



# PRIVACY STATEMENT

## SECABC Platform Ref 091

### 1. What personal data do we collect?

To feed the SECABC Platform, EASA collects the name, surname, email address, business phone number, location, department, Institution from its own staff. This included statutory staff, Temporary agents, Contract agents, service providers, trainees, SNE's, etc. ). EASA obtains its own data via its own mail server and/or other repositories.

This platform allows EASA to access the data from the other EUIBAs (European Union Institutions), which are joint-controllers of the data maintained in the platform and which responsibilities are established in the Master Data Processing Agreement co-signed by all EUI's listed in the Public Record.

This processing operation does not relate to a) any processing activity related to the user authentication via EU Login (only for EUIBAs admins); nor b) any processing activity by the participating EUIBAs related to the management of their respective individual address books and secure email certificates.

### 2. For what purpose do we collect personal data and on which legal basis?

The purposes for this processing are:

To enable SECEM (secure e-mail solution) between EASA and EUIBA's (European Union Institutions Bodies and Agencies). To do so, public key certificates must be exchanged between those who want to participate in the Secure Mail Exchange solution proposed by the European Commission.

To make available contact information from EUIBA's in the mail client address book for EASA users.

The processing is necessary for the performance of a task carried out in the public interest/ in the exercise of official authority vested in the joint controllers, in accordance with point (a) of Article 5(1) of Regulation (EU) 2018/1725.

- ✓ Registration of entities (participating EUIBAs).
- ✓ Generating and managing the email certificates (public keys).
- ✓ Exchanging and/or storing the address book.

In line with Article 36 of Regulation 2018/1725 (EUDPR) – the EC and all institutions are obliged to ensure the confidentiality of electronic communications, in particular by securing their electronic communications networks.

Under art. 1, 7 and 8 of the Commission Decision 2017/46, DIGIT and each Commission department should ensure that appropriate IT security measures are implemented for all IT tools making sure that are proportionate to the IT security risks identified including both internal/external communications from/to the EC.





In line with the obligation of the EC to keep its information systems secure, this processing is also necessary with a view to complying with Article 33.1 (a) (b) and (c) of the Regulation 2018/1046 that refers to the performance and principles of economy, efficiency and effectiveness.

All EUIBAs listed in the public record are joint-controllers of the data processed in the platform, in accordance with the MASTER DATA PROCESSING AGREEMENT.

### 3. Who may receive your personal data?

All EASA staff who has an @easa.europa.eu mail address (statutory staff, Temporary agents, Contract agents, service providers, trainees, SNE's, etc.)

Each EUIBA shall will transmit the personal data into the following IT systems: the SECABC platform only. Such transmissions take place in compliance accordance with the agreed purposes of processing as laid down in the Master Data processing Agreement.

The EASA IT System Administrators will to perform operational activities associated to the maintenance, correction, update of its data onto the Platform. The EASA IT Security officer for following up on security incidents and investigations.

DG DIGIT will provide for the development, operation, administration and maintenance of the SECABC platform.

### 4. How long are your personal data kept?

Personal data of each EUIBA will be stored for as long as they participate in the SECABC Platform and are a party to the Master Data Processing agreement.

Every time a new file is uploaded, the existing data of each EUIBA, in this case EASA, is overwritten by this new data and no copy of the old data is retained.

The Parties shall not retain or process personal data longer than necessary to carry out the purposes of this processing nor the obligations to which they commit under the Master Data Processing Agreement.

### 5. What are your rights?

You have the right to request from EASA access to and rectification or erasure of your personal data or restriction of processing.

You also have the right to object to processing of your personal data.

EASA should provide information on action taken on a request within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

A breach concerning your personal data should be communicated to you under certain circumstances. EASA should also ensure the confidentiality of electronic communications.





## 6. Who is the data controller and how to exercise your rights?

EASA should exercise the tasks of the data controller for the purpose of these processing operations.

To exercise the mentioned rights, you can contact the controller by sending an email to:

[servicedesk@easa.europa.eu](mailto:servicedesk@easa.europa.eu)

If you consider your data protection rights have been breached, you can always lodge a complaint with the EASA's Data Protection Officer ([dpo@easa.europa.eu](mailto:dpo@easa.europa.eu)) or with the European Data Protection Supervisor: [edps@edps.europa.eu](mailto:edps@edps.europa.eu).

