Record for processing of personal data

Title: E-services on JRC websites

Reference: DPR-EC-00406.2

Controller: European Commission: Joint Research Centre (JRC) (JRC)

Publication date: 17/04/2020

1. General information

Data protection record

Record reference

DPR-EC-00406.2

Title of the processing operation

E-services on JRC websites

Language of the record

English

Corporate record

No

Data Protection Officer

Contact details

EC-DPO-INTERNAL@ec.europa.eu

Controller

Responsible organisational entity

Joint Research Centre (JRC) (JRC)

Directorate / Unit

A.1

Contact Details

JRC-DATA-PROTECTION-COORDINATOR@ec.europa.eu

Joint controllership

Joint controllership is involved

N/A

Processors

Processors are involved in the processing

Yes

- **Names and contact details of processors**

  Personal data may be communicated to an external entity assisting the Commission in fulfilling the objective for which the data is managed.The Commission’s contractors are bound by a specific contractual clause for any processing operations of personal data on behalf of the Commission, and by the confidentiality obligations deriving from the transposition of the General Data Protection Regulation in the EU Member States (‘GDPR’)

2. PURPOSE AND DESCRIPTION OF THE PROCESSING

Purpose

Description of the purpose of the processing

An e-service on JRC websites is a service or resource made available on the Internet in order to improve the communication between citizens and businesses and the JRC. Most of JRC websites are accessible without giving any personal information, however in some cases personal data are required in order to provide specific e-services. This record aims to cover these cases.

Three types of e-services are, or will be, offered by JRC:

1. Information services enabling a given research community (e.g. committee, working group, project group, etc.) geographically spread across Europe (and beyond) to maintain a private space on the Internet where they can share information, documents, participate in discussion fora, download software, subscribe to JRC publications etc.
2. Information services that provide people, media, businesses, administrations and others with secure access to information.
3. Interactive communication services (communications to users, distribution of reports, information sharing within interest groups etc.) that allow better contact with people, businesses, civil society and public bodies, in order to facilitate policy consultations and feedback.

Personal data may be communicated to other DGs (within the Commission) assisting in fulfilling the objective for which the data is managed. In that case, a specific internal arrangement will be concluded.

Processing for further purposes

The purpose(s) for further processing

N/A

Modes of processing

The mode of processing

- Any other mode:

  The information is collected via on-line registration forms or through the European Commission Authentication Service (EU Login) and stored in databases on JRC servers.

  No manual intervention is normally required. However, in case of requests of modifications and/or

withdraw of all contact details, manual processing might be requested.

Registered users have password protected direct on-line access to their profile and can update their information, cancel their registration or request to unsubscribe from specific interest groups or communications.

Description/additional information regarding the modes of processing

-

Storage medium

The medium of storage (one or more)

- Electronic
- Others:
  -

Description/additional information regarding the storage medium

Servers and databases, where personal data are stored, are located on JRC premises and managed by the e-service system administrators and other JRC authorised personnel on a "need-to-know" principle.

Comments

Comments/additional information on the data processing

-

3. DATA SUBJECTS AND DATA CATEGORIES

Data subjects' categories

Data subject(s) are

- Internal to the organisation

  A description of the data subjects (internal to the organisation)

  Commission staff who register via the on-line registration forms or in the European Commission Authentication Service (EU Login).

- External to the organisation

  A description of the data subjects (external to the organisation)

  Personnel of other organisations and members of the public who register via on-line registration forms or in the European Commission Authentication Service (EU Login).

Data categories/fields

Description of the categories of data that will be processed

For the JRC e-services administrators:

The data collected are: Name, surname, affiliation, EU Login username and email.

For the users of JRC e-services:

The following data fields may be collected either through a dedicated on-line registration form or via the or in the European Commission Authentication Service (EU Login).

Title, first name and last name of person, date and place of birth, position, name of organisation, job title, IP address, place of work or residency, postal code, city, nationality, country, personal and/or professional e-mail address, website, phone, fax, preferred language, default language, gender, fields of interest, profile picture/avatar, short biography and information distribution format desired (e-mail or not), information, documents and contributions to discussion fora.

In the case of European Commission Authentication Service (EU Login) the Commission personnel number, a unique key and group membership may be collected.

A username and password could also be set up at the first registration.

The e-service may also collect the following additional data about each user:

- Date and time of most recent successful and unsuccessful authentication
- Last change of password
- Last password reset
- Account status (whether active, inactive or logged by administrator..)
- Number of good logins and failed attempts
- Most recent passwords – to make sure you follow the prevailing security policy regarding password re-use.
- Security data/log files

Cookies are managed according to the Commission corporate policy.

The processing operation concerns any 'special categories of data' which fall(s) under Article 10(1), which shall be prohibited unless any of the reasons under Article 10(2) applies

N/A

Description/additional information regarding special categories of personal data

-

Data related to ‘criminal convictions and offences’

The data being processed contains sensitive data which fall(s) under Article 11 'criminal convictions and offences'

N/A

Comments

Comments/additional information on data subjects and data categories

-

4. RETENTION PERIOD

Data categories and their individual retention periods

The administrative time limit(s) for keeping the personal data per data category

1. **Data category**

   Security data/Log files

   Retention period

   Stored for a maximum of 1 year. In context of investigations of security incidents the data could be further processed following notification DPO-3783-2 DIGIT Cybersecurity operations, where a different retention period applies.

   Start date description

   -

   End date description

   -

2. **Data category**

   Identification data: Title, first name and last name of person, username, postal code, city, nationality, country, personal and/or professional e-mail address, website, phone, fax.Personal characteristics: date and place of birth, preferred language, default language, gender and fields of interest.Professional and educational background: short biography, position, name of organisation, job title, place of work or residency,Profile picture/avatarAny other information: information, documents and contributions to discussion fora.

   Retention period

   JRC eservices administrators should provide 1 of the following options to their users:Data will be stored on the site as long as the Registered User concerned is active, and no request has been made by the Registered User to the Platform Administrator to remove him from the Platform. After two years of continuous inactivity of a user, or upon email request from the user, his/her data will be removed.Data will be stored on the site as long as the project at issue is active. At any time the user can request to be removed from he platform.Data will be stored on the site for a maximum of 4 years thereafter, unless the Controller launches an update of the registrations, asking the data subjects for their consent to update or cancel the stored information including their personal data.

   Start date description

   Date of registration of the User Profile in the Platform

End date description

-

3. **Data category**

   IP addresses

   Retention period

   Stored for a maximum of 1 year. In context of investigations of security incidents the data could be further processed following notification DPO-3783-2 DIGIT Cybersecurity operations, where a different retention period applies.

   Start date description

   -

   End date description

   -

4. **Data category**

   Additional data referred to the activity of the user in the platform:Date and time of authentication, change/reset of password or account status.

   Retention period

   Stored for a maximum of 1 year. In context of investigations of security incidents the data could be further processed following notification DPO-3783-2 DIGIT Cybersecurity operations, where a different retention period applies.

   Start date description

   -

   End date description

   -

Comments

Comments/additional information on the data retention periods

Personal data are kept for as long as users are recorded as been active and for a maximum of 4 years thereafter, unless the Controller launches an update of the registrations, asking the Data subjects to update

or cancel the stored information including their personal data. Registered users have password protected on-line access to their profile and can, at any moment, update their information, cancel their registration or request to unsubscribe from specific interest groups or communications. In several cases user_id's which are not active for a defined period of time are automatically deleted from the system. Time limits of the retention of data in the EU Login Authentication Service are defined in the privacy statement of the European Commission's Identity Management Service (DPO-839-4) In case of

5. RECIPIENTS

Origin of the recipients of the data

The origin of the data recipients

- Within the EU organisation

  A description of the indicated recipients of the data

  Officials and other staff of the JRC responsible for the data processing and the e-service system administrators. Personal data may be communicated to other DGs (within the Commission) assisting in fulfilling the objective for which the data is managed. In that case, a specific internal arrangement will be concluded.

- Outside the EU organisation

  A description of the indicated recipients of the data

  e-service registered users

Categories of the data recipients

The categories (one or more) of the data recipients

- A natural or legal person

Description of the indicated category(ies) of data recipients

E-service system administrators (EC Staff),

E-service registered users

JRC Local Information Security Officer and Commission departments responsible for the security of information systems, Directorate-General for Informatics, IT Security (DIGIT.S) and Human Resources Directorate of Security (HR.DS)

Who has access to which parts of the data

The e-service system administrators have access to all data categories. This includes Commission staff responsible for carrying out this processing operation and authorised staff according to the “need to know” principle. Such staff abide by statutory, and when required, additional confidentiality agreements. Title, first name and last name of person, position, name of organisation, job title, city, nationality, country, e-mail address, website, gender, fields of interest, profile picture/avatar, short biography and in some cases street name and number and postal code may be accessible from other internal and external registered users In case of a security incident, all data categories may be shared with the JRC LISO, DIGIT.S and HR.DS

Comments

Comments/additional information on data recipients

In context of investigations of security incidents the data could be transferred and further processed following notification DPO-3783-2 DIGIT Cybersecurity operations. Access is provided according to the “need to know” principle.

Personal data may be communicated to other DGs (within the Commission) assisting in fulfilling the objective for which the data is managed. In that case, a specific internal arrangement will be concluded.

6. INTERNATIONAL DATA TRANSFERS

Transfer outside of the EU or EEA

Data is transferred to countries outside the EU or EEA

N/A

Transfer to international organisation(s)

Data is transferred to international organisation(s)

N/A

Comments

Comments/additional information on international data transfers

If personal data are published on a publicly available internet website, this means that they are accessible worldwide. Following the opinion of the EDPS, this does not constitute a transfer of personal data under Article 46-49 of Regulation (EU)2018/1725.

7. INFORMATION TO DATA SUBJECTS ON THEIR RIGHTS

Privacy statement

Rights of the data subjects

The processing should respect the following rights of data subjects

- Article 17 - Right of access by the data subject
- Article 18 - Right to rectification
- Article 19 - Right to erasure (right to be forgotten)
- Article 20 - Right to restriction of processing
- Article 21 - Notification obligation regarding rectification or erasure of personal data or restriction of processing
- Article 22 - Right to data portability
- Article 23 - Right to object
- Article 24 - Rights related to Automated individual decision making, including profiling

The data subjects are informed about their rights and how to exercise them in the form of a privacy statement attached to this record

Yes

Guidance for Data subjects which explains how and where to consult the privacy statement is available and will be provided at the beginning of the processing operation

Yes

An explanation of the guidance on how and where to consult the privacy statement

The Privacy Statement will be available on all JRC websites which require users to register or request their EU Login credentials to access the e-service. In some cases, during the registration procedure the data subjects are asked by the system to read the privacy statement and accept or reject the conditions described, before accessing the registration form.

The privacy statement(s)

- Privacy Statement JRC e-services.docx

Comments

Comments/additional information on information to data subjects on their rights

-

8. SECURITY MEASURES

Short summary of overall Technical and Organisational measures implemented to ensure Information Security:

Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.