European Economic and Social Committee

Record of processing activity
Part 1

Name of the data processing:	Processing of mission requests and reimbursements— MiMa
Created on	28/11/2020
Last update	
Reference number	035
Year	2018
1. Controller:	European Economic and Social Committee
2.a) Service responsible	E5 FIN
2b) contact details	Head of the Finance and Financial Verification Unit – E5 FIN, Directorate E – Human Resources and Finance. missions-cese@eesc.europa.eu
3. Joint controller	Not Applicable
4. DPO: contact details	data.protection@eesc.europa.eu
5. Processor(s) (where applicable)	The Committee's travel agency acts as its subcontractor with regard to the booking, issuing and billing of transport tickets and to hotel bookings in relation to trips taken by Committee staff in the interest of the service ("missions"). The data are processed in accordance with the applicable provisions on data protection, as explained in the privacy statement available at https://www.mycwt.com/legal/global-privacy-policy/. The provisions on marketing do not apply to staff members. Staff will not be sent any marketing communications. Likewise, the provisions concerning CWT online tools do not apply to staff. Communication with the travel agency is via the Finance and Financial Verification Unit E5 FIN. Contact: globalprivacv@carlsonwagonlit.com

6. Purpose(s) of the data processing	The purpose of the processing is to manage mission requests and claims for the reimbursement of mission expenses for EESC staff using the MiMa IT application. A mission is a trip taken outside Brussels solely in the interest of the service, at the request of the immediate superior or, where appropriate, the appointing authority; the *Mission Guide* (Decision 890/10A of 14 December 2010) sets out the general implementing provisions of Articles 11, 12 and 13 of Annex VII to the Staff Regulations. The MiMa application enables: • a travel order to be drawn up and then electronically validated by all the parties involved, as set out in Decision 890/10A; • claims to be submitted and processed for the reimbursement of expenses incurred in the course of a mission; • all documents relating to a mission to be stored, including travel tickets.
7. Description of the categories of persons whose data are processed	• Officials and other staff of the EESC • EEC seconded national experts (SNEs) • Trainees.
8. Description of data categories processed	

MiMa consists of three different parts:

1. The "**Missions**" section (enabling beneficiaries to submit mission requests and then claims for the reimbursement of mission expenses):

- official on mission: surname, first name, post, staff number
- mission details: place of mission, date and time of start and end of work at the place of mission, departure and return times at the place of employment, means of transport, combination with leave (yes/no), request for payment of an advance on mission expenses, request for derogation if hotel more expensive than the ceiling allows

supporting documents: agenda, programme and reservations.

- The "**Approvals**" section for:
    - approval of the request by the immediate superior(s) of the staff member concerned;
    - processing of the request by missions service managers;
    - approval by the authorising officers of the "missions" heading.

- for approval of the request: surname, first name, post, staff number, work email address of the immediate superior(s) of the official on mission (head of sector, head of unit, director, secretary-general, president, group presidents, etc.)
- for processing the request: surname, first name, post, work email address of the two managers responsible and the functional mailbox of the missions service; surname, first name, post, work email address of the verifiers
- for approval by the authorising officer: surname, first name, post, work email address

supporting documents: agenda, programme and reservations.

The "**Search**" section (search/consultation of all travel orders and the associated reimbursement claims): surname, first name, post, place.

9. Time limit for retaining the data

	In accordance with the requirements of Article 48 of the Rules of Application of the Financial Regulation: "The authorising officer shall set up paper-based or electronic systems for the keeping of original supporting documents relating to and subsequent to budget implementation and budget implementation measures. The systems shall provide for: "(...) d) such documents to be kept for at least five years from the date on which the European Parliament grants discharge for the budgetary year to which the documents relate; Documents relating to operations not definitively closed shall be kept for longer than provided for in point (d) of the first paragraph, that is to say, until the end of the year following that in which the operations are closed. Personal data contained in supporting documents shall be deleted where possible when those data are not necessary for budgetary discharge, control and audit purposes."
10. Recipients of the data	The immediate superiors of the staff concerned, managers, verifiers and authorising officers for heading 162 (staff missions). The EESC travel agency as regards the details needed for issuing travel tickets authorised by the missions service, their proper billing and the associated payment.
11. Transfers of personal data to a third country or an international organisation	

Personal data are not sent to a third country (non-EU Member State) unless a reservation should so require (for example, when travelling to a non-EU country).

In accordance with Carlson Wagonlit Travel's privacy policy, "As a global travel management service provider, [CWT] may transfer your personal data outside of the European Union and European Economic Area. Where we do so to any country not deemed a country of adequate protection by European Commissioners, we make sure such transfers are validated via the recognised European Standard Clauses (also known as 'European Model Clauses') so that your rights are safeguarded.

Given the international nature of CWT services, international personal data transfers are made throughout CWT, its affiliates, joint ventures and global partner network to support travel-related services such as airline ticket issuance and technical help-desk requests, as well as management of meetings and events.

In circumstances where personal data is transferred to, or centrally stored in, countries in which there is not a similar level of protection as in your country, CWT has, where relevant, taken steps to ensure an adequate level of protection of the transferred data by entering into appropriate inter-company data transfer agreements based on the European Standard Contractual Clauses (also known as EU Model Clauses)."

12. General description of security measures, where possible	Access to MiMa is secured by a username and password to be entered when the application is opened. The username and password are stored in Active Directory (AD) and so are the same as the Windows identification data. Users may have up to three different profiles in the application (staff member on mission, immediate superior, financial officer). The rights are distributed by the ABAC local profile manager (LPM) (Unit E5 FIN).
13. Privacy statement	MIMA

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	Decision 890/10A of 14 December 2010
2. Are the purposes specified, explicit and legitimate?	Yes
3. Where information is also processed for other purposes, are you sure that these are not incompatible with the initial purpose(s)?	Yes
4. Do you really need all the data items you plan to collect?	Yes, all the data are necessary.
5. How do you ensure that the information you process is accurate?	The data are extracted from the Sysper application and are regularly updated by the departments responsible for human resources (STA and PER units).
6. How do you rectify inaccurate information?	If a member of staff asks for data to be changed, the corrections will be made as soon as possible and in any case within 15 days.
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?	No
9 How do you inform data subjects?	The MiMa application has a "Data Protection" link at the bottom (left) that leads to the privacy statement.
10. Access and other rights of persons whose data are processed	Data subjects are entitled to request access to their personal data. They also have the right to request modification or deletion of the data and to state their position, to object or to complain. Staff members wishing to request access, correction or deletion or to make an objection may contact the controller (missions-cese@eesc.europa.eu).
	☐ (a) data relating to health, (suspected) criminal offences or other special categories of personal data

11. Does this process involve any of the following?	☐ (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 MiMa data are located in an Oracle relational database and hosted on a physical Oracle server located in the secure computer room on the second floor of the BvS building. A standby copy of this database is located in an Oracle relational database hosted on a physical Oracle server located in the secure computer room on the first floor of the B68 building.
3. Links to other documentation	No hyperlink inserted
4. Other relevant documents	