Standard operating procedure

Number: **011**

Name: **Data protection**

Title: Procedure for protecting data hosted on the EU Pollinator Hub

Category: General

Status: Draft

Version: 1.0

Date: 2023-06-30

Authors: Michael Rubinigg

This document is intended for the regulation of processes within the EU Pollinator Hub. It is published under the CC BY 4.0 licence. You may distribute, transform, adapt and build upon the material in any medium or format, including for commercial purposes, as long as you give credit to the author.

Table of contents

1 Document history 3
1.1 Current Release 3
1.2 Change history 3
2 Abbreviation 4
3 Introduction 5
3.1 Definitions 5
4 Validity 6
4.1 Area 6
4.2 Time 6
4.3 Related Documents 6
4.1 Related Tasks 6
5 Procedure 7
5.1 Responsibilities 7
5.2 Life cycle of the System Security Guide (SSG) 8
5.3 General Data Protection measures 11
5.4 Data Protection Impact Assessment (DPIA) 12
5.5 Specific measures for the protection of personal data *in situ* 15
6 References 16
7 Annexes 17

1 Document history

1.1 Current Release

1.1.1 Drafted

Submitted on 2023-05-08 by Michael Rubinigg, quality manager.

1.1.2 Reviewed

Reviewed on 2023-06-30 by Noa Simòn Delso, general manager.

1.1.3 Approved

Approved on 2023-06-30 by Michael Rubinigg, quality manager.

1.2 Change history

n.a.

2 Abbreviation

API	Application Programming Interface
BYOK	Bring Your Own Key
DKIM	DomainKeys Identified Mail
DPIA	Data Protection Impact Assessment
EU	European Union
EUPH	EU Pollinator Hub
GDPR	General Data Protection Regulation (*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*)
SOP	Standard Operating Procedure
SPF	Sender Policy Framework
SSG	System Security Guide
n.a.	not available
QID	Quasi-Identifiers

3 Introduction

This document aims to protect data on the EU Pollinator Hub (EUPH). In accordance with the GDPR three data categories are addressed: limited protectable data and personal data. Sensitive personal data is not processed on the EUPH.

The classification of data with respect to data security meets the requirements of unambiguity (the content clearly states how to handle the data, who should have access to it and describes the impact of data misuse and possible consequences in case of unwanted data exposure). Personal data is restricted to the minimal amount possible, hidden from users working with the data, processed in separate compartments whenever possible and aggregated at the highest level with the least possible detail by which it is still useful.

3.1 Definitions

Limited protectable data is data that does not describe or contain individual data, such as technical parameters or aggregated data that are sufficiently anonymised and can therefore not be traced back to an individual.

Personal data is personal-linked data that has no direct reference but can be assigned to individuals and personal data *stricto sensu* that describes something about individuals.

Sensitive personal data is data that directly describes and individual such as ethic origin, political conviction, biological characteristics.

Anonymisation is a change of a datum so that it cannot be clearly assigned to an individual. In includes both the removal of attributes from data and the removal of attribute combinations (QID) from anonymised data that may identify individuals.

Pseudonymisation is the replacement of an attribute by an encrypted one that does not allow a datum to be assigned to an individual, but the assignment can be restored if the parameters for the algorithm are known.

4 Validity

4.1 Area

The of validity of this document is limited to the protection of data hosted on the EU Pollinator Hub.

4.2 Time

The period of validity of this SOP begins on 2023-06-30 and ends with its revocation.

4.3 Related Documents

Document type	Number	Name
SOP	001	SOP instructions
SOP	004	Organisation chart

4.1 Related Tasks

Persons who have been assigned one of the following tasks, as defined in SOP-004, assume a responsibility within this SOP:

- Data protection
- Management of the organisation
- Quality management

5 Procedure

5.1 Responsibilities

- The person responsible for data protection, as defined by SOP-004, is responsible for the tasks described in this SOP.

5.2 Life cycle of the System Security Guide (SSG)

5.2.1 Drafting the SSG

5.2.1.1 Responsibilities

- The person responsible for the tasks described in this SOP drafts the SSG.
- The SSG is confidential and may not be disclosed to anyone not related to this process without the expressed consent of the person responsible for management of the organisation, as defined by SOP-004.

5.2.1.2 Mandatory elements of the SSG

- Chapter ***Aim and Scope*.**
  - Define aim and scope of the document.
- Chapter ***Principles***.
  - Define the principles upon which the software product has been built.
- Chapter ***Authentication and Authorisation***.
  - Describe how the access to IT systems is limited to only those individuals whose job requires such access. Describe how the following principles are put into practice:
    - Least privilege (access rights are restricted to least rights necessary to perform job responsibilities):
    - Deny all (access and rights are explicitly assigned to users. Without such assignment, users shall have no access or rights on the IT system);
    - Separation of duties (separating duties of individuals as necessary to prevent malevolent activity without collusion);
  - Justify exceptions to the mandatory use of Multi-Factor Authentication for all systems if applicable.
  - Define the password policy in terms of complexity requirements.
  - Describe the following elements of the identity management system:
    - Integration of external identification services, if applicable;
    - Rate-limiting mechanism that effectively limits the number of failed authentication attempts (*e.g.* number of maximum consecutive failed attempts);
    - Showing last successful and unsuccessful logon to users in order to detect attempts to misuse an account;
    - Alerts on unusual logins;
    - Prohibition of the most common passwords by blacklisting;

    - Describe the following elements of role-based access control:
        - Mode and location of the definition of roles;
        - Definition of the roles/accounts who may access the role-based access control;
        - Definition of the security measures to prevent access to the role-based access control (*e.g.* hard-coded or shared account; password protection; place, algorithms and technology used for storage of this password, complexity requirements for this password, rules for remote access by administrator);
    - Provide specific rules for user roles and permissions.
- Chapter ***Privacy and Incidence Management***.
    - Describe all technical and organisational security measures for data protection.
    - Define the procedure in the event of:
        - a rejection of a (modified) consent for processing data;
        - a request for correction of personal data;
        - a request for deletion of personal data;
    - Define the duration of storage of personal data.
    - Describe if and how custom login screens are designed in terms of end-user policy.
    - Describe data protection options (*e.g.* export or deletion of user data)
    - Describe the process of notification in case of planned maintenance and upgrades.
    - Describe the process of notification in case of data breaches, security incidents or disasters.
    - Describe the process of notification in case of downtime beyond service level agreement?
    - Describe the process of backups in terms of configuration of frequency and scope.
- Chapter ***Audit and Accountability***.
    - Describe processing and availability of audit trails for the following elements:
        - Attempted/successful/failed logins;
        - Role assignment/removal/update;
        - Changes to security settings;
- Chapter ***Email***.
    - Describe the email policy for email sent to users for the following elements:
        - Implementation and (if applicable) configuration of email authentication methods (*e.g.* SPF, DKIM);
        - Configuration of sender;
        - Configuration and/or branding for content;
        - Integration of external applications (e.g. API, software applications);
- Chapter ***Cryptography***.

    - Describe supported encryption features (*e.g.* BYOK).
- Chapter ***Technology***.
    - Describe the technology used to run the software.
- Chapter ***Server Hosting Procurement***.
    - Define the minimum requirement for server hosting procurement.

5.2.2 Revision of the SSG

5.2.2.1 Responsibilities

- The person responsible for quality management, as defined by SOP-004, revises the draft version of the SSG.

5.2.2.2 Approval of a SSG

- The person responsible for management of the organisation, as defined by SOP-004, approves the revised draft version of the SSG.

5.2.2.3 Annual revision of the SSG

- The person responsible for data protection performs an annual revision of the SSG.
- If considered necessary the person responsible for data protection drafts an updated version of the SSG, processing it as described in section 5.2.2.

5.3 General Data Protection measures

5.3.1 Privacy policy

5.3.1.1 Maintenance of the Privacy Policy

- The person responsible for the processes in this SOP drafts and maintains the Privacy Policy of the EU Pollinator Hub.
- The Privacy Policy is published on the EUPH website (pollinatorhub.eu/privacy-policy).

5.3.1.2 Elements of the Privacy Policy

- The following information is provided to the user in an understandable form:
  - Clear specification of collected personal data, in particular:
    - Affected data attributes;
    - Granularity of with which data attributes are processed;
  - Clear legal justification for personal data collection.
  - Clear and well-defined reason for personal data collection.
  - Clear and well-defined list of analyses to be conducted on personal data.
  - Clear list of rights of the affected individual (correction, deletion)

5.3.1.3 Modification of consent

- Users are notified of the change in modifications of the consent.
- Users have to provide the consent again.

5.3.2 Terms of Use

5.3.2.1 Maintenance of the Ters of Use

- The person responsible for the processes in this SOP drafts and maintains the Terms of Use of the EU Pollinator Hub.
- The Privacy Policy is published on the EUPH website (pollinatorhub.eu/terms-of-use).

5.4 Data Protection Impact Assessment (DPIA)

5.4.1 Drafting the DPIA

5.4.1.1 Responsibilities

- The person responsible for the processes described in this SOP performs a DPIA in the case of systematic and comprehensive assessment of personal data based on automated processing (*e.g.* data from sensors such as hive scales) and extensive processing of personal data (*e.g.* visualisation module).
- The DPIA is confidential and may not be disclosed to anyone not related to this process without the expressed consent of the person responsible for Management of the organisation, as defined by SOP-004.

5.4.1.2 Mandatory elements of the DPIA

- Definition of high-risk work steps.
- Systematic description of planned processing steps.
- Description of the purpose for processing.
- Assessment of the necessity and the extent of processing:
  - Does data processing take place only for specified, clear and legitimate purposes?
  - Is data processing appropriate for the purpose and limited to what is necessary?
  - Are rights defined by GDPR being adequately communicated?
  - Does the local protection authority have to be consulted?
- Assessment of the risks in terms of GDPR compliance.
- Description of appropriate countermeasures for minimizing and/or mitigating a risk or misuse.

5.4.2 Revision of the System DPIA

5.4.2.1 Responsibilities

- The person responsible for quality management, as defined by SOP-004, revises the draft version of the DPIA.

5.4.2.2 Approval of a DPIA

- The person responsible for management of the organisation, as defined by SOP-004, approves the revised draft version of the DPIA.

5.4.2.3 Annual revision of the DPIA

- The person responsible for data protection performs an annual revision of the DPIA.

- If considered necessary the person responsible for data protection drafts an updated version of the DPIA, processing it as described in section 5.4.2.

5.5 Specific measures for the protection of personal data *in situ*

5.5.1 Principals

5.5.1.1 Storage of data

- The person responsible for the processes described in this SOP implements the necessary technologies and procedures which assure that:
  - personal data is restricted to the minimal amount possible;
  - personal data is hidden from users working with the data;
  - personal data is processed in separate compartments whenever possible;
  - a person is not identified from the data in a dataset;

5.5.1.2 Aggregation of data

- Data that might allow the identification of a person may be aggregated at the highest level with the least possible detail by which it is still useful. In this case the number of individuals or holdings that contribute to a value of a datum must be higher than 3.

5.5.1.3 Number of individuals representing one datum

- The number of one or two individuals or holdings must represent less than 85% of the value of a datum.

5.5.1.4 Data anonymisation and pseudonymisation

- Data that might allow the identification of a person may be anonymised.
- If anonymisation is not considered an appropriate measure data may be pseudonymised.

6 References

There are no sources in the current document.

7 Annexes

There are no annexes in the current document.