27 July 2016

Case Reference
2015-0633

REPORT
ON
INSPECTION PURSUANT TO
ARTICLE 47(2)
OF REGULATION (EC) N. 45/2001

European institution concerned:

European Investment Bank

EDPS
Supervision & Enforcement Unit

This EDPS report is destined exclusively to the Services to which it has been expressly addressed and its content must not be communicated to other Services or third parties without the express written consent of the EDPS. Should this report inadvertently come into your possession and you are not a designated recipient, it should immediately be given to the Security Officer of your Service or to the Security Officer of the EDPS.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 32 2-283 19 00 - Fax : 32 2-283 19 50

INSPECTION TEAM

[redacted]	Team leader, Legal Officer
[redacted]R	Inspector, ITP officer
[redacted]	Inspector, Legal Officer
[redacted]	Inspector, Legal Officer

INSPECTION SUPERVISION

[redacted]	Head of Inspections
Maria Veronica PEREZ ASINARI	Head of Unit Supervision & Enforcement

DIRECTOR

Christopher DOCKSEY	Director

SUPERVISOR

Wojciech WIEWIOROWSKI	Assistant European Data Protection Supervisor

TABLE OF CONTENTS

1. Executive summary

The European Data Protection Supervisor (EDPS) is the independent supervisory authority established by Article 41 of Regulation (EC) No. 45/2001 (hereinafter referred to as "***the Regulation***") responsible for:

- Monitoring and ensuring the application of the provisions of the Regulation and any other EU act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a EU institution or body;
- Advising EU institutions and bodies and data subjects on all matters concerning the processing of personal data.

To these ends, the EDPS fulfils the duties provided for in Article 46 and exercises the powers granted in Article 47 of the Regulation. Among his powers to investigate, the EDPS can conduct on-the-spot inspections. The power to inspect is one of the tools established to monitor and ensure compliance with the Regulation.

The inspection at the European Investment Bank ("***EIB***") was designed to investigate and ensure compliance with EDPS decisions in the framework of selected prior checking opinions, a consultation as well as a complaint[1]. It was part of the EDPS annual inspection plan for 2015 and should be viewed as the final stage before formal enforcement action under Article 47(1) of the Regulation. The formal Decision to inspect was communicated to the EIB by means of an Announcement Letter dated 21 October 2015. The fieldwork was carried out from 8 to 10 December 2015 at the EIB premises, 98-100, Boulevard Konrad Adenauer, L-2950 Luxembourg.

This report summarises the findings identified during the inspection. The **main findings** include the following:

- As regards **investigation procedures** by the Investigation Division of the Inspectorate General, the EDPS recommends notably[2]:
  - improving the information of individuals in general as well as of individuals involved in a specific case and documenting any restriction to the right of information of such individuals (Articles 11, 12 and 20 of the Regulation);
  - improving the documentation of transfers to entities outside the EIB (Articles 8 and 9 of the Regulation);

- As regards the **anti-harassment procedure** by the Employee Relations Division, the EDPS recommends notably[3]:
  - Notifying to the EDPS the procedure for selection of confidential counsellors in the context of the Dignity at Work Policy (Article 27 of the Regulation);
  - Updating the Dignity at Work Policy so as to reflect the practice of EIB (i.e. include the mediation phase) and to include the retention periods;
  - Ensuring the information of individuals subject to the Dignity at Work about the processing of personal data in this context (Articles 11 and 12 of the Regulation);

1 -Fraud investigation: Opinion of 14/10/2010 in case 2009-0459 and consultation of 26/03/2010 in case 2009-0854.
- Anti-harassment procedure: Opinion of 20 April 2005 in case 2004-0067; Complaint – L. v. EIB (EDPS case 2011-0754) in connection with the decision of the Court of Civil Service of 10 July 2014 (F-103/11).

2 All recommendations are listed under Section 4.1.6 of this report.

3 All recommendations are listed under Section 4.2.6 of this report.

- Ensuring that individuals involved in a specific case are duly informed about any procedure and documenting any restriction to the right of information of such individuals (Articles 11, 12 and 20 of the Regulation);
- As regards the data to be shared with the alleged harasser during the investigation, ensuring that only the data that are relevant and necessary for the investigation are communicated to the alleged harasser and that the alleged victim is informed about the intended communication so that he/she can exercise his/her right to object under Article 18 of the Regulation;
- Setting up a procedure to ensure effective destruction of paper and electronic files once the retention period has expired.

- As regards the **position of the DPO**, the EDPS encourages designating an Assistant DPO to help the DPO ensure his duties and to ensure continuity of the function in the absence of the DPO[4]. This would also enable the EIB to meet its obligations resulting from the accountability principle.

The recommendations contained in the report must be implemented to comply with the Regulation. The EDPS will carry out a close follow-up; if need be, powers listed in **Annex 1** may be exercised.

2. Objectives, Scope and limitations

The decision to carry out an inspection and its scope were determined by taking into account the following points.

The EIB was included in the EDPS 2015 annual inspection plan on the basis of a general risk assessment and risk analysis exercise. More generally, this inspection is part of the control measures routinely conducted by the EDPS at a number of EU institutions and bodies. The EIB had not yet been inspected except for a targeted issue (CCTV)[5]. The inspection also intended to help raise awareness about the EDPS' supervision activities, and the importance of compliance with data protection rules.

As to the specific scope, it was decided to inspect the following processing operations:
- the *fraud investigation* procedure, as it relates to EIB's core business activity and involves sensitive data as well as transfers to third countries[6];
- the *anti-harassment* procedure, as an EIB staff member filed a complaint with the EDPS in this respect and also brought the case before the Civil Service Tribunal, which condemned the EIB in 2014. The inspection aims at checking the past and current treatment by the EIB of harassment cases[7].

The EDPS inspection team examined the following issues as regards the above-mentioned processing operations:

4 See recommendation mentioned in section 4.3 of this report.

5 EDPS case number 2013-0577.

6 The notification refers to such transfers and in the framework of the Survey 2013, EIB mentioned that it sometimes carries out transfers to investigating authorities in third countries in the framework their cooperation in countering fraud (p. 19 of the Survey report of 24 January 2014).

7 Initially, the EDPS had also decided to inspect the recording of switchboard and security room phone conversations. This was subject to an inquiry launched in 2013 by the EDPS and to a subsequent prior checking notification by the EIB and an Opinion of the EDPS (case 2013-0297). In reply to the announcement letter, the EIB informed the EDPS that no recording had been recently activated and therefore it was decided to drop this part of the inspection.

- Fraud investigations: information of data subjects and exceptions (Art. 10, 11 and 20), transfers (Articles 7-9); data quality in relation to computer forensics activities (Art. 4 of the Regulation), access/incident management (Art. 22);
- Harassment investigation procedures: information (Art. 10, 11 and 20); right of access (Art. 13 and 20), retention period (Article 4), organisational, physical and electronic security (Art. 22).

3. Methodology

The inspection was performed in accordance with the procedures established in the EDPS Inspection Guidelines and by relying on the cooperation of the staff members and managers of the EIB to provide requested information, data, documents and access to premises.

In particular, meetings and interviews were set up and held with staff of the EIB to gather information and obtain access to relevant electronic databases, files and premises. Analysis, reviews and verifications of the information collected, coupled with the outcome of physical examinations carried out by the EDPS team, constitute the basis for the observations and recommendations in this inspection report. The documents collected in the framework of this inspection and mentioned in this report are listed in **Annex 2**.

Minutes of the meetings were drafted in order to document the inspection procedures applied and to provide for a transcript of the conversations with the EIB staff. Two original copies of the minutes were prepared by the EDPS, submitted for comments to EIB[8] and signed by the EDPS inspectors and by the representatives of the EIB for acknowledgment of receipt[9].

4. Analysis and recommendations

4.1 INVESTIGATIONS BY THE FRAUD INVESTIGATION DIVISION

General background

The relevant EDPS files and documents are:
- Case 2009-0459 - Prior checking Opinion of 14 October 2010 - Procedures related to fraud investigations in the EIB Group;
- Case 2009-0854 - Consultation of 26 March 2010 – Access of EIB IT administrators to the personal data stored in EIB's information systems.
- EDPS Guidelines on administrative inquiries and disciplinary proceedings (23/04/2010) ("***EDPS AI and DP Guidelines***")[10].

8 On 8 February 2016.

9 The final minutes were sent to the EIB on 8 March 2016. The EDPS received back one original copy signed by EIB on 16 March 2016.

10 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-04-23_Guidelines_inquiries_EN.pdf

Inspection activities

The inspection activities mainly consisted of: interview with Head and staff members of the Fraud Investigation Division of EIB Inspectorate General ("***IG/IN***"); collection of evidence; interview with case handlers of nine selected fraud cases[11]; demonstration on-the-spot of the selected case files in the case management system and archives; collection of evidence for selected cases; demonstration of the future IG/IN case management system; interview with persons in charge of access/incident management[12].

Inspection topics

While conducting the inspection activities, the inspection team made some general findings (Section 4.1.1.). More specifically, the inspection focussed the following topics: information of data subjects and exceptions (Section 4.1.2), transfers (Section 4.1.3), data quality in relation to computer forensics activities (Section 4.1.4) and access/incident management (Section 4.1.5)[13].

4.1.1 Preliminary observations and general findings

a. Scope of IG/IN activities

IG/IN activities cover:
- internal and external investigations;
- investigations on prohibited conducts under EIB Anti-fraud policy (corruption, fraud, collusion, coercion, obstruction, money laundering and terrorist financing)[14] and investigations on misconduct of EIB staff members, i.e. infringement to EIB's Codes of Conduct.

Moreover, although harassment constitutes an infringement to EIB's Codes of Conduct, harassment cases are subject to a separate procedure under the Dignity at Work policy and out of the scope of IG/IN activities[15].

In view of the above, the EDPS recommends **clarifying the scope** of the 'Procedures for the conduct of investigations by the Fraud investigations Division of the Inspectorate General of the EIB Group' (***'IG/IN Investigation Procedures'***)[16] so as to reflect the actual practice, i.e. that IG/IN activities:
- cover infringement to EIB Codes of Conduct by including a reference to these Codes in the introductory part (the current version only refers to EIB Anti-Fraud Policy);
- do not cover harassment investigations.

The wording of the data protection statement should be clarified in this respect too[17].

11 The EDPS made a random selection of cases based on a list of cases (period 10/2010-10/2015) communicated by EIB (Doc. I.1). The selection made by the EDPS was communicated to the EIB five calendar days before the inspection.
12 See minutes of the inspection, pp. 5-21.
13 These topics were listed in the announcement letter of 21 October 2015.
14 Doc. I.2A.
15 On anti-harassment procedures, see below Section 4.2.
16 Doc. I.2B.
17 See below Section 4.1.2.

As IG/IN investigations covers diverse infringements (Ant-Fraud Policy, Code of Conduct) and various degrees of seriousness, the EDPS also draws EIB's attention to the **necessity and proportionality** principles when processing personal data when they decide on the opening and means to be used for an investigation. Necessity of the processing must be analysed on a case-by-case basis and must be proportionate to the investigation at stake, taking into account notably the seriousness of the alleged fraud or misconduct[18]. In case of doubt, IG/IN should consult the DPO.

b. Future Case Management system

In the follow up to the EDPS prior checking Opinion, EIB announced that a new IG/IN case management system ('***CMS***') would allow notably to track the (non-)information of data subjects[19]. Later in the follow up process, they informed the EDPS that they had stopped using this CMS due to technical issues[20]. Currently the GED (*Gestion Electronique de Documents*) system is still used for storing IG/IN electronic files.

EIB is in the process of acquiring a new CMS. During the inspection, IG/IN made a short demonstration of some features of the future CMS[21], which includes notably an easy tracking of the persons involved in the investigation (data subjects) as well as of any internal and external transfers, plus related documentation[22].

As the current GED does not have these functionalities, IG/IN was not in a position to extract the information requested in the EDPS announcement letter[23] within the time-limit laid down[24]. Therefore, the inspection team limited the amount of information requested (case number, title of the case, opening and closing dates, indication whether it was an assessment or an investigation case) and made their selection of cases to be inspected on this basis.

Conclusion on preliminary observations and findings on IG/IN investigations

See below (Section 4.1.6 List of recommendations):
- recommendation No. 1 as regards the scope of IG/IN activities
- recommendations No. 6 and 8 as regards the required features of the future CMS

4.1.2 Information of data subjects

Background: In its prior checking Opinion[25], the EDPS recommended to "*provide information to data subjects in compliance with Regulation (EC) 45/2001*".

18 These principles are included in the DP Guidance for IG/IN, p. 2 (Doc. I.24).
19 cf. letter from EIB to EDPS of 22 September 2011.
20 cf. letter from EIB to EDPS of 13 November 2013.
21 Doc. II.60.
22 More details in the minutes of the inspection, p. 19.
23 Information in relation to persons involved (whether contacts and interviews have taken place), transfers (to whom) and use of computer forensics.
24 They should have gone through all 500 cases manually to find the information (Cf. email from the DPO to the inspection team of 25 October 2015).
25 Case 2009-0459, Opinion of 14 October 2014.

During the follow-up phase, the EIB informed[26] the EDPS that a special provision on giving access to interview records has been inserted in IG/IN Investigation Procedures and that a privacy statement is inserted in all outgoing correspondence.

The EDPS requested[27] an explanation on how the EIB ensure the right of the data subject to be informed in a case where a restriction is applied on the basis of Article 20 of the Regulation.

The EIB explained[28] that the new IG/IN CMS required for each data subject to specify whether they have already been informed or not and provide adequate reasons (under Article 20) if the data subject is not straight away informed. Furthermore, the system allowed to follow-up on the notification sent to data subject and to have a clear view of which data subject still needs to be notified. The EIB also informed that a special provision would be inserted in the IG/IN Investigation Procedures to ensure that the status of the information of the data subjects is regularly checked by each investigator through the CMS.

The EDPS welcomed the solution proposed by the EIB[29]. Later on, EIB informed the EDPS that IG/IN had stopped using the CMS due to technical issues. Thus, for the time being, IG/IN is entirely relying on the general information management system of the EIB (GED).

Criteria: Articles 11, 12 and 20 of the Regulation
EIB Anti-Fraud Policy[30]
IG/IN Investigation Procedures, especially paragraph 32[31]
Data Protection Guidance for IG/IN, especially paragraph 4[32]

Article 11 and 12 of the Regulation provide a minimum list of information on the processing of personal data that need to be provided to the data subjects (individuals that would be involved in a case). Such information must be twofold: (i) the information to EIB staff and the general public and (ii) the specific information on the processing of the personal information to all individuals affected by a particular investigation.

Action(s): For the selected cases, case handlers were asked to explain how the data subjects were identified in each case, how they have been informed about the opening and closure of a case (both for cases that were closed at the assessment phase and investigation cases) and to provide the EDPS with evidence that this had actually been done[33].

In case the obligation to inform had been deferred, case handlers were asked to identify (a) the note in the file reflecting that this decision has been taken, (b) the reason for restriction, and (c) evidence of regular re-assessment of the deferral decision.

26 By letter of 7 February 2011.
27 By letter of 22 June 2011.
28 By letter of 22 September 2011.
29 By letter of 4 October 2011.
30 Doc. I.2A.
31 Doc. I.2B.
32 Doc. I.24.
33 Actions are reported in the minutes of the inspection, pp. 7-16.

Observations and Findings:

a. General

General information

- No general data protection statement is published on the website or intranet of the EIB on how personal information is processed by the IG/IN.

- The EDPS welcomes that IG/IN attaches a 'privacy statement' to all their outgoing correspondence. The IG/IN has been using an improved privacy statement[34] as of 18 November 2015. However, the privacy statement does not address all the necessary information to be given to the data subject under Articles 11 and 12 of the Regulation. It does not include information about recipients, the legal basis for the processing operation, the time-limits for storing the data nor the categories of data concerned (in relation to Article 12).

Information in specific cases

- The announced CMS was not yet in operation at the time of the inspection (see section 4.1.1 - *Preliminary observations and general findings*). Since GED does not have the same technical features, the EIB cannot easily keep track of the particular information stage for each individual.

- During the assessment phase (i.e. first phase of the investigation procedure), the IG/IN assesses the relevance of the facts and whether an investigation should be opened. Information is not provided to the involved persons during this phase since IG/IN considers that the requirement to inform potentially involved data subjects is satisfied by the inclusion of data protection provisions in the Anti-Fraud Policy[35] and IG/IN Investigation Procedures[36] that are published on EIB's website. The Data Protection Guidance for IG/IN refers to the EDPS recommendation that Article 20 of the Regulation may apply even if IG/IN inquiries do not constitute criminal investigations and that such restriction cannot apply systematically and is subject to a “necessity test” to be conducted on a case-by-case basis. However, no distinction should be made between the assessment phase of the investigation procedure and the proper investigation. The same criteria are therefore applicable for both assessment and investigation phases; specific information should be given to the involved parties unless an exception in Article 20 applies.

- Some features of the **future CMS** were demonstrated during the onsite inspection. It will notably include an 'involved parties and allegations' section that will allow the investigator to identify the persons involved; their role; whether they were informed about the investigation; if so the notification date; if not, the grounds for delaying information as well as further details about the reasons (risk of destruction of evidence, risk of flight from jurisdiction, risk that data subject will inform a person concerned, etc.); an automatic alert will require from the investigator to re-evaluate on a regular basis (60 days were set for testing purposes) the justification for delaying the information[37].

34 Doc. I.17.
35 Section VIII.
36 Section H.
37 Minutes of the inspection (pp. 6 and 19) and Doc. II.67.

b. Analysis of selected cases

The nine selected cases include three assessment cases (i.e. the procedure was closed at the assessment phase) and six investigation cases.

- Data subjects have been identified in 7 out of the 9 selected cases. In 2 cases[38] the informants were not identified as data subjects, although the Data Protection Guidance for IG/IN[39] defines data subjects as the persons concerned, informants, whistleblowers and witnesses. According to the IG/IN the possibility to identify data subjects will be improved with the future CMS.

- Informants - In 2 cases, the privacy statement mentioned above was provided to the informants[40]. In the 7 remaining cases no privacy statement was provided. In 4 of those cases the EIB justified why they did not provide a statement[41] (e.g. the informant was anonymous or the IG/IN met the informant in person). The privacy statement was not provided in the remaining 3 cases[42] due to the fact that IG/IN does not inform data subjects during the assessment phase and because data subjects were not correctly identified.

- Persons under investigation - 2 out of the 9 cases did not identify any persons under investigation[43] and in the 7 remaining cases, suspected persons were identified. In 5 of those cases[44] no information was given, e.g. due to the policy not to inform within the assessment phase, or because the suspected person was identified through open sources or because that the IG/IN did not know how to contact the suspects (explanation provided by the case handlers during interviews, but not documented in the case file). In 2 cases[45] the information was deferred until the invitation of the suspect to an interview by IG/IN or until computer forensics acquisition took place; the justification provided by case handlers was to safeguard the investigation and avoid the risk of destruction of evidence. None of the deferrals were documented.

- Witnesses - One case[46] included witnesses who were informed when they were called for an interview by email and letter which contained a privacy statement.

Conclusion on information of data subjects in IG/IN investigations

Information given to staff in general or to the involved persons does not include all the necessary information pursuant to Articles 11 and 12 of the Regulation. The EIB should adopt a **comprehensive data protection statement** for IG/IN Investigations, which should contain all the information in Articles 11 and 12 of the Regulation (information on the controller, the purpose of the processing - including the scope of IG/IN activities[47]-, the legal basis, the data processed, the recipients of the data, the retention period, the rights of the data subject and the origin of the data). This data protection statement should be published on the intranet.

38 2014-IN-0052 and 2014-IN-0009.
39 Doc. I.22.
40 2015-IN-0025 and 2015-IN-0037.
41 2013-IN-0053, 2013-IN-0007, 2014-IN-0021 and 2015-IN-0021 (staff member and contacted by phone).
42 2014-IN-0052, 2013-IN-0054 and 2014-IN-0009.
43 2014-IN-0052 and 2015-IN-0037.
44 2013-IN-0007, 2013-IN-0054, 2014-IN-0009, 2015-IN-0021 and 2015-IN-0025.
45 2014-IN-0021 and 2013-IN-0053.
46 Case 2013-IN-0053.
47 See above 4.1.1 a.

In addition, specific information must be given individually to the persons involved (suspects, whistleblowers, informants or witnesses) independently of whether the personal data is processed within the assessment phase or the investigation phase, unless Article 20 of the Regulation applies. In this respect, the privacy statement used by IG/IN Investigations for **outgoing correspondence** should be completed by including a **link to the data protection statement** referred to in Recommendation No. 2.

In cases where the EIB decides to apply a restriction of data subjects' rights under Article 20(1) of the Regulation, or to defer the application of Article 20(3) and 20(4)[48] of the Regulation, such decision should be taken strictly on a case by case basis, independently of an assessment or investigation case. The EIB should be able to provide evidence demonstrating detailed reasons for taking such decision (i.e. motivated decision). These reasons should prove that they cause actual harm to the investigation and they should be documented before the decision to apply any restriction or deferral is taken. The reasons should be documented so that, if made available to the EDPS following a request in the context of a supervision and enforcement action, they allow the EIB to demonstrate compliance with Article 20 of the Regulation in the concrete case at hand (i.e. illustrating a case-by-case assessment specific to the case).

In order to help the EIB to comply with the above-mentioned obligations, the future CMS should be featured in such a way so as to identify easily, in each case file, (i) per each data subject whether information in accordance with Articles 11 and 12 of the Regulation was provided and (ii) whether there was a restriction or deferral of the information in accordance with Article 20 of the Regulation.

See below recommendations No. 2 to 6 (Section 4.1.6 List of recommendations).

4.1.3 Transfers

Background:
In the context of fraud investigations, EIB (IG/IN) is likely to transfer data to various (internal and external) **recipients**[49]:

- To other entities inside the Bank, notably for follow up to the investigation report;
- To concerned EU institutions and bodies, mainly OLAF;
- To competent judicial authorities of EU Member States for further investigation and/or criminal prosecution;
- To competent third country authorities and international organisations (such as the World Bank).

In its **prior checking Opinion** on fraud investigations[50], the EDPS insisted in particular on the need to ensure compliance with the principles of Article 9 of the Regulation. As a follow up to the prior checking Opinion, the EIB provided templates of clauses to be used by the EIB when transferring personal data outside the EIB[51].

Criteria:

48 Under Article 20(5) of the Regulation.
49 List of external recipients is listed in paragraph 35 of EIB Investigation procedures (Doc. I.2B).
50 Case 2009-0459.
51 Letter from EIB of 2 December 2011 and reply from the EDPS of 16 March 2012.

- Articles 7 to 9 of the Regulation, including use of appropriate clauses where required
- IG/IN Investigation Procedures, especially paragraphs 9 and 35[52]
- DP Guidance for IG/IN, Section 6[53]

Action(s): For the nine fraud cases selected by the EDPS, case handlers were asked to explain to whom personal data, if any, were transferred. They were also asked to show the EDPS how they complied with Articles 7, 8 or 9 of the Regulation[54].

Observations and Finding(s):

a. Analysis of selected cases

The selected cases include:
- Transfers within EIB and/or OLAF that fall under Article 7 of the Regulation (three cases)[55];
- Transfers to national judicial authorities that fall under Article 8 of the Regulation (two cases)[56];
- No Article 9 transfer[57].

Article 7 transfers
Any communication of personal data, such as final case reports, from IG/IN to other services of the EIB is a transfer under Article 7 of the Regulation[58].

In the three cases inspected, no issue has been identified as to the lawfulness of such transfers as they appeared necessary for the legitimate performance of the tasks of the recipients[59].

The documents transferred by IG/IN to other EIB entities in the cases in question include the following clause (box included in the footer):

> *'This note contains very sensitive information and notably personal data as defined by European Union legislation on the protection of individuals with regard to personal data. Recipients of this note should treat it accordingly with all necessary precautions with regard to strict confidentiality* ***and not forward it or disclose the contents to other persons'***[60].

52 Doc. I.2B.
53 Doc. II.22 (2013 version) and II.24 (2015 version).
54 Actions are reported in the minutes of the inspection, pp. 7-16.
55 Cases 2014-IN-0021; 2015-IN-0053; 2013-IN-0007.
56 Cases 2015-IN-0053; 2014-IN-0009.
57 In some of the selected cases, IG/IN requested information to public authorities outside the EU. However, IG/IN no did not transfer any personal data to these authorities, from what the inspection team could observe in the case files.
58 See the wording of Article 7(1) of the Regulation: *'Personal data shall only be transferred* ***within*** *or to other* [EU] ***institutions*** *or bodies if* (...)'.
59 The cases in question include:
- Transfer of IG/IN final case report regarding an investigation on a staff member's conduct (conflict of interest in the attribution of a contract) to the Personnel Directorate (with Chief Compliance Officer in cc) in order for the latter to decide on possible further disciplinary proceedings (see Doc. II.13);
- Transfer of IG/IN final case report regarding an investigation on a staff member's conduct (unauthorised absences) to the Personnel Directorate in order for the latter to decide on possible further disciplinary proceedings (see Doc. II. 37);
- Request for the opinion of the EIB Legal Service in the context of an investigation on corruption in a third country (Doc. II.55).

60 This is underlined by EDPS. The template of this clause is included in the DP guidance for IG/IN (Doc. I. 22 and I.24).

When a final investigation report is being circulated internally, it is with a view to take possible further action by the recipient[61] (for example a disciplinary procedure when the report concludes to an infringement to EIB Code of Conduct), hence the last sentence of the above-mentioned clause may appear confusing in this respect. In addition, it does not remind internal recipients of documents containing personal data that they must process these documents only for the purposes for which they are transmitted, in accordance with Article 7(3) of the Regulation.

Shortly before the onsite inspection, IG/IN modified the template of the clause[62] which now reads as follows:

> *'This note contains very sensitive information and notably personal data as defined by European Union legislation on the protection of individuals with regard to personal data, in particular Regulation 45/2001.In accordance with Article 7 of the said Regulation, this note is transferred because the data are necessary for the legitimate performance of tasks covered by the competence of the recipient(s). Recipient(s) of this note should treat it accordingly with all necessary precautions with regard to strict confidentiality and only for the purposes for which it is transmitted. Recipients cannot forward this note or disclose its contents to others*'.

The updated version of the clause is appropriate except for the last sentence, which is contradictory with the previous one and should therefore be removed.

In one of the selected cases, a copy of a public report from the third country authorities on local corruption was sent by IG/IN to OLAF for their consideration[63]. This transfer is compliant with Article 7 of the Regulation.

Article 8 transfers
No issue has been identified as to the two cases involving transfer of personal data to national authorities of EU Member States[64], which were made in compliance with Article 8(a) of the Regulation: the transfers at stake, made at EIB's initiative, appeared necessary for the performance of tasks carried out in the public interest or subject to the exercise of public authority. The case files did not contain, however, any **documentation of the assessment made** by IG/IN **before sending out the information**.

b. <u>Other findings</u>

(i) Identification and documentation of transfers
As already mentioned[65], the **current GED** does not allow identifying neither whether transfers occurred in a given case nor the circumstances and documents supporting any transfer, without having to go through the correspondence of the relevant file. There is no centralised register of transfers either. The only tool that enables to have an overview of external transfers is the extended status report, which is available to IG/IN team members only[66] and which contains a summary of info on each fraud case (including external referrals if any). The **future CMS**, a some features of which were demonstrated during the onsite inspection, will enable to identify easily, in each case, if personal data were transferred, to whom, the legal

61 See EIB investigation procedures, paragraph 28 (Doc. I.2B).
62 See template include in the document called 'DP Guidance for IG/IN' dated 30 November 2015 (Doc. I.24).
63 Minutes of the inspection, p.16.
64 Respectively to a local prosecutor and to local police.
65 See above Section 4.1.1.
66 Template of the status report (long version) (Doc. II.3).

basis for the transfer and the data transfer document (with underlying documents to support, justify and explain the transfer)[67].

(ii) EIB Investigation Procedures v. practical implementation
While going through the selected cases, the inspection teams noted the following **discrepancies** in the practices vis-à-vis EIB Investigation Procedures[68]:

- While EIB Investigation Procedures[69] indicate that IG/IN notify OLAF about all investigation cases (both external and internal) as soon as there are grounds to suspect any prohibited conduct, IG/IN mentioned notifying internal investigations proactively to OLAF when they involve potential fraud the financial interests of the EU, and not if they only relate to Code of conduct cases[70];
- The quarterly status report of ongoing investigations (which does not contain any personal data) is shared with external auditors[71] whereas EIB Investigation Procedures[72] do not mention them as recipients of the report.

(iii) IG/IN Guidance on data protection
Ahead of the onsite inspection, IG/IN provided a just updated 'Data Protection Guidance for IG/IN'[73]. As regards transfers, the EDPS notes significant improvements vis-à-vis the previous version of the Guidance[74]. In addition to the above-mentioned recommendation as regards the internal transfer clause, the EDPS recommends **not relying exclusively on the data subject's consent** to legitimate transfers under Article 9 of the Regulation[75]. Hence, the decision tree included in the Guidance should be adapted accordingly by explaining that consent on transfers (Article 9(6)(a) of the Regulation) would only be valid under exceptional circumstances.

Conclusion on transfers in IG/IN investigations

The analysis of the selected cases did not reveal any breach of the Regulation. However, EIB should improve the information of the internal recipients of personal data originating from IG/IN, transfer identification and documentation in the electronic management system, as well as some IG/IN internal documents dealing with transfers and data protection.

See below recommendations No. 7 to 11 (Section 4.1.6 List of recommendations)

4.1.4 Data quality in use of computer forensics by EIB

Background:
In the context of its investigations, IG/IN often relies on OLAF expertise, procedures and equipment to conduct computer forensics operations. If OLAF has no competence or decides

67 Minutes of the inspection (pp. 6 and 19) and Doc. II.67.
68 Doc. I.2B.
69 Paragraph 10 of the Investigation Procedures.
70 Minutes of the inspection, p. 17.
71 See Doc. II.1. and minutes of the inspection, p. 5.
72 Paragraph 36 of the Investigation Procedures.
73 Doc. I.24. The updated guidance dated 30 November 2015.
74 Doc. I.22 (2013 version).
75 See p. 15 of the EDPS Position Paper on the transfer of personal data to third countries and international organisations by EU institutions and bodies, see https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf.

not to investigate (for example for code of conduct cases), IG/IN may rely on the assistance of an experienced private firm, in which case the EIB adheres to the general ACPO Computer Forensics Principles. These cases are limited, since 1 October 2010 EIB has used computer forensics (without relying on OLAF) only twice, both times for internal investigations on code of conduct issues. The inspection team selected the only closed case[76].

In its **prior checking Opinion** on IG/IN investigations[77], The EDPS recommended establishing guarantees in order to ensure the respect of the data quality principle. Furthermore, the EDPS recommended the adoption of a formal protocol for the conduct of computer forensics investigations by the EIB, which would also contribute to the safeguard of the data quality principle.

As a **follow up** to the prior checking Opinion, the EIB informed that for situations where OLAF is not involved, a protocol had been prepared and would be included in the IG/IN Investigation Procedures[78]. The EDPS suggested adding the obligation for the person who gains access to original data held on a computer or storage media to justify the necessity for such access and obtain the approval of EIB's DPO prior to his access to the data[79]. The EDPS also recommended that a reference to Article 4 of the Regulation and a specific mention that data shall be processed fairly and lawfully only for specified, explicit and legitimate purposes should be included in the Investigation Procedures. EIB subsequently included the personal data quality principle and the above obligations[80] and EDPS closed the recommendations[81].

Criteria:
- Article 4 of the Regulation;
- EIB Anti-fraud Policy[82] – Articles 48, 49, 51, 52, 61 and 62;
- IG/IN Investigation Procedures[83] – Articles 20, 21, 33 and 34, Annex I (EIB Protocol for Conducting Computer Forensic Operations);
- Data Protection Guidance for IG/IN[84] – sections 3 and 7.

Action(s):
For the selected fraud case involving the use of computer forensics by the EIB, case handlers were asked to explain the procedure, how and by whom the computer forensics operations were conducted, what data was collected and to present the supporting documents on actions they took to ensure data quality in this context. General questions were also asked to the Head of IG/IN and case handlers as regards the use of computer forensics by the EIB[85].

Observations and Finding(s):
Selected case: No issue regarding data quality in the use of computer forensics performed by the EIB has been identified as to the one selected case.

Conclusion on data quality in use of computer forensics by IG/IN

76 Case 2013-IN-0053. The other case was still pending at the time of the on-site inspection.
77 Case 2009-0459.
78 Letter from EIB of 7/2/2011.
79 Reply from the EDPS of 16/3/2012.
80 Letter from EIB of 13/11/2013.
81 Reply from the EDPS of 20/12/2013.
82 Doc. I.2A.
83 Doc. I.2B.
84 Doc. I.22 and I.24.
85 Actions are reported in the minutes of the inspection, pp. 14-15.

No issue has been identified[86].
No recommendation issued.

4.1.5 Electronic and physical security - Access and incident management

[redacted]

86 This analysis is without prejudice to any possible subsequent wider analysis, findings or recommendations by EDPS on the procedure in general.

87 [redacted].

[redacted]

18

[redacted]

Conclusion in electronic and physical security in IG/IN investigations

In the light of requirements under Article 22 of the Regulation, inspection's results provide reasonable assurance that access to the concerned part of GED that is specifically assigned to IG/IN and associated files in the electronic form as well as in physical form is restricted to authorized staff members.

No recommendation issued.

4.1.6 List of recommendations

Fraud investigations - Recommendations	
Taking into account the findings reported above, the EDPS makes the following recommendations:	
General recommendation	
1.	Clarify the scope of EIB Investigation Procedures by including a reference to EIB Codes of Conduct in the introductory part (the current version only refers to EIB Anti-Fraud Policy) and by excluding harassment investigations from their scope.
Information	
2.	Draft a data protection statement meeting all the requirements of Articles 11 and 12 of the Regulation (information on the controller, the purpose of the processing - including the scope of IG/IN activities, the legal basis, the data processed, the recipients of the data, the retention period, the rights of the data subject and the origin of the data); Publish this data protection statement on the EIB website and intranet;
3.	Complete the privacy statement used by IG/IN in their template for outgoing correspondence by including a link to the data protection statement referred to in Recommendation No. 2
4.	Ensure that each person involved in a case (suspects, informants, whistleblowers and witnesses) is informed and provided with the data protection statement, according to Articles 11 and 12 of the Regulation, including during the assessment phase, unless a limitation under Article 20 of the Regulation applies. Adapt the DP Guidance for IG/IN accordingly.
5.	In cases where the EIB decides to apply a restriction of information, access,

	rectification etc. under Article 20(1) of the Regulation, or to defer the application of Article 20(3) and 20(4), such decision should be taken strictly on a case by case basis and duly documented in the file. Adapt the DP Guidance for IG/IN accordingly.
6.	Make sure that the future IG/IN CMS is featured in such a way so as to identify easily, in each case file, (i) per each data subject whether information in accordance with Articles 11 and 12 of the Regulation was provided and (ii) whether there was a restriction or deferral of the information in accordance with Article 20 of the Regulation.
Transfers	
7.	Delete the last sentence of the template of the clause used by IG/IN when transferring data to other EIB entities (p. 6 of the DP Guidance for IGN/IN dated 30 November 2015).
8.	Before transferring personal data to entities outside the EIB, ensure that the conditions of Articles 8 or 9 of the Regulation (depending on the recipients) are fulfilled and keep documentation of any assessment made by the EIB in this respect. Adapt the DP Guidance for IG/IN accordingly.
9.	When implementing the future CMS, make sure that it is featured in such a way as to identify easily, in each case, if personal data were transferred (internally and externally), to whom, the legal basis for the transfer and the data transfer document (with underlying documents to support, justify and explain the transfer).
10.	Update EIB Investigation procedures to IG/IN practice as regards the notification of investigation cases to OLAF and the recipients of the quarterly status report of ongoing investigations[91].
11.	Modify the DP Guidance for IG/IN so as not to rely exclusively on data subject's consent for transfers.

91 See Section 4.4.3.b of this report.

4.2 ANTI-HARASSMENT PROCEDURES

General background

The relevant EDPS files and documents are:

- 2004-0067 - Prior checking Opinion of 20 April 2005 - **Dignity at work** (***'D@W'***) Policy;
- 2011-0754 - Complaint v. EIB - case closed following the decision of the Civil Service Tribunal in case F-103/11;
- 2012-0088 - EDPS intervention before Civil Service Tribunal in case F-103/11;
- EDPS Guidelines on the selection of confidential counsellors and the informal procedures for cases of harassment ("***Guidelines on informal anti-harassment procedures***"[92].
- -EDPS Guidelines on administrative inquiries and disciplinary procedures ("***AI&DP Guidelines***"), applicable to formal harassment investigations[93];

Inspection activities

The inspection activities mainly consisted of: interviews with persons in charge of a selection of seven harassment investigation cases[94]; collection of evidence; interview with persons in charge of electronic security; demonstration on-the-spot of the selected case files in the case management system and archives; demonstration on-the-spot of the locked cupboard containing open harassment investigation files in paper format[95].

Inspection topics

While conducting the inspection activities, the inspection team made some general findings (Section 4.2.1). More specifically, the inspection covered: information of data subjects and exceptions (Section 4.2.2), right of access of individuals involved (Section 4.2.3), retention period (Section 4.2.4) and organisational, physical and electronic security (Section 4.2.5)[96].

4.2.1 Preliminary observations and general findings

a. Selection of confidential counsellors

There is **no written procedure** regarding the selection of confidential counsellors in the context of the D@W Policy[97]. This selection procedure should be adopted and **notified** to the

92 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/11-02-18_Harassment_Guidelines_EN.pdf

93 See p. 1 of the Guidelines on informal anti-harassment procedures, the formal D@W procedure falls into the field of "classic" administrative inquiries and therefore recommendations in the AI&DP Guidelines also apply.

94 The EDPS made a random selection of cases based on the list of cases provided by EIB (Doc. I.8). The selection made by the EDPS was communicated to the EIB five calendar days before the inspection.

95 See minutes of the inspection, pp. 22-38.

96 These topics were listed in the announcement letter of 21 October 2015.

97 See minutes of the inspection, p. 22.

EDPS for prior checking under Article 27(2)(b) of the Regulation, as the processing operations in this respect intend to evaluate personal aspects relating to the candidates[98].

b. 'Informal'/Mediation stage of the formal harassment procedure

In the announcement letter, the EDPS asked the EIB to provide an anonymized list of harassment cases. The Employee Relations Division ("***ER***") of the EIB provided a list of the D@W cases, some of them being labelled as 'formal' and other as 'informal', with different retention periods (five years for formal cases, three years for informal cases)'[99]. On-the-spot, the inspection team found out that this so-called 'informal' procedure was not the informal procedure dealt with by confidential counsellors and referred to as such in the D@W Policy. It is an ***ad hoc*** **mediation phase**, which may take place at the outset of the formal investigation procedure if the alleged victim wishes so[100]. In practice, once the alleged victim has sent a complaint to ER, a case handler makes contact with him/her and explores whether there is room for mediation and amicable settlement. This phase/procedure is not included in the current D@W Policy[101].

c. Designation of the D@W cases in EIB files

The D@W cases are named after the personnel numbers of the individuals involved[102] or after the last names of the involved parties[103]. Even if the access to D@W files is strictly limited[104], the EIB should **not use any designation that allows for a direct identification of the individuals involved (through their names or staff number)**.

d. Management of D@W files in electronic form

D@W electronic files are currently stored in an **area of GED** that is specifically assigned to ER for this purpose[105]. However, the analysis of selected cases indicated that documents related to specific cases were sometimes only stored in the **Outlook mailboxes** of the case handlers[106].

e. Scope of the D@W Policy

From the analysis of the selected cases, the EDPS understands that the D@W procedure is followed not only in the case of harassment but also for other kinds of conflicts at work[107]. In the latter case, ER tries to solve the issue at the mediation phase. Having in mind the data quality requirements of Article 4 of the Regulation (including purpose limitation and fairness), the EDPS wishes to draw EIB's attention to the fact that once a conflict has been identified as not being a harassment case, it should no longer be dealt with under the D@W

98 See EDPS Guidelines on informal anti-harassment procedures, p. 2.
99 Doc. I.8.
100 Minutes of the inspection, pp. 22-23.
101 During the onsite inspection, the ER Division mentioned that a new Policy was being prepared that will include the mediation phase (see minutes of the inspection, p. 23).
102 See list of cases communicated by the EIB to the EDPS (Doc. I.8.).
103 See for ex. Doc. II.81 and II.82.
104 See below Section 4.2.5.
105 Minutes of the inspection, p. 34.
106 Minutes of the inspection, pp. 29, 30, 36 and 37.
107 Cf. case 1 (informal case - conflict involving individuals with sensitive position within EIB - see minutes of the inspection, p. 25); case 4 (informal case - conflict between colleagues - see minutes of the inspection, p. 29) and case 5 (formal case - no individual alleged harasser but the EIB - see minutes of the inspection, p. 32 and p. 36).

Policy but under other appropriate dispute resolution mechanisms providing the same level of data protection safeguards for staff members involved.

Conclusion on the preliminary observations and findings in D@W Policy

See below (Section 4.2.6 List of recommendations):

- Recommendation No. 12 - Selection of confidential counsellors;
- Recommendation No. 13 - Mediation stage of the formal harassment procedure;
- Recommendation No. 14 - Designation of the D@W cases in EIB files;
- Recommendation No. 15 - Management of D@W files in electronic form.

4.2.2 Information of data subjects

Background:
In its prior checking Opinion on D@W Policy[108] the EDPS recommended that EIB modifies the document informing staff on the D@W Policy and the related procedure in order to comply with Articles 11 and 12 of the Regulation. The EDPS further recommended that any contract with a third party which provides that the D@W Policy shall apply, must provide the individuals affected with the relevant information concerning the processing of his/her personal data (knowing that these individuals may not have access to EIB intranet).

Contents of the D@W Policy as regards information of the affected individuals
From the D@W Policy[109], which is available on the EIB intranet, the data subjects can extract some information relating to the processing of personal data in the D@W procedures (purpose, identification of the controller, categories of personal data, possible recipients, fact that records will be maintained).

According to the D@W Policy (p. 2), upon receipt of the memorandum from the complainant setting out the complaint, "*the alleged harasser will be informed of the subject of complaint and necessary information but will not receive a copy of the memorandum*". The case officer dealing with the specific case is responsible to obtain consent of the alleged victim on the information to be shared with the alleged harasser.

Case law
By judgment of 10/7/2014 in case F-103/11, the Civil Service Tribunal ("***CST***") condemned the EIB for a breach of the obligation of confidentiality in the D@W Policy because EIB had proactively shared the memorandum from the complainant (including sensitive information about the complainant) with the alleged harasser, whereas the D@W Policy expressly states the contrary[110]. The EDPS intervened before the CST to support the complainant and indicated that the disclosure did not comply notably with Articles 4(1)(a), 5 and 10 of the Regulation[111].

Criteria:
- Articles 4, 5, 10, 11, 12 and 20 of the Regulation;
- AI&DP Guidelines;

108 Case 2004-0067.
109 Doc. I.9.
110 Article 3(c): "[the Directorate General of Personnel Directorate] *shall point out* [to the complainant] *that the alleged harasser will be notified of the grounds for the complaints and receive the necessary relevant information but will not receive a copy of the memorandum* [from the complainant]".
111 See also EDPS cases 2011-0754 (complaint) and 2012-0088 (intervention before CST in case F-103/11).

- EDPS Guidelines on the rights of data subjects[112].

Articles 11 and 12 of the Regulation provide a minimum list of information on the processing of personal data that need to be provided to the data subjects (individuals involved in a case). Such information must be twofold: (i) general information to EIB staff and other persons subject to the D@W Policy and (ii) specific information on the processing of their personal data to all individuals involved in a particular case (e.g. as alleged victim, alleged harasser or witness).

The EDPS Guidelines on data subjects rights[113] state that providing individuals with the required elements of information not only puts them in the position of effectively exercising their data subject rights, but also contributes to ensuring data quality in the sense of Article 4 of the Regulation (e.g. fair processing and accuracy of personal data). Furthermore, it may be necessary in certain cases not to specifically inform the alleged harasser or to defer him/her information, e.g. by not disclosing the identity of the alleged victim or other sensitive information in the complaint, in accordance with Article 20(1)(c) of the Regulation if the deferral of the information is necessary to safeguard "*the protection of the data subject or of the rights and freedoms of others*" (e.g. protection of the alleged victim, witnesses). For the formal procedures, the right to information may also be restricted following Article 20(1)(a) of the Regulation ('*the prevention, detection and prosecution of criminal offences*' has been interpreted by the EDPS so as to include administrative inquiries such as anti-harassment cases).

Action(s): For the selected cases, case handlers were asked to explain and show evidence how the alleged victim and the alleged harasser were informed about the protection of their personal data, whether the alleged harasser had been informed about the investigation procedure started against him/her and what kind of information was communicated to the alleged harasser[114].

In case the obligation to inform has been deferred, case handlers were asked to identify (a) the note in the file reflecting that this decision has been taken, (b) the reason for restriction, and, if relevant, (c) evidence that the decision of deferral is still valid.

Observations and Finding(s):

a. Information of individuals (Articles 11 and 12 of the Regulation)

(i) General information and templates

Some information on the D@W procedures is provided by EIB to EIB staff. The D@W Policy is made available on the intranet and that for other persons subject to the D@W Policy by contract, the D@W Policy is annexed to the contract. Information on the D@W procedures is included in the templates[115] used by ER for outgoing correspondence with persons involved in a specific case. There is a document listing the procedural steps to be taken by the ER case officers[116].

112 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/14-02-25_GL_DS_rights_EN.pdf
113 See EDPS Guidelines on the rights of individuals with regard to the processing of personal data, p. 8.
114 Actions are reported in the minutes of the inspection, pp. 23, 28-31, 35-37.
115 Doc. II.106.
116 Doc. II.107.

There is no template for outgoing correspondence with the complainant (alleged victim) in the mediation phase (i.e. between the receipt of the complaint and the formal launch of the investigation procedure). For the formal investigation procedure, there is a standard template for acknowledging receipt of a complaint launching a formal procedure[117].

There is no template for outgoing correspondence with the alleged harasser in the mediation phase. For the formal procedure, there is a standard template for informing the alleged harasser of the complaint, but not for the summary of facts to be sent to him/her[118].

The information so provided is not sufficient to comply with the requirements Articles 11 and 12 of the Regulation, i.e. information on the identity of the controller; the categories of data processed; the purposes of the processing operation for which the data are intended; the recipients or categories of recipients of the data; whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply; the existence of the right of access to, and the right to rectify, the data concerning him or her; the legal basis of the processing; the time-limit for storing the fata; the right to have recourse at any time to the EDPS; the origin of the data.

(ii) Specific information of the individuals involved in selected cases

117 Text of the template:
"*We hereby confirm that following your e-mail of [date], an official enquiry has been launched under the Dignity at Work Policy of the EIB.*
We therefore request you to:

I. Within 10 days of receipt of this letter, address a report to the Head of Personnel, in a marked confidential envelope, setting out your complaint, presenting any other documentary evidence as well as indicating whether any third parties will be called to give evidence at the hearings (no names should be given).

II. Note that the complaint cannot be withdrawn and the procedure must be followed through to its conclusion.

III. Note that the alleged harasser(s) will be reminded that at no time you, as the complainant, should be called to account.

IV. Note that the matter has to be treated with the utmost confidentiality by both parties.

Please be also informed that once the report has been received by the Head of Personnel, the alleged harasser(s) will be notified of the grounds for the complaint and will receive any information deemed necessary regarding it. He/she/they will however not receive a copy of the report itself. […]""

118 Text of the template:
"*We hereby inform you that a complaint in the context of the Bank's Dignity at Work policy has been filed against you by Mr/Ms [name]. A detailed description of the complainant's allegations and of the facts grounding them is provided in the summary of the case annexed to the present letter (Annex A). […]*

We kindly request you to:

a. acknowledge as soon as possible receipt of the present letter;

b. Within 10 days of receipt of this letter, address a report to the Head of Personnel, in a marked confidential envelop, setting out your complaint, presenting any other documentary evidence as well as indicating whether any third parties will be called to give evidence at the hearings (no names should be given).

We draw your attention to the fact that at no time should the complainant be called to account and that the matter has to be treated with the utmost confidentiality by both parties."

In the selected case that was closed at the mediation stage, no evidence of any specific information of the involved persons was found[119].

In the other selected cases that were checked in this respect[120], the documents[121] sent by ER to the alleged victims and alleged harassers did not provide the necessary information, pursuant to Articles 11 and 12 of the Regulation[122]. The alleged harasser was only informed about the start of formal procedure and the identity of the alleged victim, and received a summary of the complaint (detailed description of relevant allegations and facts grounding them) from ER.

b. Modification of EIB practices following the decision of the Civil Service Tribunal in case F-103/11

The inspection team checked whether the EIB has changed their practice since the decision of the CST as to the type of information on the complaint's contents that is communicated to the alleged harasser (Articles 4, 5 and 10 of the Regulation).

In all of the **cases selected** to check the information of the data subjects, the communication of information on the complaint to the alleged harasser was done prior to the judgment of the CST in case F-103/11. Thus, the EDPS decided not to make any findings in this respect as regards the selected cases.

During the onsite inspection ER explained that they **changed their practices** following the court case and that they now always ask for the **alleged victim's consent** on the information to be shared with the alleged harasser[123]. ER is of the opinion that they must provide information to the alleged harasser at the investigation stage so that he/she can exercise his/her right of defence. ER pointed out that even if the formal procedure does not lead to a disciplinary sanction (disciplinary proceedings, if any, will be initiated later on), facts are established at this stage and it is important for the alleged harasser to understand what the accusations against him/her are.

In this respect, the EDPS notes that while wishing to guarantee the respect of the right of defence in the context of an internal inquiry procedure might seem reasonable and justified, especially when urgent measures are to be taken at this stage[124], the data protection rules also apply in this context. Consequently, a balance must be reached between the respect of the right of defence of the alleged harasser and the respect of the rights and freedoms of the alleged victim, in particularly as regards the protection of the confidentiality of their personal data. This requires in particular a **case-by-case** examination of the categories of data to be communicated to the alleged harasser (including the identity of the complainant). Pursuant to Article 4 of the Regulation and as mentioned in the D@W Policy[125], only the data that are

119 Case 4 (see minutes p. 35). The other mediation case (case 1) has been closed for more than three years and no information was still available on GED (see below Section 4.2.4 on retention).

120 Cases 5, 6 and 7 (see minutes of the inspection, pp. 30-31, 36-37). Case 3 was not inspected as the ER Division mentioned during the onsite inspection that the case had been recently re-opened (minutes of the inspection, p. 31). Case 2 was too old (2008), there is no electronic file for cases prior to 2011 (see minutes of the inspection, p. 35).

121 Docs. II.76-80, 83, 85-88.

122 See above (i).

123 See minutes of the inspection, p.23.

124 For example a provisional suspension or transfer of the alleged harasser to another service so that he/she is no longer in contact with the alleged victim.

125 This is what the D@W Policy provides (Article 3.c)): '(...) *the alleged harasser will be notified of the grounds for the complaint and receive the necessary relevant information but will not receive a copy of the memorandum*'. See also Article 4.a).

relevant and necessary for the investigation may be communicated at this stage. If special categories of data are involved, Article 10 of the Regulation should also be taken into consideration.

The EDPS does not believe that asking for the alleged victim's consent on the data to be shared with the alleged harasser is an appropriate way to proceed in order to ensure fairness. Indeed, the use of consent in the employment context should be avoided, as the consent is hardly 'freely given' (as defined in Article 2(h) of the Regulation)[126], especially when it comes to a victim of harassment, who is likely to be even more vulnerable. Instead, once ER has assessed what information should be shared with the alleged harasser at this stage of the procedure, they should **inform the alleged victim about the data** they intend to share and about the fact that he/she has the **right to object** to such communication on compelling legitimate grounds in accordance with Article 18 of the Regulation. The alleged victim should also be informed that at a later stage (disciplinary proceedings), the alleged harasser will be, as a matter of principle, granted broader access to the file, at least the elements used against him/her, so that he can exercise his/her right of defence.

Conclusion on information of data subjects in D@W Policy

To be compliant with the DP rules, the EIB should adopt a comprehensive **data protection statement** including all the elements provided by Articles 11 and 12 of the Regulation. This statement should be made available on the intranet and communicated to any person subject to the D@W Policy by virtue of a contract. It should also be attached to the templates for outgoing correspondence with persons involved in a specific harassment case, whether alleged victim, alleged harasser or witness.

In addition, **specific information** on the processing of personal data must be given to the persons involved in a particular case (alleged victim, alleged harasser, witness), **as of the mediation phase**, unless an exception in Article 20 of the Regulation applies.

In cases where the EIB decides to apply a **restriction** of information, under Article 20(1) of the Regulation, or to defer the application of Article 20(3) and 20(4)[127], such decision should be taken strictly on a case by case basis. The EIB should be able to provide evidence demonstrating detailed reasons for taking such decision (i.e. motivated decision). These reasons should prove that they cause actual harm to the investigation and they should be documented before the decision to apply any restriction or deferral is taken. The reasons should be **documented** so that, if made available to the EDPS following a request in the context of a supervision and enforcement action, they allow the EIB to demonstrate compliance with Article 20 of the Regulation in the concrete case at hand (i.e. illustrating a case-by-case assessment specific to the case).

In order to help the EIB to comply with the above-mentioned obligations, the **future CMS**[128] should be featured in such a way so as to identify easily, in each case file, (i) per each data subject whether information in accordance with Articles 11 and 12 of the Regulation was provided and (ii) whether there was a restriction or deferral of the information in accordance with Article 20 of the Regulation.

126 For further information in this respect, see opinions of the Article 29 Working Party: 15/2011 on the definition of consent and 8/2001 on the processing of personal data in the employment context.

127 Under Article 20(5) of the Regulation.

128 Mentioned by the ER Division during the on-site inspection (Minutes of the inspection, p. 35).

As regards the **data to be shared with the alleged harasser** during the investigation, the EIB should ensure that only the data that are relevant and necessary for the investigation are communicated to the alleged harasser and that the alleged victim is informed about the intended communication beforehand so that he/she can exercise his/her right to object under Article 18 of the Regulation.

See below recommendations No. 16 to 21 (Section 4.2.6 List of recommendations).

4.2.3 Right of access

Background:
In the EDPS Opinion on the D@W Policy, one of the recommendations was to adopt adequate rules so as to provide the data subject with access to his/her personal data under Article 13 of the Regulation save where restricted in accordance with Article 20 of the Regulation. Within the follow up procedure the EIB informed the EDPS that: "*Each person involved in the investigation procedure shall be informed of the purposes of the data processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed. Furthermore, he/she shall obtain communication of the data which are processed, including their source. However, the investigating panel (during the investigation procedure) and HR (once the investigation procedure is concluded) shall limit the right of access each time it is necessary to safeguard the prevention, investigation, detection and prosecution of a disciplinary infraction and/or to guarantee the protection of one of the staff members involved and/or of the rights and freedoms of others*."[129]

Criteria:
- Article 13 and 20 of the Regulation;
- EDPS Guidelines on data subjects' rights;
- AI&DP Guidelines[130].

Articles 13 states what kinds of information data subjects have the right to receive from an EU institution about the processing of their personal data. This right can only be restricted to safeguard certain interests as described in Article 20 (see above).

As highlighted in the EDPS Guidelines on data subjects' rights[131], alleged harassers may have their right to access restricted if necessary to safeguard "*the protection of the data subject or of the rights and freedoms of others*", in particular the alleged victim and witnesses. This limitation should only be applied on a case-by-case basis and when strictly necessary to protect the rights and freedoms of others, and in order to secure the good administration of cases or the future relations of the parties.

The right of access of the alleged harasser is linked to the information he has already received on the procedure. Indeed, an alleged harasser will not request access if he is not aware of an existing procedure involving him[132].

129 By letter 25 June 2007.
130 Following the Guidelines on anti-harassment procedures (p. 1), the formal D@W procedure falls into the field of "classic" administrative inquiries and therefore recommendations in the AI&DP Guidelines also apply.
131 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/14-02-25_GL_DS_rights_EN.pdf
132 See data subject's guidelines, p. 34.

Action(s): For the selected cases, case handlers were asked to explain whether the individuals involved has requested access to his/her data in the investigation file and if so, what kind of information that was provided and show the EDPS evidence on how the request has been handled. In case the right of access has been denied or restricted, the EDPS planned to ask case handlers to identify (a) the note in the file reflecting that this decision has been taken, (b) the reason for restriction, and (c) evidence of regular re-assessment of the deferral decision[133].

Observations and Finding(s):

No requests for access to harassment files had been made since the interviewed officer started working on D@W cases, which was 4 years ago. However, as mentioned above (Section 4.2.2), in none of the selected cases the individuals involved were fully and properly informed about the processing of their personal data. In addition; none of the template letters[134] used by ER for D@W cases contain the necessary specific information to the data subjects (alleged victim, alleged harasser, witness), pursuant to Articles 11 and 12 of the Regulation, that would allow them to exercise their right of access.

Conclusion on the right of access in D@W Policy

Since there were no rights of access requests in the selected cases, the EDPS has not been able to assess the EIB's compliance with Article 13 and Article 20 of the Regulation in this respect.

As for the right of information, in cases where the EIB decides to apply a restriction of access, under Article 20 of the Regulation such decision should be taken strictly on a case by case basis and duly documented. The future CMS should be featured in such a way so as to identify easily, in each case file, (i) per each data subject whether access has been requested in accordance with Article 13 of the Regulation and (ii) whether there was a restriction or deferral of access in accordance with Article 20 of the Regulation.

See below recommendations No. 19 to 20 (Section 4.2.6 List of recommendations)

4.2.4 Retention

Background
According to the prior checking notification, all documents pertaining to a formal investigation procedure for harassment are kept in a file with strictly limited access in the ER Division for 5 years[135] starting from the date on which the parties are informed in writing of the EIB President's decision on the case. The length of the conservation period might be extended due to the initiation of a disciplinary proceeding or a judicial procedure[136].

Criteria:
- Article 4(1)(e) of the Regulation;
- D@W policy: '*HR* [now 'Personnel'] - *shall maintain, confidentially and under the supervision of the Data Protection Officer, all records containing names, dates, complaints and outcomes in line with policy and in the interests of consistency and fairness*'[137];

133 See minutes of the inspection, pp. 28-31, 35-37.
134 Doc. II.106.
135 Cf. Article 27 notification on D@W Policy. This duration is considered adequate (cf. p. 6 of the EDPS opinion in case 2004-0067).
136 Cf. EIB follow up letter to the EDPS of 5 July 2007.
137 Doc. I.9.

- Retention schedule for documents of Personnel Directorate (D@W cases: 5 years after year of closure)[138];
- *'Archives de la direction du Personnel - Manuel de procédures'*[139]*:* Confidential documents are filed in the confidential section (orange map) of the personal file. They are sent by internal post in confidential envelopes or hand-delivered to an archivist of the Personnel Archives. Envelopes on which a destruction date is mentioned must be listed according to the ID number (personnel number) in a pink map kept by the Personnel Archives. In order to proceed to their future destruction, the archivist defines an Outlook (anonymous) reminder for himself as well as for his back-up.

Action(s)

For the cases selected by the inspection team for which the retention period was expired according to the list provided by EIB[140], the persons in charge (in ER Division and Personnel Archives), were asked:

- whether the file (both in paper and electronic form) was actually destroyed and to show evidence of the date of destruction (e.g. any protocol on deletion);
- whether any document is kept about the case and if so, to show which document and where.

For the other cases, the persons in charge were asked to show any instruction as to their date of destruction.

In this context, the inspection team was given access to the Personnel Archives (personal files of staff members involved in the selected cases - no confidential envelope has been opened) and to the electronic files on GED[141].

Observations and Finding(s)

a. Mediation cases

As already mentioned[142], this phase of the investigation procedure is not included in the D@W Policy or elsewhere. The rules applicable to the retention of the cases that are settled at this stage were described orally as follows[143]:

- Conservation period: **3 years** as of closure for both electronic and paper files.
- Paper files: ER Division does not keep any paper document. However, the persons involved **may** ask ER Division to **file a final note** on the outcome of the case in their **personal file**. If so, the document in question is sent in an unsealed envelope by the Employee Relations (ER) Division to Personnel Archives with a post-it mentioning the three-year retention period to be filed as such in the personal file of the staff member concerned. The final note is filed as such in the confidential section (pink or orange map) of the personal file of the staff members involved or in a sealed envelope)[144].
- Electronic files:

138 Doc. I.11.
139 Doc. I.14.
140 See list provided by EIB (Doc. I.8.).
141 Actions are reported in the minutes of the inspection, pp. 22-37.
142 See Section 4.2.1.b of this report.
143 Minutes of the inspection, pp. 22-23, 29, 34-35.
144 Minutes of the inspection, p. 23 and p. 29.

- There is one **GED folder** for all informal/mediation cases with a subfolder for each case with the opening order of the case and the outcome note. There is no electronic file for cases prior to 2011.
- Email exchanges are also kept in the **mailboxes** of the case handlers[145]. There is **no** general **automatic email retention policy** in place for the IT email system in use at the EIB. There is no procedure in place to inform case handlers that the retention period for a case has expired. Thus, case handlers of D@W cases may happen to keep emails pertaining to a case for an indefinite duration if they do not proceed manually to the deletion.

Amongst the selected cases, two related to harassment investigation procedures that were closed at this early stage; one had been closed for more than three years, the other for less than three years[146]. For these cases, the findings are as follows:

As regards the case for which the retention period has expired, a *'**note** à l'issue de la procédure de médiation*' is filed in the confidential section of the personal (paper) file of one of the two staff members involved, with **no mention as to retention**. For the other staff member involved, there was no such document. There was no observation as regards GED, since there was no electronic file prior to 2011[147].

As regards the case for which the retention period has not yet expired, no document was found in any of the personal files of the three staff members involved[148]. The GED file contains the opening order of the case as well as the final note. There was **no instruction as to the destruction date** of the case.

b. <u>Formal investigation cases</u>

The following additional explanation was provided as regards the documents that are kept and practical implementation of the retention rules[149].

- <u>Paper files</u>: once a case is closed, the **President's decision** (with panel's opinion attached) which may be filed in the **personal file** of the persons involved, depending on the outcome[150]. If they are, the decision is sent to the Personnel Archives for filing in personal files. The archivists keep a register of incoming envelopes and their date of destruction (if any)[151]. Approximately once a month, the archivists check in their register the documents to be removed from personal files for destruction. The documents are put in a sealed container to be destroyed and the physical destruction is done by an external service provider[152].
  The other documents pertaining to the case are destroyed at closure.

- <u>Electronic files</u>:

145 See minutes of the inspection, p. 29 regarding an informal case:"(...) The case officer still has the email exchange and normally keep it until the date in which the physical file has to be destroyed (...)'.
146 These cases were identified in the minutes of the inspection respectively as Case 1 and Case 4.
147 Minutes of the inspection, p. 35.
148 Minutes of the inspection, p. 32.
149 Minutes of the inspection, pp. 23-24, 29, 34, 35.
150 If the President's decision finds that there is harassment, the decision will be put in the personal file of the harasser and, if he/she wishes so, in the personal file of the victim. If the President's decision finds that there is no harassment, the decision will be put in the personal file of the alleged victim and, if he/she wishes so, in the personal file of the cleared alleged harasser.
151 Doc. II.70.
152 See minutes of the inspection, p. 34.

- All supporting documents (notes, correspondence with the parties, etc.) are kept in **GED** (at least since 2013). In recent cases (as of 2013), a **reference with regard to destruction date** is indicated manually in the electronic file by the ER Administrative Assistant after the case's closure[153]. The destruction of electronic files is done manually at the moment. The EIB intends installing a new tool (Gopro) that will deal with automatic deletion of files in GED once the retention period has expired.
- Email exchanges in the context of the investigation procedure are also kept in the **mailboxes** of the case handlers and sometimes only kept in these mailboxes[154]. *See also comments made above regarding the absence of automatic deletion of emails*.

Amongst the selected cases, five relate to harassment investigation procedures.

Case for which the retention has expired[155]
No relevant envelope was found in the confidential section of the personal file of the staff members involved[156]. There was no observation as regards GED, since the case was closed in 2008 there was no electronic file prior to 2011[157].

Cases for which the retention period has not yet expired[158]
In one case[159], the retention period is not written directly on the envelope but on a post-it placed on the envelope. In another case[160], the expiry of the retention period is not mentioned on the envelope. In GED[161], there is no instruction as to destruction date in two cases[162], whereas instructions are present in the most recent case[163].

Conclusion on retention in D@W Policy

In order to be compliant with Article 4(1)(e) of the Regulation, the EIB should **revise** the **D@W Policy** so as to include, for each phase of the investigation procedure, (i) a clear description of (paper and electronic) documents that are retained once the procedure is closed and where as well as (ii) the retention period applicable.

153 Examples were provided for two cases (Doc. II.81 and II.82).
154 See minutes of the inspection:
- p. 30: '(...) *More information might be in the email box of the case officer who dealt with the file at the time (not the interviewed case officer; the case officer in question does no longer work with ER)* (...).'
- p. 36 (same case): '(...) *There is no record in GED of the consent given by the complainant* (...) *Explanation given* (...) *is that the case was handled by a former colleague who may have kept his exchanges with the victim in his personal mailbox*'.
- p. 37 (different case): *'Not all the relevant correspondence was available in the GED file. Some of them were stored in the mailbox of the case handler (the interviewed Personnel lawyer)*'.
155 Case identified in the minutes as Case 2.
156 Minutes of the inspection, p. 26.
157 Minutes of the inspection, p. 35.
158 Cases identified in the minutes as Cases 3, 5, 6 and 7. For Case 3, the inspection team checked the personal files but was told later during the inspection that the case had been reopened recently (cf. minutes of the inspection, p. 31). Therefore, the report does not include any findings regarding Case 3.
159 Case 7. Minutes of the inspection, p. 32.
160 Case 5. Minutes of the inspection, p. 32 and p. 36.
161 GED file for Case 3 was not inspected, as the inspection team was told on site that the case had been reopened recently (minutes of the inspection, p. 31).
162 Cases 5 and 6. Minutes of the inspection, p. 36.
163 Doc II.82. Case 7, minutes of the inspection, p. 37.

Moreover, the EIB (ER Division) should set up a **written procedure as regards** the **destruction** of:
- paper files (as soon as the procedure is closed) and
- electronic files (both in GED and in the case handlers' mailboxes)
once the retention period has expired.

This procedure should provide that any envelope enclosing a D@W-related document sent to the Personnel Archives should clearly **indicate the expiry date** of the retention period. The *'Manuel des procédures - Archives de la direction du Personnel*' should be implemented as to the **systematization of the destruction** of D@W-related documents in personal files (once a month, use of an Outlook reminder).

See below recommendations No.22 to 24 (Section 4.2.6 List of recommendations)

4.2.5 Physical and electronic security - access management

[redacted]

[redacted]

Conclusion on physical and electronic security - access management in D@W Policy

In the light of requirements under Article 22 of the Regulation, inspection's results provide reasonable assurance that an access to the concerned part of GED that is specifically assigned to ER Division and associated files in the electronic form as well as in the physical form is restricted to authorized staff members.
No recommendation issued.

4.2.6 List of recommendations

Anti-harassment procedures - Recommendations	
Taking into account the findings reported above, the EDPS makes the following recommendations	
General recommendations	
12.	Notify the procedure for selection of confidential counsellors to the EDPS.
13.	Update the D@W Policy to include the mediation phase of the harassment procedure and provide the EDPS with an updated notification of its D@W Policy.
14.	No longer designate D@W cases after the names or personnel numbers of the individuals involved.
15.	Centralise all documents related to a specific D@W case in one dedicated file.
	Information to data subjects and right of access
16.	Adopt a data protection statement for the D@W procedures, which contains the information on the processing of personal data in the D@W procedures in accordance with Articles 11 and 12 of the Regulation, i.e. information on the identity of the controller; the categories of data processed; the purposes of the processing operation for which the data are intended; the recipients or categories of recipients of the data; whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply; the existence of the right of access to, and the right to rectify, the data concerning him or her; the legal basis of the processing; the time-limit for storing the fata; the right to have recourse at any time to the EDPS; the origin of the data.
17.	Publish the data protection statement on the intranet for all staff and make it also available to any third party submitted (by contract) to the application of the D@W Policy. Include a link to the data protection statement in the templates for all outgoing correspondence.
18.	Inform each person involved in a case (alleged victim, alleged harasser, witness) individually as of the mediation phase with regard to the processing of their personal data in the specific D@W procedure and provide him*her with a data protection statement in accordance with Articles 11 and 12 of the Regulation, unless a limitation under Article 20 of the Regulation applies. Adopt internal guidance for case handlers in this respect.
19.	In cases where the EIB decides to apply a restriction of information, access, rectification etc. under Article 20(1) of the Regulation, or to defer the application of Article 20(3) and 20(4), such decision should be taken strictly on a case by case basis and duly documented in the file. Adopt internal guidance for case handlers in this respect.
20.	Ensure that the new CMS is featured in such a way so as to identify easily, in each case file, (i) per each data subject whether information or access in accordance with Articles 11, 12 and 13 of the Regulation was provided and (ii) whether there was a restriction or deferral of the information or access in

	accordance with Article 20 of the Regulation.
21.	As regards the data to be shared with the alleged harasser during the investigation, ensure that only the data that are relevant and necessary for the investigation are communicated to the alleged harasser and that the alleged victim is informed about the intended communication so that he/she can exercise his/her right to object under Article 18 of the Regulation. Adapt the D@W Policy accordingly. Adopt internal guidance for case handlers in this respect.
	Retention
22.	Revise the D@W Policy so as to include, for each phase of the investigation procedure (i) a clear description of (paper and electronic) documents that are retained once the procedure is closed and where and (ii) the retention period.
23.	Set up a written procedure to ensure the effective destruction of (i) paper files (as soon as the case is closed) and (ii) electronic files (both in GED and any document that would also be stored in the case handlers' mailboxes) by the ER Division once the retention period has expired. This procedure should notably provide that any envelope sent to the Personnel Archives containing D@W-related document should clearly indicate the expiry date of the retention period of the enclosed document.
24.	Ensure the implementation of the *'Manuel des procédures - Archives de la direction du Personnel*' as to the systematization of the destruction of D@W-related documents in personal files.

4.3 ADDITIONAL CONSIDERATION

EIB now has approximately 2.500 employees and employs 500 external consultants, which involves the processing of a substantial amount of staff related data[165]. In addition, the growing activities of the EIB also imply a growing amount of processing of data from external partners. As a result and in comparison with the practice of other institutions of a comparable size, the EDPS is of the opinion that **the DPO should be assisted by an Assistant DPO** in order to be able to fulfil his duties under Article 24 of the Regulation. In addition, several institutions, some of which having a size which is comparable to EIB, have developed networks of Data Protection Coordinators/Contact points (DPC) with a view to acting as a relay for the DPO locally within the different entities of the institutions[166]. The EDPS welcomes the fact that IG/IN already have assigned one member of their staff the task to coordinate all data protection issues in their division[167]. It would be **good practice** for the EIB to extend this practice to all divisions of the institution. This would also be in line with the accountability principle[168].

165 See minutes of the inspection, p. 4.

166 See the network of Data Protection Coordinators at the Commission: https://myintracomm.ec.testa.eu/serv/fr/dpo/home/dp_in_dgs/documents/dpc_list.pdf. See also the 2013 survey on the function of DPC at the Commission: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2013/13-01-25_DPC_Survey_Report_EN.pdf. Other institutions as the Parliament, the Council, the European External Action Service (EEAS) and the European Central Bank (ECB) also have a network of DPCs.

167 See minutes of the inspection, p. 18.

168 See accountability initiative launched by the EDPS: https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Accountability_initiative

Annex 1 – Powers of the EDPS

Art 47 of the Regulation 45/2001 sets forth the powers of the European Data Protection Supervisor as follows:

"...
1. The European Data Protection Supervisor may:
(a) give advice to data subjects in the exercise of their rights;
(b) refer the matter to the controller in the event of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, make proposals for remedying that breach and for improving the protection of the data subjects;
(c) order that requests to exercise certain rights in relation to data be complied with where such requests have been refused in breach of Articles 13 to 19;
(d) warn or admonish the controller;
(e) order the rectification, blocking, erasure or destruction of all data when they have been processed in breach of the provisions governing the processing of personal data and the notification of such actions to third parties to whom the data have been disclosed;
(f) impose a temporary or definitive ban on processing;
(g) refer the matter to the Community institution or body concerned and, if necessary, to the European Parliament, the Council and the Commission;
(h) refer the matter to the Court of Justice of the European Communities under the conditions provided for in the Treaty;
(i) intervene in actions brought before the Court of Justice of the European Communities.

2. The European Data Protection Supervisor shall have the power:
(a) to obtain from a controller or Community institution or body access to all personal data and to all information necessary for his or her enquiries;
(b) to obtain access to any premises in which a controller or Community institution or body carries on its activities when there are reasonable grounds for presuming that an activity covered by this Regulation is being carried out there.
...".

Annex 2 – List of documents mentioned in the report

I. 1. Anonymised list of investigation cases registered by the Fraud Investigation Division in the case management system since 01/10/2010
I.2A. EIB Anti-Fraud Policy
I.2B. EIB Investigation Procedures
I.7. Access authorisation request to GED section dedicated IG/IN activities
I.8. Anonymised list of harassment cases (formal investigation procedures) opened by EIB since 20/04/2005
I.9. EIB Dignity at Work Policy (Investigation Procedure)
I.11. Retention Schedule for documents of EIB Personnel Directorate
I.14. Archives de la direction du Personnel - Manuel de procédures
I.17. Privacy statement used by IG/IN to inform the people reporting fraud about their rights under the Regulation as regards the processing of their personal data
I.22 Data Protection Guidance for IG/IN (version of April 2013)
I.24 Data Protection Guidance for IG/IN (version of 30/11/2015)
II.3. template of quarterly report of IN cases (extended version)
II.13. Internal note to Personnel Directorate (Case 2013-IN-0053)
II.37. Internal note to Personnel Directorate (Case 2014-IN-0021)
II.55. Internal note from IG/IN investigator to EIB general Counsel (Case 2013-IN-0007)
II.60. Code of Conduct for IT professionals
II.61. Code of Conduct for GED Administrators
II.62. Rules for the protection of personal data for external consultants
II.67. Printscreen - future Case Management System for IG/IN
II.70 Listing "*Enveloppes confidentielles transférées du secrétariat DG Personnel/ER aux ...*"
II.76. EIB letter to complainant (Case 5)
II.77 EIB letter to complainant (Case 5)
II.78 EIB letter to complainant (Case 6)
II.79. EIB letter to alleged harasser (Case 6)
II.80. EIB letter to alleged harasser (Case 6)
II.81. Reference to sending one 2013 case to Archives with mention of destruction date
II.82. Reference to sending Case 7 to Archives with mention of destruction date
II.83. letter from EIB to 7A as alleged victim/harasser (Case 7)
II.86. email from EIB to 7B as alleged victim (Case 7)
II.87. exchange of emails between EIB and 7B as alleged victim
II.88. exchange of emails between EIB and 7A - approval on summary of complaint to be sent to 7B as alleged harasser
II.106 Screenshot of GED folder containing templates of documents used in D@W cases
II.107 List of D@W procedural documents including guidance