European Ombudsman

Secretary General
Personnel, Administration and Budget Unit

European Ombudsman

Public record of processing activity[1]:

Implementation of the European Ombudsman's Business Continuity Plan and associated Handbook

1. Last update of this record: 17.04.20

2. Reference number[2]: 7/2020

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

Responsible departments: Secretary-General (SG), with the support of the Crisis Management Group (CMG) and the Head of Personnel, Administration and Budget (PAB) Unit (coordinator) - The Crisis Management Group is composed of the Secretary-General, one liaison officer (and one substitute) for each place of work and an ICT correspondent (and one substitute).

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 processor[4]: N/A

6. Name and contact details of the joint controller(s)[5]: N/A

7. Purpose(s) of the processing[6]: to allow the institution, in the context of the BCP, to contact each staff member of the European Ombudsman when necessary.

[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).

Short description of the processing: The Business Continuity Plan (BCP) and the Business Continuity Handbook (BCH) provide the EO Office with a structured approach and guidance to business continuity in order to deal with unforeseen disruptions to the EO's activities that could affect the EO's buildings, operations or staff members. Communication channels used to circulate information to staff and to contact each staff member of the EO Office when necessary, include SMS, email and telephone numbers.

The legal basis is the « *Décision adoptant un Plan de Continuité des Opérations pour le Bureau du Médiateur européen* » of 25 July 2013 : http://www.sisteo.ep.parl.union.eu/SecretariatGeneral/Ombudsmans%20proactive%20work%20documents/Business%20continuity/Décision%20adoptant%20un%20Plan%20de%20Continuité%20des%20Opérations.pdf

8. Description of the categories of data subjects and of the categories of personal data[7]:

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

- Categories of personal data

- Name and surname;
- list of professional phone numbers with professional e-mails and location rooms;
- Private mobile phone numbers;
- The personal data contained in the BCP and Handbook (some names and contact details at the EP, Commission and EDPS, in case of need for coordination with other EU institutions- ex: coordination of security and safety issues, coordination with EP or ICT infrastructure management related to the availability of networks telephone lines)

9. Time limit for keeping the data and, where possible, for erasure[8]: The information is kept for as long as necessary to fulfil the purpose indicated above. Personal data will be kept as long as the staff member is a member of the EO. As soon as a staff member leaves the EO Office, all his/her personal data will immediately be removed from the phone lists in the emergency EO mobile phones and in the sealed envelopes.

10. Recipients of the data[9]:

The EO, the SG, the liaison officers, the ICT correspondent and the Head of PAB Unit.

Personal mobile phone numbers will not be disclosed to any third parties. The BCP is also sent to the European Parliament to the extent that the EO offices are part of

[7] In case data categories differ between different categories of persons, please explain as well (e.g.: suspects vs. witnesses in administrative inquiries)
[8] 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).
[9] 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).

the EP premises. The BCP relies only on having a permanent and reliable contact with the EP security services.

11. Are there any transfers of personal data to third countries and/or to International Organisations?[10]: N/A

12. General description of security measures[11]:

Private mobile phone numbers are stored (a) in two emergency phones kept by the liaison officers in Strasbourg and in Brussels, (b) in the print out in sealed envelopes made available to the Secretary-General and the liaison officers in Strasbourg and Brussels and stored in their private homes, and (c) in an encrypted Excel file, accessible only to the crisis management group, and stored on two USB sticks kept in the Ombudsman's safes in Strasbourg and Brussels.

The mobile 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 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. In order to safeguard personal data against any possible misuse or unauthorized access, electronic information is accessible with a restricted access only (password and sealed envelopes).

Personal mobile phone numbers will not be disclosed to any third parties. Any other personal data may be transferred to the European Parliament in the same way as the BCP itself was.

13. Information on how data subjects can exercise their rights of access and rectification, and where applicable, of erasure, restriction and data portability[12]:

The 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. The data subjects may ask the EO information concerning the processing of their personal data by e-mail (eo@ombudsman.europa.eu). Requests from data subjects will be dealt within one month as a maximum. The data subject may also contact the EO Data Protection Officer at any time: dpo-eo-ombudsman@ombudsman.europa.eu.

[10] 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).
[11] 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
[12] 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

If the 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).

Privacy Statement

relating to the implementation of the European Ombudsman's Business Continuity Plan and associated Handbook

This privacy statement explains the reason for collecting and processing the staff members' data; the way the European Ombudsman collects, handles and ensures protection of the data provided; how this information is used; and what rights they may exercise in relation to their data.

The controller is the European Ombudsman (EO).

1. What personal data will the European Ombudsman process?

The categories of personal data dealt with in the framework of the implementation of the Business Continuity Plan (BCP) are the following:

- name and surname;
- list of professional phone numbers with professional e-mails and location rooms;
- personal mobile phone numbers;
- personal data contained in the BCP (including contacts at the European Parliament, European Commission and European Data Protection Supervisor).

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

The purpose of the data processing is to allow the institution, in the context of the BCP, to contact each staff member of the EO Office when necessary. All personal data submitted will be used for the sole and exclusive purpose of informing staff in case of a BCP action.

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

The legal basis of the processing is the "Decision adopting a Business Continuity Plan for the European Ombudsman's Office" of 25 July 2013.

Processing is necessary for the performance of a task carried out in the public interest (Article 5(1) (a) of Regulation 2018/1725) and 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 departments in the EO Office are the Secretary-General (SG), with the support of the Crisis Management Group (CMG) and the Head of PAB Unit. The CMG is composed of the SG, the liaison officer (and substitute) for each place of work, and the Information and Technology (ICT) correspondent (and substitute).

5. Who will be the recipients of the data?

The EO, the SG, the liaison officers in the two places of work (and substitutes), the ICT correspondent (and substitute) and the Head of PAB Unit.

The BCP is also sent to the European Parliament to the extent that the EO offices are part of the EP premises. The BCP relies only on having a permanent and reliable contact with the EP security services.

6. How long will the data be kept?

The information is kept for so long as necessary to fulfil the purpose indicated above. Personal data will be kept as long as the staff member is a member of the EO. As soon as a staff member leaves the EO Office, all his/her personal data will immediately be removed from the phone lists in the emergency EO mobile phones, in the sealed envelopes and the two secure USB sticks.

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

Data are stored (i) in excel files on a secure driver of the EP which is only accessible to identified staff of the PAB unit; (ii) in sealed envelopes made available to the SG and the liaison officers and stored at their private homes; (iii) in the office's emergency mobile phones for personal mobile phones; (iv) in an encrypted excel file on two secure USB sticks in the Ombudsman's safes (one in Strasbourg and one in Brussels) for the list of personal phone numbers.

Personal mobile phone numbers will not be disclosed to any third parties. They are stored in a secure web-based application. This application, to which only the CMG members and the 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. Any other personal data may be transferred to the European Parliament in the same way as the BCP itself was. In order to safeguard personal data against any possible misuse or unauthorized access, electronic information is accessible with a restricted access only (password and sealed envelopes).

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 the implementation of the BCP within the EO Office, 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