

Privacy Statement

Privacy statement for users registered with the European Commission's Identity Management Service

1. What is the Identity Management Service?

The European Commission's Identity Management Service (IMS) provides a common way for users to register or be registered for access to a number of different Commission information systems or services (referred to hereafter as *sites*).

You are affected by this privacy statement if you use the European Commission authentication service (EU Login) when logging into Commission sites, as it means that you have been registered in IMS.

Users include the Commission's own staff, personnel of other organisations and members of the public.

Registration may occur:

- at the initiative of a user or of the organisation that the user belongs to or represents
- by means of an automatic transfer of information from the user's organisation to the Commission
- by means of direct entry of the relevant information by the user

IMS includes facilities for authenticating registered users and controlling their access to Commission sites.

In each case, the personal data that is recorded is governed by Regulation (EC) 45/2001.

IMS falls under the responsibility of the Controller, Ms Gertrud Ingestad, Director General, Informatics DG. Further responsibility lies with each processor of the information.

Individual Commission sites that rely on IMS for commonly required personal data may nevertheless collect additional personal data themselves. This is covered by the sites' own privacy statements.

2. What information do we collect, for what purpose and through which technical means?

In general, registration is required:

- if access to a site is restricted to authorised persons
- if there is a simple need for the site to remember you between visits and adapt itself to your needs or wishes
- to allow you to receive further information that you have requested, such as newsletters and information updates
- to grant you individual privileges that you might request or otherwise be entitled to

We store the information that you provide on the registration form (if you registered yourself) or that your organisation provides directly to us. The information you provide may be made available to Commission sites other than the one for which you originally obtained the account provided that you attempt to access them while logged in using your account. By logging in and accessing accounts you are indicating your consent to the use of the data as described in this statement.

The data obtained from the registration process includes both personal details and, if you are registered as a representative or member of an organisation, details related to your link with that organisation. Personal details include your names, geographical location, areas of interest (with respect to the Commission), e-mail address and telephone number. Concerning your organisation, the details may include its name, the department you work for, your office address, the nature of your relationship with the organisation (e.g. employee), your roles and job title and, in order to avoid creating duplicate records, a unique identifier. Information that is obtained from your organisation is subject to the regulations concerning the transfer of personal data and may be only a subset of that mentioned.

The account that we create contains enough information for us to have reasonable confidence that its subsequent usage is by yourself or someone with access to the information you provided (including the password).

We also store certain additional information (listed below) relating to the activity on the user account that we create for you, so that we can protect both your identity and the integrity of the Commission systems that you access.

The additional information is used to diagnose and resolve problems and to deal with security incidents. Much of it relates to attempts to use an identity and thus to events that occur before a user has successfully authenticated.

The Identity Management Service also stores a list of the access rights granted to you by the Commission for the purpose of granting or denying access to individual sites.

Users can inspect all the data that is maintained about their own account, allowing them to check that their account has not been used, and that attempts have not been made to use it, without their knowledge.

We may 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
- Number of good logins and failed attempts
- Your most recent passwords - to make sure you follow the prevailing security policy regarding password re-use.

When you login and / or change your password, we may record further information in log files, such as the IP address used, in line with the purposes stated above. This information can help in following up any doubtful activity relating to your account. It will **not** be used to monitor your activity, except to allow the removal of the account when no longer used.

Many Commission sites use the European Commission authentication service (EU Login) for user authentication: EU Login has a special user interface, independent of the client site and provides a single sign-on experience. Some of the information mentioned here is not relevant for the Commission sites that do not use EU Login – if you never login through EU Login it will therefore not be maintained in your account data. Note that logging in through EU Login always involves a page distinctively marked with the EU Login logo. Each time you login to a site protected by EU Login, the identifier, the site and the time will be recorded in a log file. We do not record the time you spent logged in to a site. However, if you logout of EU Login, which is not normally necessary, the time at which you do so will be recorded.

Note: use of cookies

EU Login uses cookies to allow you to log in to different applications without re-entering your email address and password. These cookies contain no personal information whatsoever, merely a pointer allowing the authentication service to find your entry in its own tables. The cookies are 'per-session' cookies, i.e. they are destroyed when you close your browser. If you have chosen

the option for your browser not to accept such cookies, you will not benefit from this feature and will have to re-authenticate yourself each time you log in to a different client application of the authentication service. A persistent cookie may be created for your convenience in order to record your choice of language, and at your discretion, your email address. In the absence of this cookie, the default language is English.

3. Who has access to your information and to whom is it disclosed?

By registering yourself, you authorise the disclosure of the details you have entered in the user registration system to any Commission site that you access after having given your email address and password. If you were registered by your organisation, your consent is assumed to have been given (implicitly or explicitly) for the transfer of your details.

The details of the activity associated with your account are never passed to any other Commission site by IMS.

The Commission will not divulge your information to third parties outside the Informatics DG with the following exceptions:

- the duly authorised support unit or help desk responsible for the domain in which you are registered
- duly authorised bodies, on a case by case basis: OLAF, internal Commission Security Directorate or disciplinary bodies, the Ombudsman, the EDPS.

To preserve your privacy, you can choose (through an option on the login screen) to be notified whenever a relying party (i.e. a Commission site) requests your identity - you will have the option to cancel the operation before any information is passed. However, this may render the application inaccessible to you. If, having logged in into EU Login, you wish to access sites anonymously, you can do one of the following before connecting to the site in question:

- open a new browser session and use it to access the site
- logout from the authentication service
- disable cookies in your browser options

Note that behaviour varies from browser to browser and may affect the results of these operations.

If you need to access a Commission site that requires you to register and authenticate, but you do not wish it to have access to the details you supplied in order to gain access to another Commission site, we suggest you create a separate account for this purpose. This will require you to provide a distinct e-mail address, which need not be traceable to you personally. Of course, this may deny you access to certain sites which require proof of identity.

Your password is stored only in an irreversible form. Apart from your password, the service administrators can view all of the data pertaining to a particular user. This helps them to perform duties such as helping users with problems and diagnosing suspected security incidents.

4. How do we protect and safeguard your information?

The Commission stores your personal information in secure computers and your information can only be accessed by authorised persons and internal sites.

When you login, the password is always encrypted on the network and is decrypted for checking against the stored password by the authentication service, not by the individual site. All passwords (including previous passwords mentioned above) are stored in a form that permits

them to be checked against a supplied value, but their actual value cannot be derived from the stored value.

The details about your user account are available only to yourself and the service administrators.

If you registered yourself directly, you should be aware that anyone with access to read your e-mail may be able to use the account you create and acquire the identity it represents. You are responsible for assessing the risk that this presents to you personally.

Similarly, certain users are allowed to reset their password using e-mail. They should bear in mind that anyone else with access to their e-mail (because of automatic forwarding, delegation or other reasons) will be able to reset the password.

For this reason, in order to perform important business or access sensitive information, the Commission requires more stringent identity checks and your account will need to be set up or transformed specifically for this purpose. You will need to contact the relevant Commission department or a delegated representative in your organisation to achieve this.

If you have any reason to believe that your password has been compromised – for example, if your password appears to have been changed without your knowledge - you should notify your normal support contact or contact the Commission as described on the user registration and authentication pages.

Notes:

In principle, and especially if you have access to sensitive systems, you should never reveal your password to anybody else: it is a secret only you should know. In particular, your EU Login password should only ever be entered on screens showing the approved EU Login logo. Do not enter it if you have doubts about the authenticity of the EU Login site.

When you enter your password, make sure your browser indicates (usually by means of a padlock or other icon) that you are on a secure connection and that you are connected to a Commission site address (e.g. ec.europa.eu, webgate.eu-admin.net).

5. How can you verify, modify or delete your information?

You can verify your account information, including the data recorded about activity on your account, in the pages of either the user registration service or the authentication service (EU Login). This excludes information that is only held in log files: if you wish to access your log file entries, you may request it by writing to the Controller at the address given below. A response will be given within a period of six weeks from the date of receipt of the request.

In case of difficulty, you can obtain help by following the contact link below (see point 7).

If you registered yourself in the Commission's system, you will be able to change or remove any personal information on-line. However, if your details were registered through a third party, this may not be possible and you will have to contact that third party in order to have the information changed: you may nevertheless have the information removed by the Commission, but if the third party re-submits this information to the Commission, it will be re-instated.

Since it is collected automatically, it is not possible to modify any of the technical data held by the authentication service, with the exception of the password itself.

6. How long do we keep your data?

The Identity Management Service keeps your data for as long as you are recorded as an active user and for a period of one year thereafter. Data concerning users automatically registered from internal sources (in the Commission and certain other EU bodies) may be kept for as long as it is retained in the source system. If you were registered through a third party, the period of activity will usually correspond to a contractual link with that party or be subject to an expiration date. In

other cases, the Commission will consider you active as long as you continue to use your account or until your account expires.

Note that in the case of users who registered with IMS themselves, the period of one year is extended in order to allow the exchange of e-mail with a user. This exchange will provide for the user to request an extension, thus resetting to zero the recorded period of inactivity. In the absence of a response from the user, all personal data will be erased.

Data from the Identity Management Service is backed up regularly by the Commission to ensure a correct system restore if necessary to restart operations. Furthermore, the Identity Management Service is closely monitored and all sensitive actions on the system are logged, including each authentication request. These logs (log files) are rotated regularly and removed from the active system after a maximum of six months in accordance with REGULATION (EC) No 45/2001. All log files backed up by the standard Commission's backup procedure will not be removed from back-up tapes until those tapes are recycled, but that log data will not be restored if system restore is required.

7. Contact Information

If you wish to ask questions or post complaints about the service with respect to the use of your personal information, you should follow the contact link that is shown on each Identity Management service page or write to the following address:

The Director General
Informatics DG
European Commission
200 rue de la Loi
B-1040 Brussels

8. Recourse

If necessary, complaints can be addressed to the European Data Protection Supervisor.