European Economic and Social Committee

Record of processing activity
Part 1

Name of the data processing:	Background checks for contractor staff
Created on	25/01/2022
Last update	
Reference number	114
Year	2022
1. Controller:	European Economic and Social Committee
2.a) Service responsible	SECU
2b) contact details	Security Service, Directorate L, Joint Services (secu@eesc.europa.eu).
3. Joint controller	
4. DPO: contact details	data.protection@eesc.europa.eu
5. Processor(s) (where applicable)	
6. Purpose(s) of the data processing	The Security service collects and uses your personal information to make an informed decision on whether to grant access to the Committee's premises. Belgian authorities and EU Institutions and Bodies (European Commission, European Parliament, European Council, Council of the European Union, European External Action Service, European Economic and Social Committee, Committee of the Regions, European Defence Agency) ('EUI') have signed in May 2019 a Memorandum of Understanding for the implementation of Security Verification's of external contractors. The verification is at the request of European Institutions and Bodies and will result in either a positive or negative security advice for each individual assessed, granted by the Belgian National Security Authority.

	Any employee of an external contractor who will be subject to a security verification will give his permission to initiate the security verification necessary to obtain a security advice. If the employee of the external contractor refuses to be subjected to a security verification, s/he may express her/his refusal by indicating it on the consent form and sending it, by registered mail. The firm will electronically transmit in an Excel sheet the following data of the person(s) involved: last name, first name, function or profession, nationality, Belgian national number, ID or passport number, date and place of birth, address, company and company ID number.
7. Description of the categories of persons whose data are processed	External contractors staff
8. Description of data categories processed	In order to carry out this processing operation the Security Service collects the following categories of personal data: • Last name and first name; • Address; • Function or profession; • Nationality; • Date and place of birth; • Nationality; • Belgian national number, • ID or passport number, • Date and place of birth, • Company and company ID number; The provision of personal data is mandatory to meet the contractual requirement on services provided on the premises of the Committees. If the personal data are not provided, possible consequences are refusal of access rights to Committees buildings.
9. Time limit for retaining the data	The Security service only keeps the personal data for the time necessary to fulfil the purpose of collection or further processing, namely for five years from obtaining the security advice, which constitutes the latter's maximum validity period
10. Recipients of the data	Access to the personal data is provided by the consent form filled in to the Committees staff responsible for carrying out this processing operation and to authorised staff according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements. The consent form is sent to the Belgian Ministry of Foreign Affairs, who will then have access to the personal data. The information we collect will not be given to any third party, except to the extent and for the purpose that we may be required to do so by law. However, when a negative security advice is received, the Committees will

	inform about it the other institutions and bodies participating in the MoU.
11. Transfers of personal data to a third country or an international organisation	data will not be transfered to a third country or international organisation
12. General description of security measures, where possible	In order to protect your personal data, the EESC/CoR 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	Background checks for external contractor 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	Processing according to lit (a) above refers to the Committee's task of ensuring security in the Committees as provided for by Article 22 (2) of European Commission Decision (EU, Euratom) 2015/443. Processing by the Belgian national authorities is then carried out within the following Belgian legal and regulatory framework on security verifications: - Act of 11 December 1998 on classification and security clearances, security certificates and security advice, its accompanying Royal Decree of 24 March

	2000 and the Royal Decree of 8 May 2018 modifying the aforementioned Decree; - Royal Decree of 8 May 2018 establishing the activity sectors and the competent administrative authorities as referred to in Article 22 quinquies, § 7, - Royal Decree of 8 May 2018 establishing the list of data and information that can be consulted in the context of the execution of a security verification.
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)?	information is not processed for any other purpose
4. Do you really need all the data items you plan to collect?	yes, all the data collected is necessary
5. How do you ensure that the information you process is accurate?	the information is provided by the contractors staff (but checked by the security officer of the contractor) and is checked by the Belgian authorities
6. How do you rectify inaccurate information?	a request for rectification is send to the security officer of the contractor
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?	via a privacy statement
10. Access and other rights of persons whose data are processed	You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access, rectify or erase your personal data and the right to restrict the processing of your personal data. Where applicable, you also have the right to object to the processing or the right to data portability. You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor.
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	