



## **Proactive FET Observatory for early trends, project building and social responsibility**

Call - FET Open – Novel ideas for radically new technologies  
FETOPEN-02-2018: FET-Open Coordination and Support Actions  
Subtopic c: FET Observatory

---

### **Deliverable No. D1.3**

### **Data Management Plan**

**This project has received funding from the  
European Union's Horizon 2020 Research and Innovation Programme  
Under Grant Agreement no.824748**



## Document Control

Deliverable	D1.3 Data Management Plan
WP/Task Related	WP1 – Project Management
Delivery Date	17/09/2019
Dissemination Level	Confidential, only for members of the consortium (including the Commission Services)
Lead Partner	LINKNOVATE – Manuel Noya
Contributors	<ul style="list-style-type: none"><li>• TRI – Agata Gurzawska</li><li>• RTDI – Eva García Muntión</li><li>DMU – Martin de Heaver, Paul Keene</li></ul>
Reviewers	RTDI – Eva García Muntión TRI – David Wright
Key Words	Big data, Data sharing, Data storage, Data access, Fair use, GDPR, Data Mining, Search, Information Retrieval, Data Processing, Open access

## Revision History

Version	Date	Notes
V0.0	09/04/2019	Draft contents by RTDI
V1.0	22/07/2019	First complete draft, by LINK
V2.0	4/09/2019	Edits by LINK for 2 <sup>nd</sup> draft
V2.1	5/09/2019	Additions by TRI and DMU into the 2 <sup>nd</sup> draft
V2.2	9/09/2019	Review, TRI
V2.3	16/09/2019	Additions by TRI sections: 2, 7, 8, 9, 10, Appendix 2
V2.4	16/09/2019	Additions by DMU, Appendix 1
V2.5	17/09/2019	Additions by LKN
V3	17/09/2019	Final revision and check for submission by RTDI

## Content

<b>1. Introduction</b>	<b>4</b>
<b>2. Data Summary</b>	<b>4</b>
2.1 Applicable standards, guidelines and principles	5
2.2 Purposes and legal basis of personal data processing	6
<b>3. FAIR Data</b>	<b>8</b>
3.1 Making data findable, including provisions for metadata	8
3.2 Making data openly accessible	8
3.3 Making data interoperable	9
3.4 Increase data reuse	9
<b>4. FAIR data allocation of resources</b>	<b>9</b>
<b>5. Data security</b>	<b>10</b>
<b>6. Ethical aspects</b>	<b>11</b>
<b>7. Allocation of resources</b>	<b>12</b>
<b>8. Responsibilities</b>	<b>12</b>
<b>9. Management of compliance</b>	<b>12</b>
<b>10. Conclusion</b>	<b>12</b>
<b>APPENDIX 1: WWW.PREFET.EU</b>	<b>13</b>
APPENDIX 1.A: PREFET SURVEY – INFORMED CONSENT FORM	13
APPENDIX 1.B: Website terms & conditions	15
<b>APPENDIX 2: PREFET Legitimate interest assessment (LIA) of the creation of contact lists for stakeholder engagement and dissemination of information</b>	<b>23</b>

# 1. Introduction

PREFET has been chosen to participate in the Open Research Data Pilot (<https://www.openaire.eu/opendatapilot>), which aims to make the research data generated by selected Horizon 2020 projects accessible with as few restrictions as possible, while at the same time protecting sensitive data from inappropriate access.

The Data Management Plan (DMP) addresses the life cycle of the data to be collected, processed and generated by the project. In order to make research data findable, accessible, interoperable and re-usable (FAIR), during the project all partners will invest strong efforts for gathering information related to:

- the handling of research data during and after the end of the project
- what data will be collected, processed and/or generated
- which methodology and standards will be applied
- whether data will be shared/made open access
- how data will be curated and preserved (including after the end of the project).

Following the EU's guidelines regarding Data Management Plans, this document will be reviewed, revised, and updated as needed during the project (within Project Periodic Report, **D1.2**).

This DMP contains the specification and availability of data, including what data the project will generate, whether and how it will be made accessible for verification and re-use, and how it will be curated and preserved. It is structured as recommended in the template for DMP in [Guidelines on FAIR Data Management in Horizon 2020](#).

## 2. Data Summary

PREFET aims to deliver tools and methodologies to pre-validate trending future and emerging technologies (FET), providing the responsible research and innovation (RRI) context. These tools and methodologies will support FET successful implementation and help researchers improve their project building integral processes of FET-like ideas at early stages for good planning and decision making.

These goals will be achieved by developing a methodology platform with specialised unique tools enabling a systematic identification of new and emerging technologies beyond the FET portfolio, on the one hand, and by supporting researchers in their early-stage decision and ideation steps, on the other hand.

For identifying new and emerging technologies beyond the FET portfolio, different open and publicly available data sources will be both humanly and automatically scouted to detect, identify and “predict” which emerging ideas have the best projections. These data sources

include Science and Technology sources like scientific publications conferences proceedings, patents, grants, specialised news and web monitoring; and other sources beyond the S&T landscape like science fiction literature and TV series, blogs, social media, and others.

Once we have detected which emerging ideas have the best projections, we will identify the most promising researchers working on them (mainly based on the scientific research they have published, which is publicly available data that includes their name and contact details). Furthermore, to support these researchers in their early-stage decision and ideation steps, they will be offered to join a 2-months capacity building program named IdeAcademy to help them develop innovation skills.

All relevant information, peer-reviewed scientific publications and similar documents that do not contain sensitive data will be made available in an open-access format. This will also include the reports, roadmaps, presentations from panels and workshops, and so on.

The data will be collected in different formats like (but not limited to) text documents, PDFs, html pages, RSS feeds, online videos, images, and podcasts. It will be processed to generate different analysis reports and data visualisations to identify the emerging trends and the FET-like candidates.

Likewise, all the training materials to be provided in the IdeAcademy courses will be generated and disseminated in different formats like (but not limited to) videos, PDFs, podcasts, and images.

Analytical data will be anonymised. Personal data will not be gathered and used, and by no means in other contexts than the PREFET project. Only professional, scientific and business-related data will be collected. Third parties will not have access to these data.

In summary, this DMP covers two types of data subject to FAIR use:

- a) The open and publicly available data collected and to be analysed by the consortium.
- b) The insights (in form of data visualisations, reports, and deliverables), the training materials and the dissemination materials generated by the consortium.

## 2.1 Applicable standards, guidelines and principles

The PREFET project will follow the below-listed standards, guidelines and principles in the management of its data collection, use, sharing and preservation:

- European Parliament and the Council, Regulation (EU) 2016/679 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 or GDPR)<sup>1</sup>

---

<sup>1</sup> 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)

- European Commission Directorate-General for Research & Innovation, H2020 Programme Guidelines on FAIR Data Management in Horizon 2020, Version 3.0, 26 July 2016<sup>2</sup>
- European Commission, H2020 Programme Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020, Version 3.2 21 March 2017<sup>3</sup>
- Research integrity standards, for instance, in the ALLEA European Code of Conduct for Research Integrity<sup>4</sup>
- Applicable national data protection regulations.

## 2.2 Purposes and legal basis of personal data processing

The project will collect and process personal data only if, and insofar as, it is necessary for its research and engagement activities, i.e., research, consultations and events, and to share its findings and results with stakeholders via mailings and the website. Our primary legal basis for processing personal data are:

- The processing of personal data with the **consent** of the individual (the data subject) (Article 6(1)(a) of GDPR)
- Processing necessary for the legitimate interests pursued by the controller or by a third party (Article 6(1)(f) of GDPR)

**Appendix 1** shows the participant information sheet and informed consent form used for Open Trend Consultation as part of task T2.3.

**Appendix 2** provides a legitimate interest assessment (LIA) conducted by PREFET partners. Each partner keeps a signed copy of LIA on file. We will inform our contacts that we are relying on legitimate interest for the processing of their contact details, and we will explain what this interest is especially to draw to the attention of FET stakeholders, our target stakeholders, the results of our project and how those results can help them in their efforts in building successful FET-like projects. We understand that if we want to process the personal data for a new purpose, we may be able to continue processing under the legitimate interest provision as long as our new purpose is compatible with our original purpose. If necessary or useful, we will conduct a new LIA to demonstrate compliance with the legislation. At this stage and in accordance to the consortium's grant agreement with the EC, the partners do not envisage repurposing this data.

We will keep this record of our LIA on file in order to demonstrate compliance with legislation, if required. We will keep our LIA under review, and repeat it if circumstances change.

Table 1 identifies the PREFET activities that collect personal data, purposes of the collection, types of data that will be processed, its storage formats, modes of collection, sharing, location, accountability and access arrangements. PREFET will mostly collect personal data that is largely

---

<sup>2</sup> [https://ec.europa.eu/research/participants/data/ref/h2020/grants\\_manual/hi/oa\\_pilot/h2020-hi-oa-data-mgt\\_en.pdf](https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf)

<sup>3</sup> [http://ec.europa.eu/research/participants/data/ref/h2020/grants\\_manual/hi/oa\\_pilot/h2020-hi-oa-pilotguide\\_en.pdf](http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilotguide_en.pdf)

<sup>4</sup> [https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics\\_code-of-conduct\\_en.pdf](https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf)

available in the public domain. Project partners will collect such data from respondents from EU and non-EU countries. Personal data may be collected from members of the consortium, members of external organisations or individuals in their capacities as experts, respondents or participants.

Activity/task/W P (and purpose)	Type of personal data being processed	Storage format	Mode of collection	Sharing	Location	Account ability	Access
T2.1 AI Massive Data Consultation, T2.2 Manual Scanning and T3.3 Trendington Purpose: to develop contacts for PREFET project research and engagement activities	Name, title, organisation, email, key activities/relevance to PREFET	xlsx, doc, csv	From project partner networks, from publicly available sources only and the subscription form on PREFET website	Internal only; restricted	Local hard drives, password protected In the case of personal network contacts: email provider (password protected)	DMU, LKN, RTDI, TRI	Restricted to PREFET partners.
T2.3 Open Trend Consultation	Name, title, organisation, email, key activities/relevance to PREFET, number of years of experience in specific area	Xlsx, csv	From project partner networks, from publicly available sources only and the subscription form on PREFET website	Internal only; restricted	Local hard drives, password protected In the case of personal network contacts: email provider (password protected)	DMU, LKN, RTDI, TRI	Restricted to PREFET partners.

**Table 1 PREFET personal data mapping**

**Note: Table shows activities carried out in the first reporting period. It will be updated in D1.2 Periodic Project Report at the end of the second period.**

Regarding task T2.3, led by DMU, the PREFET Survey’s Informed Consent Form and Website Privacy Policy<sup>5</sup> and Terms & Conditions<sup>6</sup> have been shared with all participants and made publicly available (attached in the Appendix 1A and 1B).

PREFET considers that email extraction from academic records (i.e., scientific publications and conference proceedings), following data mining processing at Linknovate, constitutes **fair use** of a professional contact email for professional purposes. The rationale behind the contact is three-fold:

1. Contact about the professional topic related to the expert professional activities (e.g., homomorphic encryption experts would only receive the survey because they have been identified to co-author a publication in that space).

<sup>5</sup> <https://www.prefet.eu/terms-conditions/>

<sup>6</sup> <https://www.prefet.eu/terms-conditions/>

2. Contact for professional purposes: to provide feedback for trend identification, in an activity that supports EC roadmapping and policymaking. The ultimate goal is to improve and support the research activities in which these professionals are immersed.
3. Contact info is provided by the author/co-author of the publication precisely for the purpose of fostering academic and research collaborations, like the ones PREFET pursues.

## 3. FAIR Data

### 3.1 Making data findable, including provisions for metadata

FAIR stands for data that is Findable, Accessible, Interoperable and Reusable. The data produced and/or used in the project will be discoverable with metadata, and communication with CORDIS data service, and open access repositories will be in place. Naming conventions for metadata have not yet been defined, but will be in place once public reports and dynamic web applications are presented to the public and their reuse and visibility promoted.

End data products to be produced by PREFET, such as reports, whitepapers, datasets, etc. will have version numbers; although we anticipate several of the more basic datasets (data visualisations, for instance) will be dynamic in nature. Also, some providers of publicly available data may not define versions.

### 3.2 Making data openly accessible

PREFET covers two types of data subject to FAIR use:

- a) The open and publicly available data collected and to be analysed by the consortium.
- b) The insights, training materials and dissemination materials generated by the consortium (in form of data visualisations, reports, images, videos, audios, and deliverables).

Regarding the non-confidential and non-personal data to be analysed by the partners, it is publicly available in data repositories and in different websites to be used and consulted by anyone. Sensitive project data has been kept in RTDI's own server complying with GDPR regulation.

Data access (access logs) are monitored for suspicious activity; other security measures include the use of individual logins and passwords and encryption of back-ups.

As for the data and insights generated by the consortium, part of it will be open and part will have a commercial use to further explore the sustainability of the methodology, technologies and services developed under PREFET.

The PREFET Portal (<https://www.prefet.eu/>) and the training platform IdeAcademy will be the key tools to make the data and data products accessible to a broad range of stakeholders, including researchers, academia and the industry. Access will be possible for both verification



and re-use purposes and the training platform will contain view, search and visualisation services alongside standardised view- and download-features.

Software needed to access data that will be made publicly available is not expected, aside from (dynamic) web applications to “play” and visualise data insights (e.g., pre-validated trends, final trend selection, outcomes from the Trendington, presentations).

The consortium will consider the different types of data, associated metadata, documentation, and code that will be made public to be deposited in certified repositories, such as [OpenAire](#) (the consortium will explore appropriate arrangements with the repository), and in the project’s website (<https://www.prefet.eu/>).

Registered access to the data (e.g., training courses, data insights, graphics, etc.) accessible via the project’s website will be required via log-in. However, the data hosted in OpenAire will be publically available (complying with the repository policy) and no logs will be required.

### 3.3 Making data interoperable

The consortium will have a focus on the interoperability of the data produced. The consortium will allow for data exchange and re-use between researchers, institutions, organisations, countries and others.

In order to make the data produced in the project interoperable and consumable, the consortium will explore the possibility to use CERIF (the Common European Research Information Format) for the data that is not restricted (data produced by the consortium); and when possible (e.g., information retrieval efficiency is not a concern).

Interoperability in the OpenAIRE repository, which PREFET considers a preference, is a key focus, and in constant evolution, as it poses a big challenge not only for datasets to be able to “communicate” with repositories, but for repositories to communicate among themselves. A roadmap for the CERIF-XML profile was put in place in the workshop in U Minho by OpenAIRE in 2013 and updated in April 2018.

### 3.4 Increase data reuse

Increase data re-use (through clarifying licences): in order to permit the widest re-use possible of the data, the openly accessed datasets will be CC-BY licensed, requiring attribution (giving the author or licensor the credits in the manner specified) but allows for copying, distributing, displaying and performing the work and making derivative works and remixes based on it.

## 4. FAIR data allocation of resources

Considering the amount of data analysed during the project, PREFET could be considered as a data intensive project. Nonetheless, data processing is reduced in terms of collection and periodicity during the project lifetime, hence reducing the data management process complexity. For this reason, we estimate the costs for making the data FAIR between one and

two persons month. Costs associated with the data gathering, cleaning and indexing, as well as open access capacities of research data have been considered in the grant agreement.

The project partner in charge of the lead of the data management in the project is LINK. All partners are responsible to contribute to the DMP and the *fair data* use.

The consortium will preserve the data preservation for five years after the EC has paid the balance of its funding to PREFET partners. Longer term data preservation will be considered with the mentioned data repositories (e.g. openAIRE) and the project website.

## 5. Data security

Provisions for data security will differ depending on the nature of the data.

Information coming from open datasets will not receive any special treatment (e.g., datasets not including personal information shared by experts over email, by organisations and by public authorities). This information will be directly processed as it arrives to the platform and then indexed. Temporal copies of the original data will be kept in PREFET's information processing nodes, but no extra security measures will be put in place for this kind of information given its public nature.

Confidential Information in the consortium and information including personal information will be shared in a common repository maintained by the coordinator (see full description in **D1.1**).

Example: Sensitive project data has been kept in RTDI own server complying with GDPR regulation:

<http://myowncloud.rtdi.eu/index.php/apps/files/?dir=/PREFET&fileid=4349>

Each partner accesses it with a user and password.

Data access (access logs) are monitored for suspicious activity. Other security measures include encryption of back-ups.

Information from restricted datasets shared with the consortium will be uploaded via SFTP<sup>7</sup> by partner LINKNOVATE, given it provides secure file transfer and manipulation functionality over any reliable data stream. Information will be stored in a dedicated GNU/Linux server with state-of-the-art safety measures. Access policies to the server will be restricted to LINK employees, who have signed appropriate non-disclosure agreements (NDAs). Weekly incremental backups are planned in a secondary, equally secure repository. Nonetheless, so far (M10), it has not been

---

<sup>7</sup> SFTP, which stands for SSH File Transfer Protocol, or Secure File Transfer Protocol, is a popular protocol packaged with SSH (Secure Shell) for transferring files between two remote systems over a secure connection.

foreseen any such data sharing tasks and it is not anticipated that it will be needed during project lifetime.

Regarding data and cybersecurity, the following standard measures are in place in order to reduce the risk:

- End to end encryption of data in transition.
- Encryption of sensitive data at rest in order to minimise the exposure to a non-authorised access event.
- Periodic vulnerability testing of the secure servers.
- Standardised enforced data deletion policy of sensitive data when required by a user.
- Advance user-level data security measures with fine-grained access control.

Regarding personal information, we will act according to the GDPR and comply with the applicable measures for controlling personal data. We will act according to the procedures of the local Data Protection Agency (AGPD<sup>8</sup>). In that case, Sabela Cereijo, as our Data Protection Delegate, will coordinate the data processing activities and will be in charge of the risk analysis over the personal data.

According to the GDPR and AGPD regulations, we will communicate immediately any breach of the security controls over the personal data.

## 6. Ethical aspects

The PREFET consortium has not identified any specific ethical issues related to the work plan, outcomes or dissemination, as the project core activities does not deal with personal data (other than the Open Trend Consultation email campaigns explained above), medical data, biology, gender, sex, political views or religion.

The data management and compliance team are undertaking a significant review of all policies and procedures on ethics and data use. We continue to work on the current data protection policy with the commitment to protect and process data with adherence to current legislation and policies.

The project adheres to the commitment to holding any data in secure conditions and will make every effort to safeguard against accidental loss or corruption of data.

FET-like candidates, researchers and advisors will participate in the project based on informed consent, may withdraw at any time, and are able to request information not to be published. Informed consent forms describe how data is stored and used and how confidentiality is maintained in the long-term. Measures include data anonymisation, aggregating individual-level data and generalising the meaning of detailed text.

---

<sup>8</sup> <http://www.agpd.es>

## 7. Allocation of resources

The PREFET project has a specific task dedicated to data management - “Task 1.3: Data Management.” This task is led by Linknovate and supported by contributions from the Trilateral Research and De Montfort University. Specific human efforts has been allocated to this task over the duration of the project, and are continuously monitored as part of WP1 activities (fully reported in **D1.2**).

## 8. Responsibilities

The planning and overall co-ordination of the data management task will be the responsibility of Linknovate. Each project partner who handles and is responsible for data collected, stored or used will ensure compliance with the strategy outlined in this document. Linknovate will review and revise this plan, consult with partners and implement any corrective actions, if required. Revisions to the DMP may become necessary in the following cases: new or unanticipated datasets become available, existing datasets are re-classified into a different data sharing category due to emerging/newly discovered data privacy or commercial concerns, or external factors, including changes to data protection law, the removal of a project partner, or technological advancements that could impact data security. PREFET partners should notify Linknovate if any such cases arise and advise of any updates to their institutional data management policies and procedures that might have an impact on PREFET’s data management.

## 9. Management of compliance

Linknovate will oversee compliance with the data management plan along with RTDI (project co-ordinator). Each PREFET partner will be responsible for adhering to the strategy and procedures outlined in this document and other relevant documents.

## 10. Conclusion

This deliverable presented the PREFET consortium’s plan to manage the production, collection and processing of its research data and scientific publication. This deliverable will be reviewed by the consortium in the final year of the project. Updates will be made to the plan to take into account new data, changes in consortium policies, and external factors (reported under D1.2). Each project partner handling and responsible for data collected, stored or used in PREFET will ensure compliance with the strategy outlined in this document.

# APPENDIX 1: [WWW.PREFET.EU](http://WWW.PREFET.EU)

## APPENDIX 1.A: PREFET SURVEY – INFORMED CONSENT FORM

### **Important Information**

The EC has tasked PREFET with choosing the top 50 trends in Future and Emerging Technologies. Results of this survey will directly influence research funding policy at the European level for the coming years.

Also, by providing a detailed response to this survey, you:

- Could be selected to join a group of leading experts to select the top 15 trends in Environment/Climate, ICT & Biotech/Health. This will take place during an event in Madrid 21/11/2019.
- Will get early access to the insights and details we have learnt about each trend through AI-supported technology scouting (subtrends, networking opportunities...).

Please take time to read the information here carefully and ask us if there is anything that is not clear or if you would like more information.

Joining this Survey is entirely up to you; you do not have to take part. If you decide to take part, we ask you to agree to this consent form by clicking next. If you agree to join, you may stop your participation at any time without any impact to you.

### **Survey Overview**

As a participant in the PREFET Survey on key emerging science-based technologies, you will be asked some questions on key trends and sub-trends towards the future of science and technology in the world in general and Europe in particular. We ask for answers to be objective and based on your expertise and deep knowledge.

In the first section, we ask for some statistical information that will help completing the perspective around the answers received: area of expertise and years of experience in the area, from which type of organisation has this experience been developed, gender, age and nationality.

### **Study Procedures**

After you have clicked **NEXT** and have agreed to this consent form, we will provide you access to the PREFET Survey. You will be able to answer the survey remotely. The questionnaire is divided into sections. Completing all sections will take about an hour.

We will use your User ID only for statistical analysis. We will anonymise and aggregate survey results.

### **Confidentiality**

Only PREFET consortium partners and the European Commission will have the right to look at survey records. You have the right to see your records and statistics.

Consortium partners may present the results of this survey at scientific meetings or in publications. However, your identity will not be disclosed at any time. The consortium will fully comply with the EU General Data Protection Regulation. Questions: You are free to ask questions at any time. If you would like to know more about our research, please e-mail [evagarcia@rti.eu](mailto:evagarcia@rti.eu).

### **Voluntary Participation / Withdrawal**

Your participation in this survey is purely voluntary. You may refuse to join or withdraw at any time with no penalty.

Although we do not expect it to happen, we advise all participants that the survey could be cancelled at any time without their consent, either by the PREFET project management board or by the European Commission to which the consortium reports. Otherwise, the survey will run from **1 June 2019** to **31 October 2019**.

### **Acceptance**

Please note that, at the behest of the European Commission, the PREFET project co-ordinate will store your signed consent form for five years from the date of your signature.

## APPENDIX 1.B: Website terms & conditions

### **Preamble**

Please read the following Terms of Service (hereinafter “Agreement”) carefully before accessing or using this website (hereinafter “Website”).

The Website is offered subject to your acceptance without modification of all of the terms and conditions contained herein.

IF YOU DO NOT AGREE TO ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT, THEN YOU MAY NOT ACCESS THE WEBSITE, POST MATERIAL ON THE WEBSITE OR DOWNLOAD MATERIAL ON THE WEBSITE OR USE ANY SERVICES.

### **Ownership and Operation of Website**

The Website is owned and operated by the PREFET project, a collaboration between De Montfort University and the University of Oxford, funded by the UK Engineering and Physical Science Research Council.

### **Scope of the Terms of Service**

The following terms and conditions of this Agreement govern all use of the [www.PREFET-rrri.org](http://www.PREFET-rrri.org) website and all content, services and products available at or through the website.

### **Amendments to the Terms of Service**

PREFET reserves the right, at its sole discretion, to modify or replace any part of this Agreement at any time, without prior notice. It is your responsibility to check this Agreement periodically for changes. YOUR CONTINUED USE OF OR ACCESS TO THE WEBSITE FOLLOWING THE POSTING OF ANY CHANGES TO THIS AGREEMENT CONSTITUTES ACCEPTANCE OF THOSE CHANGES. PREFET may also, in the future, offer new services and/or features through the Website (including, the release of new tools and resources). Such new features and/or services shall be subject to the terms and conditions of this Agreement.

### **Purpose of the Website**

The Website promotes the purposes of PREFET, i.e. to foster awareness and a culture of responsible research and innovation (RRI), in particular in the area of ICT. It does this by providing resources, explaining and delivering PREFET services, hosting the PREFET journal and creating a community of users interested in RRI.

### **Creation of an account – user’s responsibility**

Some of the services available on this Website require prior registration. You must provide correct and complete information when registering, and update it if necessary. You must not misuse any access authorisation granted to You (for example by transferring data to unauthorised third persons). By registering, You agree to being contacted by the PREFET team via email.

If you create an account on the Website, You are responsible for maintaining the security of your account and are fully responsible for all activities that occur under the account. You must immediately notify PREFET of any unauthorized uses of your account or any other breaches of security. PREFET will not be liable for any acts or omissions by You, including any damages of any kind incurred as a result of such acts or omissions.

### **User contributions**

If You post material to the Website, post links on the Website, or otherwise make (or allow any third party to make) material available by means of the Website (any such material, “Content”), You are entirely responsible for the content of, and any harm resulting from, that Content, regardless of the format of the Content (e.g. text, graphics, an audio file, or computer software).

In particular:

- You may not upload any viruses, worms, Trojan horses, or other forms of harmful computer code, nor subject the Website’s network or servers to unreasonable traffic loads, or otherwise engage in conduct deemed disruptive to the ordinary operation of the Website;
- You are strictly prohibited from communicating on or through the Website any unlawful, harmful, offensive, threatening, abusive, libelous, harassing, defamatory, vulgar, obscene, profane, hateful, fraudulent, or otherwise objectionable material of any sort, including, but not limited to, any material that encourages conduct that would constitute a criminal offense, give rise to civil liability, or otherwise violate any applicable local, state, national, or international law.

Notwithstanding anything to the contrary, PREFET does not want to receive confidential or proprietary information from You through the Website. Any material, information, or other communication You transmit or post to the Website will be considered non-confidential.

PREFET has the right (though not the obligation) to, at PREFET’s sole discretion, (i) refuse or remove any content that, in PREFET’s reasonable opinion, violates any PREFET policy or is in any way harmful or objectionable, or (ii) terminate or deny access to and use of the Website to any individual or entity for any reason.

### **Links to other websites**

The Website may have links to third party websites. Such links to third party websites lie outside the scope of responsibility of PREFET.

By linking to a non-PREFET website or webpage, PREFET does not represent or imply that it endorses such website or webpage. You are responsible for taking precautions as necessary to protect yourself and your computer systems from viruses, worms, Trojan horses, and other harmful or destructive content. PREFET disclaims any responsibility for any harm resulting from your use of non-PREFET websites and webpages. Access and use of such websites occurs entirely at the your own risk. PREFET expressly states that it has no influence whatsoever over the content of any linked site. Responsibility for information and services of linked sites rests entirely with the relevant third parties. PREFET can in no case be held liable in respect of the content of such websites.



## **Intellectual Property**

This Agreement does not transfer from PREFET to You any PREFET or third party intellectual property or license to use any Content, and all right, title and interest in and to such property will remain solely with PREFET or such third party as the case may be. Your use of the Website grants You no right or license to reproduce or otherwise use any PREFET or third-party trademarks.

## **General warranty by User**

You represent and warrant that (i) your use of the Website will be in strict accordance with the PREFET Privacy Policy, and other guidelines, with this Agreement and with all applicable laws and regulations and (ii) your use of the Website will not infringe or misappropriate the intellectual property rights of any third party.

## **Indemnification by User**

You agree to indemnify and hold harmless PREFET, and its respective directors, officers, employees and agents from and against any and all claims and expenses, including attorneys' fees, arising out of your use of the Website, including but not limited to your violation of this Agreement.

## **No warranty**

The Website and its Content are provided on an "as is" and "as available" basis. PREFET makes no warranty of any kind, express or implied, as to the Website, including, but not limited to:

- warranties of merchantability and fitness for a particular purpose;
- warranties of non-infringement of intellectual property;
- warranties that the Website will meet your requirements;
- warranties that your use of the Website will be uninterrupted, timely, secure, or error free;
- warranties as to the results that may be obtained from the use of the Website.
- warranties as to the operation of the Website or the information, Content, materials, or products included on the Website.

By operating the Website, PREFET does not represent or imply that it endorses the material there posted, or that it believes such material to be accurate, useful or non-harmful. You are responsible for taking precautions as necessary to protect yourself and your computer systems from viruses, worms, Trojan horses, and other harmful or destructive content. The Website may contain content that is offensive, indecent, or otherwise objectionable, as well as content containing technical inaccuracies, typographical mistakes, and other errors. The Website may also contain material that violates the privacy or publicity rights, or infringes the intellectual property and other proprietary rights, of third parties, or the downloading, copying or use of which is subject to additional terms and conditions, stated or unstated.

You understand and agree that any content downloaded or otherwise obtained through the use of the Website is at your own discretion and risk and that you will be solely responsible for any damage to your computer system or loss of data or business interruption that results from the

download of content. PREFET shall not be responsible for any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information or ideas contained, suggested or referenced in or appearing on the Website. Your participation in the Website is solely at your own risk. No advice or information, whether oral or written, obtained by you from PREFET or through PREFET, its employees, or third parties shall create any warranty not expressly made herein. You acknowledge, by your use of the Website, that your use of the Website is at your sole risk.

### **Limitation of liability**

In the event that under applicable law, PREFET may be liable for any direct damages arising out of this Agreement, such liability will be limited to acts of fraud or gross negligence. Under no circumstances and under no legal or equitable theory, whether in tort, contract, negligence, strict liability or otherwise, will PREFET, its suppliers or licensors be liable to user or to any other person for any indirect, special, incidental or consequential losses or damages of any nature arising out of or in connection with the use of or inability to use the Website or for any breach of security associated with the transmission of sensitive information through the Website or for any information obtained through the website, including, without limitation, damages for lost profits, loss of goodwill, loss or corruption of data, work stoppage, accuracy of results, or computer failure or malfunction, even if an authorized representative of PREFET has been advised of or should have known of the possibility of such damages.

### **Severability**

If any provision of this Agreement is for any reason held to be illegal, void or unenforceable, the remainder of the provisions shall continue to be valid and enforceable.

### **Termination**

PREFET may terminate your access to all or any part of the Website at any time, with or without cause, with or without notice, effective immediately. If You wish to terminate this Agreement or your PREFET account (if you have one), you may simply discontinue using the Website. All provisions of this Agreement which by their nature should survive termination shall survive termination, including, without limitation, ownership provisions, warranty disclaimers, indemnity and limitations of liability.

### **Governing law/jurisdiction**

This Agreement is governed by the substantive laws of England, without regards to principles of conflicts of laws thereof.

Any controversy, claim or dispute between PREFET and you arising out of or in relation with this Agreement shall be subject to the exclusive jurisdiction of the ordinary courts of Leicester, UK.

### **Privacy Policy**

#### **What is this Privacy Policy for?**

The policy sets out the different areas where user privacy is concerned and outlines the obligations & requirements of the users, the website and website owners. Furthermore the way

this website processes, stores and protects user data and information will also be detailed within this policy.

### **The Website**

This website and its owners take a proactive approach to user privacy and ensure the necessary steps are taken to protect the privacy of its users throughout their visiting experience. This website complies to all UK national laws and requirements for user privacy.

### **Use of Cookies**

This website uses cookies to better the users experience while visiting the website. Where applicable this website uses a cookie control system allowing the user on their first visit to the website to allow or disallow the use of cookies on their computer / device. This complies with recent legislation requirements for website's to obtain explicit consent from users before leaving behind or reading files such as cookies on a users computer / device.

Cookies are small files saved to the users computers hard drive that track, save and store information about the users interactions and usage of the website. This allows the website, through its server to provide the users with a tailored experience within this website.

Users are advised that if they wish to deny the use and saving of cookies from this website on to their computers hard drive they should take necessary steps within their web browsers security settings to block all cookies from this website and its external serving vendors.

This website uses tracking software to monitor its visitors to better understand how they use it. This software is provided by Google Analytics which uses cookies to track visitor usage. The software will save a cookie to your computers hard drive in order to track and monitor your engagement and usage of the website but will not store, save or collect personal information. You can read Google's privacy policy here for further information [ <http://www.google.com/privacy.html> ].

Other cookies may be stored to your computers hard drive by external vendors when this website uses referral programs, sponsored links or adverts. Such cookies are used for conversion and referral tracking and typically expire after 30 days, though some may take longer. No personal information is stored, saved or collected.

### **Contact & Communication**

Users contacting this website and/or its owners do so at their own discretion and provide any such personal details requested at their own risk. Your personal information is kept private and stored securely until a time it is no longer required or has no use, as detailed in the Data Protection Act 1998. Every effort has been made to ensure a safe and secure form to email submission process but advise users using such form to email processes that they do so at their own risk.

This website and its owners use any information submitted to provide you with further information about the products / services they offer or to assist you in answering any questions or queries you may have submitted. This includes using your details to subscribe you to any email newsletter program the website operates but only if this was made clear to you and your

express permission was granted when submitting any form to email process. Or whereby you the consumer have previously purchased from or enquired about purchasing from the company a product or service that the email newsletter relates to. This is by no means an entire list of your user rights in regard to receiving email marketing material. Your details are not passed on to any third parties.

### **Email Newsletter**

This website operates an email newsletter program, used to inform subscribers about products and services supplied by this website. Users can subscribe through an online automated process should they wish to do so but do so at their own discretion. Some subscriptions may be manually processed through prior written agreement with the user.

Subscriptions are taken in compliance with UK Spam Laws detailed in the Privacy and Electronic Communications Regulations 2003. All personal details relating to subscriptions are held securely and in accordance with the Data Protection Act 1998. No personal details are passed on to third parties nor shared with companies / people outside of the company that operates this website. Under the Data Protection Act 1998 you may request a copy of personal information held about you by this website's email newsletter program. A small fee will be payable. If you would like a copy of the information held on you please write to the business address at the bottom of this policy.

Email marketing campaigns published by this website or it's owners may contain tracking facilities within the actual email. Subscriber activity is tracked and stored in a database for future analysis and evaluation. Such tracked activity may include; the opening of emails, forwarding of emails, the clicking of links within the email content, times, dates and frequency of activity [this is by no far a comprehensive list].

This information is used to refine future email campaigns and supply the user with more relevant content based around their activity.

In compliance with UK Spam Laws and the Privacy and Electronic Communications Regulations 2003 subscribers are given the opportunity to un-subscribe at any time through an automated system. This process is detailed at the footer of each email campaign. If an automated un-subscription system is unavailable clear instructions on how to un-subscribe will be detailed instead.

### **External Links**

Although this website only looks to include quality, safe and relevant external links users should always adopt a policy of caution before clicking any external web links mentioned throughout this website.

The owners of this website cannot guarantee or verify the contents of any externally linked website despite their best efforts. Users should therefore note they click on external links at their own risk and this website and it's owners cannot be held liable for any damages or implications caused by visiting any external links mentioned.

### **Adverts and Sponsored Links**

This website may contain sponsored links and adverts. These will typically be served through our advertising partners, to whom may have detailed privacy policies relating directly to the adverts they serve.

Clicking on any such adverts will send you to the advertisers website through a referral program which may use cookies and will tracks the number of referrals sent from this website. This may include the use of cookies which may in turn be saved on your computers hard drive. Users should therefore note they click on sponsored external links at their own risk and this website and it's owners cannot be held liable for any damages or implications caused by visiting any external links mentioned.

### **Social Media Platforms**

Communication, engagement and actions taken through external social media platforms that this website and it's owners participate on are custom to the terms and conditions as well as the privacy policies held with each social media platform respectively.

Users are advised to use social media platforms wisely and communicate / engage upon them with due care and caution in regard to their own privacy and personal details. This website nor it's owners will ever ask for personal or sensitive information through social media platforms and encourage users wishing to discuss sensitive details to contact them through primary communication channels such as by telephone or email.

This website may use social sharing buttons which help share web content directly from web pages to the social media platform in question. Users are advised before using such social sharing buttons that they do so at their own discretion and note that the social media platform may track and save your request to share a web page respectively through your social media platform account.

### **Shortened Links in Social Media**

This website and it's owners through their social media platform accounts may share web links to relevant web pages. By default some social media platforms shorten lengthy url's [web addresses].

Users are advised to take caution and good judgement before clicking any shortened url's published on social media platforms by this website and it's owners. Despite the best efforts to ensure only genuine url's are published many social media platforms are prone to spam and hacking and therefore this website and it's owners cannot be held liable for any damages or implications caused by visiting any shortened links.

### **GDPR Statement**

The new General Data Protection Regulation (GDPR) will become enforceable from the 25th of May 2018 and will replace the Data Protection Act (DPA) currently in use at the time of writing. PREFET prepared for the GDPR by addressing the following points:

- Awareness: all members of the team are aware that the law is changing to the GDPR.
- Information it holds: PREFET is documenting which personal data it holds, where it comes from and who has access to it. The personal data that is collected consists of name, email address and affiliation of the people registered on the website. These informations are stored on the PREFET server using 256 bit SSL encryption protected by CloudFlare and SSL. Only three members of PREFET can access this via encrypted password secure admin access.
- Communicating privacy information: the [privacy notices of PREFET website](#) have been changed according to the GDPR implementations. This includes an explanation of PREFET lawful basis for processing the data, the data retention period and the how the data will be used. These concepts are expressed in an easy to understand language.
- Individual's rights: PREFET's procedures have been checked to ensure that they cover all the rights that individuals have. This has been reflected in the privacy notices of the PREFET website.
- Subject access requests: the way in which subject access requests are handled take into account the new GDPRs rules.
- Lawful basis for processing personal data: the lawful basis of PREFET for processing data are described in the [privacy notices](#) of the project and are available online to all the visitors of the website.
- Consent: An explicit consent is required when registering on the PREFET website and filling the Terms and Conditions of the services.
- Children: PREFET does not offer any online service specific to children and thus will not require a parental or guardian consent for any data processing activity. Furthermore, a system to verify individuals' ages is not necessary as the website does not contain any material that is considered inadequate to certain age groups.
- Data breaches: the project has procedures to detect, report and investigate personal data breaches. This is achieved by running hourly checks on the website and diagnostics via Cloudflare to ensure there are no data breaches.
- Data Protection by Design and Data Protection Impact Assessments: PREFET adopts a privacy by design approach as it takes privacy into consideration from the start. A Data Protection Impact Assessment (DPIA) would not be necessary as the processing of the data collected does not result in any high risk to individuals.
- Data Protection Officers: since PREFET does not carry out a regular and systematic monitoring of data of individuals on a large scale, nor it deals with special categories of data, a Data Protection Officer is not required.
- International: the project operates for now only in the UK. As such, a lead data protection supervisory authority is not necessary. Should PREFET expand its activity to other countries in the EU then this point will be re-considered.

### **Your information and protection**

The PREFET website is encrypted using 256-bit SSL security, and is hosted at one of the largest and most secure data centres in the UK. We also work directly with Cloudflare and our website is scanned every 4 hours for potential issues which are then dealt with in real time. If you would like to learn more about our commitment to data protection, please contact us.

# APPENDIX 2: PREFET Legitimate interest assessment (LIA) of the creation of contact lists for stakeholder engagement and dissemination of information

13 September 2019

This document, prepared by **PARTNER**, provides the justification for its processing of personal data in the PREFET project and, specifically, the compilation of a contact list of stakeholders whom we will contact periodically regarding Open Trend Consultation (OTC), Trendington and IdeAcademy by means of an e-mail or press release or other means to fulfil our communications requirements.

The PREFET contact list contains the names, titles, organisations and e-mail addresses of stakeholders whom we believe might be interested in the results of our project as well as stakeholders who have asked to be added to our contact lists. We have collected contact list data from our visiting various publicly available websites and noting the contacts. Each consortium partner manages its own contact list, which is not shared between the partners for a minimal privacy impact.

Data processing in the PREFET project includes collecting contact details as well as sending information to contacts. Most lawful bases require that processing is ‘necessary’ for a specific purpose. In the instance of our project, the collection of contact data and sending contacts information about our project results are necessary for the project to achieve impact, to ensure that FET stakeholders, our target stakeholders, are informed of the results of our project and how those results can help them in their efforts in building successful FET-like projects. Hence, our project results have a larger social purpose than simply benefiting the consortium partners (“the beneficiaries” in the EC’s terminology).

For EU-funded projects, such as ours, two legal documents are particularly relevant.

The first is the Multi-beneficiary Grant Agreement (MGA), Article 38(1)(1) of which states that beneficiaries of H2020 projects have an obligation to promote the project and its results: “The beneficiaries must promote the action and its results, by providing targeted information to multiple audiences (including the media and the public) in a strategic and effective manner.” Article 38(1)(1) clearly indicates that consortia are obliged to disseminate their results to multiple audiences, which implies the need to compile a contact list targeted at multiple audiences in a strategic and effective manner, i.e., not just a random list of people who visit the project’s website and ask to be put on the contact list. It has to be a *targeted* and *strategic* contact list. Hence, we consider that the MGA serves as a valuable justification for the PREFET consortium to process personal data for this purpose.

The second is the General Data Protection Regulation (GDPR), Article 6 of which provides for several possible legal bases for the processing of personal data. For example, Article 6(1)(a) allows the processing of personal data with the **consent** of the individual (the data subject). The GDPR sets a high standard for consent to be considered valid and it can always be withdrawn.

Another basis is Article 6(1)(f) which allows processing necessary for the **legitimate interests** pursued by the controller or by a third party. Our project has a legitimate interest for processing personal data, which stems from MGA Article 38(1)(1), as referenced above. We are obliged to inform stakeholders, including the public, about our project, disseminate and communicate its results.

Legitimate interest is the most flexible lawful basis for processing, but must be carefully assessed in each specific case. The existence of a legitimate interest also depends on the **reasonable expectations** of the persons concerned, where we use people's data in ways they would reasonably expect and where such use would have a minimal privacy impact, and where there is a compelling justification for the processing. Most stakeholders on our contact list have their e-mail addresses on their organisation's website, that is, they have already made their contact details public, hence, they must have a reasonable expectation that others will contact them. Others have asked to be on the contact list, for example, they may have heard about the project and have contacted one of the partners to receive periodic news and information about the project. Or we may have met the contact at a conference or workshop. There are various ways contacts may offer their consent, but it is important that their consent is documented; for example, even with a note on the back of their business card, it is then possible to e-mail the contact and ask for confirmation of their consent.

In addition, a balancing exercise must be conducted between the legitimate interests of the project and the interests of the data subjects concerned. For this balancing, PREFET consulted the website of the Information Commissioner's Office (ICO), the UK data protection authority, which offers detailed guidance on how to conduct the balancing exercise<sup>9</sup> and on which the following is adapted. We also consulted the Article 29 Working Party Opinion on legitimate interest.<sup>10</sup>

The ICO says that there are three elements to the legitimate interest basis. We must

- *identify a legitimate interest* – As stated above, we have a legitimate interest, under Article 38(1), to process personal contact details, as mentioned above, in order to create impact for our EU-funded project.
- *show that the processing is necessary to achieve it* – 'Necessary' means that the processing must be a targeted and proportionate way of achieving our purpose. We must collect the contact details for LEAs across the EU in order to inform them about

---

<sup>9</sup> <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>

<sup>10</sup> Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217, Brussels, Adopted on 9 April 2014. <https://www.dataprotection.ro/servlet/ViewDocument?id=1086>



how our project results could help them combat crime and terrorism. The processing is necessary as we could not reasonably achieve the same result in another way.

- *balance it against the individual’s interests, rights and freedoms* – see below, where we have done a balancing test, and are confident that the consortium’s legitimate interests do not override the individual’s interests or fundamental rights.

As noted below, our processing of personal data will not cause harm any more than any other e-mail to our stakeholders. We are not using people’s data in ways they would find intrusive or which could cause them harm. We will always offer stakeholders an option to unsubscribe from our contact list.

**Safeguards**

Even though we believe there are no significant risks to the data subjects of their being on our contact list and sending them relevant news, we have considered safeguards to reduce further any risks, as follows: PARTNER commits to keep its contact list in a secure, password-protected file to which only a limited number of individuals will have access on a need-to-know basis.

As we wish to rely on legitimate interests as the basis for processing data on our contact list, we have conducted this legitimate interest assessment (LIA) before we start the processing. According to the ICO, a LIA is a type of light-touch risk assessment based on the specific context and circumstances. It helps ensure that processing is lawful. Recording our LIA also helps to demonstrate compliance in line with our accountability obligations under GDPR Articles 5(2) and 24.

The ICO posits the following questions as part of its LIA exercise. Opposite each question in the left-hand column, we give our response in the right-hand column.

First, identify the legitimate interest(s).

<p>Why do you want to process the data – what are you trying to achieve?</p>	<p>In compliance with Art 38.1 of the PREFET Grant Agreement (see above), we wish to inform FET stakeholders, especially researchers interested in FET-like projects, about PREFET trends.</p>
<p>Who benefits from the processing? In what way?</p>	<p>The consortium partners benefit from the processing because they are able to inform our contacts about the results of our project. FET stakeholders benefit, particularly researchers aiming at improving their project building integral processes of FET-like ideas at early stages for good planning and decision making. Other stakeholders benefit too, e.g., EC policymakers who expect a positive impact from the project, i.e., an indication of promising FET-like candidates that would strengthen <i>European leadership in the early exploration of visionary, new and emerging technologies and with a</i></p>

	<i>strong engagement of scientists, citizens, innovators and policy makers.</i>
Are there any wider public benefits to the processing?	Yes, enhanced researchers' capabilities from the use of the PREFET results, particularly providing the responsible research and innovation (RRI) context for accelerating the kick-off of their ideas to achieve a successful project implementation, will positively affect the public (societal and ethical impact).
How important are those benefits?	Important, especially since future and emerging technologies will transform the way we live. The project will give researchers knowledge they don't currently have. The project will benefit researchers across the EU.
What would the impact be if you couldn't go ahead?	It would affect our ability to fulfil our contractual obligation and would deprive researchers across the EU of these important new findings.
Would your use of the data be unethical or unlawful in any way?	No, we will follow good data protection practices and follow established ethical guidelines and comply with Article 34 (Ethics and Research Integrity) of the Grant Agreement.

Second, apply the necessity test.

Does this processing actually help to further that interest?	Yes, this processing will help our legitimate interest to inform researchers about the PREFET findings aimed at helping them.
Is it a reasonable way to go about it?	Yes, it is the only way to enter into direct contact with the relevant researchers – apart from telephoning the researchers directly, which would be more intrusive than an e-mail.
Is there another less intrusive way to achieve the same result?	No, see above. Calling would be more intrusive. We have also been exploring another way of doing this, through the EC services.

Third, apply the balancing test.

By applying the balancing test (based on the questions below), we consider the impact of our processing and whether it overrides the interest we have identified.

What is the nature of your relationship with the individual?	The individuals in this case are researchers from across the EU. Researchers in the areas of (1) ICT; (2) health and life sciences; (3) Energy, Environment and Climate Change; (4) experts in RRI and ethics of technology are our targets for the PREFET activities, especially Trendington and IdeAcademy, so this relationship is significant.
Is any of the data particularly sensitive or private?	No. We are collecting only basic contact data that is already publicly available. In addition to the contact details we have compiled, some stakeholders visiting the PREFET website have asked to be put on our contact list or provided their details via OTC. We keep a log of such requests.
Would people expect you to use their data in this way?	Yes, especially researchers, who have put their contact details on their websites. Hence, they must expect that people will contact them.  In addition, the circulation of e-mails informing stakeholders about EU-funded project outcomes is a widespread practice in the field, and we assume that the carefully-selected stakeholders will receive this communication positively.
Are you happy to explain it to them?	Yes. We will inform our contacts about the mission of our project and how its results could be of assistance to them. We will also inform them about the project's privacy policy. We will always inform contacts they can be removed from our list by simply clicking on unsubscribe or similar action.
Are some people likely to object or find it intrusive?	No, as mentioned above, they have an interest in knowing about the project's results.
What is the possible impact on the individual?	There is no negative impact on the individual. We expect only a positive impact, in the sense that researchers will become aware of how our project's results could help them. Typically, we would expect to e-mail our FET stakeholders contacts no more than a few times a year.
How big an impact might it have on them?	As above.

Are you processing children’s data?	No. We do not aim to do this.
Are any of the individuals vulnerable in any other way?	Not that we are aware of.
Can you adopt any safeguards to minimise the impact?	We want to maximise the (positive) impact of our project. However, as noted above, we are implementing safeguards to protect our contact lists – notably, each partner manages their own contact list file, which is securely stored and only a few individuals have access to the file. The partners do not share the lists among each other to minimise privacy impact. For further details, see the project’s Data Management Plan (DMP).
Can you offer an opt-out?	Yes, we include an “unsubscribe” option for all our communications with stakeholders such as newsletters, press releases and project flyers.

**The decision on legitimate interest**

Based on the foregoing, we conclude that legitimate interest, Article 6 (1)(f), is an appropriate basis for our processing personal data, as described above. We are confident that our legitimate interests are not overridden by any risks to the data subject.

**Next steps**

We will inform our contacts that we are relying on legitimate interest for the processing of their contact details, and we will explain what this interest is especially to draw to the attention of researchers how the PREFET solutions will help them in successfully developing FET-like projects.

We understand that if we want to process the personal data for a new purpose, we may be able to continue processing under the legitimate interest provision as long as our new purpose is compatible with our original purpose. If necessary or useful, we will conduct a new LIA to demonstrate compliance with the legislation. At this stage and in accordance to the consortium’s grant agreement with the EC, the partners do not envisage repurposing this data.

We will keep this record of our legitimate interest assessment (LIA) on file in order to demonstrate compliance with legislation, if required. We will keep our LIA under review, and repeat it if circumstances change.