

From: [REDACTED]
To: [REDACTED]
CC: European Data Protection Supervisor
<EDPS@edps.europa.eu>; [REDACTED]
Sent at: 18/10/19 12:38:45
Subject: FW: By 18.10.2019 - FW: Follow-up on the EDPS recommendations on EIB -Dignity at Work - case number 2015-0633

Dear [REDACTED],

Please find here the EIB replies to EDPS in your message below (they are highlighted so they can be easily spotted) together with the attachments. The changes in the attachments are tracked in order to facilitate your review.

Attached:

- Data Protection statement
- Internal Guidance Mediation Procedure
- Archives Procedure Manual
- EIB Retention of Documents and Records
- Data Protection Record

In case you need any further clarification or information please do not hesitate to contact me.

Best regards and have a nice weekend

Pelopidas

[REDACTED]

Pelopidas Donos
Data Protection Officer
p.donos@eib.org

From: [REDACTED]
Sent: Thursday 10 October 2019 09:14
To: [REDACTED]
Cc: [REDACTED]
[REDACTED] European Data Protection Supervisor
<EDPS@edps.europa.eu>

Subject: RE: Follow-up on the EDPS recommendations on EIB -Dignity at Work - case number 2015-0633

Dear [REDACTED],

We still haven't heard from you in relation to our questions and comments below. Since it was almost one month ago we sent you this email, please get back to us with the requested information as soon as possible and at the latest by the end of next week, i.e. **18 October 2019**.

Kind regards,
[REDACTED]

From: [REDACTED]

Sent: 13 September 2019 11:43

To: [REDACTED]

Cc: [REDACTED]

[REDACTED] European Data Protection Supervisor

<EDPS@edps.europa.eu>

Subject: Follow-up on the EDPS recommendations on EIB -Dignity at Work - case number 2015-0633

Dear [REDACTED],

Many thanks for your email and the documentation provided in relation to the follow-up of the recommendations made by the EDPS. I will comment on the different documents separately under the specific recommendation it concerns, but also I have some general comments and questions in relation to the record, please see below.

Recommendation 13

The EDPS has received the new Dignity at Work Policy, with the mediation phase included. This recommendation is therefore closed.

Recommendation 16

The data protection notice provided does not seem to be updated in light of Regulation 2018/1725 (with the exception of references to the Regulation), specifically in light of Articles 14, 15 and 16 thereof. It does not distinguish between the personal data processed for the different procedures, doesn't include contact details to the controller nor the DPO, the different retention periods are not specified etc. The reference under point (vii), where it is mentioned that the data subjects right of access to and rectify their personal data by contacting [...] once the formal procedure has been launched, is not correct since these rights apply independently where in the procedure the data subject request access or rectification. Neither does this paragraph refer to other rights of the data subject nor the mediation procedure. The data protection statement should therefore be updated to cover all the required information included in Article 15 and 16 of the Regulation. Since all the information about the procedures is included in the record provided (however, please see my comments in relation to the record below), I assume that parts of it could easily be used to update the data protection notice. I would also suggest that you include a link to the record in the notice, if the data subjects want to read more about the processing operation. The recommendation could therefore be closed provided that the data protection notice is updated in line with Articles 14, 15 and 16 of Regulation 2018/1725.

-

Please see the attached Dignity At Work Data Protection Notice

Recommendation 17

This recommendation can be closed provided that the updated data protection notice is published on the EIB intranet for all EIB staff and made also available to any third party covered by the Dignity at Work Policy.

Will be published early next week; as of now this version will be provided to third parties.

Recommendation 18

The record states (under i) *Information to be given to the data subject*) that all data subjects have access to or will be provided with the related privacy notice [...]. It is however not clear from the internal guidance when the persons concerned will be provided with the data protection notice. I suggest this to be added under M1 when replying to the alleged victim or the accused person (by including a link to the data protection notice in the email) and under M5 when informing the other party/parties of the request/suggestion. This recommendation could therefore be closed subject to the inclusion of when the information to data subjects should be provided into the internal guidance, also in relation to the formal procedure.

Please find attached, the updated "Internal Guidance Mediation Procedure". As visible from the track changes, a link to the Data protection statement will be included in the recommended emails. The same will be applied to the "Internal Guidance Formal Procedure as well as to any correspondence with the counterparties in the process.

Recommendation 19

The EIB has adopted their internal rules on restrictions under Article 25 of the Regulation (after consulting the EDPS based on Article 41(2) of the Regulation, with case number 2019-0201). The internal rules cover the processing of personal data in relation to activities set out in the Dignity at Work Policy and state that, when information to the data subjects is restricted, the reasons for the restriction should be documented and apply as long as the reasons justifying it remain applicable. This recommendation is therefore closed. Regarding your Article 25 consultation, please be reminded that the EDPS made specific recommendations in relation to the data protection notice to be included in the updated version.

Recommendation 21

The internal guidance doesn't specify what information is to be shared with the other party/parties by the MO (under M5), except information about the request/suggestion. This recommendation could be closed provided that only data that is relevant and necessary for the Mediation procedure is shared with the other party/parties. This is without prejudice to any EDPS assessment or decision in any specific case. In addition, the alleged victim or accused person should be informed on what information will be provided to the other party/parties and about his/her right to object under Article 23 of the Regulation.

Implemented, as per your recommendations. Please see M5 of the attached "Internal Guidance Mediation Procedure".

Recommendation 22

Since the Dignity at Work Policy includes the specific retention periods for the different procedures, this recommendation can be closed.

Recommendation 23-24

These recommendations remains open since the EIB has not provided the documents requested.

Regarding your comment on the Archives procedures manual, its confidentiality and whether the EDPS consider it necessary to receive this document, please see our following comment.

In line with investigative powers of the EDPS set out in Article 58(1) of Regulation (EU) 2018/1725, the EDPS has the power to:

- order the controller and the processor to provide any information it requires for the performance of his or her tasks;
- obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of his or her tasks;
- obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union law.

This entails that, in accordance with and the EDPS' inspection procedures and practices, the inspection team have access to any relevant information, regardless of the medium on which it is stored, falling within the scope of the inspection as well as to any paper files or documentation related to the concerned data processing operations and means. If necessary, this information may be collected and removed for further review at EDPS offices.

It is up to the mandated inspectors to assess and decide which personal data and/or information they require for the performance of their task, as well as which premises of the controller and the processor, including any data processing equipment and means, to access.

Confidentiality of business, trade or commercial secrets or of other information cannot be a reason to refuse to disclose that information to the EDPS and the mandated inspectors in the context of an inspection. The confidentiality of privileged information (attorney-client, medical secret, trade secret,...) and protection of EU classified information will be given appropriate due care and accessed in line with EDPS' rules, procedures and practices.

Please refer to the attached "Archives Procedure Manual" as well as the "EIB Retention of Documents and Records".

Comments on the record

As mentioned above, the record sets out how personal data is processed for the different procedures laid down in the Dignity at Work Policy. Please see my comments and questions below.

- Is this the record that is publicly accessible in line with Article 31(5) of the Regulation or is it accessible only internally for the EIB staff (and other persons covered by the Dignity at Work Policy)? It is publicly accessible upon request. The DPO is in the final stages of making the DPO register available in Intranet. The DPO will update you once this is accessible.

For all points below please see the attached updated Data Protection record. Changes are visible via track changes. The document will be finalised upon EDPS' confirmation.

- Under b) it is written that the Policy establishes two procedures for which personal data is processed, mediation procedure and the formal procedure. The Policy does however also include a section called "Preliminary Steps", where the



Les informations contenues dans ce message et/ou ses annexes sont
reservees a l'attention et a l'utilisation de leur destinataire et peuvent
etre
confidentielles. Si vous n'etes pas destinataire de ce message, vous etes
informes que vous l'avez recu par erreur et que toute utilisation en est
interdite. Dans ce cas, vous etes pries de le detruire et d'en informer la
Banque Europeenne d'Investissement.

The information in this message and/or attachments is intended solely
for
the attention and use of the named addressee and may be confidential.
If
you are not the intended recipient, you are hereby notified that you
have
received this transmittal in error and that any use of it is prohibited. In
such a case please delete this message and kindly notify the European
Investment Bank accordingly.

Les informations contenues dans ce message et/ou ses annexes sont
reservees a l'attention et a l'utilisation de leur destinataire et peuvent etre
confidentielles. Si vous n'etes pas destinataire de ce message, vous etes
informes que vous l'avez recu par erreur et que toute utilisation en est
interdite. Dans ce cas, vous etes pries de le detruire et d'en informer la
Banque Europeenne d'Investissement.

The information in this message and/or attachments is intended solely for
the attention and use of the named addressee and may be confidential. If
you are not the intended recipient, you are hereby notified that you have
received this transmittal in error and that any use of it is prohibited. In
such a case please delete this message and kindly notify the European
Investment Bank accordingly.

Dignity At Work Data Protection statement for data subjects

As defined in Article 1.3 of the Dignity at Work Policy, the Persons working for the EIB being the data subjects in the context of the Policy are hereby informed that:

1. personal data submitted will be processed in accordance with e.g. (EU) 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data. Any restrictions of the data protection rights shall be based on the internal rules adopted in accordance with Article 25 of the Regulation (hereinafter the "[Internal Rules](#)");
2. within the scope of the Dignity at Work Policy, the Director General of Personnel shall act as the "Controller" according to the definition given in Article 3(8) of Regulation (EU) 2018/1725; the Controller can be reached at the following address: dignityatwork@eib.org.
3. the purpose of the processing of personal data is the implementation of a procedure for ensuring Dignity at Work within the Bank, in particular by protecting all Persons working for the EIB against any form of harassment in the workplace;
4. within the scope of the Dignity at Work Policy, the following procedures in the context of which personal data are processed are established: a) a network of Occupational Psychologists and Confidential Counsellors b) a Mediation Procedure c) a Formal Procedure,
5. in the context of the Dignity at Work procedures as described above, the categories of data processed are as follows:

Data collected and exchanged in the course of communication with the Occupational Psychologists and the Confidential Counsellors:

- the name and position of the Alleged Victim and potentially of the Accused Person

Data collected and exchanged in the course of the Mediation Procedure:

- personal data on the data subjects (Accused Person and/or Alleged Victim) collected in the context of the Mediation Procedure - the name and position of the Alleged Victim and of the Accused Person; data shared during the Mediation by the Alleged Victim and the Accused Person,

Data collected and exchanged in the course of the Formal Procedure:

- the name and position of the Alleged Victim and of the Accused Person
- personal data on the data subjects (Accused Person and/or Alleged Victim) related to the factual background of the alleged Harassment, namely the relevant events, situations and/or incidents, including their dates, places, reactions and effects
- personal data on the data subjects (Accused Person and/or Alleged Victim) related to the documented outcome of the Mediation Procedure (if any) personal data on the witnesses that will support the Alleged Victim's complaint - i.e. their names and a brief explanation on why those persons can help establishing the facts as well as personal data from the witnesses (if applicable)
- any other relevant personal data on the data subjects (Accused Person and/or Alleged Victim) that might be contained in a supporting document or evidence
- personal data on the data subjects (Accused Person and/or Alleged Victim) contained in the final report issued by the Dignity at Work Panel describing

the findings of the Inquiry and concluding whether or not the denounced facts qualify as Harassment for the purpose of the Policy.

Personal data on the data subject, which may include special categories of data within the meaning of Article 10.1 of Reg. (EU) 2018/1725, processed lawfully according to Article 5 of this Regulation. The Dignity at Work Panel may use personal data for the sole purpose of establishing the facts leading to their recommendation.

6. in the context of the procedures under the Dignity at Work, the categories of recipients of data are as follows:

- Mediators appointed by DG Personnel;
- Confidential Counsellors (as described by Confidential Counsellors notification);
- Occupational Psychologists;
- Dignity at Work Secretariat – authorized staff that is part of the Personnel Directorate for the EIB to ensure the administration of the Formal Procedure related to the Dignity at Work Policy;
- Legal Consultant (in cases when the Dignity at Work Secretariat is outsourced)
- authorized staff that is part of the Personnel Directorate ensuring the administrative follow up of the Mediation Procedure;
- Members of the Dignity at Work Panel as appointed by DG Personnel;
- DG Personnel;
- EIB President and staff authorized by him;
- Authorized staff within the EIB Office of the Chief Compliance Officer (OCCO) in case of potential conflict of interest cases;
- Authorized staff within the EIB Inspectorate General in case of investigation;
- Authorized staff within another EIB Directorate in case Personnel is considered as conflicted to handle a Dignity at Work complaint;
- the parties involved – i.e. the Alleged Victim, the Accused Person and Witnesses.

7. they may decline to answer questions or requests for additional information made to them in the context of the Formal Procedure. However, any failure to reply might prevent or impede proof of the alleged harassment or the absence of the alleged harassment;

8. they have a right of access to, a right to request from the Controller rectification or erasure of data concerning them. Under certain conditions, they have the right to ask that their personal data are deleted or that its use is restricted. Where applicable, they have the right to object to the processing of their personal data, on grounds relating to their particular situation, at any time, and the right to data portability.. These rights may be exercised at any stage of the Mediation, by contacting the Controller, or at any stage of the Formal Procedure by contacting the Dignity at Work Panel or the Dignity at Work Secretariat in the Personnel Directorate.. The Dignity at Work Panel or the Dignity at Work Secretariat will consider their request, take a decision and communicate it to them without undue delay;

9. the legal basis of the processing operation are:

the EIB Staff Regulations, the EIB Code of Conduct, the EIB Management Committee decision of 5 March 2019 approving the Dignity at Work Policy, the Dignity at Work Policy. The EIB Decision of 26 February 2019 laying down internal rules concerning the

processing of personal data by the Personnel Directorate of the European Investment Bank in relation to the provision of information to data subjects and the restriction of certain of their rights pursuant to Article 25 of Regulation 2018/1725; Article 5(1)(a) of Regulation 2018/1725;

10. all data collected and exchanged in the course of the Dignity at Work procedures shall be adequate, kept secure and confidential, processed only for the purposes related to the implementation of the Dignity at Work Policy, not transferred to unauthorised third parties and not kept for longer than necessary for processing and for further formal action, including legal redress;

11. the relevant retention periods for each type of procedure under the Dignity at Work Policy, are as follows:

Preliminary assessment not leading to the launching of an ex officio Formal Procedure (Article 9.4 of the Policy)

Two years, from the adoption of the decision that no Formal Procedure will be launched *ex officio*, for all documents and personal data collected during the preliminary assessment carried out by DGP in case s/he becomes aware of serious allegations of Harassment.

Mediation Procedure (Article 19.1 of the Policy)

Three years, commencing on the day of the conclusion of the Mediation Procedure, for all documents retained as part of the Mediation Procedure by the Mediator and Personnel. The documents will be stored in a special electronic or paper folder clearly marked as strictly confidential. At the expiry of the retention period, all relevant data must be destroyed.

Formal Procedure (Article 35 of the Policy)

All documents, including the Complaint or the Note and any relevant supporting documents or evidence, submissions by the Accused Person and any relevant supporting documents or evidence, the Final Report and electronic communications of the Dignity at Work Secretariat with the Alleged Victim and/or the Accused Person pertaining to the Formal Procedure up to and including the Final Decision will be kept in a special file marked strictly confidential with strictly limited access within the EIB Personnel Directorate for a period of five years from the day on which the parties are informed in writing of the Final Decision. They may be stored for periods longer than five years after conclusion of the case, if relevant to judicial procedures or other inquiries.

Hearings (Article 30 of the Policy)

The hearings may be recorded by audio means, provided that all participants to the hearing in question have been previously informed. The recordings shall be made available to the Panel Members for the purpose of enabling them to conclude their assessment.

The recordings shall be kept for a period of six months after the delivery of the Dignity at Work Panel's recommendation to the EIB President, in a special file marked "strictly confidential" and with strictly limited access in the electronic document management system within the EIB Personnel Directorate. The recordings will be destroyed following the expiry of the retention period. Longer retention periods could be applied in exceptional and duly justified cases, subject to agreement of the DPO.

Where one of the parties so requests, a copy of the recording of their individual hearing shall be provided to them.

Investigations (Article 31 of the Policy)

The electronic files, telecommunication electronic traffic data and recorded data collected during the investigation and relevant to the needs of the Inquiry can be kept by the Dignity at Work Panel for a maximum retention period of six months from the Final Decision. They may be stored for periods longer than six months after conclusion of the case, if relevant to judicial procedures or other inquiries. This would include where files are transferred to other competent authorities or bodies for determination. In such instances, the DPO will be informed accordingly. After the Final Decision is communicated to the parties, the parties may have access to their personal data collected during the investigation in line with the applicable rules adopted by the competent service, in case any restrictions laid down in the Internal Rules were applied.

Personal File (Article 34 of the Policy)

- A copy (paper and/or electronic) of the decision dismissing a Complaint as inadmissible shall be placed in the personal file of the Alleged Victim.

- A copy (paper and/or electronic) of the Final Decision, along with the Final Report, shall be placed in the personal file of the Alleged Victim and the Accused Person. If the Final Decision concludes that no Harassment was found, the Accused Person may request that it is not placed in or removed from his/her Personal file. .

- The retention period for the documents placed in the personal file of the staff members is 3 years after staff member's departure from the Bank.

an exception to the confidentiality of data shall apply when this is necessary to safeguard the prevention, investigation, detection and/or prosecution of criminal offences. In this case, the Director General of Personnel shall inform the Alleged Victim and/or the Accused Person of the possible transmission of data to the competent national authorities unless this may risk undermining the prevention, investigation, detection and/or prosecution of criminal offences. In this case the Alleged Victim and/or the Accused Person will be informed at a later stage in accordance with the Internal Rules;

12. they will also have access to all evidence which designates their person and to personal data in order to ensure their completeness and accuracy and have the right to obtain from the Controller the rectification without delay of inaccurate or incomplete personal factual data;

13. the provision of information, right of access data related to him/her, rights of rectification, erasure and of restriction of processing and the communication of personal data breaches to the data subject may be restricted in accordance with the Internal Rules, if this is necessary to protect other persons involved in the Procedures or to safeguard the effectiveness of the procedure;

14. any unjustified breach of the provision about data protection may be sanctioned under the Disciplinary Procedure of the EIB;

15. they have the right to consult the EIB Data Protection Officer and have recourse to the European Data Protection Supervisor at any time.

16. the EIB Data Protection Officer can be reached at the following address: dpo@eib.org

17. more information about the processing operation under that Dignity at Work Policy can be found at the [RECORD of Processing of Personal Data regarding the Dignity at Work Policy](#)

Step	Activity Description	Role	D@W Policy Article	Related Docs
M1	Alleged Victim (the “AV”) or Accused Person (the “AP”) submit request for mediation to Director General Personnel (the “DGP”) OR DGP suggest to Mediation Officer within ER&W (the “MO”) to organise a Mediation procedure between the 2 parties Go to step M2	AV or AP OR DGP	17.1.	via email, a link of the D@W policy and the Data protection statement will be included in the email sent by DGP ¹
M2	DGP delegates the case to an officer in charge of the Mediation – i.e. to MO Go to step M3	DGP		via email to Mediation Officer within ER&W
M3	MO allocates the case to the appropriate Well-Being Coordinator Go to step M4	MO		via email
M4	MO: - assigns a Mediation case number and Go to step M5	MO		

¹ As well as in all communication between the parties

Step	Activity Description	Role	D@W Policy Article	Related Docs
M5	<p>MO acknowledges the receipt of the request and inform the other party(parties) of the request/suggestion*</p> <p>Go to step M6</p> <p>* The parties have 5 working days to accept or refuse the proposed Mediation</p>	MO	17.1	via email (at the same time providing link (or attachment) of the D@W policy and the Data protection statement)
M6	<p>The party /parties - accept(s)/refuse(s) the Mediation Procedure</p> <p>Go to step M7</p>	AV or AP	17.1.	via email/letter
M7	<p>If Mediation Procedure is accepted</p> <ul style="list-style-type: none"> ➤ MO selects a qualified external Mediator (the “ME”) from the Mediators with which EIB has established a contract ➤ MO contacts the Mediation company and the company assigns a Mediator to the case <p>Go to step M8</p>	OM	17.2.	<p>Communication with the Mediator - via email;</p> <p>Assignment of the Mediator - by return email</p>
M8	<p>Mediation session(s)</p> <ul style="list-style-type: none"> • MO organises Mediation session(s) (having checked the availability of the ME and AV, AP) <p>In the first session the parties (AV, AP and ME) sign a Mediation Agreement. ME keeps this agreement and does not send it to EIB/MO.</p> <p>Go to either step M9 or step M11 (depending on the outcome)</p>	AV AH Mediator	17.3.	Mediation Agreement (provided by Mediator)

Step	Activity Description	Role	D@W Policy Article	Related Docs
M9	<p>Mediation failed</p> <ol style="list-style-type: none"> 1. Either party (or both parties - AV & AP) withdraws from Mediation <p>Or</p> <ol style="list-style-type: none"> 2. ME reaches the conclusion that an amicable solution is not possible <p>Or</p> <ol style="list-style-type: none"> 3. A Formal Procedure is initiated <p>Go to step M10</p>	ME or AV or/and AP	17.4.;	<p>via email:</p> <ul style="list-style-type: none"> - for #1 and#2 ME informs MO - for #3 lawyers inform MO
M10	<p>Mediation failed</p> <ul style="list-style-type: none"> • ME acknowledges the failure of the Mediation Procedure and informs the parties and the MO or MO informs ME (case #3 Step 9) (via email) • MO informs DGP (as part of the quarterly reporting) <p>Go to step M13</p>	Mediator	18.3.	
M11	<p>Mediation succeeded</p> <ul style="list-style-type: none"> • Parties agree on and sign a Mediation Settlement • Each party receives a copy • ME keeps the signed Mediation Settlement and DOES NOT SEND it to MO • ME informs MO that a Mediation Settlement has been signed <p>Go to step M12</p>	AV & AP	18.1	Mediation Settlement

Step	Activity Description	Role	D@W Policy Article	Related Docs
M12	<p>Mediation succeeded</p> <ul style="list-style-type: none"> MO informs DGP <p>Go to step M13</p>	ME	18.1.	via email
M13	<p>Case closure, Archiving and Application of the Retention Schedule</p> <ul style="list-style-type: none"> MO downloads and stores the relevant Mediation emails messages related to the case in the dedicated GED folder MO deletes all messages related to the case from her/his mailbox MO formally confirms the case closure by emailing ER&W Secretariat and instructs them to proceed with Archiving of the case <p>Go to step M14</p>	MO	19.	via email
M14	<p>Archiving and Application of the Retention Schedule</p> <ul style="list-style-type: none"> ER&W Secretariat assign retention period to the case (via GED settings and in their specific tracking sheet for destruction) (date of the email sent by MO (step M13) + 3 years) and set a reminder in their Outlook Calendar for destruction of the folder on that day <p>Go to step M15</p>	ER&W Secretariat	19.	NA
M15	<p>(takes place on date of the email sent by OM (step M13) + 3 years)</p> <p>ER&W Secretariat inquires within ER&W whether there is an on-going case/investigation/proceeding re. AV or AP</p> <ul style="list-style-type: none"> If yes, go to the relevant procedure 	ER&W Secretariat	19.	Via email

Dignity At Work Policy: Internal Guidance - Mediation Procedure

CS-PERS/HRS&G/ER&W
v. 20191007

Step	Activity Description	Role	D@W Policy Article	Related Docs
	<ul style="list-style-type: none">If not, mediation related exchanges are to be destroyed End of process			



PERSONNEL Archives

Procedures Manual

- CONFIDENTIAL -

Approved 31 October 2012

Updated 5 October 2015

Translated 5 August 2016

Updated 31 July 2017

(approved by J. Lavigne for CS-PERS/QMS/QS & A. Murdock for CS/IMP/IMD/PAS)

Updated 26 July 2019



CONTENTS

1.	INTRODUCTION.....	3
2.	SECURITY MEASURES	4
2.1	Access to CS-PERS Archives.....	4
2.1.1	Locking of the archive rooms	4
2.1.2	Key cabinet.....	4
2.1.3	Document safes	4
2.1.4	Access management.....	5
2.1.5	Maintenance	5
2.2	Records storage and security	5
2.1.2	Records storage conditions.....	5
3.	DOCUMENT ARCHIVING	6
3.1	Insertion into personal file	6
3.1.1	Format of personal file	6
3.1.2	Documents relating to new EIB employees.....	6
3.1.3	Documents from CS-PERS and OCCO.....	7
3.1.4	Deposit of special files	8
3.2	Adding "General" documents.....	8
3.2.1	Transfer to CS-PERS Archives.....	8
3.2.2	Transfer to Central Archives.....	8
3.3	Gestion électronique des Documents – Electronic Document Management	9
3.3.1	GED – Institutional Workspace	9
3.3.2	GED – Knowledge Centre	10
4.	CONSULTING DOCUMENTS	11
4.1	Consulting personal files	11
4.1.1	Conditions for borrowing personal files.....	12
4.1.2	Inter-departmental exchange of borrowed files	13
4.1.3	Returning borrowed documents.....	13
4.2	Consulting "General" files.....	13
5.	RETENTION PERIODS.....	14
5.1	Personal files.....	14
5.1.1	Pre-archiving	14
5.1.2	Destruction.....	14
5.2	"General" documents in CS-PERS Archives and Central Archives.....	15
5.2.1	Inventory	15
5.2.2	Document retention table.....	15
5.2.3	Destruction.....	15
5.3	Working documents in CS-PERS offices and corridors	15
	List of annexes.....	16
	List of hyperlinks.....	17

1. INTRODUCTION

CS-PERS Archives, under the governance of CS-PERS Directorate, are handled by the Personnel Archives Service (PAS) team within the Information Management Division of the Corporate Services Directorate. CS-PERS Archives contain the following two collections:

- The "Personal Files" collection: part of CS-PERS/IMD Archives, with an archivist responsible for managing the individual files of all EIB employees (active, inactive/without rights and retired), requests to borrow and/or consult files, security and storage.
- The "General" archives collection: part of CS-PERS/IMD Archives, with an archivist responsible for managing all historical documentation excluding personal files.

Legal basis:

- Article 27.5 of [Regulation 45/2001](#) (hyperlink 01)
- Article 26 of the [Staff Regulations of Officials of the European Union](#) (hyperlink 02) and the [EIB staff rules](#) (hyperlink 03)
- [Register of recommendations of the EIB DPO \(Data Protection Officer\)](#) (hyperlink 04)

Historical background: naming of Personnel since the founding of the EIB

- 1958 – 1962 Secrétariat Général/Service du Personnel
- 1963 – 1974 Direction des Affaires Générales/Service du Personnel
- 1974 – 1994 Direction de l'Administration Générale/Service du Personnel (AG/PE)
- 1994 – 2007, 2008 – 2011 RH
- 2007 – 2008 SG-JU-RH
- 2011 HR (Human Resources)
- 2012 PERSONNEL
- Since June 2014 CS-PERS

Definitions:

(in accordance with ISO 15489 on the standardisation of current and intermediate records management policies)

Records: All documents produced or received by EIB/CS-PERS as part of its activities, regardless of date. Kept after an administrative period of use in compliance with the producer's legal obligations.

Active records: Open or recently closed working documents and files kept in offices for administrative processing.

Semi-active records: All documents no longer in day-to-day use but needing to be kept temporarily for administrative or legal reasons (including documents that will be kept as permanent records after sorting).

Permanent records: Documents that, following assessment, are kept for an indefinite period for historical or reference purposes.

Central Archives: Service responsible for managing and receiving the EIB's hardcopy and electronic records to enable them to be kept indefinitely.

Personal files: All documents associated with an EIB employee's career, access to which is strictly confidential and restricted. Each employee's individual personal file is created for administrative management purposes only.

General: All documentation connected with management regulations, policy and strategy, all notes to the MC and management's notes to staff since the founding of the EIB, other collections associated with management's key operational topics.

Document and Records Management: [Note to MC Documents and Records management policy 2006 02 24](#)
[Note to MC Retention of Documents and Records 2015-06-10](#)
([hyperlink 05](#))

3. DOCUMENT ARCHIVING

3.1 Insertion into personal file

3.1.1 Format of personal file

Personal files are split into five colour-coded sections. Each section is classified as strictly confidential and has restricted, monitored access levels.

MAIN (brown/dark blue)	General documents, split into four sub-sections 1. Start and departure dates 2. Financial entitlements and commitments 3. Civil status and insurance documents 4. Application documents and diplomas relevant to the position
CFP / Private Personal Data (orange)	<u>Sensitive</u> documents relating to the employee's personal life
APP / Appraisal (light blue)	Documents relating to the employee's appraisal exercises
CFC / Career Personal Data (red)	<u>Sensitive</u> documents relating to the employee's career and relationship with the Bank
OCCO / Compliance (yellow)	Documents relating to potential conflicts of interest: Declaration of External Activities, Declaration of Gifts, Declaration of External Appointments, Declaration of Interest

The full list of the content of a personal file can be found in [Annex II](#) to this procedure.

3.1.2 Documents relating to new EIB employees

Since 1st March 2016, new employees must submit electronically via Newcomers Portal the following documents before joining the Bank:

	Document type code
Passport or ID card	IDCARD
Diplomas and certificates	DIPLOMA
Birth certificate (including where applicable that of spouse/registered partner and dependent children)	BIRTH, BIRTHDEP, BIRTHSPOUSE
Marriage/Registered Partnership/divorce certificate (where applicable)	WEDDING, PARTNER, DIVORCE
Latest salary slip	SALARY
Statement attesting to spouse's employment (where applicable)	EMPLSP
Statement attesting to children's school/university attendance (where applicable)	EDUCA
Centre of Interest declaration form	CI
Health Insurance affiliation	HISAFF

As from 1st March 2016, only the co-signed employee contract plus salary simulation slip are sent as paper version to CS-PERS Archives where it is filed in MAIN section of the employee's personal file. This record is manually added by PAS archivist to the relevant e-personal file. All other electronic documents are migrated 1 month after entry date from NewcomersPortal/PeopleSoft to GED PERSONNEL House/e-personal files ([see DPO notification Nr 92](#)). Designated CS/IMP/IMD archivists are able to retrieve them via MyPortal/NewcomerAdministration/Document Administration or in the above mentioned specific area in GED.

The CS-PERS Staffing division delivers the contract to the IMD archivist responsible for personal files via confidential internal mail accompanied by a transfer form.

The process for the transfer of documents to e-personal files in GED is outlined in [Annex XI](#) and available on GED.

CS/IMP/IMD archivist creates the personal file for the new arrivals: opening the "MAIN" section for the filing of the contract and if relevant the "Confidential Personal" (CFP) section if confidential documents which have been provided in paper form. A green stamp is added to the MAIN section of these personal files making reference to the electronic files in GED.

Electronic documents of all active staff members which are sent by CS-PERS services to Personnel Archives will be stored in the e-personal file. No print out is added to the paper personal file. The original countersigned employment contract and its amendments and original countersigned OCCO declarations are kept as paper record in the relevant section of a personal file and a scan of the document is added to the e-personal file. The naming convention for e-personal files is to be applied. ([see Modus Operandi](#)).

The process for creating a personal file is outlined in [Annex III](#), the process for creating an e-personal file is outlined in [Annex X](#); the process mappings are both available on GED.

Psychometric tests and recruiters' handwritten notes, together with a copy of the contract, pre-recruitment email exchanges must be kept in the recruitment file by the CS-PERS/HROPS/-/SSC welcoming team.

In the event that an employee is transferred from the EIF to the EIB, the archivist must open a new file. The staff member joining EIB from EIF is responsible to submit all requested documents before starting date. He /she can make a written request to the EIF Human Resources Department for certified copies of missing documents.

The same procedure applies when an EIB staff member is joining EIF. A copy of documents of the personal file can be requested via email to personnel-archives@eib.org. The archivist will send them directly to the concerned staff member. In no case there should be an exchange of documents between the archivists of EIB and EIF. To ensure the veracity of each scan copy the latter is mitigated by having each document stamped with Personnel-Archives' stamp and dated accordingly.

If a former EIB employee returns under a new ID number, his/her old file must be added to the new file.

Personal file Quality Checks

The process of quality checks of personal files is under review by CS-PERS.

3.1.3 Documents from CS-PERS and OCCO

CS-PERS and OCCO must deliver documents for personal files to CS/IMP/IMD Archives either in confidential envelopes by internal mail or by hand to the archivist. The quality of the documents (paper or electronically) must respect the requirements of ISO15489: authenticity, reliability, usability, integrity.

OCCO documents arrive on a quarterly basis with a transfer form ([hyperlink 23](#)) which is returned to the sender after checking (registering). A copy of the original form is saved by the archivist in a GED folder. If the employee concerned does not yet have an OCCO file, the archivist must create one.

Documents are added to the employee's personal file throughout his/her career. **For confidentiality reasons and unless otherwise instructed by DG CS-PERS or OCCO , any document that does not feature the employee as sender or recipient (or recipient in copy) cannot be placed in his/her file.**

This process is outlined in [Annex IV](#), and can also be consulted on GED.

The internal CS-PERS services are requested to send documents on a regular basis – ideally once a month – pre-sorted by ID number, accompanied by a transfer form available in GED. ([hyperlink 08](#)) Alternatively an email listing all documents sent to the archivist can replace the transfer form. Any batch of more than 10 documents sent without transfer form will be returned to CS-PERS.

3.1.4 Deposit of special files

Ref.: DPO notification from Jan 2017 - Dossiers spéciaux du ressort du Directeur ERA et de la Division Relations sociales et Bien-être au Travail (ER). ([hyperlink 09](#))

Documents transferred by hand in a sealed confidential envelope from the CS-PERS/DIR office, the CS-PERS/HRS&G directorate or CS-PERS/HRS&G/ER&W division to the archivist are filed in the ORANGE ("Confidential Personal") section of the personal file. The internal procedure can be consulted on special request.

Each staff member is allowed to consult this part of his/her personal file.

Access restrictions and retention periods are defined in the DPO notification.

3.2 Adding "General" documents

3.2.1 Transfer to CS-PERS Archives

In order to avoid documents being stored in offices and to ensure the CS-PERS Archives are complete, CS-PERS employees must regularly send any "General" files in their possession.

The list of documents/files to be sent to CS-PERS Archives for permanent or temporary archiving is included in [Annex V](#) to this procedure and is also available to PERSONNEL division secretaries on GED.

A table outlining the filing procedure for the various notes & letters can be found on GED. ([hyperlink 10](#))

A transfer form, available on GED ([hyperlink 11](#)), is filled out by the divisions before the documents are added to the CS-PERS Archives. This form lists the files transferred to CS-PERS Archives to facilitate checks and provide a record of documents added.

Once the form has been filled out, the division contacts IMD Archives using the PERSONNEL-archives@eib.org generic mailbox so that the documents added can be checked and to agree a transfer date.

The process for receiving and filing by the archivist is outlined in [Annex VI](#), and is also available on GED.

Since March 2013, all documents added to the file have been accompanied by a green stamp indicating the date of receipt and filing date.

3.2.2 Transfer to Central Archives

All "General" documents added to the Central Archives must be approved by the archivist responsible for "General" documents.

Only files considered permanent records are to be sent to the Central Archives after evaluation by the archivist.

To add documents to the Central Archives, the archivist must fill out a transfer form and then send an email to CENTARCH@eib.org to agree a sending date.

3.3 Gestion électronique des Documents – Electronic Document Management

3.3.1 GED – Institutional Workspace

An Institutional Workspace is an intra-departmental or intra-divisional electronic workspace containing documents in the process of being drafted. These documents can be shared with colleagues from the same division or department.

Each division has a directory in the Institutional Workspace (IWS), managed by the division secretary. Only members of a particular division can work in their respective workspace. All access and permission changes must be approved by the CS-PERS principal GED correspondent.

-  [CS-PERS \(All Departments\)](#) ▾
-  [CS-PERS/ERA/BA](#) ▾
-  [CS-PERS/ERA/BA/-/MS](#) ▾
-  [CS-PERS/ERA/BA - PERSONNEL Infodesk](#) ▾
-  [CS-PERS/ERA/ER](#) ▾
-  [CS-PERS/ERA \(Management\)](#) ▾
-  [CS-PERS/ERA/SPHI](#) ▾
-  [CS-PERS \(Management\)](#) ▾
-  [CS-PERS/QMS/ACB](#) ▾
-  [CS-PERS/QMS/-/COORD](#) ▾
-  [CS-PERS/QMS \(Management\)](#) ▾
-  [CS-PERS/QMS/QS](#) ▾
-  [CS-PERS/S&D/D&P](#) ▾
-  [CS-PERS/S&D \(Management\)](#) ▾
-  [CS-PERS/S&D/STA](#) ▾

Files saved on GED must respect the NAMING CONVENTION ([hyperlink 12](#)) for documents produced by the CS-PERS directorate.

Since 1 January 2012, divisions have been obliged to save all notes/letters with a note register number in their division's e-chrono folder, which can be found in their IWS directory. A DPO notification on this subject entitled "Harmonization of filing methods using e-chrono folders saved in GED" was implemented on 16 April 2012 and can be found on GED. ([hyperlink 13](#))

The CS-PERS (All Directorate) directory includes all notes to the MC and their corresponding minutes as well as opinions on notes to the MC since 2010. Every time a note to the MC or opinion is distributed, the relevant secretary must add the final version of the note to this directory in PDF format. The original hardcopy version must be sent to CS-PERS General Archives.

A guideline explaining how to save notes to the MC and opinions is available on GED. ([hyperlink 14](#))

3.3.2 GED – Knowledge Centre

The Knowledge Centre is an electronic archiving space where only the final versions of documents are stored in pdf format. All Bank employees have read-only access (excluding some confidential directories).

Notes to staff collection

All CS-PERS notes to staff issued since 1958 can be found in the Notes to Staff directory. Staff communications (e.g. appointments or other communications with no impact on the Staff Regulations) are also saved in a different sub-folder for each year. ([hyperlink 15](#))

Enterprise > Knowledge Centre > 12 - PERSONNEL MANAGEMENT >

03- Notes to Staff

GEDRM Search Notes to Staff

Look for: All Words

Title Text Any

Date Range: From: Month Year To: Month Year

Note N°:

Search Reset

Useful Information

This collection contains all existing notes to staff since 1958 till today

- The coordinators of this area are Daniela Pfaltz and Susan Goodwin.
- The folder structure of this area is organized by year folders, which contain the legal notes to staff, and for each year a 'Communication au personnel' subfolder, which contains the informative note to staff.
- [Intranet PERSONNEL](#)
- [How to bookmark this page as a Favorite?](#)

Specific conditions apply to saving notes to staff, particularly in terms of naming conventions and the addition of metadata to facilitate searching.

A guide to saving notes is available on GED. ([hyperlink 16](#))

Staff Regulations, Administrative Conditions, Code of Conduct and Pension Scheme Regulations collection

This space includes the various staff regulations. ([hyperlink 17](#))

Divisions adding documents must regularly update their collections in coordination with the archivist responsible for "General" documents.

4. CONSULTING DOCUMENTS

4.1 Consulting personal files

Only requests made by email to PERSONNEL-archives@eib.org are considered official and admissible. The archivist will otherwise ask the person concerned to submit his/her official **written request and authorisation (specified below)** to PERSONNEL-archives@eib.org for consultation purposes.

NB for information: only archivists can be the "Owner" of the PERSONNEL-archives@eib.org inbox. This enables them to grant access rights to third parties.

Request by an employee (or former employee) outside CS-PERS

All employees have the right to access their entire personal file. All documents and reports used in an internal decision-making process at the Bank relating to the administrative status, ability and efficiency of the employee are kept in their personal file. The file may be consulted in CS-PERS Archives in the presence of the archivist.

For requests from former employees, PAS archivist is obliged to check the identity to ensure secure treatment of personal data in line with the EIB's data protection policy and in the interest of the requestor. The requestor is asked to communicate to PERSONNEL-Archives@eib.org the date of birth, the ID number as former EIB staff member and the last private address registered in EIB database.

If an employee requests a copy of a document from his/her file, the archivist is providing a scan of the record or if necessary a paper copy. No document can be removed from a personal file, and no original document can be replaced with a copy. Certified copies can only be done for the documents which have been produced by EIB. In this case, CS-PERS Infodesk adds the EIB stamp and the date, and the Head of Division for CS-PERS/HROPS/BA signs the document. To obtain certified copies for documents not edited by EIB, staff members have to go to the Bierger Center for a certified copy.

Exceptions: Staff members outside CS-PERS without authorisation to access other staff member's personal files must request special written authorisation from Director General CS-PERS and DPO.

Request by a CS-PERS employee

Measures are taken to comply with EU personal data protection regulations, in particular by limiting the access of CS-PERS employees to the documents necessary for their role only. Users from each division are only authorised to access certain sections of the personal file as outlined in [Annex I](#) "Authorised access of PERSONNEL employees to each personal file section", which can also be consulted on GED.

The list of authorised accesses is updated on a regular basis by CS-PERS.

Exceptions: CS-PERS staff members without authorisation to access personal files must request special written authorisation from the relevant head of division or from Director General CS-PERS.

Request from OCCO

Access rights for the OCCO file are exclusively reserved for the Group Chief Compliance Officer, the Deputy Chief Compliance Officer and the assistant Chief Compliance Officer, the Head of Corporate Compliance Division and a designated compliance officer who inform Director General CS-PERS in advance when they exercise their access rights.

Director General CS-PERS, which has custody of the personal files, may also have access to this part of the file but must notify the Group Chief Compliance Officer accordingly prior to exercising this right.

Request from IG and from MC/IA

Access rights for the complete personal file of a staff member are exclusively reserved for the Inspector General and the Director of Internal Audit who inform Director General CS-PERS in advance when they exercise their access rights.

4.1.1 Conditions for borrowing personal files

Borrowing/consultation requests

Requests are centralised by the archivist responsible for personal files using the PERSONNEL-archives@eib.org shared inbox. Since 01/10/2017 the BMC ticketing tool can also be used to submit requests. If the message is sent to the personal inbox of an archivist, he/she will forward the email to the shared inbox and ask the sender to address any future requests to this inbox.

The request will be processed within 24 hours. Urgent requests will be processed within an hour. A maximum of three personal files can be borrowed per request.

The continuity of CS-PERS Archives must be ensured as far as possible to overcome any unforeseen issues.

The process for consulting and requesting loans of personal files is outlined in [Annex VII](#), and is also available on GED. As this process is requesting two ICF key controls, one in IMD, one in CS-PERS, the mapping has been duplicated and the relevant area of responsibility is highlighted in red.

CS-PERS Archives Register - Actions Logbook

The register is used to keep a record of every file borrowed by duly authorised CS-PERS employees or the employees themselves since 1996. It also serves as a record and safeguard of appropriate access management, confidentiality and preservation of CS-PERS Archives files.

This register is also used as the basis for calculating the borrowing and consultation statistics presented to the Head of Division CS/IMP/IMD each quarter.

For confidentiality reasons, only designated IMD archivists may use the register.

The old hardcopy register has been replaced and digitised. Historical entries dating back to 1996 are also saved on GED ([hyperlink 18](#)) in PDF format.

The ongoing borrowing log is saved on GED and is accessible only to IMD archivists and for monthly quality checks to the assigned person within CS-PERS. Breaches detected through these checks are reported to the archivists and to the Head of Division CS/IMP/IMD and escalated if needed to HoDEP CS-PERS/HROPS. ([hyperlink 19](#))

Files borrowed and kept for longer than 24 hours must be stored in a locked cabinet by the borrowing CS-PERS employee. **The principles of discretion and confidentiality must be respected while working on the files in offices.**

4.1.2 Inter-departmental exchange of borrowed files

The exchange of files borrowed from CS-PERS Archives between colleagues or CS-PERS units/divisions will only be permitted provided that a notification is systematically and simultaneously sent to the archivists using the PERSONNEL-archives@eib.org inbox.

The original borrower is responsible for the file until the change of borrower email is received by CS-PERS Archives.

4.1.3 Returning borrowed documents

For security and confidentiality reasons, files borrowed from CS-PERS Archives must be returned **within 48 hours and always before the weekend** or a period of absence. A 48-hour extension can be granted by making a written request to PERSONNEL-archives@eib.org.

Except in exceptional cases, the employee must inform the archivist that the file will not be returned on time and specify the new return date. If the file is not returned, the archivist will go to the borrowing CS-PERS employee's office to retrieve it. If the employee is absent, the archivist will ask his/her colleagues.

A reminder will be sent by IMD archivist after four days. Files are returned to the archivist by hand – for security and confidentiality reasons, deliveries by internal mail are not permitted.

If the files are still not returned 24 hours later, the archivist informs the head of division, who sends a reminder to the employee and his/her line manager to ensure the immediate return of the documents.

The archivist must systematically monitor borrowed files using the borrowing register.

4.2 Consulting "General" files

Document/consultation requests

Files from the "General" section can only be accessed through the "General" files archivist. Files must not leave the archive rooms, meaning that copies or scans must be made.

On-site consultation of public files is possible via written request to PERSONNEL-archives@eib.org. The same access restrictions applicable to the confidential sections of personal files also apply to consulting confidential "General" files.

[Annex V](#) defines the access category for "General" documents.

The full "General" document list (CS-PERS Archives and Central Archives) is available on GED.

[\(hyperlink 20\)](#)

5. RETENTION PERIODS

5.1 Personal files

5.1.1 Pre-archiving

Documents for personal files in hardcopy (usually original documents) or electronic format (to be printed by the archivist) should be deposited regularly by the various divisions to avoid backlogs in CS-PERS Archives where possible.

The different depositing services (PERSONNEL, OCCO) must indicate the employee's ID number on the document in advance to make filing easier.

The transfer of documents from CS-PERS services to CS-PERS Archives has to be documented on the transfer form added to the files designated for filing in the personal files.

These pre-archiving documents are stored in a locked cabinet in the office of the archivist before filing.

Documents must be filed within three days of receipt, or the same day for confidential documents (orange and red).

5.1.2 Destruction

Once the administrative period of use has elapsed, archivists are responsible for destroying files after assessing their historical interest.

MAIN (brown/dark blue)	Retention period: permanent (120 years after birth date)								
CFP / Private Personal Data (orange)	Retention period: permanent (120 years after birth date)								
APP / Appraisal (light blue)	To be destroyed three years after the employee leaves the EIB.								
CFC / Career Personal Data (red)	To be destroyed three years after the employee leaves the EIB.								
OCCO / Compliance (yellow)	<table> <tr> <td>Declaration of External Activities</td> <td>ten years (OCCO notification)</td> </tr> <tr> <td>Declaration of Gifts</td> <td>five years (OCCO notification)</td> </tr> <tr> <td>Declaration of External Appointments</td> <td>five years (OCCO email)</td> </tr> <tr> <td>Declaration of Interest</td> <td>five years (OCCO email)</td> </tr> </table>	Declaration of External Activities	ten years (OCCO notification)	Declaration of Gifts	five years (OCCO notification)	Declaration of External Appointments	five years (OCCO email)	Declaration of Interest	five years (OCCO email)
Declaration of External Activities	ten years (OCCO notification)								
Declaration of Gifts	five years (OCCO notification)								
Declaration of External Appointments	five years (OCCO email)								
Declaration of Interest	five years (OCCO email)								

The archivist uses the LAB container within the archives to destroy files. For large volumes, a Remedy ticket via BMC application must be sent. The archivist must be present for the transfer to the place of destruction, and for the destruction itself.

The process for destroying personal files is outlined in [Annex VIII](#), and is also available on GED.

A DPO joint record (data controller & data processor) on management of personal files for EIB staff members and members of the EIB Management Committee is available via the DPO register on EIB Intranet. ([hyperlink 21](#)).

5.2 "General" documents in CS-PERS Archives and Central Archives

5.2.1 Inventory

All "General" documents (stored in CS-PERS Archives and Central Archives) are indexed in an inventory available on GED. ([hyperlink 20](#))

This inventory is subject to continual changes in line with cleaning operations and additions made by the archivist responsible for "General" documents.

The inventory can be consulted by CS-PERS employees and, on an exceptional basis, by duly authorised JU (legal) Directorate employees via a request to the PERSONNEL-archives@eib.org shared inbox.

5.2.2 Document retention table

"General" documents are sorted by type/theme with a defined retention period in accordance with EU legislation or Bank DPO notifications.

A table outlining the different retention periods ([approved by the DPO](#)) is included in [Annex IX](#) to this procedure, and is available on GED.

5.2.3 Destruction

Documents/files deposited with CS-PERS Archives that are not to be kept for historical purposes must have a retention period indicated on the back of the file.

The IMD archivist sends a destruction form ([hyperlink 22](#)) to the owner of the documents (relevant head of division) and destroys the indicated files once the confirmation for destruction received.

Copies are also systematically destroyed if the original is already in CS-PERS Archives.

The archivist uses the LAB container within the archives to destroy files. For large volumes, a Remedy ticket via BMC application must be sent. The archivist must be present for the transfer to the place of destruction, and for the destruction itself.

5.3 Working documents in CS-PERS offices and corridors

Files/folders in offices and corridors containing active documents – i.e. those used on a daily basis for work or reference – are the responsibility of the employee concerned. This involves regular cleaning and destruction in accordance with the retention table ([Annex IX](#), see 5.2.2).

All CS-PERS office/corridor/general files destroyed must be entered into the "Destruction" Excel spreadsheet managed by the archivist responsible for "General" documents. There is no need to complete a destruction form.

CS-PERS employees must use the LAB containers in each corridor to destroy files. In the event that a document has been mistakenly placed in a LAB container, the assistant to Director General CS-PERS can be contacted so that it may be opened in his/her presence.

List of annexes

I.	Authorised accesses to personal files of staff members	(p.5, 11)
II.	Full list of personal file content	(p.6)
III.	Process outline – Create Personal File	(p.7)
IV.	Process outline – Receive and File Documents in Personal File	(p.8)
V.	List of documents and files to be sent to CS-PERS Archives/Generalities for definitive or temporary archiving	(p.8, 13)
VI.	Process outline – Receive and file documents “Generalities”	(p.8)
VII.	Process outline – Request and consult records from personal files	(p.12)
VIII.	Process outline – Destroy physical records in personal files	(p.14)
IX.	Retention Schedule for documents of CS-PERS Directorate	(p.15)
X.	Process outline - Creation of e-personal files GED Personnel House	(p.7)
XI.	Process outline - Transfer of documents to e-personal files in GED	(p.6)

List of hyperlinks

01. [EC regulation 45/2001](#) (p.3)
02. [Staff Regulations of Officials of the European Union](#) (p.3)
03. [EIB staff rules](#) (p.3)
04. [Register of recommendations of the EIB DPO \(Data Protection Officer\)](#) (p.3)
05. [Notes to MC on Documents and Records management](#) (p.3)
06. [CS-PERS Archives Key cabinet inventory](#) (p.4)
07. [CS-PERS General Archives WKI-5002 - Filing Plan of General Archive collections](#) (p.4)
08. [Transfer form for CS-PERS documents for personal files](#) (p.7)
09. [DPO notification ERA/ER – Special files](#) (p.8)
10. [Filing procedure CS-PERS notes & letters](#) (p.8)
11. [Transfer form for CS-PERS General Archives documents](#) (p.8)
12. [Naming conventions for documents CS-PERS directorate](#) (p.9)
13. [DPO notification - Harmonization of filing methods using e-chrono folders saved in GED](#) (p.9)
14. [GUIDELINE Saving MC notes and opinions on GED](#) (p.9)
15. [Notes to staff collection](#) (p.10)
16. [GUIDELINE Saving notes to staff on GED](#) (p.10)
17. [EIB staff regulation collections](#) (p.10)
18. [Historical borrowing register for personal files \(1996-2011\)](#) (p.13)
19. [CS-PERS Archives Register - Actions Logbook](#) (p.12)
20. [CS-PERS General Archives inventory table](#) (p.13, 15)
21. [DPO Record 178. Management of personal files for EIB staff members and EIB MC members](#) (p.14)
22. [Destruction form for CS-Archive General documents](#) (p.16)
23. [Transfer form for OCCO documents for personal files](#) (p.7)

TACIT PROCEDURE

FOR DECISION

The proposal will be considered approved unless otherwise indicated by

25 JUN 2015

AB

Note to the Management Committee

A Murdock¹

Subject: Retention of Documents and Records

Ref.: Internal Control Framework AI-2014-ICF-01²

1 DECISION REQUESTED

The Management Committee is requested to approve the attached *Policy on the Internal Management and Retention of Documents and Records (Annex 1)*.

2 BACKGROUND INFORMATION

2.1. Current situation

The Bank's current *Document and Records Management Policy* was approved by the Management Committee in 2006 (**Annex 2**)³.

The Document and Records Management Policy (2006) includes Articles relative to the retention of documents and records. Current practice is oriented towards permanent or long-term retention in order to fulfil the Bank's institutional, administrative, operational and financial requirements. Following the approval of the Directorate concerned, document destruction has been restricted to fulfilling EIB's legal or regulatory obligations or to eliminate duplication.

Since 2006, the current Policy has been complemented by Directorate Document and Records Retention Schedules⁴. Document retention requirements have also been impacted by the increased importance given by the Bank to implementing notifications and recommendations made by the Data Protection Officer and in the *EIB Transparency Policy*⁵.

Internal Audit has also drawn attention to the growing number and complexity of Mandates and Partnership Agreements which contain numerous clauses specific to reporting and document retention. In these circumstances the detailed knowledge

¹ The author of the note confirms that the approval of the Director General has been sought and that the relevant Members of the Management Committee have been consulted before distribution of the note.

² Internal Control Framework – Corporate Services (Part 3) PROCUR & IMD: IG/AI/2014-167/CH/CL7za : AI-2014-ICF-01.

³ Note to Management Committee: Document and Records Management Policy; 24 February 2006; SG-JU/AG C&I/I&IC/2006-213/AM/abb; approved by TACIT procedure.

⁴ Notably in FI and Personnel.

⁵ Transparency Policy (2015) ; Clause, 5.1.4

of the services concerned is an essential part of the successful implementation of agreed retention periods.

EIB complies with document management and retention requirements in applicable EU laws and Policies. In regard to document management EIB complies with Regulation (EC) 1049/2001 regarding public access to European Parliament, Council and Commission documents and Regulation (EEC, Euratom) 354/83 concerning the opening to the public of the historical archives of the EEC and Euratom⁶. Both regulations are relevant to document retention and have been complemented in other EU institutions by Retention Policies and Schedules.

2.2 Internal Control Framework – AI-2014-ICF-01⁷.

In 2014 Internal Audit carried out and concluded an audit of the Corporate Services Internal Control Framework including Information Management Division (IMD). The Agreed Action Plan (AAP) remarked that *'a Bank-wide records retention schedule is not yet formalized. A Document and Records Management Policy note was issued in 2006 but was not implemented'* and that the Management Committee note accompanying the Policy *'refers to the future creation of a retention schedule and to the application of retention periods'*.

Consequently, AAP3 of the Internal Control Framework required IMD to *'formalise a corporate Records Retention Policy to be applied to electronic as well as paper based records'*.

IMD regards Management Committee approval for a revision of the current *Document and Records Management Policy* as the necessary step to close AAP3 of the Internal Control Framework. IMD propose to update the current Policy by including revised Articles on Document and Records Retention which will provide the guiding principles required for *'the future creation of a retention schedule and to the application of retention periods'*.

The development and implementation of a Bank-wide Records Retention Schedule was the subject of a separate AAP in the Internal Control Framework⁸. Although part of the note submitted to the Management Committee in 2006, full implementation of a Bank-wide Records Retention Schedule has been delayed due to successive changes in organisational priorities and lack of appropriate tools. With IMD taking a lead role and a Records Management Database now in place, the conditions are in place to close AAP4 by the end of the year without further recourse to the Management Committee.

3 KEY ELEMENTS FOR DECISION

3.1. Update of articles on retention of documents and records

⁶ Amended by Regulation (EU) 2015/496 as regards the deposit of the historical archives of the institutions at the European University Institute in Florence

⁷ Internal Control Framework – Corporate Services (Part 3) PROCUR & IMD: IG/AI/2014-167/CH/CL7za : AI-2014-ICF-01.

⁸ AAP4 of the Internal Control Framework required IMD to *'perform a feasibility study for the development and implementation of a Bank-wide Records Retention Schedule [including] an implementation plan, timetable for its implementation and persons responsible'*.

In view of changing document retention requirements IMD propose to replace the *Document and Records Management Policy (2006)* with an updated *Policy on the Internal Management of Documents and Records* (the 'Policy').

The Policy includes updates to the definition of 'documents', rules for the management of e-mail and a revised section on Document and Records Retention (Article 2.5 of the Policy).

The principles underpinning the proposed Articles on Document and Records Retention can be summarized as

1. The Document and Records Retention Articles apply to any document repository of the Bank and to documents held in both paper and electronic form.
2. EIB complies with document management and retention requirements in applicable EU laws and Policies. If no existing legal or regulatory document retention requirements exist, EIB will determine retention requirements following an assessment of its institutional, operational, financial or administrative record-keeping needs.
3. EIB will continue to provide long-term document retention in order to ensure that the Bank can fulfil its institutional, operational, financial and administrative obligations and responsibilities.
4. Document destruction will be regulated by legal or regulatory requirements or following approval by the responsible Directorate, according to the Directorate Document and Records Retention Schedule'.
5. Document destruction will be suspended in the event of litigation, audit or ongoing investigation, pending the resolution of such actions.

3.2 Objectives of the revised retention articles

Article 2.5 of the *Policy on the Internal Management and Retention of Documents and Records* will formalise current practices in order to

1. Fulfil EIB legal obligations.
2. Provide a framework for document retention requirements in EIB Policies, Procedures and Guidelines, including enhanced reporting requirements for Partnerships and Mandates.
3. Provide a framework for the development and approval by senior management of Directorate Document and Records Retention Schedules.
4. Provide internal and external transparency in EIB document retention policies in line with the Bank's Transparency Policy and policies of the other European institutions. For this reason, the Policy will be published on the EIB's website.
5. Manage the costs of document storage whilst providing easy and rapid access to all documents which are required for business purposes, preventing duplication, accidental loss or unauthorised destruction.

4 FINANCIAL AND OTHER IMPACTS

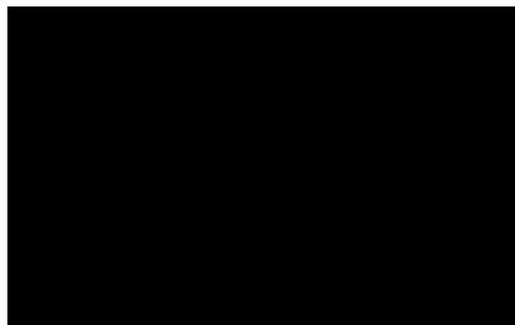
No additional financial costs will be incurred.

The allocation of staff resources in Corporate Services (1-2 FTE) to support the implementation of this Policy is to be considered alongside the recommendations contained in recently submitted MC notes on Internal Document Classification (approved 26th May 2015) and Use of E-mail Guidelines. The positions are to be financed either through internal reallocation of posts within CS or through a future ARP request.

5 NEXT STEPS / IMPLEMENTATION

In order to 'formalise a corporate Records Retention Policy to be applied to electronic as well as paper based records' as required by AAP3, the following approach is proposed:

1. The current *Document and Records Management Policy* (2006) will be renamed '*Policy on the Internal Management and Retention of Documents and Records* (**Annex 1**).
2. The *Policy on the Internal Management and Retention of Documents and Records* has been updated to include Document and Records Retention.
3. Directorates will continue to develop and update their own Document and Records Retention Schedules with the assistance of IMD.
4. IMD will develop procedures for the implementation of retention requirements including the secure destruction of documents and records in order to render them unrecoverable and prevent accidental disclosure of classified or confidential information.
5. Directorate Retention Schedules will be progressively harmonized through an annual review process led by IMD in order to provide a Bank-wide Retention Schedule.
6. IMD will update the Policy and Articles on Document and Records Retention when required in order to formalise changing document retention requirements.



6 COMMENTS FROM THE SERVICES

6.1 MCO Opinion

SG/IS/PBA has reviewed the financial impacts of the proposal, has no comments, and agrees to use this tacit procedure to obtain the decision from the MC requested in this note.

6.2 Personnel Opinion

Personnel has been consulted and has no further comments



6.3 Others JU, DPO and SG

JU, DPO and SG have been consulted and their comments incorporated into this Note and proposed Policy.

The Secretary General agrees to use this tacit procedure to obtain the decision from the MC requested in this note.

C.c.: Distribution list for MC Notes

Annexes:

1: *Policy on the Internal Management and Retention of Documents and Records.*

2: Note to Management Committee: Document and Records Management Policy; 24 February 2006; SG-JU/AG C&I/I&IC/2006-213/AM/abb.



Policy on the Internal Management and Retention of Documents and Records

Table of contents

1	EXECUTIVE SUMMARY	3
1.1	SCOPE	3
1.2	DEFINITIONS	3
2	THE ORGANISATION AND MANAGEMENT OF DOCUMENTS AND RECORDS	4
2.1	DOCUMENT MANAGEMENT	4
2.2	THE CAPTURE OF DOCUMENTS AS RECORDS	4
2.3	ACCESS.....	4
2.4	STORAGE	4
2.5	DOCUMENT AND RECORDS RETENTION.....	4
2.6	PRESERVATION.....	6
3	RULES SPECIFIC TO THE MANAGEMENT OF OTHER DIGITAL RECORDS	6
3.1	E-MAIL	6
3.2	SCANNING	6

1 Executive summary

This Policy aims to establish standard rules and actions for the organisation and management of the Bank's documents and records to ensure their reliability as evidence of the Bank's business activities.

All of the Bank's activities and decisions ultimately lead to the production of documents and records. These documents and records are a strategic information resource and are the basis of institutional memory. Efficient document management is an essential prerequisite for an effective policy of public access, good governance and financial accountability.

This Policy is made with due regard for existing EIB Policies and Procedures on document creation approval, distribution, confidentiality and e-mail.

1.1 Scope

This Policy is relevant to all documents and records which are drawn-up or received by the EIB concerning a matter relating to the policies, activities and decisions falling within its competence and in the framework of its official tasks, regardless of their format or physical location.

The Policy incorporates the actions required for the organisation and management of documents and records throughout their life-cycle, including document capture, organisation, access, storage, retention, and preservation.

1.2 Definitions

Document

For the purposes of this Policy, 'document' as defined by Regulation (EC) 1049/2001 of the European Parliament and of the Council of 30th May 2001 regarding public access to European Parliament, Council and Commission documents is understood to mean

'any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording) concerning a matter relating to the policies, activities and decisions falling within the institution's sphere of responsibility'.

2 The Organisation and Management of Documents and Records

2.1 Document Management

Rules for the organisation and management of documents within departments will be subject to Procedures in place within the relevant department with a view to determining if documents must be captured as records.

2.2 The capture of documents as records

Documents or files should be captured as records when:

- They commit the organisation or individual to an action renders the organisation or individual accountable, or which documents an action, a decision or decision-making process.
- They are attached to an enterprise-wide file plan, available by computer and based upon a common nomenclature which defines the Bank's activity-based functions
- They are relevant to the same activity-based functions of the enterprise-wide file plan. and linked through the application of relevant classification and metadata, regardless of their format or physical location.

2.3 Accessibility

Documents captured as records have to be:

1. Easily retrievable by all staff who have been granted permissions to access documents and records through the application of physical access controls or management of electronic permissions management controls'.
2. Easily identifiable, regardless of their format or storage location through the application of relevant metadata describing their information value
3. Protected against unauthorized addition, deletion, alteration, use and concealment
4. Maintained via an auditable trail for all record transactions
5. In line with EIB rules in force on transparency, internal classification and Personal Data Protection, these rules will be uniformly applied to documents and records held in paper and electronic format to ensure that they are applied for specified periods and removed when warranted.

2.4 Storage

Documents and records, in any medium, must be stored and made secure from unauthorised access and physical damage arising from daily use, system failure or breakdown, water or fire.

2.5 Document and Records Retention

The retention and disposition of documents and records applies to any document repository of the Bank. The classification of documents and records according to their retention requirement applies to both paper and electronic documents. Documents and records may be held in both paper and electronic format for the duration of their retention requirement.

Retention schedules

The Bank-wide Retention Schedule is understood to be the compilation of Directorate Document and Records Retention Schedules.

The classification of documents and records according to their retention requirements will be formalised within Directorate Document and Records Retention Schedules.

Retention requirements

Documents and records will be classified according to their legal, regulatory, or EIB institutional, operational, financial, and administrative retention requirements.

The Policy takes into account the other EIB Policies and rules and will be read in conjunction with them.

Legal or regulatory retention requirements, notably EU Regulations on public access to documents and historical archives of the EU, will take precedence over EIB institutional, operational, financial and administrative retention requirements.

In all cases document destruction will be suspended in the event of ongoing litigation, audit or investigation pending the resolution of such actions.

The classification and retention values assigned to documents in the Retention Schedule will result in one of the following:

Permanent retention of documents

- Documents identified for permanent retention may be transferred to the Historical Archives of the European Union, Florence only if approved in the Directorate Document and Records Retention Schedules.

Prolonged retention of documents required for EIB institutional, operational, financial or administrative purposes

- Documents which may be retained for up to 30 years following a significant and agreed date or event.
- Documents will be assigned a 5 year, 15 year or 30 year retention period following a significant and agreed date or event.
- Documents which have exceed their retention requirement will be destroyed following Directorate approval or may have their retention requirement extended for a maximum of 5 years if justified by the Directorate concerned.

Destruction of documents in order to comply with legal or regulatory requirements

- Documents which are required to be destroyed following proscribed retention periods.
- Documents held by Directorates will be destroyed according to Directorate Document and Retention Schedules.
- Documents held in Archives or Electronic Document Management System (EDMS) which have exceeded their retention requirement will be destroyed following Directorate approval.

Destruction of documents in order to fulfil EIB institutional, operational, financial, or administrative retention requirements

- Documents which are to be destroyed in order to eliminate duplication and manage storage costs.
- Documents will be assigned a 5 year, 15 year or 30 year retention period in order to satisfy institutional, operational, financial, or administrative use.
- Documents may have their retention requirement extended for a maximum of 5 years before destruction.
- Any documents held for short-term retention periods of less than 5 years will be held and destroyed by Directorates.
- Any document held by Archives or in EDMS for retention periods of more than 5 years and which have exceeded their retention requirement will be destroyed following Directorate approval.

2.6 Preservation

Documents and records will normally be held in the form in which they were drawn up, approved, sent, or received with certified or true copies retained for legal or Business Continuity Planning purposes only.

Long-term access to the Bank's records will be preserved through appropriate conservation and preservation measures including their conversion or migration to other formats.

3 Rules specific to the management of other digital records

3.1 E-Mail

An e-mail and its attachment should be considered as a document as defined by Regulation (EC) 1049/2001 of the European Parliament and of the Council of 30th May 2001.

Guidelines for the internal use, organisation, management and retention of e-mails will ensure that e-mails are retained in their original format preserving the link between the e-mail message and its attachments or in a form, which preserves the integrity of the message content and relevant metadata

3.2 Scanning

The scanning of documents shall provide identifiable benefits to the organisation through enhanced workflows or processes, or improved access to document collections.

Scanned documents will be captured as records, when attached to an enterprise-wide file plan and subject to the above rules for their subsequent organisation and management.

ANNEX 2: Note to Management Committee: Document and Records Management Policy; 24 February 2006; SG-JU/AG C&I/I&IC/2006-213/AM/abb



Luxembourg, 24 February 2006
SG-JU/AG C&I/I&IC/2006-213/AM/abb

Note to the Management Committee

E van der Elst / A Murdock

Subject: Document and Records Management Policy

1. Purpose of Note

The Management Committee is requested to approve a Document and Records Management Policy which contributes to the Banks' recent commitments to *Personal Data Protection*, *Public Disclosure* and *Financial regulatory compliance* by demonstrating management control over its documents and records

Objective of Policy

The objective of this Policy is to provide a set of common principles to ensure the reliability of the Bank's documents and records as evidence of the Bank's business activities. Policy principles will be adapted to new and existing EIB Policies and Procedures and can be applied to e-mail, documents, databases and other record-keeping systems. After consultation with Directorates, several Procedures have been identified for priority action following approval of this Policy (see Implementation below)

2. Background

Records Management and Corporate Governance

As a consequence of several notable corporate scandals in Europe and USA, records management is now viewed as an effective tool within corporate governance to manage institutional record-keeping obligations and comply with personal data protection and financial reporting requirements. Other IFI's, such as the World Bank, have adopted Records Management programs, with supporting tools, to strengthen their good governance initiatives in developing countries¹. The Management Committee should also take note of the developments in this field made by the European Institutions².

Records as evidence of business activities

Records can be regarded as reliable evidence of business activities if they are proven to be authentic, reliable and usable³. The ease with which electronic documents can be created, sent and manipulated presents an added complication to their evidential value. This is a particular problem for the management and storage of e-mail which now forms part of many key business activities and decisions and which is a principal communication tool with the Bank's stakeholders and counterparties. This Policy proposes a set of common principles for the management of documents

¹ See <http://www.irmt.org> in relation to the anti-fraud and anti-corruption objectives in Corporate Social Responsibility Statement

² Commission Decision of 23 January 2002 (2002/47/EC, ESC, Euratom) 'rules of procedure for document management' ; Règlement (CE) 1049/2001 du Parlement Européen et du conseil du 22/09/2003 relatif à l'accès du public aux documents de PE, du Conseil et de la Commission ; Commission Decision (2001/844/EC, ECSC, Euratom) 'Commission Provisions on Security' relevant to Confidentiality, Classification, electronic records and archives ; Commission Decision (2004/563/EC, Euratom) 'provisions on electronic and digitised documents'

³ ISO 15489 Information and documentation- Records Management

and e-mails as records, which can be regarded as reliable evidence of the Banks' business activities. On this basis the Bank's documents and records can be used in support of its public commitments to good governance and financial accountability.

Integrated Document and Records Management

Several recent Audit Reports have highlighted the absence of key business documents from the Bank's record collections, making the identification of key business records difficult. In practice, many of the Bank's key business records are held in both paper and electronic repositories with no single collection being a complete record of the Bank's business activities. This Policy proposes an integrated approach to document and records management, to ensure that the Bank's files are complete and reliable evidence of its business activities regardless of their location or format in which they are held.

3. Policy Principles

The proposed Policy is based upon a set of common principles:

- Documents received, created, approved, and distributed will be organised and managed according to rules established within existing policies and procedures⁴
- Documents will be 'captured as records' in repositories which associate records with an enterprise-wide file plan
- Documents will be 'captured as records' in their original format, except for legal or business continuity purposes
- Document and Records will be classified and de-classified according to the confidentiality rules in force
- The retention and destruction of records will be regulated under the Bank's retention schedule
- Records will be preserved and conserved in appropriate formats and storage conditions for the duration of their retention period

4. Implementation

Following approval of the proposed Document and Records Management Policy, in consultation with the Directorates concerned, notably JU and OCCO, SG-JU will initiate the development of rules and procedures incorporating the above record-keeping principles, including:

- *Records Retention Schedule*; to include rules and procedures for document retention and destruction; for Management Committee approval 4Q 2006
- *Rules on management and use of e-mail*; to include record-keeping rules for the management of e-mail systems, and use of e-mail within the Bank; for approval 4Q 2006
- *Confidentiality rules*; to include record-keeping rules for safeguarding the confidentiality of the Banks counterparties ; for approval 2007

5. Budgetary Impact and opinion of the Management Controller

Any costs associated with the amendment of procedures or application of these principles to future or legacy record-keeping systems will be subject - within the present budget framework - to justification made through existing budgetary procedures and business cases made at the request of responsible Departments and Services. The Management Controller has no particular comments at this stage.

Request for Decision

The Management Committee is requested to:

- a) approve the attached Document and Records Management Policy; and
- b) mandate SG-JU to initiate, in consultation with the Directorates concerned, notably JU and OCCO, the development of rules and procedures aimed at enforcing the approved policy.

⁴ Existing Policies for the management of the Bank's documents and records can be found in *Staff Regulations, Staff Code of Conduct, Rules of Procedure, and Code of Good Administrative Behaviour*. Policies for the organisation and management of documents and records can also be found in the Bank's *Disclosure Policy* and rules on *Personal Data Protection*. Existing Procedures for the management of the Bank's documents and records, including e-mail and confidentiality, can be found in *General Office Procedures Manual* and *Departmental Procedures Manuals*.

Copy: All Directorates
Attachment: Document and Records Management Policy

Document and Records Management Policy

Whereas

All of the Bank's activities and decisions ultimately lead to the production of documents

Documents and records are a strategic information resource and are the basis of institutional memory

Efficient document management is an essential prerequisite for an effective policy of public access, good governance and financial accountability

This Policy is made with due regard for existing EIB Policies and Procedures on document creation approval, distribution, confidentiality and e-mail

Article 1

Purpose

The establishment of standard rules and actions for the organisation and management of the Bank's documents and records to ensure their reliability as evidence of the Bank's business activities.

Article 2

Scope

All records which are drawn-up or received by the EIB concerning a matter relating to the policies, activities and decisions falling within its competence and in the framework of its official tasks, regardless of their format or physical location

This Policy is relevant to the actions required for the organisation and management of documents and records throughout their life-cycle, including document capture, organisation, access, storage, retention, and preservation.

Article 3

Definitions

For the purposes of this Policy, 'document' is understood to mean any document which is drawn-up or received by the EIB concerning a matter relating to the policies, activities and decisions falling within its competence and in the framework of its official tasks, in any medium

For the purposes of this Policy, 'record' is understood to mean any document, or communication (e-mail phone, fax, photo, video) which commits the organisation or individual to an action, renders the organisation or individual accountable, or which documents an action, a decision or decision-making process.

Article 4

The Organisation and Management of Documents and Records

4.1 Document Management

4.1.1 Rules for the organisation and management of documents within departments will be subject to Procedures in place within the relevant department with a view to determining if documents must be captured as records.

4.2 The capture of documents as records

4.2.1 Documents should be captured as records in their original format when they commit the organisation or individual to an action, renders the organisation or individual accountable, or which documents an action, a decision or decision-making process

4.2.2 Documents, or files will be *captured as records*, with the addition of metadata describing the administrative and informational value of the document or file

4.2.3 Documents, or files *captured as records*, shall be attached to an enterprise-wide file plan, available by computer and based upon a common nomenclature which defines the Bank's activity-based functions

4.2.4 Documents or files captured as records and relevant to the same activity, regardless of their format or physical location, shall be linked through the application of relevant classification and metadata.

4.3 Access

4.3.1 Documents captured as records will be made easily identifiable and retrievable, regardless of their format or storage location through the application of relevant metadata describing their information value

4.3.2 Documents captured as records will be protected against unauthorized addition, deletion, alteration, use and concealment

4.3.3 An auditable trail will be maintained for all record transactions

4.3.4 Rules in force on Confidentiality and Personal Data Protection will be uniformly applied to documents and records held in paper and electronic format to ensure that they are applied for specified periods and removed when warranted.

4.4 Storage

4.4.1 Documents and records, in any medium, must be secure from unauthorised access and physical damage arising from daily use, system failure or breakdown, water or fire.

4.5 Retention

4.5.1 The retention and disposition - ie, destruction or transfer to historical archives -- of documents and records will take into account operational requirements and respect all relevant legal or regulatory record-keeping obligations as detailed in the EIB Records Retention Schedule

4.5.2 The retention and disposition of records shall be applied uniformly to records held in paper and electronic format

4.5.3 The destruction of records will be carried out in confidentiality and render the records unrecoverable.

4.6 Preservation

4.6.1 Documents and records will normally be held in the form in which they were drawn up, approved, sent, or received with certified or true copies retained for legal or Business Continuity Planning purposes only

4.6.2 Long-term access to the Bank's records will be preserved through appropriate conservation and preservation measures including their conversion or migration to other formats.

Article 5

Rules specific to the management of other digital records

5.1 E-Mail

5.1.1 Any e-mail which commits the organisation or individual to an action, renders the organisation or individual accountable, or which documents an action, a decision or decision-making process must be captured as a record

5.1.2 E-Mail captured as records must be retained in their original format preserving the link between the e-mail message and its attachments or in a form, which preserves the integrity of the message content and relevant metadata

5.1.3 E-mail captured as records will be subject to the above rules for their subsequent organisation and management.

5.2 Scanning

5.2.1 The scanning of documents shall provide identifiable benefits to the organisation through enhanced workflows or processes, or improved access to document collections

5.2.2 Scanned documents will be captured as records when attached to an enterprise-wide file plan and subject to the above rules for their subsequent organisation and management

5.2.3 Scanned documents will be captured as records i

RECORD of Processing of Personal Data

regarding

Dignity at Work Policy
Submitted by Controller

*(in accordance with Article 31 of Regulation (EU) 2018/1725 of 23rd October 2018
on the protection of individuals with regard to the processing of personal data)*

a) i) Controller/organisational parts responsible for the processing:
European Investment Bank/CS-PERS/HRS&G - Pascale Hecker, Head of Employee Relations and Wellbeing Division

ii) Processor:

In exceptional circumstances, and only for specific cases, the Dignity at Work Secretariat may be outsourced to an external legal consultant.

iii) Name of DPO to whom this record is sent:

Pelopidas Donos

b) Purpose(s) of the processing:

The purpose of the processing is to implement the Dignity at Work Policy¹. This Policy sets out the appropriate procedures dealing with all forms of harassment in the workplace. Harassment may take the form of psychological harassment and/or sexual harassment.

The Policy establishes the following procedures for which personal data is processed:

- Preliminary steps - a network of Confidential Counsellors² or Occupational Psychologists is offered;
- Mediation Procedure - a procedure involving an independent and impartial third party, the mediator, and aiming to resolve cases of alleged Harassment informally³;
- Formal Procedure - a formal procedure of inquiry, involving a comprehensive fact-finding exercise and, where necessary, the adoption of appropriate measures⁴.

c) i) Category(ies) of data subjects concerned:

As per Article 1.3. of the Dignity at Work Policy:

1. members of the EIB Management Committee;
2. persons whose relations with the EIB are governed by individual contracts under Article 14 of the Staff Regulations, regardless of their place of assignment;

¹ [Dignity at Work Policy](#)

² [Dignity at Work policy - Selection of Confidential Counsellors Data Protection record](#)

³ For the full definition, please refer to art. 2.1. of the Policy

⁴ For the full definition, please refer to art. 2.1. of the Policy

3. persons working at the EIB on secondment from their parent administration;
4. persons working at the EIB under the traineeship program;
5. persons working at the EIB as students on summer jobs;
6. persons hired by the EIB to work in an external office and employed under local legislation.
7. persons not directly employed by the EIB, such as temporary staff, consultants and other service providers, shall be covered by the Policy only as Alleged Victim⁵.
8. persons who worked for the EIB Group and left service, for acts committed during employment with the EIB or for a professional activity related to the EIB even after having left service - only the Formal Procedure⁶ is applicable to that category of data subjects.

ii) Categories of personal data:

Data collected and exchanged in the course of the Preliminary steps:

- personal data on the data subjects (Accused Person and/or Alleged Victim) collected in the context of the Preliminary steps - the name and division of the Alleged Victim and of the Accused Person

Data collected and exchanged in the course of the Mediation Procedure:

- personal data on the data subjects (Accused Person and/or Alleged Victim) collected in the context of the Mediation Procedure - the name and division of the Alleged Victim and of the Accused Person; data shared during the Mediation by the Alleged Victim and the Accused Person;

Data collected and exchanged in the course of the Formal Procedure:

- the name and position of the Alleged Victim and of the Accused Person
- personal data on the data subjects (Accused Person and/or Alleged Victim) related to the factual background of the alleged Harassment, namely the relevant events, situations and/or incidents, including their dates, places, reactions and effects
- personal data on the data subjects (Accused Person and/or Alleged Victim) related to the documented outcome of the Mediation Procedure (if any) personal data on the witnesses that will support the Alleged Victim's complaint - i.e. their names and a brief explanation on why those persons can help establishing the facts as well as personal data from the witnesses (if applicable)
- any other relevant personal data on the data subjects (Accused Person and/or Alleged Victim) that might be contained in a supporting document or evidence

⁵ Alleged Victim - a Person working for the EIB Group, as defined below, who considers himself/herself to have been or to still be subject to Harassment by another Person working for the EIB Group (as per art. 1.2. of the Dignity at Work Policy)

⁶ Formal Procedure - a formal procedure of inquiry, involving a comprehensive fact-finding exercise and, where necessary, the adoption of appropriate measures (as per art. 2.1. of the Dignity at Work Policy)

- personal data on the data subjects (Accused Person and/or Alleged Victim) contained in the final report issued by the Dignity at Work Panel describing the findings of the Inquiry and concluding whether or not the denounced facts qualify as Harassment for the purpose of the Policy.

Personal data on the data subject, which may include special categories of data within the meaning of Article 10.1 of Reg. (EU) 2018/1725, processed lawfully according to Article 5 of this Regulation. The Dignity at Work Panel may use personal data for the sole purpose of establishing the facts leading to their recommendation.

iii) Categories of processing carried out on behalf of each Controller (only to be filled in by the Processor):

N/A

d) Recipients or categories of recipient to which the data might be disclosed, including recipients in Member States, third countries or international organisations:

- Mediators appointed by DG Personnel;
- Confidential Counsellors (as described by Confidential Counsellors notification);
- Occupational Psychologists;
- Dignity at Work Secretariat – authorized staff that is part of the Personnel Directorate for the EIB to ensure the administration of the Formal Procedure related to the Dignity at Work Policy;
- authorized staff that is part of the Personnel Directorate ensuring the administrative follow up of the Mediation Procedure;
- Members of the Dignity at Work Panel as appointed by DG Personnel;
- DG Personnel;
- EIB President and staff authorized by him;
- Authorized staff within the EIB Office of the Chief Compliance Officer (OCCO) in case of potential conflict of interest cases;
- Authorized staff within the EIB Inspectorate General in case of investigation;
- Authorized staff within another EIB Directorate in case Personnel is considered as conflicted to handle a Dignity at Work complaint;
- the parties involved – i.e. the Alleged Victim, the Accused Person and Witnesses.

e) Transfers to third country(ies) or international organization(s), including the identification of the third countries or international organisations, and the documentation of suitable safeguards:

May only be authorised if required by a court order/request from by the national competent authorities.

f) Time limits/storage deadlines for erasure of the different categories of data:

Preliminary assessment not leading to the launching of an ex officio Formal Procedure (Article 9.4 of the Policy)

Two years, from the adoption of the decision that no Formal Procedure will be launched *ex officio*, for all documents and personal data collected during the preliminary assessment carried out by DGP in case s/he becomes aware of serious allegations of Harassment.

Mediation Procedure (Article 19.1 of the Policy)

Three years, commencing on the day of the conclusion of the Mediation Procedure, for all documents retained as part of the Mediation Procedure by the Mediator and Personnel. The documents will be stored in a special electronic or paper folder clearly marked as strictly confidential. At the expiry of the retention period, all relevant data must be destroyed.

Formal Procedure (Article 35 of the Policy)

All documents, including the Complaint or the Note and any relevant supporting documents or evidence, submissions by the Accused Person and any relevant supporting documents or evidence, the Final Report and electronic communications of the Dignity at Work Secretariat with the Alleged Victim and/or the Accused Person pertaining to the Formal Procedure up to and including the Final Decision will be kept in a special file marked strictly confidential with strictly limited access within the EIB Personnel Directorate for a period of five years from the day on which the parties are informed in writing of the Final Decision. They may be stored for periods longer than five years after conclusion of the case, if relevant to judicial procedures or other inquiries.

Hearings (Article 30 of the Policy)

The hearings may be recorded by audio means, provided that all participants to the hearing in question have been previously informed. The recordings shall be made available to the Panel Members for the purpose of enabling them to conclude their assessment.

The recordings shall be kept for a period of six months after the delivery of the Dignity at Work Panel's recommendation to the EIB President, in a special file marked "strictly confidential" and with strictly limited access in the electronic document management system within the EIB Personnel Directorate. The recordings will be destroyed following the expiry of the retention period. Longer retention periods could be applied in exceptional and duly justified cases, subject to agreement of the DPO.

Where one of the parties so requests, a copy of the recording of their individual hearing shall be provided to them.

Investigations (Article 31 of the Policy)

The electronic files, telecommunication electronic traffic data and recorded data collected during the investigation and relevant to the needs of the Inquiry can be kept by the Dignity at Work Panel for a maximum retention period of six months from the Final Decision. They may be stored for periods longer than six months after conclusion of the case, if relevant to judicial procedures or other inquiries. This would include where files are transferred to other competent authorities or bodies for determination. In such instances, the DPO will be informed accordingly. After the Final Decision is communicated to the parties, the parties may have access to their personal data collected during the investigation in line with the applicable rules adopted by the competent service, in case any restrictions laid

down in the Internal Rules were applied.

Personal File (Article 34 of the Policy)

- A copy (paper and/or electronic) of the decision dismissing a Complaint as inadmissible shall be placed in the personal file of the Alleged Victim.

- A copy (paper and/or electronic) of the Final Decision, along with the Final Report, shall be placed in the personal file of the Alleged Victim and the Accused Person. If the Final Decision concludes that no Harassment was found, the Accused Person may request that it is not placed in or removed from his/her Personal file. .

- The retention period for the documents placed in the personal file of the staff members is 3 years after staff member's departure from the Bank.

g) General description of the technical and organizational security measures referred to in Article 33:

Organizational measures

All persons involved in the Procedures must comply with Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

All data collected and exchanged in the course of the Procedures shall be adequate, kept secured and confidential, processed only for the purposes related to the implementation of the Policy, not transferred to unauthorised third parties and not kept for longer than necessary.

All information and documentation is treated as strictly confidential and access is limited to a minimum number of persons as described in point d).

Mediators involved in the Mediation will sign confidentiality agreements.

Occupational Psychologists are bound by medical secrecy.

All discussions with the Confidential Counsellors and the Occupational Psychologists are confidential and no record shall be kept of those.

Technical measures

EIB:

Electronic files are stored in a secured dedicated GED area only accessible to the recipients specified under point d).

The paper documents are stored in cabinets that remain locked at all times. Only the recipients specified under point d) have a key for them.

Dignity At Work Panel:

The contracts between the EIB and the Dignity At Work Panel members obliges the latter to store any documentation or information that is provided to them in a secure manner.

h) Legal basis of the processing for which the data is intended:

Staff Regulations

Code of Conduct

Management Committee decision of 5 March 2019 approving the Dignity at Work Policy.

EIB Decision of 26 February 2019 laying down internal rules concerning the processing of personal data by the Personnel Directorate of the European Investment Bank in relation to the provision of information to data subjects and the restriction of certain of their rights pursuant to Article 25 of Regulation 2018/1725

Dignity At Work Policy

Article 5(1)(a) of Regulation 2018/1725

i) Information to be given to data subjects:

All data subjects as described in point c) above have access to (or will be provided with) the Dignity at work Policy as well as the related Privacy Notice and the Internal rules concerning the processing of personal data by the Personnel Directorate of the European Investment Bank in relation to the provision of information to data subjects and the restriction of certain of their rights.

j) Procedures to grant rights to data subjects:

Upon the establishment of a Dignity at Work Panel, the Dignity at Work Secretariat shall provide the Accused Person with a copy of the Complaint or of the Note (excluding the elements of the Complaint or the Note that have been considered as “confidential”).

The Dignity at Work Secretariat shall send a copy of the Accused Person’s submission to the Alleged Victim, without the documents that the Dignity at Work Secretariat has marked as “confidential” if any, and without the names of the persons proposed as witnesses, if any.

In case of a Formal Procedure initiated by the Director General of Personnel, as described in Article 23.2 of the Policy, the Dignity at Work Secretariat shall provide the Alleged Victim with the Note and with the documents they intend to share with the Accused Person.

The Note prepared by the Dignity at Work Secretariat will be transmitted to the Accused Person in its entirety subject to the exceptions provided for in Article 23.2 of the Policy.

A copy (paper and/or electronic) of the Final Decision shall be placed in the personal file of the Alleged Victim and the Accused Person. Data subjects may consult their own personal files.

Data subjects can exercise their rights by contacting the Data Controller.

Regarding the right of access - for those elements that will be considered as “confidential”), their access can be restricted in accordance with the restrictions laid down in the Internal Rules.

k) Automated/manual processing operation:

Manual

l) Any further necessary information:

N/A

m) Is this processing operation subject to a Data Protection Impact Assessment (DPIA) under Article 39? (sensitive data as defined by Art. 10, large scale processing operations, new technologies etc.....)

Yes

Date:

Signed:

Controller:

