European Economic
and Social Committee

Record of processing activity
Part 1

Name of the data processing	Management of Directorate for Translation's intranet
Created on	26/09/2020
Last update	01/09/2020
Reference number	055
Year	2019
1. Controller:	European Economic and Social Committee
2.a) Service responsible	T1 TMU
2b) contact details	Head of Translation Management Unit, Directorate for Translation contact: dt-strategy@eesc.europa.eu
3. Joint controller	Not applicable
4. DPO: contact details	data.protection@eesc.europa.eu
5. Processor(s) (where applicable)	Matomo Web Analytics (privacy@matomo.org)
6. Purpose(s) of the data processing	DT intranet is an internal tool for the staff of the Directorate, as well as for other staff at the Committees. The intranet allows staff, *inter alia*, to find out other staff members and their contact details, find administrative information, view media files and internal communications or access different applications needed in their everyday work. To serve its purpose, its use needs to be continuously monitored and evaluated.

7. Description of the categories of persons whose data are processed

EESC and CoR staff and members (only authenticated users)

8. Description of data categories processed

Who Does What pages – a webpart on some intranet pages displays information (name, official work title, office number, phone number, email) by automatically retrieving it from the staff database (Sysper). The information is structured per unit. Photos are automatically imported from Sysper, if the person has agreed with the publication.

Intranet usage – Matomo Web Analytics extracts information about user traffic. The information collected is summarised in reports with the purpose to measure, evaluate and further develop the DT intranet.

Collected data include, for example: IP address, user ID, number of unique visitors, search keywords, unique downloads, unique outlinks, entry and exit pages, acquisition channels (direct entry, referral from elsewhere).

Matomo is hosted in the cloud (servers are located in France) and is accessible by authorised users through dedicated accounts.

All data is anonymised. IP addresses are anonymised by default, by the removal of the last several bytes, resulting in the same IP address being assigned to all users. Users are assigned unique alphanumeric strings – user IDs – which are used to track their actions. While anonymisation can be turned off by authorised IT staff, it is impossible for the DT to physically identify users from these user IDs.

9. Time limit for retaining the data

Intranet content (text, images, videos, calendars, links) is accessible until removed by the content owner.

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

Matomo user traffic data is kept for 744 days.

Generated anonymous data reports regarding intranet usage are kept indefinitely by the DT.

10. Recipients of the data

Access to intranet content is defined via SharePoint permission groups.

Intranet visitors: all authenticated EESC/CoR users, identified by their username and password. They have read-only access. This allows them to view pages and items, open documents and items, and see the content of Who Does What pages. They have no access to Matomo web analytics data.

Intranet members: Directorate for Translation staff. They have Contribute – no delete access. This allows them to view, add and update list items and documents, view pages on which such items and documents are displayed, and see the content of Who Does What pages. They have no access to Matomo web analytics data.

Unit webmasters: have full control over their unit's websites. This allows them to: view, edit, add or delete items, documents, lists, libraries, pages and websites; create and manage sub-sites; view, edit, add or delete access groups. They have no access to Matomo web analytics data.

Intranet owners: a very limited group of people who have full control over the whole DT intranet. Group members can: view, edit, add or delete items, documents, lists, libraries, pages and websites; create and manage sub-sites; view, edit, add or delete access groups. They have no access to Matomo web analytics data.

DT webmaster:

The DT webmaster has full control over the whole DT intranet. This allows him to: view, edit, add or delete items, documents, lists, libraries, pages and websites; create and manage sub-sites; view, edit, add or delete access groups.

The DT webmaster is also the Matomo web analytics administrator for the Directorate for Translation. This allows him to view anonymised analytics data, generate anonymised reports and grant or revoke access to Matomo web analytics for the DT intranet.

Matomo web analytics superuser: authorised staff of the IT unit have superuser access to Matomo web analytics. They can enable and disable the anonymisation of personal data, such as IP addresses and user IDs. User traffic is anonymised by default.

Third parties: anonymised data transfer to third parties may be carried out only for the purpose of generating anonymised reports used for DT intranet performance monitoring and evaluation. Examples of data collected include: number of unique visitors, number of pages viewed, search keywords used.

Anonymised data from DT intranet are automatically transferred to the Matomo/InnoCraft cloud servers. DT staff have no access to these files. InnoCraft guarantees the confidentiality of the data and will not access them unless explicitly asked by EESC/CoR.

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

There is no transfer of personal data to third countries. The Matomo/InnoCraft cloud is hosted on servers located in France.

12. General description of security measures, where possible	Only a very limited number of authorised staff at the IT unit (Matomo superusers) can disable the anonymisation of personal data. For the Matomo/InnoCraft data protection agreement, see https://www.innocraft.cloud/dpa
13. Privacy statement	Directorate T intranet

Part 2
Compliance check and risk screening

1.a) Legal basis and reason for processing	☑ (a) 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 □ (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	
2. Are the purposes specified, explicit and legitimate?	Yes. The purpose of data processing is to ensure the smooth operation of the DT intranet as a working tool for DT staff
3. Where information is also processed for other purposes, are you sure that these are not incompatible with the initial purpose(s)?	Not applicable. There is no data collection for other purposes.
4. Do you really need all the data items you plan to collect?	All data are necessary.
5. How do you ensure that the information you process is accurate?	Information is automatically extracted from official databases and is not processed.
6. How do you rectify inaccurate information?	Anyone can request the rectification or removal or erroneous information by contacting the DT webmaster.

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?	Retention periods are indeed split (see section I.9).
9 How do you inform data subjects?	A privacy statement is published in the intranet. A record of the processing is also published in the data protection register.
10. Access and other rights of persons whose data are processed	Data subjects can contact the controller with questions on data collection and processing.
11. Does this process involve any of the following?	□ (a) data relating to health, (suspected) criminal offences or other special categories of personal data □ (b) evaluation, automated decision-making or profiling □ (c) monitoring data subjects □ (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	