# Policy on the Processing of Personal Data

Draft for WLCG - as agreed at Joint Security Policy Group meeting, Ljubljana, 3-5 June, 2019.
(Date: 7 June 2019)
Main editor: Ian Neilson (STFC)

## 1 INTRODUCTION

This policy ensures that data collected as a result of the use of the Infrastructure is processed fairly and lawfully by Infrastructure participants. Some of this data, for example that relating to user registration, monitoring and accounting contains "personal data" as defined by the European Union (EU) [R 1]. The collection and processing of personal data is subject to restrictions aimed at protecting the privacy of individuals.

## 2 DEFINITIONS

Infrastructure

The bounded collection of universities, laboratories, institutions or similar entities, which adhere to a common set of policies [R 2] and together offer data processing and data storage services to End Users.

Participant

Any entity providing, managing, operating, supporting or coordinating one or more Infrastructure service(s).

Personal Data

Any information relating to an identified or identifiable natural person [R 1].

Processing (Processed)

Any operation or set of operations, including collection and storage, which is performed upon Personal Data [R 1].

End User

An individual who by virtue of their membership of a recognised research community is authorized to use Infrastructure services.

## 3 SCOPE

This policy covers Personal Data that is Processed as a prerequisite for or as a result of an End User's use of Infrastructure services. Examples of such Personal Data include registration information, credential identifiers and usage, accounting, security and monitoring records.

This policy does not cover Personal Data relating to third parties included in datasets provided by the End User or the research community to which they belong as part of their research activity. Examples of such data are medical datasets which may contain Personal Data.

## 4 POLICY

By their activity in the Infrastructure, Participants:

a) Declare that they have read, understood and will abide by the Principles of Personal Data Processing as set out below.

b) Declare their acknowledgment that failure to abide by these Principles may result in exclusion from the Infrastructure, and that if such failure is thought to be the result of an unlawful act or results in unlawful information disclosure, they may be reported to the relevant legal authorities.

# 5 PRINCIPLES OF PERSONAL DATA PROCESSING

i. The End User whose Personal Data is being Processed shall be treated fairly and in an open and transparent manner.

ii. Personal Data of End Users (hereinafter "Personal Data") shall be Processed only for those administrative, operational, accounting, monitoring and security purposes that are necessary for the safe and reliable operation of Infrastructure services, without prejudice to the End Users' rights under the relevant laws.

iii. Processing of Personal Data shall be adequate, relevant and not excessive in relation to the purposes for which they are Processed.

iv. Personal Data shall be accurate and, where necessary, kept up to date. Where Personal Data are found to be inaccurate or incomplete, having regard to the purposes for which they are Processed, they shall be rectified or purged.

v. Personal Data Processed for the purposes listed under paragraph ii above shall not be kept for longer than the period defined in a relevant Infrastructure service policy governing the type of Personal Data record being Processed (e.g. registration, monitoring or accounting) and by default shall be anonymised or purged after a period of 18 months.

vi. Appropriate technical and organisational measures shall be taken against unauthorised disclosure or Processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data. As a minimum, Infrastructure Participants shall:
    a. Restrict access to stored Personal Data under their control to appropriate authorised individuals;
    b. Transmit Personal Data by network or other means in a manner to prevent disclosure to unauthorised individuals;
    c. Not disclose Personal Data unless in accordance with these Principles of Personal Data Processing;
    d. Provide to the Infrastructure the location (publicly accessible url) of a Privacy Policy as required by vii below.;
    e. Respond to suspected breaches of this Policy promptly and effectively and take the appropriate action where a breach is found to have occurred;
    f. Perform periodic audits of compliance to this Policy and make available the results of such audits to other Infrastructure Participants upon their request.

vii. Each Infrastructure service interface provided for the End User must provide, in a visible and accessible way, a Privacy Policy (see example policy in section 7 below) containing the following elements:

a. Name and contact details of the Participant Processing Personal Data;
b. Description of Personal Data being Processed;
c. Legal basis [R1] for and purpose or purposes of Processing of Personal Data;
d. Explanation of the rights of the End User to:
    i. Obtain a copy of their Personal Data being stored by the Participant without undue delay;
    ii. Request that any Personal Data relating to them which is shown to be incomplete or inaccurate be rectified;
    iii. Request that on compelling legitimate grounds Processing of their Personal Data should cease;
e. Contact details which the End User should use to direct requests in relation to their rights as described above;
f. Retention period of the Personal Data Processed;
g. Reference to this Policy.

viii. Personal Data may only be transferred to or otherwise shared with individuals or organisations where the recipient -

a) has agreed to be bound by this Policy and the set of common Infrastructure policies, or
b) is part of a recognised Computer Incident Response Team framework and as part of an incident investigation to prevent active or suspected misuse of Infrastructure services, or
c) presents an appropriately enforced legal request.

# 6 REFERENCES


| | |
|---|---|
| **R 1** | 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) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 |
| **R 2** | Approved EGI/WLCG Security Policies. https://wiki.egi.eu/wiki/SPG:Documents |

# 7 INFRASTRUCTURE PARTICIPANT EXAMPLE PRIVACY POLICY

This section provides an example of a privacy policy as required by the section 5vii above. It does not form part of the Policy on the Processing of Personal Data.

*(still to be provided - start from WLCG Draft Privacy Notice)*