European Economic and Social Committee

Record of processing activity
Part 1

Name of the data processing	Covid-19 pandemic crisis - follow-up of staff health and safety
Created on	17/04/2020
Last update	17/04/2020
Reference number	069
Year	2020
1. Controller:	European Economic and Social Committee
2.a) Service responsible	E3 STA
2b) contact details	Unit STA.E.3 " Working Conditions, Rights and Obligations, Pensions" Medical and social Service Rue Belliard/Belliardstraat 99 1040 Bruxelles/Brussel
3. Joint controller	
4. DPO: contact details	data.protection@eesc.europa.eu
5. Processor(s) (where applicable)	
6. Purpose(s) of the data processing	

	HRF collects and uses your personal information to establish a list of staff and members infected or potentially infected by the COVID-19 virus and, where necessary, of colleagues who have had contact with them (contact tracing) in order to be able to do the necessary follow up and implement the mitigation measures to protect its staff during the COVID-19 pandemic crisis. This listing will help the EESC to verify the fitness to work, according to the applicable legal and statutory obligations, and continue implementing policies to promote EESC staff health and wellbeing. The collected information will enable the EESC to implement procedures and policies to reduce the risk of infection in its premises, to protect the health of its staff and to provide adequate follow up.
7. Description of the categories of persons whose data are processed	list of staff and members infected or potentially infected by the COVID-19 virus and, where necessary, of colleagues who have had contact with them (contact tracing)
8. Description of data categories processed	In order to carry out this processing operation HRF collects the following categories of personal data: • first name • last name • service • medical status (COVID-19 symptoms; info on COVID-19 symptoms of household members - no names) • result of the test (when the need for testing has been confirmed) • time of onset of COVID-19 symptoms • list of close contacts with the staff member concerned over a period to be determined on a case-by-case basis after appearance of the first symptoms • number of the office and building floor of the staff member concerned • time of recovery necessary for resuming work.
9. Time limit for retaining the data	Your personal data are only kept for the time necessary to fulfil the purpose of collection or further processing, namely: 1. Your personal data are kept by the controller on the drive of the Medical Service for 7 years 2. All the data collected are kept in your medical file in accordance with the retention period applicable to these files, 30/40 years (see privacy statement on the intranet page of the Medical Service)
10. Recipients of the data	

- **Full access**:

- Director of Directorate E, HRF (Human Resources and Finance), controller of this processing and his assistant;
- The Head of Unit of the Medical and Social Service;
- One administrative staff member of the Medical and Social Service designated to follow the list of COVID-19 cases;
- Doctor of the EESC;
- Medical Doctor of the CoR if there is a possibility that the CoR could also be concerned by the case in question

- **Specific access regarding individual case:**

- Directors and their Assistants to the Director of the staff member have access only to the information of the specific case concerning their service that they have reported themselves;
- Line managers of the person concerned inform the Head of Unit of any situation requiring particular attention. They also inform the Medical and Social Service and they list close contacts established together with the Medical and Social Service.
- Business Continuity Officer EESC
- Contact point in DL in order to provide necessary sanitation of offices and shared spaces.

- **Access to the data collected (access to aggregated data only without names):**

- EESC Secretary General and assistants

11. Transfers of personal data to a third country or an international organisation	The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law.
12. General description of security measures, where possible	In order to protect your personal data, the EESC has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored on the servers of the EESC. Decision 223/19A on information security policy of the EESC and of the CoR, adopted on 4/9/2019, provides for security measures for the protection of both Committees' information systems and the information processed therein against threats to the availability, integrity and confidentiality of these systems and information. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

13. Privacy statement	Covid19 - follow up of staff

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	We need to process your personal data because it is necessary: - for the performance of a task carried out in the public interest (Article 5(1) (a) of Regulation 2018/1725), - and also for compliance with Article 1 (e) of the Staff Regulations of officials according to which "Officials in active employment shall be accorded working conditions complying with appropriate health and safety standards at least equivalent to the minimum requirements applicable under measures adopted in these areas pursuant to the Treaties" (Article 5(1) (b) of Regulation 2018/1725). Your medical data is processed for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health (Article 10 (2) (b) of the Regulation 2018/1725).
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
5. How do you ensure that the information you process is accurate?	medical report; information received from the data subject
6. How do you rectify inaccurate information?	

	if a discrepancy is detected, the person concerned is contacted
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?	yes
9 How do you inform data subjects?	we call them
10. Access and other rights of persons whose data are processed	
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	