualitative) research data on synergies and conflicts between different sectors in managing WFRM.
Standards to be used	Project partners will adhere to the standards contained in, but not limited to: The General Data Protection Regulation, ISO/IEC 29100:2011 and ISO/IEC 27001:2005 - both on Security, Charter of Fundamental Human Rights of the European Union 2009, Council of Europe's Convention for the Protection of Individuals regarding Automatic Processing of Personal Data 1980, Guidelines on FAIR Data Management in Horizon 2020.
Data collection	The collection and use of personal data for research should be limited to include only that information which is legitimately and exclusively required and necessary to complete the specified task. Partners will limit the collection of sensitive personal data to the ones widely accepted to influence the adoption of DRM actions. The partners will ensure that any sensitive personal data collected will be anonymised and not able to be linked to the data subject protecting their rights. As such, the consortium will not publish personal information in the project reports and other published documents in a style that would enable the participant to be identified either directly or indirectly unless they wish otherwise. To ensure this, partners will abide by the principle and methodology of anonymisation, following recommendations, best practices, and anonymization techniques. Participants will be asked if their answers can be quoted directly. Interview participants will be invited to consent to the research interview itself and to the storage, preservation, opening and sharing of data.
How this data will be curated and preserved	The consortium will deposit its research data in a research data repository, e.g. Zenodo, which allows deposit of data and publications. Personal data will be stored in secure, encrypted systems. Furthermore, the appointment of data managers (and their deputies) will ensure the negotiation of access rights and (storage and metadata) standards for the course of the project. These authorities

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

	become particularly important in their role as contact persons and coordinators, when data sources are modified, added or interlinked.
Data security	The consortium will ensure data security (including data recovery, secure storage and transfer) and that data is safely stored in certified repositories (e.g. MS Sharepoint, Fraunhofer Owncloud, Fraunhofer INT local servers) for long-term preservation and curation. The data stored on the local Fraunhofer INT servers is protected by the highest security standards applying to the use of information and communication technology (ICT), as the premises are subject to official secrecy protection granted by the German Ministry of Defence (geheimschutzbetreutes Unternehmen).
Ethical and legal aspects	The Ethics Protocol (as specified in D7.3) describes the procedures for ensuring compliance with ethical standards and points out aspects that require special attention. As it also deals with the collected personal data and the protection measures to be taken within the project, there is a close link between the DMP and the Ethics Protocol. Both, the Ethics Protocol and DMP will review and address any ethical or legal issues that might impact data sharing. In case they arise, the procedures for addressing ethical and legal issues related to project data management will be outlined in future updates to the DMP.
Management of knowledge and intellectual property	One of the main tasks of Firelogue will be to manage and disseminate the knowledge of the IAs. Hence, the project will mainly include meta-information in its platform. The Firelogue project will, however, generate proprietary data and knowledge, some of which will be confidential and some of which will be for dissemination and communication to the public. Firelogue will handle IPR as follows: The joint Consortium Agreement addresses (a) confidentiality of the information disclosed by Partners during the project, ownership of results resulting from the execution of the project, (b) legal protection of results deriving from the execution of the project through patent rights, (c) commercial utilisation of results, also taking into account joint ownership of the results, (d) patents, know-how and information related to the use of knowledge owned by one of the partners, resulting from work carried out prior to the agreement and (e) sub-licenses to third parties within clearly defined limits. To ensure these goals are achieved, the description will be updated if and as required during the project. The general outline of the intellectual property rules agreed by Firelogue partners is as follows: Pre-existing partners' knowledge (background) has been specified in the Consortium Agreement; Knowledge that is generated within the framework of Firelogue (foreground) shall remain the property of the partner that generated it. If more than one partner generates that knowledge and it is not possible to separate their contributions, the knowledge will be jointly owned.

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

	Access rights to knowledge that is needed by a partner for the execution of its part in Firelogue shall be granted to the partner on a royalty-free non-transferable basis, unless otherwise agreed in the Consortium Agreement. A partner will not publish any knowledge provided by another partner and identified as confidential, without the other partner's prior written approval. However, if open source software licenses apply, the open source software license rules will apply for publishing knowledge. Dissemination assets will be submitted to the Project Coordinator and the Dissemination Leader and distributed to the other relevant Partners who may object within a short period (no more than a month) which is agreed upon in the Consortium Agreement. Otherwise, the dissemination may proceed. Regarding the publishing of results, e.g. in academic journals, Firelogue will privilege self-archiving, i.e. the published article or the final peer-reviewed manuscript is archived by the researcher - or a representative - in an online repository before, after or alongside its publication ("green open access"). Moreover, partners will inform one another of planned publications well in advance of writing the publication to identify whether any additional partners with relevant insight are interested in being involved or to enable partners to raise any issues regarding the ownership of results included in the publication. Firelogue has also allocated a budget for covering the Article Processing Charge (APC) for publishing along the "gold open access" route. In this type of publishing, the version of the research paper is freely available immediately after publication without embargo. Background IPR (pre-existing know-how) will be made accessible provided that the Partner concerned is free to grant it and that this background is needed to carry out the activities foreseen. The consortium agreement has already identified any background that partners will make freely available to Partners for access and use, and any that is subject to commercial restrictions or payment of license fees. A partner may explicitly exclude specific background from its obligation before the start of the project. The other partners may only withhold their agreement if they demonstrate that the implementation of the project will be significantly impaired thereby. As mentioned above, Foreground IPR will be the property of the partner carrying out the work unless several partners have jointly carried out work and where their respective share of work cannot be ascertained, they will have joint ownership of such foreground. Firelogue promotes the use of repositories that support the principles of open science (e.g. Zenodo by OpenAIRE, Open Research Europe).

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

5 Outlook

The DMP will be updated and revised throughout the project whenever significant changes occur, such as (but not limited to): Introduction of new data types, changes in consortium policy, or changes in consortium composition and external factors (e.g. new consortium members joining or old members leaving). One such case is the Firelogue platform. Once the platform is developed and operational, data sharing policies will be redefined and each partner organisation will appoint a data manager (and a deputy data manager) reporting to the consortium leader. These designated individuals will be given access to sensitive personal or classified data for which they are liable.

Efforts will be made to update the DMP at the same time as the periodic evaluation/assessment of the project. Regular reporting will be sought to take account of developments in data processing.

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020
RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

Selected References

Amnesia V1.3.1. Open Air Advance ONLINE: https://amnesia.openaire.eu/index.html [last accessed: 20 March 2022]

Article 29 Working Party – European Commission (2016). ONLINE: https://ec.europa.eu/justice/article29/documentation/opinionrecommendation/files/2014/wp216_en.pdf [last accessed: 20 March 2022].

European Commission, Executive Agency for Small and Medium-sized Enterprises, *Your guide to IP in Horizon 2020*, Publications Office (2019). https://data.europa.eu/doi/10.2826/002896 [last accessed: 23 March 2022].

European Commission, Executive Agency for Small and Medium-sized Enterprises, *European IP Helpdesk factsheet: joint ownership* (2022). ONLINE: https://data.europa.eu/doi/10.2826/865944 [last accessed: 23 March 2022].

European IP Helpdesk. ONLINE: https://intellectual-property-helpdesk.ec.europa.eu/regional-helpdesks/european-ip-helpdesk_en [last accessed: 20 March 2022].

European Union. (2016). *Charter of Fundamental Rights of the European Union – 2016*. Official Journal C202, 7 June, pp. 389-405.

The Fair Data Principles FORCE11 (2021). ONLINE: https://force11.org/info/the-fair-data-principles [last accessed: 21 March 2022].

Martín, D., Vendrell, J., Prat, N., Borràs, M. (2022). Stakeholder clustering report. Deliverable D7.2 FIRELOGUE.

Open Reseach Europe (ORE). European Commission. https://open-research-europe.ec.europa.eu/ [last accessed: 25 March 2022].

Owncloud Fraunhofer. ONLINE: https://owncloud.fraunhofer.de/index.php/login; https://www.fraunhofer.de/de/datenschutzerklaerung.html [last accessed: 11 February 2022].

Petersen, K., Pettinari, M. L., Overmeyer, M. (2022). Ethics Protocol and Equality Management Plan. Deliverable D7.3. Firelogue.

RealtimeBoard, Inc. dba Miro, Privacy Policy (2021). ONLINE: https://miro.com/legal/privacy-policy/ [last accessed: 15 February 2022].

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (OJ L 119 04.05.2016, p. 1, ONLINE: CELEX: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX. [last accessed: 11 February 2022].

The Plan for the Exploitation and Dissemination of Project Results in Horizon (2020). ONLINE: https://www.iprhelpdesk.eu/sites/default/files/newsdocuments/Fact-Sheet-Plan- for-the-Exploitation-and-Dissemination-of-Results-H2020.pdf [last accessed: 15 February 2022].

Wilkinson, M., Dumontier, M., Aalbersberg, I. et al. (2016). The FAIR Guiding Principles for scientific data management and stewardship. Sci Data 3, 160018.

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

Zenodo. OpenAIREplus. ONLINE: https://zenodo.org/ or https://www.openaire.eu/zenodo/ [last accessed: 09 February 2022].

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020
RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534

Firelogue

THIS IS THE END OF THIS DOCUMENT

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020
RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 101036534