



EUROPEAN COMMISSION

PROTECTION OF YOUR PERSONAL DATA

Processing operation: EU Verify

Controller: European Commission, Directorate-General for Digital Services, Unit B.3

Record reference: DPR-EC-27509

Table of Contents

- 1. Introduction**
- 2. Why and how do we process your personal data?**
- 3. On what legal ground(s) do we process your personal data?**
- 4. Which personal data do we collect and further process?**
- 5. How long do we keep your personal data?**
- 6. How do we protect and safeguard your personal data?**
- 7. Who has access to your personal data and to whom is it disclosed?**
- 8. What are your rights and how can you exercise them?**
- 9. Contact information**
- 10. Where to find more detailed information?**

1. Introduction

The European Commission (hereafter 'the Commission') is committed to protect your personal data and to respect your privacy. It collects and further processes personal data pursuant to [Regulation \(EU\) 2018/1725](#) of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (repealing Regulation (EC) No 45/2001).

This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure the protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.

This information relates to the processing of personal data in relation to the processing operations of EU Verify service, undertaken by the European Commission, Directorate-General for Digital Services (DG DIGIT), Unit B.3.

2. Why and how do we process your personal data?

EU Verify is the Commission's corporate advisory and training service on Web3 technologies offered by DIGIT.B.3 to the European Institutions, Bodies and Agencies (EUIBAs). It acts as a "single point of contact" for EUIs aiming to implement innovative technologies in order to improve their verification processes.

EU Verify provides different sets of services:

- Advisory: EU Verify provides guidance and support to understand if a project can benefit from Web3 technologies, which one(s) would be best suited for the user's specific use case(s) and how to get started. The EU Verify team analyses the business requirements, advises on the best solution, helps to define the architecture and assists with the development and/or integration. It offers a set of technological solutions based on cost and risk assessment, advises on the most appropriate choice for the user's project and offers fully managed solutions.
- Trainings and events: EU Verify coordinates, organises, manages and follows-up on meetings, workshops, seminars, webinars, training courses and other similar events to help European Institutions and Agencies understand Web3 technologies, the standards in use, the potential use cases and how to use these new technologies in their projects. Personal data is collected to provide stakeholders with information about a meeting or event (before, during and after) organised in relation to the EU Verify services, to process applications for participation in that meeting or event and to assist stakeholders with any follow-up activities related to EU Verify. This processing activity is covered by the record of processing DPR-EC-01063.
- Development and integration: EU Verify defines and analyses the architecture and the design of the user's solution as well as supports in its development and/or management. Additionally, EU Verify team provides resources, helps with or takes over the development, and offers complete managed services.
- Piloting: EU Verify helps to pilot projects with users to determine how successful a project might be once it is implemented. This is done by building a smaller version of the project and test it to give you a better understanding of how well it may perform at full scale. The EU Verify team provides resources, helps with or takes over the development, and offers complete managed services.
- Proof-of-Concept: EU Verify helps to test an initial idea involving Web3/decentralised technologies to demonstrate its potential for the user's specific use case. It provides resources, help with or takes over the development, and offers a complete solution.

- *“My EU Credentials” Proof-of-Concept*: A working Proof-of-Concept by the EU Verify service. It represents a set of services and modules that can be easily tested and integrated with a wide range of work-related items for EU Staff members. “My EU Credentials” features three apps that cover, respectively, the creation and issuance of verifiable credentials (tamper-proof documents), the storage of those credentials in a desktop/mobile app (“digital wallet”), and the instant verification of those credentials by a third party in a privacy-preserving way. This Proof-of-Concept has been built to showcase the potential of Verifiable Credentials and how it can be used in a practical use case.

This set of modular solutions by EU Verify provides users with a turnkey solution to demo/test the issuance, storage and verification of (verifiable) credentials. The three components are:

- **An Issuer portal**: a portal to become a trusted issuer of Verifiable Credentials for the community of users, allowing to manage and issue credentials;
- **A Holder wallet**: a digital wallet (web-based or as an application) for users to store and present (share) their credentials to verifiers (both for in-person and remote verification);
- **A Verifier portal**: a portal to verify holders’ credentials (both for in-person and remote verification).

My EU Credentials Proof-of-Concept is used for different types of use cases (e.g.: access pass for meetings and events, certificates of attendance or of qualifications, service cards, etc.).

You may submit a request for the creation of a Verifiable Credential via a registration form hosted on the [EU Verify domain](https://issuer.eu-verify.eu/) (<https://issuer.eu-verify.eu/>). The authentication necessary to access this form is done through EU Login service (DPR-EC-03187). EU Verify may also receive your contact details from the EU Verify stakeholder (e.g. the organiser of a meeting, event, training, etc. for which EU Verify service is used).

EU Verify then processes personal data, which was either provided by you, automatically collected from EU Login or provided to EU Verify by the organiser of the meeting/ event/ training. These data are used to generate a keypair (private and public keys) using the Amazon Web Services Key Management Service ([AWS KMS](#)). These keys unlock the access to the "digital wallet" on the [EU Verify domain](https://holder.eu-verify.eu/) (<https://holder.eu-verify.eu/>) and Verifiable Credential that are issued to said wallet.

The Amazon Web Services Key Management Service ([AWS KMS](#)) has access to the alias (EU Login username) that is used to generate the keypair for the creation of the “digital wallet”, to which Verifiable Credentials are issued. Amazon only stores the user’s public and private key as well as their alias as part of the AWS KMS service and does not store any other personal data provided for creating Verifiable Credentials. The public and private keys are only accessible and can only be decrypted by the owner of the keys (the user). AWS does not access, use, or disclose to any third party, any personal data, except as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). AWS restricts its personnel from processing personal data without authorisation by AWS.

AWS may use sub-processors to provide processing activities on personal data. This list of AWS Sub-processors can be found [here](https://aws.amazon.com/compliance/sub-processors/) (<https://aws.amazon.com/compliance/sub-processors/>). Where AWS authorises a Sub-processor, AWS will restrict the Sub-processor’s access to personal data only to what is necessary to provide or maintain the Services. AWS shall only disclose the personal data to a third party on documented instructions from the data controller.

EU Verify staff can issue and/or revoke Verifiable Credentials using the Issuer Portal on [EU Verify domain](https://issuer.eu-verify.eu/) (<https://issuer.eu-verify.eu/>). Once a Verifiable Credential is issued, you will receive an

email notification with a link to your “digital wallet” hosted on [EU Verify domain](https://holder.eu-verify.eu/) (https://holder.eu-verify.eu/). To access the wallet, you must go through an EU Login authentication. Once logged in the “digital wallet”, you have a possibility to “Accept” or “Reject” the Verifiable Credential. If accepted, the Verifiable Credential is stored in your “digital wallet”. If rejected, the issued credential is deleted.

The Verifiable Credential has a format of a QR code, which when scanned by a verifier, provides such information about the user as their name, title, DG, etc., information about the issuer of the Verifiable Credential, its validity or revocation status and information about the meeting, event, or training for which this credential was issued. The verifier can be any user who has access to the Verifier portal (“EU Verify It” web application) hosted on [EU Verify domain](https://verifier.eu-verify.eu/) (https://verifier.eu-verify.eu/).

EU Verify displays personal information present on a Verifiable Credential, however, such data is not collected/stored by EU Verify.

Your personal data will not be used for any automated decision-making, including profiling.

3. On what legal ground(s) do we process your personal data

The lawfulness of the processing of personal data for the processing operations *Advisory, Trainings and events, Development and integration, Piloting, and Proof-of-Concept* is laid down under Article 5(1)(a): “Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body.”

The lawfulness of the data processing for the processing operation “*My EU Credentials*” *Proof-of-Concept* is identified as Article 5(1)(d) – the data subject has given consent to the processing of his or her personal data for one or more specific purposes. According to Article 5(1)(d), the data controller will be collecting users consent for processing their personal data either through a tick box in the online registration form or through email.

Your consent for these services can be withdrawn at any time by contacting the data controller at EU-VERIFY@ec.europa.eu.

4. Which personal data do we collect and further process?

In order to carry out this processing operation, the Data Controller, DG DIGIT B.3, collects data from the data subjects internal to the organisation (EU staff that use the service), and the following data subjects external to the organisation (natural persons or organisation that has to use the EU Verify service in the context of an EU project, an event or a training organised by EUIBAs where “My EU Credentials” is used). The following categories of personal data will be collected and processed:

- **Data necessary for the creation and management of your Verifiable Credential:**
 - Personal data collected from EU Login (DPR-EC-03187):
 - First name, last name;
 - e-mail address;
 - Commission generated User ID of the requestor;
 - European Institution (if applicable);
 - DG/Unit (if applicable).
 - Data present on the Verifiable Credential (it can be/but is not limited to: first/last name, data related to the organisation the user works for, title/role, qualifications, data related to the certification or the event attended, etc.);
 - Date of Verifiable Credential request;
 - Date of the Verifiable Credential issue;
 - Information about Verifiable Credential validity and revocation status;
 - Private and public key, created through Amazon Web Services Key Management

Service (AWS KMS).

- **Data collected in the context of providing Advisory, Trainings and events, Development and integration, Piloting, Proof-of-Concept services:**
 - Contact details (first and last name, function/title, city, country, e-mail address, telephone number);
 - EU Login Unique ID;
 - Information about the company/organisation the data subject represents;
 - Nationality, passport or identity card number and its date of issue and expiry date, date of birth, name, surname, organisation they belong to, gender, may be collected, so that the data subjects may obtain access to the premises where the meeting or event is held.
- **Log data about the performed operations for troubleshooting and security auditing purposes.**

5. How long do we keep your personal data?

Unit B.3 keeps your personal data necessary for the creation and management of your Verifiable Credential for 5 years to allow for its easier re-issuance. You may also request to delete your data earlier by reaching out to EU Verify via the functional mailbox (EU-VERIFY@ec.europa.eu).

Personal data stored on Amazon Web Services (AWS) will be permanently deleted either upon your request or after 5 years of inactivity (5 years after the last time you have accessed your key pairs created in the Amazon Web Services Key Management Service (AWS KMS), that are derived from your EU Login). After this personal data has been deleted, you will no longer be able to access your digital wallet, or any Verifiable Credential stored therein.

Unit B.3 keeps your personal data collected in the context of providing *Advisory, Trainings and events, Development and integration, Piloting, Proof-of-Concept services*:

- Personal data related to the organisation and management of the meeting, consultation, training or event (this includes the information given during the registration, before, during or after the event) will be kept for **5 years** after the meeting or event to assist stakeholders with any follow-up activities related to EU Verify.
- Personal data related to piloting, development and integration, proof-of-concept services is kept for the duration of a service and will be retained for up to **5 years** after the request for a service was registered or until you request to delete your data by reaching out to EU Verify via the functional mailbox (EU-VERIFY@ec.europa.eu).
- Personal data shared with the Directorate-General for Human Resources and Security of the European Commission to provide you access to Commission buildings is kept for 6 months after the termination of the link between you and the Commission. More information is available in the Record of Processing DPR-EC-00655 (Commission Physical Access Control System (PACS)).

Log data about the performed operations for troubleshooting and security auditing purposes is kept up to 12 months for security auditing purposes unless there is an explicit requirement or request to do otherwise from the domain owner.

6. How do we protect and safeguard your personal data

All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored on the servers of the Commission. All processing operations are carried out pursuant to [Commission Decision \(EU, Euratom\) 2017/46](#) of 10 January 2017 on the security of communication and information systems in the Commission.

In order to protect your personal data, the Commission has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

7. Who has access to your personal data and to whom is it disclosed?

Access to personal data is provided to the Commission staff working in DIGIT B.3, responsible for carrying out this processing operation and to other authorised staff according to the “need to know” principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

Personal information presented on your Verifiable Credential can be accessed by the Commission staff and any other user of the EU Verify “My EU Credentials” service only by requesting it from you directly and by using the dedicated “EU Verify It” web application hosted on EU Verify domain (<https://verifier.eu-verify.eu/>). The user acting as a “verifier” needs to login to the “EU Verify It” web application via EU Login and request you to present their Verifiable Credential. The Verifiable Credential can be accessed from your “digital wallet” hosted on EU Verify domain (<https://holder.eu-verify.eu/>), which you can open from their phone, tablet or PC. Once the Verifiable Credential is presented, the verifier can then scan it with their own phone, tablet or PC using “EU Verify It” web application hosted on EU Verify domain (<https://verifier.eu-verify.eu/>).

8. What are your rights and how can you exercise them?

You have specific rights as a ‘data subject’ under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access your personal data and to rectify them in case your personal data are inaccurate or incomplete. Under certain conditions, you have the right to erase your personal data, to restrict the processing of your personal data, to object to the processing and the right to data portability.

You have consented to the certain processing of your personal data to the Data Controller for the present processing operation(s). You can withdraw your consent at any time by notifying the Data Controller at EU-VERIFY@ec.europa.eu. The withdrawal will not affect the lawfulness of the processing carried out before you have withdrawn the consent.

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given under Heading 9 below.

Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description (i.e. their Record reference(s) as specified under Heading 10 below) in your request.

9. Contact information

- The Data Controller

If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the

collection and use of your personal data, please feel free to contact the Data Controller: European Commission, Directorate-General for Digital Services (DG DIGIT), Unit B.3, at EU-VERIFY@ec.europa.eu.

The Data Protection Officer (DPO) of the Commission

You may contact the Data Protection Officer DATA-PROTECTION-OFFICER@ec.europa.eu with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

- The European Data Protection Supervisor (EDPS)

You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.

10. Where to find more detailed information?

The Commission Data Protection Officer (DPO) publishes the register of all processing operations on personal data by the Commission, which have been documented and notified to him. You may access the register via the following link: <http://ec.europa.eu/dpo-register>.

This specific processing operation has been included in the DPO's public register with the following Record reference: DPR-EC-27509.