

D7.1 - POPD REQUIREMENT 1

|  |  |
| --- | --- |
| Work Package | WP7, Ethics requirements |
| Lead Author (Org) | Jayesh Wagh, CNRS-LAPP |
| Contributing Author(s)(Org) | H2020-ESCAPE workpackage leaders |
| Due Date | 30.04.2019 |
| Date | 02.02.2019 |
| Version | 0.1 |

|  |
| --- |
| Dissemination Level |
|  | PU: Public |
|  | PP: Restricted to other programme participants (including the Commission) |
|  | RE: Restricted to a group specified by the consortium (including the Commission) |
| X | CO: Confidential, only for members of the consortium (including the Commission) |

### Versioning and contribution history

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Authors** | **Notes** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Disclaimer

ESCAPE - The European Science Cluster of Astronomy & Particle Physics ESFRI Research Infrastructures has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement n° 824064.

Table of contents

1. [Executive summary 4](#_bookmark0)
2. [Introduction 5](#_bookmark1)
3. [List of tasks concerning data collection 5](#_bookmark2)
4. [Personal data collection, storage and protection 9](#_bookmark3)
	1. [Events 9](#_bookmark4)
	2. [Website 9](#_bookmark5)
	3. [IT services 9](#_bookmark6)
5. [Annex 1: H2020 ESCAPE internal IT services 11](#_bookmark7)

# Executive summary

In this deliverable, we first enlist the tasks where personal data collection will be required within H2020-ESCAPE. We then describe why such personal data collection is necessary and how this personal data will be collected, processed and stored. Although most of the IT tools that will be used for personal data collection during the project are yet to be developed, we are aiming to make all the IT tools GDPR compliant. This document shall be updated through further Annexes explaining GDPR compliance of these IT tools by the partners who will be operating them.

# Introduction

As per the H2020-ESCAPE grant agreement POPD requirement 1 concerns the ethics issues on personal data collection, processing and storage. The description of action describes POPD requirement no.1 as follow.

* 1. The applicant must check if a declaration on compliance and/or authorisation is required under national law for collecting and processing personal data as described in the proposal. If yes, the declaration on compliance and/ or authorisation must be kept on file.
	2. If no declaration on compliance or authorisation is required under the applicable national law, a statement from the designated Data Protection Officer that all personal data collection and processing will be carried out according to EU and national legislation must be kept on file.
	3. Detailed information on the procedures for data collection, storage, protection, retention, and destruction, and confirmation that they comply with national and EU legislation must be kept on file.
	4. Detailed information on the informed consent procedures in regard to the collection, storage, and protection of personal data must be kept on file.
	5. Templates of the informed consent forms and information sheets (in language and terms intelligible to the participants) must be kept on file.

# List of tasks concerning data collection

In this section, we enlist the tasks concerning personal data collection in each of the workpackages.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Workpackage Number** | **Deliverable/Milestone number** | **Task title** | **Task type** | **Lead beneficiary** |
| WP1 | MS1 | Project Kick-Offmeeting | Event | CNRS |
| WP1 | MS2 | 1st E-GA meeting | Event | CNRS |
| WP1 | D1.1 | Final Integration Event | Event | CNRS |
| WP2 | MS7 | First WP2 workshop on theinitial design and goals of thefirst pilot data lake | Event | CERN |
| WP2 | MS9 | Second WP2 workshop to analyse the performance of the pilot | Event | CERN |
| WP2 | MS13 | Third WP2 workshop to review performance of the full prototypes, and to explorefuture directions | Event | CERN |
| WP3 | D3.4 | Establishing of innovation competence group (all hands meeting) | Event | EGO |
| WP3 | D3.5 | Thematic training event - first school for software development anddeployment in the EOSC | Event | CNRS |
| WP3 | D3.8 | Thematic training event - second school for software developmentand deployment in the EOSC | Event | CNRS |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Workpackage Number** | **Deliverable/Milestone number** | **Task title** | **Task type** | **Lead beneficiary** |
| WP3 | MS18 | Final workshop to evaluatethe outcome of WP3 with respects to the mainobjectives of the call anddefine the necessary futuresteps | Event | FAU |
| WP3 | NA | Internal IT services for efficient internal communication and information sharing. within consortium members only | ITservices | FAU |
| WP4 | D4.3 | First Science withinteroperable data school | Event | INTA |
| WP4 | D4.6 | Second Science withinteroperable data school | Event | INTA |
| WP4 | MS24 | Hands-on workshop for dataProviders | Event | CNRS |
| WP5 | MS27 | First WP5 workshop onScience Platform design andrequirements | Event | NWO-I |
| WP5 | MS31 | Second WP5 workshopto analyse prototype performance | Event | NWO-I |
| WP5 | MS25 | Final WP5 ESFRI user training workshop on the Science Platform | Event | NWO-I |
| WP6 | D6.1 | ESCAPE projectwebsite live | Website | Trust-IT |
| WP6 | D6.4 | Citizen science experiments with embedded educational resources (midterm) | Event | OU |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Workpackage Number** | **Deliverable/Milestone number** | **Task title** | **Task type** | **Lead beneficiary** |
| WP6 | D6.6 | Citizen science experiments with embedded educational resources | Event | OU |

# Personal data collection, storage and protection

From section 3, we observe that there are three categories of tasks concerning personal data collection during the project. In this section, we describe the purpose for collection of personal data and general principles that will be followed for the processing and storage.

## Events

A GDPR compliant event organization tool allowing project partners to manage complex internal and public conferences, workshops, training events and meetings will be setup by CNRS-LAPP. All the project partners shall be using this tool to organize project related internal and public events during the project lifetime. This tool will be used to collect personal information of the registrants. This personal information shall contain first name, last name, organization, function within the organization, email, telephone number, dietary preferences. This personal data stored are required exclusively for organisational purposes; no comparison with other data or disclosure to third parties occurs, not even in part. This personal information shall be deleted post events. This tool will be hosted at IN2P3 computing centre (CC-IN2P3) in Lyon, France. A letter attesting GDPR compliance of this tool will be provided once the tool is completely functional.

For the events concerning citizen science experiments, only email addresses shall be collected using zooinverse, a citizen science experiment platform. As per the privacy policy of zooinverse platform the email addresses of the participants will never be visible to other participants. These email addresses shall never be shared with third parties.

More details on data collection and data storage of zooinverse platform are available on <https://www.zooniverse.org/privacy>

## Website

The project website is yet to be developed. It will collect basic personal information from project partners to grant them webpage editing rights. This personal information will contain first name, last name and email address. This personal data stored are required exclusively for authentication purposes; no comparison with other data or disclosure to third parties occurs, not even in part. These data are not stored together with other personal data. This website will be hosted at IN2P3 computing centre (CC-IN2P3) in Lyon, France. A GDPR compliant privacy policy of this website will be provided once the website is fully operational and online.

## IT services

For efficient internal communication and information sharing FAU shall setup Chat Server, Project Server, Document Server for H2020-ESCAPE consortium memebrs. Users’ personal data will be processed only to the extent necessary to provide services,

content and functional IT services for the ESCAPE project. As a rule, personal data are only processed after the user gives their consent. An exception applies in those cases where it is impractical to obtain the user’s prior consent and the processing of such data is permitted by law. These services will be hosted on FAU servers. More details on the data collection and processing are provided in annex 1.

# Annex 1: H2020 ESCAPE internal IT services

* Name and address of the data controller

Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) is responsible its websites within the meaning of the General Data Protection Regulation (GDPR) and other national data protection laws as well as other data protection regulations. It is legally represented by its President. For contact details, please consult the [legal notice](https://www.fau.de/impressum) on FAU’s central website.

The respective FAU institutions are responsible for any content they make available on the websites of Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU). FAU hosts IT services for the ESCAPE project, the contact person is Kay Graf, Erwin-Rommel-Str. 1, 91058 Erlangen, e-mail: kay.graf@fau.de, phone: +49-9131-8527265.

* Name and address of the Data Protection Officer

[Norbert Gärtner, RD](https://www.fau.de/universitaet/leitung-und-struktur/geschaeftsverteilungsplan-der-verwaltung/besondere-funktionsbereiche/datenschutzbeauftragter/)

* + Address:

Postanschrift: Schloßplatz 4

91054 Erlangen

* + Phone number: +49 9131 85-25860
	+ E-mail: norbert.gaertner@fau.de
	+ E-mail: datenschutzbeauftragter@fau.de
* Scope of processing of personal data

We only process our users’ personal data to the extent necessary to provide services, content and functional IT services for the ESCAPE project. As a rule, personal data are only processed after the user gives their consent. An exception applies in those cases where it is impractical to obtain the user’s prior consent and the processing of such data is permitted by law.

* Legal basis for the processing of personal data

Art. 6 (1) (a) of the EU General Data Protection Regulation (GDPR) forms the legal basis for us to obtain the consent of a data subject for their personal data to be processed. When processing personal data required for the performance of a contract in which the contractual party is the data subject, Art. 6 (1) (b) GDPR forms the legal basis. This also applies if data has to be processed in order to carry out pre-contractual activities. Art. 6 (1)

(c) GDPR forms the legal basis if personal data has to be processed in order to fulfil a legal obligation on the part of our organisation. Art. 6 (1) (d) GDPR forms the legal basis in the case that vital interests of the data subject or another natural person make the processing of personal data necessary.If data processing is necessary in order to protect the legitimate interests of our organisation or of a third party and if the interests, basic rights and

fundamental freedoms of the data subject do not outweigh the interests mentioned above, Art. 6 (1) (f) GDPR forms the legal basis for such data processing.

* Deletion of data and storage period

The personal data of the data subject are deleted or blocked as soon as the reason for storing them ceases to exist. Storage beyond this time period may occur if provided for by European or national legislators in directives under Union legislation, laws or other regulations to which the data controller is subject. Such data are also blocked or deleted if a storage period prescribed by one of the above-named rules expires, unless further storage of the data is necessary for entering into or performing a contract.

* Provision of IT Services for the ESCAPE Project

Each time the IT services of ESCAPE (namely Chat Server, Project Server, Document Server) is accessed, our system automatically collects data and information from the user’s computer system.

In this context, the following data are collected:

* + Address (URL) of the website from which the file was requested
	+ Name of the retrieved file
	+ Date and time of the request
	+ Data volume transmitted
	+ Access status (file transferred, file not found, etc.)
	+ Description of the type of web browser and/or operating system used
	+ Anonymised IP address of the requesting computer

The data stored are required exclusively for technical or statistical purposes; no comparison with other data or disclosure to third parties occurs, not even in part. The data are stored in our system’s log files. This is not the case for the user’s IP addresses or other data that make it possible to assign the data to a specific user: before data are stored, each dataset is anonymised by changing the IP address. These data are not stored together with other personal data.

For granting access to the above named IT services, account have to be generated. In this context, the following data are collected:

* + Full name of the acount holder
	+ Institutional e-mail address
	+ Personal login name
	+ Individual password (only hashed, not in clear text)
	+ Working group affiliation

These data are required exclusively for technical purposes; no comparison with other data or disclosure to third parties occurs, only after login the name and login of the account holder is visible to all partners with logins.

* Legal basis for data processing

The legal basis for the temporary storage of data and log files is Art. 6 (1) (f) GDPR, the legal basis for providing access to the IT services is Art. 6 (1) (b) GDPR.

* Purpose of data processing

The temporary storage of the IP address by the system is necessary in order to deliver the website to the user’s computer. For this purpose, the user’s IP address must remain stored for the duration of the session. The storage of such data in log files takes place in order to ensure the website’s functionality. These data also serve to help us optimise the website and ensure that our IT systems are secure. They are not evaluated for marketing purposes in this respect. The purposes stated above constitute our legitimate interests in processing data in accordance with Art. 6 (1) (f) GDPR.The storage of user details for the IT services is necessary to provide these service as part of the ESCAPE project, in accordance with Art. 6

(1) (b) GDPR.

* Storage period

Data are deleted as soon as they are no longer necessary for fulfilling the purpose for which they were collected. If data have been collected for the purpose of providing the website, they are deleted at the end of the respective session. If data are stored in log files, they are deleted at the latest after seven days. A longer storage period is possible. In this case, the users’ IP addresses are deleted or masked so that they can no longer be assigned to the client accessing the website. If the data are stored for access to the IT services, they are deleted after the account becomes inactive or the project ends.

* Options for filing an objection or requesting removal

The collection of data for the purpose of providing the website and the storage of such data in log files is essential to the website’s operation. As a consequence, the user has no possibility to object. For the access information, the user can request the deletion at admins@escape2020.de.