



European Economic
and Social Committee

Record of processing activity Part 1

Name of the data processing	Management of the EESC intranet site
Created on	15/10/2018
Last update	04/05/2020
Reference number	018
Year	2018
1. Controller:	European Economic and Social Committee
2.a) Service responsible	D3 INF
2b) contact details	webeesc@eesc.europa.eu
3. Joint controller	Not applicable
4. DPO: contact details	data.protection@eesc.europa.eu
5. Processor(s) (where applicable)	Matomo for web analytics (privacy@matomo.org)
6. Purpose(s) of the data processing	The EESC intranet is an internal working tool and information channel for the staff and members of the EESC and the CoR, and the Joint services staff.
7. Description of the categories of persons whose data are processed	EESC and CoR staff and members (authenticated users)

8. Description of data categories processed

"Who does what" display on intranet pages: automated procedure for collecting information (name, official work title, office number, phone number, e-mail) from the staff database (Sysper, [[ECAS/Sysper data protection notice](#)]), structured according to Directorates/units. Photos are automatically imported from the Sysper database, in case the person agreed with the publication [[EESC staff pages data protection notice](#)]

User traffic: The *SharePoint Analytics tool* and the *Matomo web analytics tool* extract information regarding authenticated user traffic. Information obtained is used only to create anonymised reports and is used solely for EESC intranet data collection regarding measurement purposes, usage monitoring and performance evaluation.

It does not entail any kind of staff evaluation or personal preferences data usage.

Examples of data collected are: top pages, average number of daily unique visitors, page views, busiest day and time, search words.

Data is anonymised.

9. Time limit for retaining the data

Intranet content (texts, documents, calendars, images, videos, references): accessible until the Intranet contributors or Intranet owners removes it.

Who does what: data from the staff database (Sysper) is accessible until the person's user id is no longer active (name, official work title, office number, phone number, e-mail, photo). Users can remove their photo from Who does What [<http://intranet.eesc.europa.eu/EN/Pages/picture-who-is-who-sysper.aspx>]

User traffic:

- The EESC intranet data in the SharePoint environment is stored for 15 calendar days (with backups on tapes, kept for a period of 3 months).
- The Matomo web analytics tool extracts user traffic data. All user traffic data is deleted after 24 months and 24 days.
- Published reports with anonymised data: no time limit.

10. Recipients of the data

Access to anonymised data is disclosed to staff and members of the EESC and the CoR and Joint services staff via the regular reports.

Access to data is defined by SharePoint permission groups:

Intranet Visitors: All EESC-CoR intranet end users are identified with a user name and password. They have read-only rights.

Read-only rights = This permission level allows to view items and pages and open items and documents. They can see the pages displaying the Who is who lists. They do not have access to any web analytics data.

Intranet Contributors: Intranet Contributors are responsible for uploading content on their respective sections of the intranet (texts, documents, calendars, images, videos, references), having obtained the consent from the persons appearing in them. They have read and contribute rights.

Contribute rights = This permission level allows to add, edit and delete items in existing lists and libraries pertaining to pre-defined specific sites. They do not have access to any web analytics data.

Intranet Owners: Intranet Owners are the intranet webmasters and IT staff dealing specifically with the EESC intranet. They have full control rights.

Full control = All permissions. This permission level allows to add, edit and delete items in existing lists and libraries pertaining to all sites, create lists and libraries and access to statistics. They have access to the anonymised web analytics data, with a specific password.

Matomo web analytics superuser: authorised staff of the IT unit have super user access to the Matomo web analytics tool. They have the possibility to enable or disable anonymisation of personal data, such as the IP addresses and user id. By default the user traffic is anonymised.

Third parties: Transfer of anonymised data to third parties (such as external contractors) may be performed only to create analytics reports and is used solely for EESC intranet data collection regarding measurement purposes, usage monitoring and performance evaluation and analysis. Examples of data collected are: top pages, average number of daily unique visitors, page views, busiest day and time, search words.

Via an automated procedure non-anonymised data from the EESC intranet is transferred to the Matomo/InnoCraft cloud server. EESC staff does not have access to these log files. InnoCraft guarantees the confidentiality of personal data processed and will not access it except on express demand from the EESC. For more information see point 13.

11. Transfers of personal data to a third country or an international organisation

No transfer of personal data to a third country takes place. The EESC intranet data is stored in a database in the Innocraft/Matomo Analytics Cloud, on servers located in Paris, France.

12. General description of security measures, where possible

See DPA of Innocraft <https://www.innocraft.cloud/dpa>.

Only a very limited number of authorised staff (Matomo web analytics superuser in the IT Unit) have the possibility to disable the anonymisation of personal data processed.

13. Privacy statement

[EESC Intranet](#)

Part 2 Compliance check and risk screening

1.a) Legal basis and reason for processing

- necessary for the performance of a task carried out in the public interest
- (a) or in the exercise of official authority vested in the Union institution or body
 - (b) necessary for compliance with a legal obligation to which the controller is subject (see point 1b) below)
 - (c) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
 - (d) the data subject has given consent to the processing of his or her personal data for one or more specific purposes
 - (e) necessary in order to protect the vital interests of the data subject or of another natural person

[Tick (at least) one of the boxes]

1b) Legal basis

The legal basis is article 5, par. 1, letter (a) of Regulation(EU) No 2018/1725 as it is necessary for the EESC's performance of its tasks. Some personal data are processed on the basis of consent (Article 5, par. 1, letter (d) of Regulation (EU) No 2018/1725).

2. Are the purposes specified, explicit and legitimate?

The purpose of the processing is to guarantee the good functioning of the intranet of the EESC.

3. Where information is also processed for other purposes, are you sure that these are not incompatible with the initial purpose(s)?




Not applicable.

4. Do you really need all the data items you plan to collect?

Yes, all the data is necessary.

5. How do you ensure that the information you process is accurate?

Not applicable

6. How do you rectify inaccurate information?	Not applicable
7. Are they limited according to the maxim "as long as necessary, as short as possible"?	Yes
8. If you need to store certain information for longer, can you split the storage periods?	Not applicable
9 How do you inform data subjects?	This information is included in a privacy notice available in the footer on all pages of the EESC intranet.
10. Access and other rights of persons whose data are processed	In order to exercise their rights, data subjects can contact the controller. Questions will be answered within 15 working days.
11. Does this process involve any of the following?	<input type="checkbox"/> (a) data relating to health, (suspected) criminal offences or other special categories of personal data <input type="checkbox"/> (b) evaluation, automated decision-making or profiling <input type="checkbox"/> (c) monitoring data subjects <input type="checkbox"/> (d) new technologies that may be considered intrusive
Part 3 Linked documentation	
1. Links to threshold assessment and DPIA (where applicable)	 No hyperlink inserted
2. Where are your information security measures documented?	 No hyperlink inserted
3. Links to other documentation	 No hyperlink inserted
4. Other relevant documents	