Personal data breaches in access to documents

A personal data breach is defined by Regulation (EU) 2018/1725 as an ‘unauthorised disclosure of, or access to, personal data’. Fiche 22 ‘Personal data breach in access to documents’ explains what are personal data breaches in access to documents, namely the scenario of unauthorised disclosure of personal data in documents released in reply to the request. There are further scenarios by which a personal data breach can occur when handling an access-to-documents request, for example by sending a reply to the wrong applicant or disclosing the identity of an applicant to a third party in the context of a third-party consultation.

Division of tasks and responsibilities

There are two main data protection roles in the access-to-documents processing operation: the corporate (operational) controller, i.e. SG.C1 acting on behalf of the Secretariat-General, and the de-facto (operational) controller, i.e. the unit/department responsible for the handling of the specific request for access to documents acting on behalf of their DG/service.

The de-facto (operational) controller is responsible for:

- establishing the facts of the personal data breach and informing their hierarchy and SG.C1 thereof;
- undertaking all necessary measures to contain the breach and mitigate/eliminate its consequences (including to rectify the erroneous access-to-documents reply and ask the unauthorised recipient for deletion of the data, contact online platforms such as AskTheEU for removal if applicable and conduct an internet search to see whether any of the erroneously disclosed information got indexed/published elsewhere);
- notifying the personal data breach to the corporate (operational) controller using the IT tool provided by the Commission Data Protection Officer (DPO) for recording personal data breaches, including a detailed risk assessment;
- communicating the breach to the data subject(s) affected, if necessary;
- implementing follow-up measures to avoid such an incident from happening again.

The corporate (operational) controller (SG.C1) is responsible for:

- revising the personal data breach notification received by the de-facto (operational) controller and ensuring their transmission to the Commission DPO and EDPS, if applicable;
- further liaising with the Commission DPO and EDPS, if necessary.

IT tool to manage personal data breaches in access to documents

As of 1 January 2021, it is mandatory to use the Personal Data Breach (PDB) module of the Data Protection Record Management System (DPMS) of the Commission DPO for the management of personal data breaches in the Commission. A personal data breach record in DPMS that has been completed and closed constitutes the controller’s documentation of a personal data breach, in accordance with Article 34(6) of Regulation (EU) 2018/1725.

The Commission DPO has circulated detailed guidance on how to correctly produce a personal data breach record in the PDB module to departments. Your local Data Protection Coordinator (DPC) will be able to grant you access to DPMS where the PDB module is located in case you do not have access yet.

---

2 As explained at the access-to-documents coordinators network meeting of 23 October 2020 and subsequently circulated by e-mail.
3 Corporate (centralised) processing operation ‘Handling requests for access to documents lodged under Regulation 1049/2001’, published in the Commission DPO’s register under reference number ‘DPR-EC-00793’.
4 Access to the PDB module is via the DPMS homepage.
Steps to take in case of a personal data breach

1. The member of staff who becomes aware of a (potential) personal data breach informs immediately:
   - the Head of Unit of the unit in charge of handling the request, responsible for the processing operation where a personal data breach has occurred (i.e. de-facto [operational] controller);
   - the DG DPC and the ATD coordinator of the DG/service (the DG DPC provides assistance to the de-facto operational controller and ensures that they have access to the DPMS).

2. The de-facto (operational) controller undertakes all necessary measures to contain the breach and mitigate/eliminate its consequences, namely, if applicable:
   - To rectify the erroneous access-to-documents reply;
   - To ask the unauthorised recipient to delete the data and not to use them in any way, and to provide a written confirmation that he/she has erased all personal data, has not disseminated them (i.e. shared with third parties) and will not use them in any other way (see template);
   - If the initial request and subsequent communication with the applicant have been done online platforms such as AskTheEU, to contact the platform asking for removal of the erroneously disclosed information (see template);
   - To conduct an internet search to verify whether any of the erroneously disclosed information got indexed/published elsewhere, and if the information got indexed/published, to request their removal from the search results / the cache by the search engine or platform.

   \[
   \text{The requests and replies shall be registered in Ares as part of the documentation of the data breach.}
   \]

3. At the same time, the de-facto (operational) controller creates and fills in a PDB record in the DPMS. On request, the DG DPC can assist the de-facto (operational) controller in carrying out the risk assessment and documenting the personal data breach. Consult the PDB record manual for detailed guidance (accessible through your DPC and the guidance tabs in the PDB record).

   \[
   \text{Filling in the PDB record:}
   \]
Under ‘1. General Information / I.1. General information on the personal data breach / Reference of the related processing operation’ indicate the record reference DPR-EC-00793. Some spaces in the record will be filled automatically.

Under ‘1. General Information / I.2 Data Controller / Entity of the Operational Controller (DG.UNIT) you have to indicate the unit of the de-facto operational controller (not SG.C1) where the personal data breach occurred, the record editor(s) of that unit and the Head of the de-facto operational controller (usually, HoU) (otherwise you will lose access to the personal data breach record). Under ‘I.2.1 Operational Controller’ choose the person that heads the entity you selected (usually, HoU). Under I.1 ‘Date and time when the Operational Controller became aware of the breach’, include the time when the de-facto (operational) controller informed the corporate (operational) controller in writing about the existence of a personal data breach. This will usually be the moment of the ARES note sent as explained under step 4 below, unless the de-facto (operational) controller provided already clear, factual and conclusive information about the occurrence of a personal data breach to the corporate (operational) controller under step 1 (in which case the latter correspondence must be registered in ARES and uploaded to the PDB record in DPMS).

Fill in tabs II to IV with the relevant information. Consult the PDB record manual for detailed guidance (accessible through your DPC and the guidance tabs in the PDB record).

4. Without undue delay, and at the latest within 24h of having informed the corporate (operational) controller of the personal breach (if applicable), or of having been informed of the personal data breach by the corporate controller (if applicable), the de-facto (operational) controller generates a draft DPO report (if a EDPS notification is not required based on the risk assessment) or a EDPS notification (if such notification is required) and sends it via ARES note to the HoU of the corporate controller (SG.C1) and the SG DPC (ve_sg.dataprotectioncoordinator) as well as a copy by e-mail to SG DATA PROTECTION COORDINATOR, with EC DPO INTERNAL in cc. The de-facto (operational) shall include in the communication all information relevant for the corporate (operational) controller to assess the personal data breach, including a (registered) proof of the detection date/time of the breach, the correspondence by which the unauthorised disclosure occurred and a copy of the letter sent to the unauthorised recipient/AskTheEU (if applicable).

5. The Commission DPO team changes the access to the PDB record from the de-facto (operational) controller to the corporate (operational) controller (SG.C.1). The corporate (operational) controller revises the PDB record and submits a final version to the Commission DPO (a DPO report or an EDPS notification, if required). The de-facto operational controller must remain available throughout the process for any additional information or assistance the corporate (operational) controller would need for the further management of the breach.

If an EDPS notification is required, the corporate (operational) controller sends a registered notification (as encrypted .zip file) via email to the EDPS (DATA-BREACH-NOTIFICATION@edps.europa.eu), communicating the password to the encrypted file via phone/sms.

6. If, following the risk assessment, the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject(s), the de facto (operational) controller shall inform without undue delay the concerned data subject(s) of the breach (see template letter to the data subject) and shall document this in the PDB record (if the record is still at their level) or forward the registered communication to the corporate (operational) controller.

7. If an EDPS notification is not required, the corporate (operational) controller takes into account Commission DPO’s recommendations and closes the PDB record once the de-facto (operational) controller has provided proof that the personal data breach has been contained and mitigation and follow-up measures completed (cf. explanatory box under step 2).

If the personal data breach was notified to the EDPS, after a conclusive notification to the EDPS, the corporate (operational) controller closes the PDB record once the EDPS has informed the operational controller that he has closed the case.

Reference documents/links:
Fiche 22 ‘Personal data breach in access to documents’, Fiche 9 Third-parties’ personal data (names, signatures, contact details, etc) and Guidance note on access to names and functions of Commission staff of 16 December 2019.

- Standard letters
- PDB record guidance
- DPO Guidance on Personal Data Breach Notifications
- EDPS Guidelines on Personal Data Breach Notification