



Secretary General

Personnel, Administration and Budget Unit

European Ombudsman

Public record of processing activity¹:

Collection and use of personal telephone numbers of the EO staff members in the context of the Business Continuity Plan (BCP) and for granting an EU Login access to the Health Insurance tool from outside the office.

1. Last update of this record: 23.03.2020

2. Reference number²: 8/2020

3. Name and contact details of the controller³: European Ombudsman, 1 avenue du Président Robert Schuman, CS 30403, F-67001 Strasbourg Cedex. Contact: PAB Unit, e-mail: EO@ombudsman.europa.eu

Responsible department: Personnel, Administration and Budget (PAB) Unit

4. Name and contact details of the Data Protection Officer: Mr Juliano Franco, Dpo-Euro-Ombudsman@ombudsman.europa.eu

5. Name and contact details of the processor⁴: N/A

6. Name and contact details of the joint controller(s)⁵: the European Commission manages the access to EU Login outside the Office, for the Health Insurance tool (Joint Sickness Insurance Scheme): email: EU-LOGIN-EXTERNAL-SUPPORT@ec.europa.eu

7. Purpose(s) of the processing⁶: to collect the private phone numbers of the EO staff members to contact them in the framework of the implementation of the BCP

¹ To be filled in by the controller. See Article 31(1) and (5) on records of processing activities of Regulation 2018/1725: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725>

² For tracking. If the office decides to keep a central register, contact the keeper of that register to obtain a reference number.

³ Use functional mailboxes as far as possible to ensure business continuity.

⁴ Where applicable. If you use a processor (contractor) to process personal data on your behalf, please indicate so (e.g. 360° evaluations, outsourced IT services or pre-employment medical checks).

⁵ Where applicable. If you are jointly responsible with another EU institution, please indicate so here (e.g. two institutions with shared medical service). If this is the case, make sure to mention in the description who is in charge of what and who people can address for their queries.

⁶ Very concise description of what you intend to achieve; if you do this on a specific legal basis, mention it as well (e.g. staff regulations for selection procedures).



and to grant them an EU Login access to the Health Insurance tool, from outside the EO Office.

Description of the processing: Upon recruitment of a staff member, the PAB Unit asks the staff member to make his/her personal phone number available in SYSPER.

For staff members of the EO Office, the PAB Unit asked each of them whether the data they made available upon recruitment was still correct or asked them to upload the correct data in SYSPER. Existing staff were informed of the new purpose of the data.

The legal basis are Articles 55(1)⁷, 55(3) of the Staff Regulations⁸ and Articles 16 and 91 of the CEOS, the [Ombudsman's Decision on the adoption of a Business Continuity Plan of 25 July 2013](#) and the affiliation to the Joint Sickness Insurance Scheme (JSIS) for EU officials and agents.

8. Description of the categories of data subjects and of the categories of personal data⁹:

- Categories of data subjects: All staff of the European Ombudsman

- Categories of personal data: name and surname, private phone numbers, username or email address.

9. Time limit for keeping the data and, where possible, for erasure¹⁰: Personal data are kept as long as the staff member is a member of the EO Office. As soon as he/she leaves the EO Office, the phone number is kept only if the staff member signals that it has to be used for future contacts with the Administration.

10. Recipients of the data¹¹: Members of PAB Unit who have access to the databanks in which the data is stored. Private phone numbers data are not disclosed to any third parties, except for granting an access to EU Login outside the Office, where the relevant personal data is transferred to the European Commission. In the case of a BCP action, the relevant phone numbers are made available to the Secretary-General, the liaison officers in Strasbourg and Brussels and the crisis management group (CMG).

11. Are there any transfers of personal data to third countries and/or to International Organisations?¹²: N/A

⁷ Article 55(1) SR: "Officials in active employment shall at all times be at the disposal of their institution".

⁸ Article 55(3) SR: "An official may, moreover, be required because of exigencies of the service or safety rules to remain on standby duty at his place of work or at home outside normal working hours. The appointing authority of each institution shall lay down detailed rules for the application of this paragraph after consulting the Staff Committee."

⁹ In case data categories differ between different categories of persons, please explain as well (e.g.: suspects vs. witnesses in administrative inquiries)

¹⁰ Indicate your administrative retention period including its starting point; differentiate between categories of persons or data where needed (e.g. in selection procedures: candidates who made it onto the reserve list vs. those who did not).

¹¹ Who will have access to the data within the European Ombudsman? Anyone outside the office? No need to mention entities that may have access in the course of a particular investigation (e.g. OLAF, EDPS, Court of Auditors).

¹² If yes, include the identification of the country or International Organisation and the documentation of suitable safeguards (e.g. processor in a third country using standard contractual clauses, a third-country public authority you cooperate with based on a treaty).



12. General description of security measures¹³:

Private phone numbers are stored

(a) in SYSPER

(b) in the BCP SMS tool (not linked to a name, only initials).

The phone numbers communicated by each staff member are stored in a secure web-based application. This application, to which only the CMG members and the Information, Communication and Technologies (ICT) team have access, allows the sending of group SMS messages. The data is partly anonymised in the sense that it only links the mobile phone number with the initials of each staff member.

13. Information on how data subjects can exercise their rights of access and rectification, and where applicable, of erasure, restriction and data portability¹⁴:

Data subjects have the right of access to their own personal data and to relevant information concerning how the EO uses it. They have also a right to request from the EO rectification of any incomplete or inaccurate data concerning them. They have a right to object to the use of their data by the EO on grounds relating to their particular situation, at any time. Under certain conditions, they have the right to ask that the EO deletes their personal data or restricts its use. The EO will reply to their requests as soon as possible and within one month at the latest. Data subjects may ask the EO information concerning the processing of their personal data by e-mail (eo@ombudsman.europa.eu). Data subject may also contact the EO Data Protection Officer at any time: dpo-eo-ombudsman@ombudsman.europa.eu.

If data subjects wish to complain about the Ombudsman's handling of their personal data, they may contact the European Data Protection Supervisor: www.edps.europa.eu]

A specific privacy statement is available (in attachment to the record).

¹³ Where possible. Include a general description of your security measures that you could also provide to the public. See Article 33 on security of processing of Regulation 2018/1725: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725>

¹⁴ Consider publishing the relevant part of the privacy statement and providing a link. See Articles 15 and 16 on the information to be provided to the data subject(s) and Article 17 to 22 on the rights of data subjects of Regulation 2018/1725: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725>



Privacy Statement

relating to the collection and use of personal telephone numbers of the staff members of the European Ombudsman's Office

This privacy statement explains the reason for collecting and processing the personal telephone numbers of the staff members of the European Ombudsman's (EO) Office in the context of the Business Continuity Plan (BCP) and for granting an EU Login access to the Health Insurance tool (Joint Sickness Insurance scheme [JSIS] on line) from outside the office; the way the European Ombudsman collects, handles and ensures protection of the data provided; how this information is used; and what rights the candidates may exercise in relation to their data.

The controller is the European Ombudsman. The joint controller is the European Commission, for an access to EU Login (the European Commission Authentication Service) outside the Office, for the Joint Sickness Insurance Scheme on line.

1. What personal data will the European Ombudsman process?

The categories of personal data dealt with in are the names and surnames, private phone numbers, usernames or email addresses.

2. Why does the European Ombudsman process these personal data?

The purpose of the data processing is to contact the staff members of the EO Office in the framework of the implementation of the BCP and to grant them access to the JSIS on line, from outside the EO Office.



3. What is the legal basis and necessity for processing this data?

The legal basis are Articles 55(1), 55(3) of the Staff Regulations and Articles 16 and 91 of the Conditions of Employment of Other Servants, the [Ombudsman's Decision on the adoption of a Business Continuity Plan](#) of 25 July 2013 and the affiliation to the JSIS for EU officials and agents.

Processing is necessary

- for the performance of a task carried out in the public interest (Article 5(1)(a) of Regulation 2018/1725);
- for compliance with a legal obligation to which the controller is subject (article 5(1) (b) of Regulation 2018/1725);
- 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 (article 5(1) (c) of Regulation 2018/1725);
- in order to protect the vital interests of the data subject or another natural person (Article 5(1) (e) of Regulation 2018/1725).

4. Who is responsible for processing the data?

The responsible department in the EO Office is PAB Unit (HR Sector).

5. Who will be the recipients of the data?

The members of the PAB Unit (HR Sector) who have access to the databanks in which the data is stored. In the case of a BCP action, the recipients are the Secretary-General, the liaison officers in Strasbourg and Brussels, the crisis management group (CMG) and the Information, Communication and Technologies (ICT) sector (for access to the application where private phone numbers are stored). Furthermore, the European Commission also receives the private phone numbers for granting an access to the JSIS online outside the Office.

6. How long will the data be kept?

The information is kept for so long as the staff member is a member of the EO Office. As soon as a staff member leaves the EO Office, all his/her personal data will immediately be removed from the phone lists.



7. How do we protect the data subject's data?

Private phone numbers are stored in SYSPER and in the BCP SMS tool.

Private phone numbers are not disclosed to any third parties, except for granting an access to EU Login outside the Office, where the relevant personal data is transferred to the European Commission. The phone numbers communicated by each staff member are stored in a secure web-based application. This application, to which only the CMG members and the ICT sector have access, allows the sending of group SMS messages. The data is partly anonymised in the sense that it only links the mobile phone number with the initials of each staff member.

8. What are your rights and how can you exercise them?

You have the right of access to your own personal data and to relevant information concerning how the EO uses it. You have also a right to request from the EO rectification of any incomplete or inaccurate data concerning you. You have a right to object to the use of your data by the EO on grounds relating to your particular situation, at any time. Under certain conditions, you have the right to ask that the EO deletes your personal data or restricts its use.

The EO will reply to your requests as soon as possible and within one month at the latest.

9. Who to contact in case of queries or complaints concerning data protection issues?

At any time, you may send data protection related questions concerning this processing, at the following address: eo@ombudsman.europa.eu

Head of Personnel, Administration and Budget Unit
European Ombudsman
1 avenue du Président Robert Schuman
CS 30403
F-67001 Strasbourg Cedex

You also may contact the Data Protection Officer of the European Ombudsman at the following address: DPO-Euro-Ombudsman@ombudsman.europa.eu

You may lodge a complaint with the European Data Protection Supervisor at any time at the following address: EDPS@edps.europa.eu