Inspection EIB - implementation of the EDPS recommendations

Fraud investigations - Recommendations		Reply EIB	Comments EDPS	Actions to take in the follow-up
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.	IG/IN is not in charge of investigating Code of Conduct breaches; this is within the remit of the Office of the Chief Compliance Officer (OCCO). IG/IN has provided in the past assistance to OCCO on Code of Conduct cases but the full responsibility regarding Code of Conduct's breaches remains with OCCO. For this purpose, IG/IN considers that there is no need to clarify the scope of EIB investigation Procedures.	I do not recall it like this. As I understood it, IG/IN quite often deals with Code of Conduct investigations... But irrespective of who's in charge, the scope should still be clarified since the IG/IN Procedures still mention investigations on misconduct and nothing about that it does not cover harassment investigations (see section 4.1.1. of the report).	Recommendation remains open, EIB should clarify the 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	Comprehensive draft data protection statement available as annex 1. This statement is still subject to internal clearance at EIB before publication. Implementation date: The statement will be published on EIB and EIF's websites and intranets as	OK, except from the fact that origin of the data is not mentioned (see Article 12(f)(iv)of the Regulation). Might not be that easy though to inform about the origin of the data on a general basis for the privacy statement on the intranet. See point 2, second paragraph of the data protection statement. More	To be discussed.

1

	period, the rights of the data subject and the origin of the data); Publish this data protection statement on the EIB website and intranet;	soon the necessary internal clearance process and necessary IT development will be completed.	important to inform the persons involved? Furthermore, does not mention transfer on a "case by case basis" but "in order to ensure the appropriate conduct of the investigation". Enough?	
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	The following sentence will be added in the privacy statement in parallel to the publication of the data protection statement on EIB's website: "The related data protection statement may be accessed on the EIB group's website under the following link […].".	Ok, depends though when the data protection statement will be published. See their comment under recommendation 2.	The recommendation can be closed (or do we wait until we actually see that the data protection statement is piblished?)
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	IG/IN already inform relevant data subjects with whom it is in direct contact during the assessment phase about the processing of their data through the privacy statement, notably the informant, the whistleblower and witnesses already contacted at assessment stage. This practice will be duly reflected in the DP Guidance, also	Good that information is provided already within the assessment phase, but how? They are referring to the privacy statement, the same as they used before? (not in compliance with Articles 11 and 12, see 4.1.2.a second bullet point of the report). The adaption of DP Guidance	EIB should provide us with the DP Guidance when adopted

	the Regulation applies. Adapt the DP Guidance for IG/IN accordingly.	including others relevant data subjects such as person concerned if already identified at assessment stage, unless a limitation under Article 20 applies. Implementation date: Q1 2017	foreseen Q1 2017, ok but since it is a 'serious' recommendation should be followed-up.	
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.	Awaiting the development of IG/IN's CMS, the following interim measure will be implemented: deferrals will be documented by preparing a note to the file to be stored in the case file in GED. See templates in annexes 2a and 2b. The procedure will be reflected in IG/IN internal procedures, including the DP Guidance. Implementation date: Q1 2017	Ok templates, the recommendation relates however to the implementation of the DP Guidance.	See above
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	This feature will be provided in IG/ IN's CMS – see print screens in annex 3. Status of implementation: The procedure to procure IG/IN's CMS had to be cancelled because the selected provider was unable to	Ok but in relation Article 20(5) - some kind of reminder in CMS to re-assess whether the conditions still apply? Seems like they will not have a CMS in the near future.	Maybe a reminder about Article 20(5)...

3

	the information in accordance with Article 20 of the Regulation.	perform the requested services. The process has to be relaunched.		
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 IG/IN dated 30 November 2015).	In order to prevent undue transfer of personal data within EIB, IG/IN will keep this sentence but will revise it as follows in order to take into account the EDPS' recommendation: "Recipients cannot forward this note or disclose its contents to others without the Head of IG/IN's prior knowledge and authorisation." Implementation date: already done	This means that the clause currently says: [...] 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 ***without the Head of IG/IN's prior knowledge and authorisation***	To be discussed
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.	Awaiting the development of IG/IN's CMS, the following interim measure will be implemented: a note to the file will be prepared, in case of transfers of personal data under Articles 8 or 9, and stored in the case file in GED. See template in annex 4. The procedure will be reflected in the DP Guidance. Implementation date: Q1 2017	Ok	Provide the EDPS with the DP Guidance when adopted (see also recommendation 4-5)

4

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).	This feature will be provided in IG/ IN's CMS – see print screens in annex 5. Status of implementation: the procedure to procure a CMS had to be cancelled because the selected provider was unable to perform the requested services. The process has to be relaunched.	Check Annex 5, think it looks ok.	If ok, the recommendation can be closed.
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[1].	Notification to OLAF: as mentioned in the context of recommendation 1, IG/IN is not in charge of investigating Code of Conduct breaches; this is within the remit of the Office of the Chief Compliance Officer (OCCO). The notification to OLAF, as currently described in the Investigation Procedures, is therefore valid. Status report: The fact that status reports are also sent to external auditors will be added in the Investigations Procedures during its next review Date of implementation: the next	Ok as long as they do not investigate any code of conduct cases, but the EIB investigation procedure should still be amended, see my comment under *Recommendation 1*. Ok, not sure though what about the fact that this will be implemented in 2018, also in relation to the fact that we listed it as a recommendation that is "easy to implement"...	To be discussed

1 See Section 4.1.3.b of this report.

		review of the Investigation Procedures will start in 2018.		
11.	Modify the DP Guidance for IG/IN so as not to rely exclusively on data subject's consent for transfers.	IG/IN may have legitimate reasons to rely exclusively on a data subject's consent for transferring data on the basis of article 9(6)(a) of the Regulation, e.g. transfer of the contact details of a national authority member with his/her prior knowledge and consent to an EIB partner. IG/IN would then need to keep the possibility for certain cases to rely exclusively on article 9(6)(a) in its DP Guidance. In any case, the transfer will always be done only if the recipient has a legitimate reason to access the data.	The example they give my be ok... Anyway, they could still add a sentence that this is only valid under exceptional circumstances (and mention the example)?	To be discussed

Anti-harassment procedures - Recommendations	**Reply EIB**	**Comments EDPS**	**Actions to take in the follow-up**
General recommendations			

12.	Notify the procedure for selection of confidential counsellors to the EDPS.	The EIB will send the notification by 31 January 2017.	Ok	Recommendation can be closed when we receive the notification.
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.	A first draft of the Dignity at Work policy has been prepared and will shortly be circulated internally for comments, (draft is attached) still subject to modifications...	Ok, maybe check the policy more in detail?	
14.	No longer designate D@W cases after the names or personnel numbers of the individuals involved.	This change will be implemented in two phases: (1) temporary solution from 1 Feb 2017 and (2) when the new CMS in place 31 Dec 2018	Ok	Recommendation can be closed
15.	Centralise all documents related to a specific D@W case in one dedicated file.	The centralisation of documents with reference to Dignity at Work procedures will be implemented for all new cases. However, for ease of reference, emails will be saved by the case manager during the course of the procedure and on finalisation and closure of the case, all e-mails will be archived in the GED database.	Will be implemented? When? The road map mention that this will be prepared once the D&W policy is approved (30 June 2018). This was however before we sent our email in which we consider recommendation 15 to be easy to implement and that it should not await the adoption of the policy.	Clarification needed
	Information to data subjects and right of access			
16.	Adopt a data protection statement for the D@W procedures, which contains the	Information on data protection has been included in the draft of the updated policy but it should	Good that they inform staff but what about the data subjects? They have not provided any data	EIB should provide the EDPS with the (draft) data

7

	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.	be noted that the EIB already informs staff on the processing of personal data in the D@W procedure. Same reply for recommendations 16-19	protection statement as "proof"	protection statement.
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	See above	They do not mention anything about a privacy statement nor the publication of it.	Ask them to clarify whether the data protection statement is available on the intranet.

	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.	See above	EIB does not address this in the draft policy	Remind them that this is an important recommendation for compliance.
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.	See above *"EIB already informs staff on the processing of personal data in the D@W procedure"*	Does it mean that the staff are informed about decisions to be taken when information is deferred? Cf. the template from IG/IN.	Should be clarified
20.	Ensure that the new CMS is featured in such a way so as to identify easily, in each case file,	Will make sure that this is included in the ToR of the Call of Tender for the new CMS.	Ok (cf. IG/IN's reply recommendation 6)	Recommendation can be closed?

	(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.	The recommendation will be delivered with the go-live of the new CMS.		
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.	It should be noted that this is already applied with regard to new D@W procedures (we ensure that only relevant and necessary data are communicated to the alleged harasser and that the alleged victim is informed about the intended communication).	See page 27 first paragraph of the inspection report and 2.1.iv) in relation to the draft D@W Policy page 9 (formal procedure). Not really in line with the "right to object"	To be discussed
	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	A first draft of the Dignity at Work policy has been prepared and will shortly be circulated internally for comments, (draft is attached) still subject to	The policy mention "no longer than necessary" in 12.3., for a period of 2 years in relation to the Informal Procedure (3.1) but nothing in relation to the Formal	Remind them that the recommendation is not included in the formal procedure.

10

	retained once the procedure is closed and where and (ii) the retention period.	modifications...	Procedure.	
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.	A procedure already exists on the destruction and retention period for files relating to D@W. The procedure will be updated and modified in the new policy.	EIB has not attached the procedure.	Should we ask them to provide us this 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.	A procedure already exists on the destruction and retention period for files relating to D@W. The procedure will be updated and modified in the new policy.		See above