

Category		Title of the processing	Controller EIF / EIB	Processor	Purpose(s) of the processing	Category of Data subjects	Category of data	Legal basis	Recipients	Retention Period	Transfer to third countries or	Technical & Organizational Security Measures
	1.1.1	External Recruitment of Staff	HR	EIF	Collection, registry, maintenance, transfer and assessment of personal data for the purpose of filling staff vacancies in EIF	Candidates for externally published EIF vacancies	Name etc, CV, information on family members, general data on professional competencies etc	EIF Statutes and Staff Regulations Service Level Agreement EIF - EIB	EIF HR Staff EIB HR Staff Chief Executive and Deputy Chief Executive Members of Selection Panel Requesters	*Electronic application: indefinitely (for statistical and resource planning purposes) *Application after first selection: 2 years *Psychological tests: 18 months	n/a	Access to applicants' personal data is restricted exclusively to HR Staff, requesters and members of the selection panel IT access to applicants' personal data restricted to HR Staff Personal data communicated outside HR for recruitment purposes is destroyed immediately following the closure of the selection process
	1.1.2	Recruitment of EIF non-agents	HR	EIF	Collection, registry, maintenance, transfer and assessment of personal data for the purpose of selection and hire of non-employees (interim staff, trainees, summer students, staff seconded from other organisations) Meeting temporary staff needs, acquiring expert know-how, providing a "first hands-on" experience to young students or graduates participating in specific projects and initiatives	interim staff, trainees, students for summer jobs, secondees	Name etc, CVs and similar data	EIF Statutes, Staff Rules and Staff Regulations HR Manual of Procedures SLA EIF - EIB EIB guidelines for in-house training, Luxembourg law (for interim staff)	EIF HR Staff EIB HR Staff Chief Executive and Deputy Chief Executive Requesters	Data is retained for the periods indicated below following departure: *Trainees: (paper files) three years (for reasons of establishing working certificates): indefinite for statistical purposes in PeopleSoft *Secondees: three years following the end of secondment - indefinite for statistical purposes in PeopleSoft *Summer students: (paper files) three years	n/a	Access to applicants' personal data is restricted exclusively to HR Staff, requesters and interviewers during selection process. IT access to applicants' personal data restricted to HR Staff Personal data communicated outside HR for recruitment purposes is destroyed immediately following the closure of the selection process
	1.1.3	Recruitment of Interim Staff	HR	TAPFIN sub-processor: Beeline	To manage the provision of temporary staff to replace absent staff (support and professional) or to meet short-term requirements for additional staff (support and professional) at the EIF headquarters in Luxembourg.	All temporary interim staff Hiring managers and EIF HR staff within the hiring team	All candidates for interim positions 20-Oct-20 - Curriculum vitae (that contains only name and surname). Purpose: To identify the most suitable interim staff via Beeline. 2) Selected interim staff - "Le contrat de mise à disposition" with the interim agency (name, surname, address, social security number, monthly salary rate and coefficient of the agency) and confidentiality clause : hard copy only - Signed timesheets (that contain name and surname of the interim staff and of the hiring manager). Purpose: to be verified before sending to the interim agencies for salary and invoicing purposes 3) Hiring managers and/or HR Staff Last name, first name, department, role in Beeline Client satisfaction surveys carried out by the Data Processor: Name, surname, department, role. The survey may also contain the name and surname of candidates or selected interim staff.	Art. 21.5 of EIF Statute	The data is treated and kept within Beeline and PeopleSoft HR. The Data Processor is also the recipient of the data. 1) Curriculum vitae: EIF HR Staff dedicated to the administration of interim staff, Data Processor's staff (on & off-site via Beeline), interim agencies' staff, EIF hiring managers and their personal assistants, recruitment panel members. 2) "Contrat de mise à disposition": EIF HR Staff dedicated to the administration of interim staff, the Data Processor's staff on-site, interim agencies' staff and dedicated EIF Procurement Staff member. 3) Signed timesheets: EIF HR Staff dedicated to the administration of interim staff, the Data Processor's staff on-site, interim agencies' staff, EIF hiring managers. 4) Satisfaction surveys: EIF HR Staff dedicated to the administration of interim staff, Data Processor's staff on and off-site The Data Processor is bound by confidentiality and data protection clauses, as outlined in the Data Protection Agreement signed with the EIF. The interim agencies are bound by confidentiality and data protection clauses imposed by local legislation	Personal data of all candidates (selected and non-selected): 3 years in Beeline and GED Paper documents related to the interim staff recruitment campaign are destroyed at the end of the selection process. "Contrats de mise à disposition" and confidentiality clause: 5 years (hard copies), originals are kept under lock, accessible only to the EIF HR Staff dedicated to the administration of interim staff and to the Data Processor's staff on-site. 20-Oct-20 Signed timesheets (hard copies) are destroyed within 6 months of the submission date. They are kept under lock, accessible only to the EIF HR Staff dedicated to the administration of interim staff and to the Data Processor's staff on-site. On-line client satisfaction survey reports are deleted after 3 years (no hard copies).	The Data Processor and each of its affiliates have entered into an Intragroup Agreement for the processing of personal information outside the EEA, which includes the Model Contractual clauses of the Commission. ManpowerGroup Solution teams servicing EIF off-site are located in Brussels and Woluwe (Belgium). While the data will be stored in Beeline European data centers in Switzerland, Beeline Support teams servicing EIB (located in London (UK), Manila (Philippines) and Jacksonville (USA)) have access to the data.	The consultant employed by the Data Processor on-site will have a restricted access to PSFT HR module and EIF applications. The Data Processor warrants that it has implemented technical and organisational security measures, which are intended to protect Personal Data from unauthorised and/or unintended access, modification and/or deletion and which represent the state of the art for processing Personal Data within and outside the EEA.
	1.1.4	GRAD Programme	HR	EIF	Collect, analyse and process applications for the EIF GRAD Programme, as part of the EIF e-recruitment process. The GRAD Programme aims to offer new and recently qualified graduates the opportunity to acquire professional experience.	Applicants to the EIF GRAD Programme	During the online application process the candidate will upload the following personal data: <input type="checkbox"/> Personal data: name, first name, date and place of birth, nationality and second nationality (if applicable), gender, contact details (telephone, email, address) in order to identify and contact applicants. <input type="checkbox"/> Qualifications: secondary school education, higher education, professional qualifications in order to check eligibility to apply for the GRAD Programme and to select profile sought by the hiring department/team. <input type="checkbox"/> Statement of motivation in order to evaluate the reason for the application Shortlisted candidates are required to undertake an online assessment that includes numerical and verbal reasoning as well as completion of an Occupational Personality Questionnaire. Shortlisted candidate(s) invited for in-house interviews, will complete an application form providing the following additional personal data: <input type="checkbox"/> Civil status including the following information: Name of dependents (spouse/registered partner and any children), relationship, and date of birth, in order to establish allowances and benefits. <input type="checkbox"/> Dependents' current occupation and employer name (where relevant) In the application form the candidate is requested to declare: gross annual salary, net annual salary, last net bonus and required notice period (where applicable). For selected candidates: medical questionnaire to be submitted directly to the EIB Occupational Health Services	Art. 21.5 of EIF Statute	In addition to the EIF H&RM team, the EIF colleagues/managers participating in the selection process	Storage: candidate data is stored for three years (unless candidate deletes the application before) and during that time candidates may access their application to rectify, add or delete information. Applicants may also send an email to the H&RM Recruiter requesting the withdrawal of an application. Erasure of applications: after three years Professional tests and online assessments: three years after entry into service Medical tests: held by the Occupational Health Services of the EIB Group, according to their retention rules established for medical questionnaires during the standard recruitment process.	n/a	Candidates apply online through the common EIB Group website (EIB Group Careers Portal) through a secured connection (https environment) where a detailed description of the GRAD Programme is posted, including information regarding the terms and conditions (http://www.eif.org/jobs/grad/index.htm). Lists of candidates resulting from the download of applications will be retained by the hiring department/team only during the recruitment process and destroyed upon completion of the selection process (at the latest within 30 days of completion). Same 30-Sep-20 approach is applied for the professional test.
	1.1.5	Recruitment of Trainees	HR	EIF	Recruitment of trainees as part of the EIF internship programme	Candidates applying for EIF internship programme and selected candidates	During online application: : • name, first name, date and place of birth, nationality (ies), gender, contact details - Qualifications For selected candidates: • traineeship contract, copy of the passport, copy of the last diploma, medical certificate (fit to work), proof of Health insurance, contact details (in case of emergency), certificate of residency, extract of police certificate of character, bank account details	Art. 21.5 of EIF Statute	In addition to the EIF HR team, the EIF colleagues/managers participating in the selection process.	Storage: two years (unless candidate deletes the application before)	n/a	Candidates apply online through the common EIB Group website (Candidate Gateway) through a secured connection

Category		Title of the processing	Controller EIF / EIB	Processor	Purpose(s) of the processing	Category of Data subjects	Category of data	Legal basis	Recipients	Retention Period	Transfer to third countries or	Technical & Organizational Security Measures
	1.1.6	Recruitment Panels (Constitution of Panels)	HR	EIF	Recruitment panels are convened for the interview/selection process for management staff vacancies (i.e. for posts graded "C/6" (Head of Division) and above. The process may be applied also to other sensitive or strategic positions or positions requiring staff management. Panels are composed of 5 senior voting members (at the level of Head of Department or Head of Division), one of whom is a senior HR manager, and one observer representing COPEC. The Chairperson of the panel usually represents the hiring department. The 5 voting members have equal voting rights. It is recommended that the panel composition is as diverse as possible in terms of different departments, nationality and gender (at least one female voting member). It is	Internal and external candidates	<p>The application form, and CV of external candidates, are circulated to the panel members. The application form contains the following data:</p> <ul style="list-style-type: none"> • Personal data: first name, date and place of birth, nationality (and second nationality if applicable), gender, contact details (telephone, email, address) • Qualifications: higher education and professional qualifications • Professional experience: current and former employers, date of employment, description of key responsibilities <p>The recruitment panel members take notes on the individual candidates and complete a scoring sheet which is returned to EIF HR.</p>	<ul style="list-style-type: none"> • Compliance with EIF Statutes, Staff Rules and Staff Regulations, EIF HR Manual of Procedures, EIB Group "Guidelines on Internal Mobility and Promotions". • Public interest 	EIF HR and the recruitment panel members. The Chief Executive and Deputy Chief Executive, who may be asked to attend the Panel as observers.	<p>EIF HR ask the panel members to return any CVs/application form once the panels have taken place and the scoring sheets have been completed.</p> <p>In terms of the candidates other documentation, the retention is as follows:</p> <ul style="list-style-type: none"> • Motivation letters of candidates are kept in PeopleSoft for the entire period of employment of the applicants. • External candidates: on-line data is retained indefinitely for statistical purposes. • Personality tests: 18 months • Candidates' electronic profile : 3 years from application date for each application • Statistical data (such as number/nationality/gender split of applications per recruitment campaign) are retained indefinitely. 	n/a	<p>The panel members are bound by the utmost confidentiality regarding any information or data shared during the recruitment panel process. Panel members are given a letter reminding them of their obligation to destroy or return all personal data to EIF HR once the recruitment process is complete.</p> <p>IT access to applicants' personal data is restricted to HR Staff, the panel members do not have access to the HR IT system.</p> <p>Personal data communicated outside HR for recruitment purposes is destroyed immediately following the closure of the selection process</p>

Category		Title of the processing	Controller EIF / EIB	Processor	Purpose(s) of the processing	Category of Data subjects	Category of data	Legal basis	Recipients	Retention Period	Transfer to third countries or	Technical & Organizational Security Measures
1.2 - Human Resources - Evaluation and Career	1.2.1	Recruitment Probation Periods in SuccessFactors	HR	SAP Luxembourg S.A., Branch of SAP Belgium S.A.	The purpose of the probation document is to set evaluation criteria, track progress and evaluate the staff member's performance during the probation period. Probation documents are managed online via the SuccessFactors application	All new EIF recruits subject to a probationary period, as stipulated in their letter of appointment	Individual online probation documents, with the following sections: <ul style="list-style-type: none"> o Staff Member Information <ul style="list-style-type: none"> • First name • Last name • Middle name • Job Title (Generic Role title) • Functional level • Staff Category (Support/Executive/Management/Senior Management) • Name of manager o Organisational information <ul style="list-style-type: none"> <input type="checkbox"/> Company (EIF) <input type="checkbox"/> Directorate <input type="checkbox"/> Department <input type="checkbox"/> Division <input type="checkbox"/> Unit <input type="checkbox"/> Location o Objectives o Competencies At the beginning, middle and end of the process, the manager will document the progress in the relevant section of the document. At mid-probation the manager confirms whether the staff member 22 July 2020 is on-track. At the end of probation evaluation section, the manager documents the performance assessment, discussion and final probation decision (manager and manager's manager) to which the staff member may add his comments.	The rules and procedures governing Probationary Periods (Annex IX of Staff Rules)	At the EIF (controller): Online access to the staff member on probation and his hierarchy, the Chief Executive of the EIF and his assistant, Heads of Department and their assistants (if delegated), and EIF HR staff (list of staff who require access, authorised by the Head of Human & Resources Management of EIF). The data may also be disclosed when required to EIB Personnel staff for analytical reasons, to the EIB Legal Services if called upon to defend the EIB Group. At SAP (processor): SAP employees managing the SuccessFactors application and data requiring access for technical reasons (cf. notification "SuccessFactors Talent Management software"), under SAP confidential rules and rights of access agreed with the EIB Group.	Probation documents are stored electronically and may be printed if required. After decision by the Head of Human and Resources Management of EIF regarding the confirmation, extension, or non-confirmation of the probationary period, the probation document is automatically locked. Time limit to block, rectify and erase is 10 working days. EIF HR staff (according to the list indicated in section "e" above) will have access to all probation documents of all staff throughout their careers. Staff members have access to their probation document in SuccessFactors throughout their active service in the EIB Group. Staff member's managers have access to the probation document in SuccessFactors as long as the staff member is assigned to the manager and Department. When a staff member is	n/a	Online access granted only to staff on probationary period, their current hierarchy, and authorised EIF HR and EIB Personnel staff members
	1.2.2	EIF Appraisal Process	HR	EIF	Evaluate the performance of EIF staff members in relation to their annual objectives. HR coordinates the exercise to ensure that it runs smoothly.	All EIF Staff with either a fixed-term ("CDD") or indefinite ("CDI") employment contract	Electronic evaluation forms, which include various categories relating to responsibilities, objectives, competences and development; correspondence between Staff and different departments; notes and e-mails on salary adjustments and Performance Award	Article 22 of the EIF Staff Regulations EIF Performance Evaluation Guidelines	EIF HR, Chief Executive, Deputy Chief Executive, Line Manager	Performance documents are kept electronically and in paper form in HR for a period not exceeding three years following the termination of a particular appraisal procedure.	n/a	Confidential hard copy documents and electronic hardware media are double-locked, only accessible to authorised members of HR. Individual electronic data is password protected and accessible only to Staff concerned, their superior(s) and any person referred to above and registered with HR. Internal files/documents used during the Performance Evaluation exercise is password protected when containing personal salary-related data
Resources - Leave Management	1.3.1	EIF Salaries and Pension	HR	EIF	Process all the elements related to Salary and Pension. The aim of the processing is to meet all the financial obligations as laid down by contracts, rules and policies with an impact on salary and pension	EIF Staff members, pensioners and their dependents, Chief Executive and Deputy Chief Executive and their dependents	Identification data, Professional data, Pension data, Dependents data	EIF Staff Rules and EIF Staff Regulations, Council Regulation no. 260/68 of 19 February 1968 on Community taxes, as amended from time to time, Decision of the EIF Board of Directors on the remuneration of the Chief Executive/Deputy Chief Executive	Staff working on Personnel/Operations. Certain personal salary and/or pension are disclosed upon specific instructions in the form of a court order or decision. Personal salary and pension data are disclosed to the EIB's actuary in order to carry out actuarial calculations	Data on salaries and pension rights is available on-line until 8 years following the expiration of the respective rights for the EIF Staff member and all his/her dependants. Data is destroyed at latest 120 years after the birth of the EIF Staff member concerned. Rights for the blocking and erasure of personal data within 60 days following the respective claim	Data relating to salaries and pension may be transferred to third countries or international organisations in the context of secondments. The EIF Staff member concerned will receive a copy of the secondment agreement with such third country or organisation	Access to Salaries and Pensions data in the application Global Payroll within PeopleSoft (PSFT) and data within the database within PSFT HRMS (PeopleSoft Human Resources Management System) are subject to a password. The scope of the access to Salaries and Pensions data in the application Global Payroll within PeopleSoft (PSFT) and data within the database within PSFT HRMS (PeopleSoft Human Resources Management System) is attributed as restrictively as possible
	1.3.2	Absence and Time Management	HR with EIB Personnel & Medical Services	DSK	To allow EIF staff members to register their working hours, overtime, sickness without certificate and to request leave (annual leave, special leave, flexi leave, parental leave). For external agents (consultants, temporary agents and subcontractors) and agents seconded to the EIF group the Absence and Time Management tool does not include any calculation for leave entitlements, it simply provides access to the clocking function to provide an overview of time spent in the office for information purposes only. Trainees also have access to the time registration tool (time events are limited to external meetings and away days). To allow EIF managers to review the presence and absence of staff members and to validate requests for leave (annual leave, flexi leave and parental leave).	All EIF staff members and trainees, with the exception of subcontractors. Some nonemployees (secondees and temporary agents) use the system to provide an overview of presence only, without the calculations for leave and time	Personal data in TIM: First Name, Last Name, Badge number, Staff ID number, birth date, gender, contract start date, working regime (full-time/part-time), profile code category (clocker or non-clocker). Time event data visible in TIM and Peoplesoft Absence & Time Management <input type="checkbox"/> Calculation of hours worked based on staff registration of entry and departure times in and out of the workplace by swiping their id badge ("clocking in" and "clocking out") at the clocking machines situated at the entry and exit points of the EIF and EIB premises. <input type="checkbox"/> Registration of staff members' absences for leave, flexi time, business travel, training, sickness without certificate, away days, working time outside premises (telework), external meetings. These absences are registered by the staff members. <input type="checkbox"/> Staff member's requests for parental leave. <input type="checkbox"/> Registration of automatic and manual requests from staff members (unpaid leave, secondment, transfer between offices, special leave, part-time work arrangements). <input type="checkbox"/> Registration of the absences of staff members by the EIB Group OHS including certified sick leave, maternity leave, partial invalidity, temporary full time invalidity, medical part-time arrangements, family leave	EIF Staff Regulations Articles 25-28, 30 and 31 EIF Staff Rules chapters 3 to 5 and Annex VI concerning part-time working arrangements Contractual agreements between EIB and related parties	Management, managers and certain members of the EIF H&RM Department may access the data from the Time Management tool and TIM. Limited EIB Personnel staff may have access to the Time Management screens within PeopleSoft and TIM. Dashboards are available to managers with the following information: (overtime performed, leave/flexi taken, number of days of sickness without 21 October 2020 certificate, data on 2 consecutive weeks of leave, dates of breastfeeding and anomalies). Managers also have access (notification under MyPortal) to overtime done over a period of 4 months as well as anomalies and the annual requirement for the two consecutive weeks of leave and to reports including leave taken, total of days to be taken before 30/04 and the remaining balance of annual leave entitlements for their staff. Authorized staff within the FM team has access to the data of subcontractors. The EIB Group Occupational Health Services register (in PeopleSoft) and have access to individual data relating to certified sick leave, maternity leave, partial invalidity, temporary full-time invalidity and part-time for medical reasons. The EIB PERS and EIF HR time management administrators, and the EIB PERS BO Reporting team, have access to all absence data.	Absence and time management data is stored in PeopleSoft and accessible to staff members and managers via MyPortal. For each staff member data from the current year is visible together with historical data from the past 5 years (on a read only basis). 21 October 2020 A staff member may correct their time registration data for the current month and those going back over the past 12 months. A staff member may make inputs relating to absences (leave/flexi) going back over the past 6 months and going forward up to 18 months in the future. Information processed through the BMC ticketing service is retained during 3 years (current year + 3 years in the past). For example, data relating to 2016 will be erased on 01/01/2019.	n/a	Data are stored and managed within EIB's ERP (Enterprise Resources Planning) system: PeopleSoft HCM 9.2, which is role/permission based with row level security in place. This means that apart from the administrators, staff members can only access their own data and the data of people reporting to them. PeopleSoft also leaves an audit trail recording all actions on data. Data is stored in Oracle 12c database. Apart from the system administrators, the system itself, or authorized known interfaces, no one is able to connect directly to the database.

Category		Title of the processing	Controller EIF / EIB	Processor	Purpose(s) of the processing	Category of Data subjects	Category of data	Legal basis	Recipients	Retention Period	Transfer to third countries or	Technical & Organizational Security Measures
1.3 - Human Resources												
	1.3.3	Access to personal data of staff members in case of absence/death	Human & Resources Management		To ensure that the privacy of personal data is respected whilst accessing professional data (either electronic or physical) stored on the EIF's equipment or premises to retrieve work documents in the event of an absence, departure from EIF service or death of a staff member. To facilitate the retrieval of personal data or belongings stored on the EIF's equipment or premises upon request of the staff member (or close relative) in the event of an absence, departure from EIF service or death of a staff member.	All EIF staff members including Graduates, Trainees and Temporary workers	Any electronic data you have stored on the EIF's equipment or any personal belongings stored on the EIF premises. All data stored on the EIF's equipment or premises will be considered as professional data, unless labelled 'personal' or 'private'	Article 3.7 of the EIF Staff Code of Conduct. EIF Note to Staff "The procedure to access professional/personal data of staff members in the event of absence, departure from service or death" 2017-4551 dated 9th March 2017	Professional data may be disclosed to the respective Department/Division/team of staff member concerned for business continuity purposes. Upon request, personal data may be disclosed, to the departed staff member or to a close relative in the event of the death of a staff member. In the above cases, the disclosure will be done in the presence of a representative from EIF HR and the EIF DPO. In the event of an investigation both personal and professional data may be accessed by IG and the labelling of data as 'personal' or 'private' will not guarantee full privacy	a) in the event of departure: - Personal electronic data kept 3 months before deletion - Personal belongings/physical data may be retrieved within 1 month b) in the event of death: - Close relatives may request to retrieve any personal physical data or personal electronic data within 3 months following the death. After the above deadlines have passed, the electronic data will be deleted and personal documents/belongings destroyed.	n/a	EIF HR will take the necessary steps to reconcile the respect for privacy and the business continuity requirements of the team. In the event of death, the office of the deceased (or cupboard in a shared office) will be locked until personal and professional documents may be separated (in the presence of a representative of EIF HR and the EIF DPO) so that professional documents and files may be made available to the team. The assistance of EIB IT-SEC may be requested to access electronic documentation in order to separate professional/personal electronic data. The access of any electronic files will be done in the presence of a representative of EIF HR and the EIF DPO and due care will be taken to respect the privacy of any files/folders marked 'personal' . The family of the deceased staff member will be contacted to retrieve any personal documents and belongings at their convenience within 3 months following the death. After that period the documents and belongings will be destroyed

Category		Title of the processing	Controller EIF / EIB	Processor	Purpose(s) of the processing	Category of Data subjects	Category of data	Legal basis	Recipients	Retention Period	Transfer to third countries or	Technical & Organizational Security Measures
1.4 - Human Resources - Conduct	1.4.1	Disciplinary Measures	HR		The management and follow-up of disciplinary procedures and sanctions relating to incidents and misconduct of EIF staff members in line with section 6 of the Staff Regulations (Articles 38 to 41) and the EIF Staff Code of Conduct	EIF Staff	Type of incident and respective sanction in the context of the Staff Regulations Date at which the relevant sanction is enforced Details of the incident leading to the sanction Term of sanction	EIF Staff Regulations (Art. 38) Service Level Agreement EIF - EIB for HR administrative measures	EIF HR Staff EIF Compliance EIF Legal Services EIF Board of Directors EIB Personnel Staff	Personal data concerning sanctions is retained until termination of the employment contract. Information remains part of the personal file of the staff member concerned	n/a	Access to personal data is restricted exclusively to HR Staff. IT access to applicants' personal data restricted to HR Staff. Hard copy files are stored in a locker accessible only to authorised EIF HR staff.
	1.4.2	Dignity at work (Informal procedure for cases of harassment)	HR		informal close-to-the problem procedure for cases of harassment and bullying where matters can hopefully be put right with a minimum of fuss and embarrassment	EIF Staff	Personal data usually contained in a report about harassment or bullying allegations such as identity data of the concerned staff members, i.e. complainant, alleged harasser and witnesses (if any)	1) art 5 (a) regulation 45/2001 2) EIF Dignity at Work policy 3) art 3.6 EIF Staff Code of Conduct	restricted EIF HR staff members and potentially with Internal Audit, Court of Justice, European Ombudsman or the EDPS (on demand)	Any personal data collected and processed in the context herein will be retained by the EIF, as the case may be, for a maximum period of ten years maximum from the date of closure	n/a	Complainant report and ensuing correspondence (hard copy and/or electronic file) will be saved by Head of HR and, when necessary, his/her delegate(s) on the K drive (the most restricted drive)
	1.4.3	Selection of confidential counsellors	HR		To select a number of confidential counsellors for a three-year mandate to assist in the informal procedure for addressing alleged bullying and harassment (linked to the Dignity at Work Policy).	All EIF Staff	Personal data usually contained in an Application (CV) from the candidates; identity data on the covering letter (name, first name, nationality, department, division, team), candidates' assessment on Panel's selection note, identity and assessment data on the Note to the EIF Chief Executive to select and appoint confidential counsellors, identity data on letters of appointment to selected confidential counsellors	EIF Dignity at Work policy – informal procedure, as referred to in Article 3.6 of the EIF Staff Code of Conduct (Dignity at Work).	The files are destined for use by the members of the Selection Panel, the staff of the EIF HR division and potentially with Internal Audit, Court of Justice, European Ombudsman or the EDPS	The CVs and cover letters of the candidates who have been selected will be stored until the end of the term of the confidential counsellors (max 3 years). Personal data of the non-selected candidates will be kept for six months after the conclusion of the selection process. The deadline for requesting to block and/or erase different categories of data: within 10 working days.	n/a	Files stored in the EIF HR (h area) only available to designated EIF HR staff member and to the Head of Human & Resources Management.
1.5 - Human Resources - Health and Safety	1.5.1	Accident Insurance	HR	Third party provider ----- EIF	Processing of insurance claims linked to: *the accident of an EIF staff member or family member *the loss or theft of the personal belongings of an EIF staff member whilst on a business trip	EIF Staff and family members	*Personal data of EIF Staff and family members luggage *Data related to	EIF Insurance contracts	Insurers, medical examiners	Five years in central EIB Group archives	n/a	Information and personal data is known, managed and filed by the specific responsible for the relevant file
	1.5.2	Occupational Health Services	HR		In conformity with clinical practice and national laws, the EIB Group Occupation Health Services (OHS) team is responsible for the provision of occupational health services to staff and for retaining accurate medical records The OHS team retain information related to the health of individual EIF staff members for the purposes of prevention, diagnosis, provision of care, treatment and follow-up of medical problems at individual level. In addition, the OHS survey the health situation of the EIB Group, including the EIF, on a more general level.	Current and retired EIB Group staff members, including EIF staff members, are required to undergo annual medical exams (as per Chapter 7 of the Staff Rules) either by the OHS or a medical practitioner of their own choice. In the event when the staff member opts to carry out the annual medical elsewhere, a report following the examination must be communicated to the OHS	The processing concerns special categories of data (cf. Article 10.3 of EC/45/2001) "for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services". Data includes information revealed by EIF staff members to EIB OHS personnel concerning their health status. For example, findings from physical examinations done at the EIB OHS; results of laboratory analyses e.g. x-rays and other image diagnostics; ECGs; cardiology exams; discharge letters from hospitals; reports following operations; reports from speech therapists, psychologists, nutritionists; vision tests; audiograms; physiology tests; videos and other renderings of endoscopies; physiotherapy records; photographs, slides and other information from providers of diagnostic, preventive, promotive, therapeutic and rehabilitative medical services. Data related to sick leave	Staff Regulations, Staff Rules, relevant Notes to Staff	Data from the medical records of EIF staff members held by the EIB OHS will only be disclosed to third parties, including EIF HR and other services, against signed consent by the staff member in question, or in certain circumstances where consent may be implied, e.g. referral or emergency, and then only to health professionals providing healthcare to the data subject concerned	Storage: Medical data of EIF staff members originating from the EIB OHS itself, or from external providers of services, will be kept on file for the duration of the staff member's employment with the EIB Group. Records older than 10 years will be stored in the EIB central archives, with access to those files restricted to authorised EIB OHS personnel. Records relating to the management of the EIB OHS, such as timetables of appointments, will be retained for a period of 5 years with restricted access to authorised EIB OHS personnel. Medical questionnaires following the recruitment process are held by the EIB OHS, according to the applicable retention period.	Transfer of data to third countries and international organisations can only take place on the basis of written approval, or when consent may be implied, e.g. referral or emergency, and then only to health professionals providing healthcare to the data subject.	All information held in the medical records is stored by the EIB OHS in accordance with strict security measures which guarantee exclusive access by the authorised EIB OHS personnel (physician, nurse/medical assistants, secretary/receptionist).

Category		Title of the processing	Controller EIF / EIB	Processor	Purpose(s) of the processing	Category of Data subjects	Category of data	Legal basis	Recipients	Retention Period	Transfer to third countries or	Technical & Organizational Security Measures
	1.6.1	Training - Register of Presence	HR	SAP Luxembourg S.A., Branch of SAP Belgium S	To monitor the participation of EIF staff members attending internally organized training events, including a number of mandatory Compliance training sessions. Enrolment to training courses is processed in the SuccessFactors Learning tool.	Data subjects in this processing are the EIF staff members who attend internally organized training courses	EIF HR extract lists of registered participants per training course (including the name and date of the training course, with a full list of the name and first name of participants) and signatures are gathered to document attendance. As enrollment to training courses is processed in the SuccessFactors Learning tool, attendance is validated by HR upon the receipt of the signed attendance list, in the SuccessFactors Learning tool, where the course name, course category, duration, dates and completion date are logged. Following validation those details are visible in PeopleSoft in the data subject's profile under the 'professional training' tab.	EIF Staff Rules, HR Manual of Procedures, Compliance Policy and the annual HR Training & Development Portfolio)	The Chief Executive, Deputy Chief Executive, Compliance Department, HR and linemanagers. Data subjects may request proof of attendance to training sessions. For example, staff members may need to provide such information to external companies (ACCA, CFA etc.) when they are required to attend a certain amount of courses per year to adhere to their membership rules. The individual professional training summary is disclosed to the hiring manager (and those colleagues involved in the selection process) in the context of internal mobility.	The professional training history registered in SuccessFactors is stored until the data subject is no longer an active member of staff. The attendance lists for registered participants are retained as per the established retention period	n/a	Access restricted to recipients
	1.6.2	Staff Engagement Survey	HR	PricewaterhouseCoopers EU Services EESV ("PwC") – responsible for carrying out and managing all the different project phases; - Qualtrics (sub processor of PwC) – for the survey execution phase (to distribute the questionnaire to the EIB Group survey population), for carrying out survey related activities (distribution of reminders and final thank you message), to analyse and report the data	To measure how engaged EIF staff members are and in which areas improvements are needed. The survey allows an analysis of factors that may hamper engagement, including strategic alignment with its organisational goals, the quality of the line manager-employee relationship, and efficiency in processes and procedures. The results from the survey will provide a good understanding of the EIF needs to take action to support and align its internal stakeholders towards achieving the EIF's vision and organisational goals	All staff with EIF indefinite or fixed term contracts will be invited to participate in the staff engagement survey (for the 2019 survey, all staff in service on 1st September 2019 will be invited to participate). Participation is voluntary and anonymity guaranteed by secure data processing. In particular: - survey inputs: separation of functions within the Service Provider's staff in charge of sending survey invitations and reminders to participants and staff administering the survey contents and results - survey outputs: survey answers and results will be anonymous and it will not be possible for PwC and for EIF to link the answers provided to the email address of each respondent. Furthermore, responses will be aggregated safeguarding the individuals' anonymity. This means that breakdowns will only be shown when the number of respondents is	Personal data shared with PwC/Qualtrics: first name, last name and recipients' e-mail addresses Categories of processing carried out on behalf of each Controller (only to be filled in by the Processor):	Consent of the concerned staff members who voluntarily decide to participate the engagement survey. Art. 23 from Rules of Procedure of the EIF. Article 1.1. of Code of Conduct. The EIF aims to provide a positive working environment that enables and encourages staff to work together in a culture of mutual support and cooperation.	<ul style="list-style-type: none">• The detailed survey results will only be disclosed by the external provider (PwC) in amalgamated form (i.e. reports for each entity as described above will only be produced when a minimum of 10 people responded to the survey.• Demographic data (e.g. gender, managerial level, contract level) will only be used for analysis at EIF-wide level – no cross-analysis (e.g. information about 'female colleagues' in 'division X') will take place. Communication of the survey results and verbatim comments by the external provider to EIF management and staff will be done in amalgamated form in the following way:• Detailed EIF-wide report (with a summary of the verbatim (e.g. a word cloud or theme analysis) and a summary of amalgamated EIF-wide results: recipient category: All EIF Staff (distribution via the Intranet);• Detailed EIF-wide, Departments and Division reports (including full verbatim comments, anonymized by PwC): recipient category: Head of Human & Resources Management, selected members of the Human & Resources Department, Chief Executive and Deputy Chief Executive. In its role as the team dealing with the Staff Engagement Survey project, the Performance Management Unit supports the distribution of the reports in the organisation by PwC and reviews all verbatim comments to ensure no staff member can be identified;• Department reports, including those Division reports belonging to this Department as well as the full verbatim from staff belonging to this Department: recipient categories of amalgamated data and full verbatim for the Department: respective Head of Department, and other colleagues designated by the Head of Department. The Head of Department takes the decision to share the Department report (without full verbatim) further in their teams. They may also decide to share the full verbatim reports further within their management team (including Heads of Division and Unit).• Division reports (including a summary of the verbatim through e.g. word cloud or theme analysis): recipient category of amalgamated data and survey results: Head of Division (and any people in their team they designate). Heads of Division (together with the Head of Department, where applicable) take the decision to share their Division report (without full verbatim) further in their teams. Reports for each entity are only produced when a minimum of 10 responses are received. Demographic data (e.g. on gender) is only used for EIF-wide analysis.	Personal data will be retained only for the time necessary to perform the analysis of data and related reporting activities. As soon as the survey related activities will be over PwC will delete all the personal data provided by EIF	The list of questions from the EIF Staff Engagement Survey can be shared with other IFIs via the EIF College of Staff Representatives. In addition, in case the College wishes to share parts of the EIF-wide anonymized, amalgamated staff survey results with other IFIs, they need to contact and obtain the permission of the Head of Human Resources Division.	Anonymity and confidentiality guaranteed 1) legally, by the detailed and technically-specific contractual provisions of the confidentiality statement signed by the provider and the related Data Protection Agreement, 2) organisationally, by separation of functions within the Service Provider's staff in charge of sending survey invitations and reminders to participants and staff administering the survey contents and results, 3) technically by the use of alias (unique per survey) to render email addresses (of staff) non-identifiable by survey administrator Separation of security functions: 1) EIB Group - IT administrator of interface and EIB Group IT security requirements; 2) external provider: IT survey tool manager: administrator of emails, using secure IT systems; and 3) external provider: administrator of the survey contents and results. This separation guarantees that 1) EIB Group controls the security of its IT systems in the process, 2) the survey provider, through certified technical IT systems and data management processes, ensures data protection and IT security for the survey data.
	1.6.3	Recruitment Tools	HR	External providers: Le consortium "Deloitte Tax & Consulting sàrl et SHL Belgium sa"	Using state of the art tools throughout: <ul style="list-style-type: none">• Recruitment process for external and internal candidates in addition to standard selection tools (such as interviews and professional tests)• Development Centres for EIF staff members The tools include psychometric tests used to screen candidates and a personality questionnaire to help structure interviews.	Internal and external candidates and EIF staff members identified for Development Centres	To be sent to SHL Belgium sa: <ul style="list-style-type: none">• Internal and external candidates may be subject to psychometric tests and filling the personality questionnaire.• EIF staff members identified for Development Centres may be subject to psychometric tests and filling the personality questionnaire. To be sent to Deloitte Tax & Consulting sàrl: <ul style="list-style-type: none">Concerning the external candidates who will be subject to an assessment centre, the Processor will be provided with the CV submitted by the candidates themselves when applying for a position, as well as the application details form that they have completed at the time of application (details of the personal data collected in Annex 1).Concerning the internal candidates/EIF staff members identified who will be subjected to an assessment/development centre, the Processor will be provided with the application details (details of the personal data collected in Annex 2).	EIF Manual of Procedure	<ul style="list-style-type: none">• Relevant staff at the service providers,• Recruiters, assistants and managers/panel members participating in the recruitment processes, other HR staff members when managing Development Centres,• External and internal candidates and staff members selected for Development Centres may be provided tailored reports for their own profile upon request.	Data pertaining to internal and external candidates will be wiped/deleted 3 years after the closure of the recruitment campaign, in line with the EIB Group's retention schedules for recruitment documents. In order to facilitate the Processor's data management, a period of 6 months will be added as from the date of submission of the candidate report. Data pertaining to staff members identified for Development Centres will be wiped/deleted after 3 years from the date of the report, in line with the EIB Group's retention schedules for development documents.	CEB (company that owns SHL entities, including SHL Belgium is Privacy Shield certified. They have an Intragroup Agreement in place between all CEB/SHL entities, which includes the EU Model clauses. While the data will be stored in their UK data centre (and thus be processed mainly by an EU sub-processor), they cannot limit access to only those personnel in the EU, as some personnel from the US and India will have access to the data in order to provide the services. Data are encrypted readable to those with authorized access, including staff from the US and India who are involved in maintaining the system/providing the services.	The providers do not have access to EIB Group IT systems.

Category		Title of the processing	Controller EIF / EIB	Processor	Purpose(s) of the processing	Category of Data subjects	Category of data	Legal basis	Recipients	Retention Period	Transfer to third countries or	Technical & Organizational Security Measures
1.6 - Human Resources - Other	1.6.4	Carte de Legitimation	HR	EIB under EIF- EIB SLA	To carry out the administration linked to Carte de Légitimation ("CdL") documents - including issuing, modifying and cancelling them	The data subjects in this processing are EIF staff members residing in Luxembourg along with the spouse/registered, and any dependent children below 26 years of age. Secondees to the EIF and their family members are also entitled to a CdL, providing that the following conditions are met: <ul style="list-style-type: none"> <input type="checkbox"/> They are not Luxembourg nationals <input type="checkbox"/> They reside in Luxembourg (a hotel address is not acceptable) <input type="checkbox"/> They do not already hold a Luxembourg residency permit (an attestation d'enregistrement) 21-Oct-20 <input type="checkbox"/> For a partner/spouse or dependent child – they are registered at the same address as the staff member, and the dependent child does not work. 	<ul style="list-style-type: none"> <input type="checkbox"/> Employer name and type of Institution (Embassy or EU Institution/International Organisation) <input type="checkbox"/> Description of status (Person with diplomatic status, Official, Administrative and technical staff, Family member) <input type="checkbox"/> Date of arrival in Luxembourg <input type="checkbox"/> Work start date <input type="checkbox"/> Likely duration of stay (number of years or permanent contract) <input type="checkbox"/> Name and surname <input type="checkbox"/> Date and place of birth <input type="checkbox"/> Nationality <input type="checkbox"/> ID type and number <input type="checkbox"/> Civil status <input type="checkbox"/> Address 	Luxembourg law on immigration	The data subject has access to all their own data and the date of their family members and retains the CdL document where the information is visible. Appointed EIB PERS staff members dealing with the administration linked to CdLs (cartedelegitimation@eib.org) Data are disclosed to the Luxembourg Ministry of Foreign Affairs, to the Centre Informatique de l'Etat and to the commune where the data subject resides. The data subject may be requested to disclose the CdL to the Luxembourg authorities or to the local police (in the same way that the data subject would disclose a standard residency permit).	The information registered in peoplesoft under the 'identification data' tab is kept for the entirety of the staff member's service. Deadline for blocking or erase data following a demand from the data subject: 30 days.	n/a	Basic CdL data is stored electronically in PeopleSoft. This includes CdL issue date, status, expiry date and CdL number. Data is entered under the data subject's personal ID number. The details of the eventual CdLs issued to eligible family members are also stored in the same PeopleSoft screen. Once the document is cancelled or has expired, the CdL is recovered from the data subject (or eligible family member), stamped "cancelled" and destroyed securely. The cancellation form is stored in GED for 5 years. This time-frame enables EIB PERS/EIF HR to assist with eventual questions from the Luxembourg authorities concerning either residence in Luxembourg, which is important in the event of a staff member opting for Luxembourg nationality, or the residence of dependent children in the context of requests for CEDIES financial assistance
	1.6.5	VAT Exemption	HR	EIB under EIF- EIB SLA	To provide the competent Luxembourg tax authorities with information on EIF staff members in the context of a request from the staff member to obtain VAT exemption on vehicles and household items.	EIF eligible staff members.	Electronic request submitted via the self-service screen My Compensation & Benefits – VAT Exemptions (by FC). <ul style="list-style-type: none"> <input type="checkbox"/> Name, address, date of birth, address, civil status, entry date at EIF, employee ID number, nationality, of staff member <input type="checkbox"/> Item(s) purchased, name of the shop, VAT number, invoice number, amount without VAT, member state (for purchases outside of Luxembourg) 	Luxembourg law on VAT Protocol on Privileges and Immunities of the European Communities as implemented by Luxembourg Directive 2006/112/EC – Article 151 Directive 2008/118/EC – Article	Competent Luxembourg Tax Authorities: Administration de l'Enregistrement et des Domaines Office address: Bureau d'imposition 11 – département franchises, 67-69 rue Verte, L-2627 Luxembourg Postal address: BP 31, L-2010 Luxembourg Internal and/or External Auditors (upon request) EIF Staff (for business purposes only)	The EIB Financial Control – Administrative Expenses unit store the data for as long as necessary to complete the processing operation, to ensure compliance with audit controls and to allow queries on past payments. Any supporting document and/or form submitted is archived physically and electronically in the EIB's document management system for 10 years	n/a	Data is based on the invoices scanned by the Scanning team and stored in secured part of GED. The Account Payable Team introduces the invoices to the Peoplesoft Application. The certificates are issued through Business Object queries. Business Objects/GED (Electronic Document & Records Management) environment: accesses are restricted and protected in line with EIB Group general policy: password protection and access review done on a monthly basis by the relevant business owners. For purchases in Luxembourg: The certificates are provided to the competent Luxembourg Tax Authorities by the EIB FM service. For purchases outside of Luxembourg: The appropriate VAT certificate is printed and sent to the supplier/consultant by post
	1.6.6	Annual Review of Personal Data	HR		Each year an EIB-Group-wide exercise is launched calling for staff members to validate (correct and modify, as necessary) their personal data held in the PeopleSoft Human Resource Management System (PSFT HRMS). To facilitate this exercise an overview of the personal data held on file is available via the MyPortal self-service screen My Personal Data & Documents - Edit Personal Information, which can be accessed and updated by the staff member at any time. The 'Edit Personal Information' screen also allows staff members to submit a request to change certain elements of their personal data (for example their civil status, dependents, address etc.) and prompts them	EIF Staff members	Identification data : name, maiden name (if relevant), date of birth, birth country, gender, nationality(ies), civil status, private contact details (home and mailing addresses, phone numbers), emergency contacts; Professional data: work location, job title, professional contact details (office number, telephone numbers); Dependent data: name, gender, date of birth, relationship, employment situation for spouse/registered partner, health insurance coverage, eligibility to child allowances paid by another source; Other data: location of centre of interest, Luxembourg residency permit (Titre de legitimation) details;	Article 5 of the Staff Regulations states that staff members have an obligation to declare their personal and family circumstances each year (including any change with the spouse/registered partner's employment situation), and whenever there is a change with them. Any misstatement or omission, even unintentional, may lead to disciplinary sanctions under Articles 38-41 of the Staff Regulations. In addition, staff members are obliged to declare any change to their Centre of interest in line with Article 6.2 of the Staff Regulations.	The personal data stored in the PSFT HRMS is confidential and can only be seen by a restricted number of people within EIF Human Resources and EIB Personnel/Operations	Personal data impacts individual rights and benefits and so they are stored electronically and are available on-line during the entire period of service and beyond. To respect the validity of pension rights, including the rights of any eligible dependents, data are not destroyed before 120 years after the birth of the data subject. Deadline for blocking or erasure (following a sound request from the data subject or well documented and recognised material error on processing): 60 days	n/a	Access to personal data held in the PSFT HRMS is password protected. All requests for access are centralised within one unit in EIB Personnel (Personnel-/ASP/Systems) and accesses are attributed as restrictively as possible. As per article 8 of the Staff Regulations and article 2.1 of the EIF's Code of conduct, all staff members are bound by the obligation of confidentiality in respect of information received in the course of their duties, both during and after leaving the EIB Group
	1.6.7	Archiving of consultancy contracts	HR	1. EIF HR 2. EIF internal services acting as requesters for consultancy services 3. EIF Compliance 4. EIF Internal Audit	Adequate management of contracts containing personal data concluded by the EIF with external consultants	Individual consultants & Service providers	Personal data of consultants	Regulation CE 45/2001 Article 5(a) EIF Statutes EIF Standard Consultancy Contract EIF Guide on Procurement	1. Requesting internal services (requester) 2. HR 3. EIF Legal Service 4. EIF Compliance and Operational Risk 5. European Court of Auditors 6. OLAF 7. European Ombudsman 8. European Court of Justice	Up to seven years after the signature of the respective contracts. Personal data of staff provided to EIF by agencies shall be retained for a period not exceeding three years following the termination of the assignment	n/a	To the extent data is stored electronically, data security is part of the PeopleSoft and Gestion de Temps systems Hard copy files are stored in locked cupboards with access limited to the HR team

Category		Title of the processing	Controller EIF / EIB	Processor	Purpose(s) of the processing	Category of Data subjects	Category of data	Legal basis	Recipients	Retention Period	Transfer to third countries or	Technical & Organizational Security Measures
	1.6.8	Archiving of the personal file of EIF staff members	HR	EIF	The creation and management of a hard copy personal file for each staff member (including members of the GRAD Programme). Personal files are created for active staff and maintained following departure from service. Paper files are stored in locked cupboards in the locked EIF HR Archives. Since 2018 newcomers documentation is also saved and stored in the electronic personal file on the EIF HR H-drive	All EIF staff members	<p>After selection the successful candidate will be asked to upload copies of the following personal documentation onto the newcomers portal:</p> <ul style="list-style-type: none"> o Passport or identity card o Birth certificate, including, where applicable, those of the spouse and any child(ren) o Wedding certificate, Registered Partnership (PACS) or certificate of Divorce (as applicable) o Diplomas, university certificates etc. o Latest salary slip o A statement/certificate to confirm the spouse or registered partner's employment details o School certificates for children (as applicable) o Completed enrolment form for CIGNA o Signed accident insurance policy o Signed employment contract o Special Remarks form: particular financial commitments o Signed copy of the Staff Regulations o Signed copy of the Staff Code of Conduct <p>The newcomer will be asked to provide an extract of the police register (police certificate of character) from the last country of residence (less than 6 months old). This document is not filed, instead a form to acknowledge its receipt is completed by the HR officer and the form is retained.</p> <p>Some of the abovementioned documentation is destined to define the staff member's remuneration and justify the granting of certain allowances. Other filed documents that impact remuneration are issued by the EIF to the staff member including: the contract, offer letter, transfer between offices, internal mobility, parental leave, part-time arrangements, unpaid leave, promotions, pension transfer documents, resignation letter and sums due upon departure information</p>	EIF Staff Regulations I and II, EIF Staff Rules, for the issuance of an EIB employment contract, EIF HR Manual of Procedures.	In addition to the EIF H&RM team, the EIF colleagues/managers participating in the initial selection process receive some of the personal documentation (CV and application form). If a staff member moves between the EIB and the EIF in the context of internal mobility, then some documentation may be transferred between the institutions. Personal data may be disclosed to another institution in the context of establishing a staff exchange or secondment or in the context of a request to transfer pension rights to/from another pension scheme. Remuneration data may be disclosed in the event that an EIF staff member is married or in a registered partnership with someone working in another institution (in order to establish which spouse/partner has the highest basic salary). The EIF has an obligation to disclose personal data upon request of a judge of a European Member State.	Main file: Historical permanent conservation Appraisal related: 3 years after date of departure Personal confidential: Historical permanent conservation Career confidential: 3 years after date of departure	n/a	<p>Restricted physical access to the HR archive room: The personal files are stored in fire-proof archive cupboards, with the keys kept by the assistant to the Head of H&RM.</p> <p>Staff members may consult the entirety of their own personal file.</p> <p>For the management of the electronic personal files: access is restricted to the members of the EIF HR Division. On a quarterly basis EIF H&RM contact EIB IT Identity & Access Management (IAM) to verify the list of staff members who have access to the h-drive</p>
	1.6.9	EIF Intranet (Find People & Welcome message)	HR	EIF	The 'Find People' application is an EIB Group wide internal employee directory facilitating contact between staff members. Welcome messages are published by the EIF HR team on a regular basis with a photo, list of new joiners (EIF agents) with a short introduction on each person.	All EIF agents. Data on the secondees, consultants, temporary staff, GRADs and trainees are also available via the 'Find People' application	'Find People': photo, employee ID, name and forename, nationality, cost center, date of birth (excluding the year), unit along with full work contact details and e-mail address. 'Welcome Messages': group photo and a brief introduction to the new joiners (EIF agents)	The EIF aims to provide a positive working environment that enables and encourages staff to work together in a culture of mutual support and cooperation in line with Article 1.1. of the Code of Conduct. Art.23 of Regulation 45/2001 of 18th December 2000 (Processing of personal data on behalf of controllers).	Data in both the 'Find People' application and 'Welcome Messages' are disclosed to all staff members, secondees, consultants, temporary staff, GRADs, and trainees (included those staff members, members of the EIB Management Committee, secondees, consultants, temporary staff, GRADs, trainees and summer students working at the EIB). Data is not disclosed outside of the EIB Group.	Data is retained in the 'Find People' application during the period of service. Data is removed once the data subject leaves the service of the EIF. For the 'Welcome Messages' published on the EIF intranet it is proposed to limit data to 12 months.	n/a	<p>No special security of processing (except for photo and date of birth – see below) as all data are public.</p> <p>For the photo and date of birth, ICC/IT/Enterprise Applications/IAS ensures that the information is not available if the related box is ticked (see section j).</p>
	1.6.10	Exit Interviews	HR	EIF	To gather feedback from departing staff member and statistical data on the reasons for departure. Understand the impact of HR policies (CDD-CDI), to gather feedback, to allow continuous improvement. Participation is on a voluntary basis.	EIF staff members leaving service	<p>Information about reasons to leave and potential improvements suggestions are gathered in a word report, stored within HR. These reports remain undisclosed.</p> <p>Reasons for departure are indicated in an excel file used for reporting on HR data. Statistics including such information are provided to management, without linking the data to the names of the former staff members.</p> <p>Identification data : name, first name; ID number; date of the interview</p> <p>Professional data: work location, job title;</p> <p>Other data: internal or external mobility; reasons and date for departure; suggestions to improve work processes, workplace organisation, identification of pain points in EIF's procedures.</p>	Participation is on a voluntary basis, therefore, by agreeing to participate, staff members are expressing their consent	Notes taken during the exit interview are summarized in a short report and then, are destroyed. Only the reason for departure is reported in an excel file (Masterfile) in order to produce statistics to be shared anonymously with Management (in terms of departure trends etc). Circulation of the report is extremely restricted to certain staff working the HR Division and the H&RM Director .	2 years after departure	n/a	The interview report and the excel file containing the reasons for departure are stored on the EIF drive where accesses are attributed as restrictively as possible
	1.6.11	Managerial Development Program (Cubiks)	HR	Cubiks	The processing is linked to a development program for EIF future managers. This is a highly confidential development program, whose purpose is to develop an individualized training plan for each staff member who will ask to participate. The report that will be produced by an external provider (Cubiks) will be shared only with the concerned employee and	Mainly Heads of Unit or staff members of a similar hierarchical level	The data subject will be asked to fill out a personality questionnaire and to have a face-toface assessment with Cubiks. As a result, an individualized report will be generated. The personal data mentioned in the report will be the following: name and last name of the data subject, their job title, department/unit, people management responsibility, team size as well as the name and last name of the Cubiks' assessors. The individualized report will contain the opinion/assessment of Cubiks concerning the potential development of the data subject's managerial capabilities.	Consent of the concerned data subjects who expressly ask to participate and EIF HR Manual of Procedures (art. 1.2 & 6.2)	the Head of H&RM Departement and the H&RM team members identified by the Head of H&RM Department and the data subject. The staff member is free to disclose the content with their hierarchy.	A copy of the report will be saved in the confidential career section of the individual file of the data subject. It will be destroyed once the person leaves EIF (within 12 months from the date of departure).	n/a	Cubiks does not have access to the EIB Group IT systems, in addition as mentioned in point g), a copy of the report will be save only in the confidential career section of the individual file accessible only to the concerned employees and to the EIF HR team.

Category		Title of the processing	Controller EIF / EIB	Processor	Purpose(s) of the processing	Category of Data subjects	Category of data	Legal basis	Recipients	Retention Period	Transfer to third countries or	Technical & Organizational Security Measures
	1.6.12	Laissez-passer	HR	EIB under EIF-EIB SLA	To process, review, issue and cancel Biometric LP requests. The LP is a travel document governed by Council Regulation 1417/2013. It is issued upon request to EIF staff members who travel regularly for professional reasons.Biometric LPs are valid for a maximum period of six years.	EIF eligible staff members	Application form of staff member : Institution, place of enrolment, type of application, Last name, first name, nationality, date of birth, gender, place of birth. Biometric features (facial image and fingerprints). Copy of passport.	Article 11 of the Staff Regulations, which is based on text in the protocol on the privileges and immunities of the European Economic Community. Council Regulation (EEC, Euratom, ECSC) No 123/86 of 20 January 1986 amending Regulation (EEC, Euratom, ECSC) No 1826/69 laying down the form of the LP to be issued to members and servants of the Institutions. The EU laissez-passer is a travel document governed by Council Regulation 1417/2013. Authorities in EU Member States must recognise it as a valid document. In order for it to be internationally recognised as a valid travel document, the laissez-passer complies with the security standards and technical specifications applicable to national travel documents issued by Member States under Council Regulation (EC) No 2252/2004 and with International Civil Aviation Organisation (ICAO) specifications, in particular those appearing in ICAO Document 9303 on	European Commission LP Services. The data subject retains the LPData may be disclosed, at the request of the data subject, to embassies in order to obtain travel visas. 14-Oct-20 EIF Staff (for business purposes only)	Information stored electronically in PeopleSoft is kept for the full length of service of the staff member. The physical LP is destroyed when the staff member leaves service or the LP expires. The EU Commission is responsible for registering information, including biometric data.	n/a	Basic LP data is stored electronically in PeopleSoft – Identification Data – Visa/Permit Data under the data subjects Staff ID (LP issue date, status, expiry date and LP number) Application forms and copies of passport are sent to the EIB LP team via email EIB-EULP-LPIILUX@eib.org or internal post. Countersigned original copy is provided to the data subject
	1.6.13	EIF Staff Representatives	Staff Representatives		The mission of the Staff Representatives (as per Article 3 of the Convention) is to be the representative body of the entirety of the staff. Whilst in principle the College shall not represent the interests of individual staff members, it may do so if those individual rights are of general interest to staff. It is understood that no such representation of individual interests shall be made without the express approval of the individual staff member concerned. In the light of the above, the purpose of the processing of personal data by the EIF College of Staff Representatives is exclusively linked to the activities carried out in pursuit of its mission as	All EIF staff members, including anyone employed on an interim basis or seconded from another institution or company, who approach the College of Staff Representatives	In the context of their duties the College of Staff Representatives may be processing personal data originating from different sources including name, first name, nationality, gender or special categories of data (e.g. any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation). The Staff Representatives will respect the principle of data minimization, meaning data retained should be limited to the process it is needed for.	• EIF Statutes, Article 2 "The task of the Fund shall be to contribute to the pursuit of the objectives of the European Union". • Article 24 of the Staff Regulations I and II provides the basis for a College of Staff Representation to represent the general interests of the staff vis-à-vis management. • Article 14 of EIF Staff Rules refers to the Convention governing relations with the College of Staff Representation and the full current Convention is appended to the Staff Rules (Annex III).	The College of Staff Representative may disclose data to each other. The College of Staff representatives may disclose personal data to EIF HR or to EIF Management, upon receiving consent by the concerned individual(s). The SR assistant has access to data as the SR assistant has an active role in supporting the College in the pursuit of its mission by operating the outlook shared mailbox and being in charge of coordination of the SR work.	Personal data sent to the College will be erased once no longer required for the pursuit of College's mission. Personal data sent to individual SRs can be shared with other SRs and stored in the SR Outlook shared mailbox. Such data should be erased from SR mailbox once no longer required for the pursuit of College's mission. The mandate of the individual SRs is limited in time. Following expiration of their mandate SRs must erase all such data from their individual mailbox immediately. Successor SRs gain access to stored data upon assuming their role.	n/a	The storage and access to data by the College of Staff Representation is limited to: - Outlook shared mailbox (only area where personal data is persistently kept by SRs) - G:drive folder - Individual mailboxes Whereby all individual authorizations and accesses are aligned with the duration of the mandate of the College and all its members.

Category		Title of the processing	Controller EIF / EIB	Processor	Purpose(s) of the processing	Category of Data subjects	Category of data	Legal basis	Recipients	Retention Period	Transfer to third countries or	Technical & Organizational Security Measures
2.1 - Compliance - Governance	2.1.1	Declaration of Interest	Compliance	EIF	Enhance the accountability and transparency standards of EIF in line with EIB Group principles (publication of CVs by members of the EIF BoD, CE and DCE To	Members of EIF Board of Directors, Chief Executive, Deputy Chief Executive	Outside activities, financial interests, assets, major liabilities including those of spouses	Para. 3 of the Code of Conduct for Members and Alternate Members of the Board of Directors	Chairman of the Board of Directors	To be confirmed	n/a	Each member submits its Declaration of Interest to the Chairman of the BoD. The Secretary of the Fund initiates the publication on the EIF website
	2.1.2	Fraud Investigations	RM Compliance with EIB-IG	EIB	Maintain the highest level of integrity and efficiency in relation to all EIF activities and operations. EIF as a member of EIB Group has a zero tolerance policy against prohibited conduct in its activities and operations	IG-IN may process data of staff members, EIF counterparts, suppliers and consultants, who are relevant for the investigation	Personal files of EIF staff memebers	(i) Article 325 of the Treaty on the Functioning of the European Union (TFEU); (ii) Article 2/1 of the EIF Statute; (iii) Article 18 of the EIB Statute; (iii) Council Regulation (EC, Euratom) No 966/2012 of 25 October 2012.	Senior Management Executive OLAF Audit Board of EIF Chief	Data shall be retained for at least five years and up to ten years maximum from the date of closure of the case. As regards allegations where the Head of IG/IN decides not to open a case (Prima Facie Non Case) or a case closed because the allegations are not substantiated, data shall be retained for up to five years maximum from the decision not to open a case or the closure of the case.	National authorities within and outside the EU. Other International Financial Institutions' investigation functions.	Paper files are archived in specific locked archives only accessible to IG/IN Electronic files are stored in a restricted area of GED only accessible to IG/IN and whose access is protected by individual password. Emails exchanges with OLAF are secured by providing confidential information through attached documents protected with secured ZIP
	2.1.3	Internal Audit Process	EIF CE	Internal Audit Department of the EIB	The EIF Internal Audit Charter defines the Mission of Internal Audit. The general objective of Internal Audit is to provide to management a reasonable assurance that EIF is operating properly and efficiently	Data subjects are mainly EIF active and non-active staff and their family members, but can also be people external to EIF (for instance personal data of Venture Capital fund management, or CVs of consultants during a Procurement audit).	The personal data identifier can for instance be a name (including a username for accessing computers and applications), an identification number, a date (e.g. birthday, death, wedding, divorce, etc), a location (e.g. a private address), a social identity (e.g. marital status), a generic physical information without medical details (e.g. invalidity status, sickness leave, maternity leave, etc). In some circumstances, the personal data are subject to "pseudonymisation".	EIF Statutes, Art.2(1): The task of the Fund shall be to contribute to the pursuit of the objectives of the European Union. According to Internal Audit Charter, Internal Audit can process personal data in order to give management a reasonable assurance that EIF is operating properly and efficiently	In no circumstance, Personal Data are ever disclosed in audit reports in any member state, third country or international organization. However, OLAF – in the course of an investigation - might be entitled to access audit working papers where personal data might be stored and processed. External Auditors might have access to personal data in the sense of a quality assurance review of the audit file of a specific audit (e.g. for reliance of internal audit).	All audit files (audit working papers with potential personal data) saved in electronic version are stored permanently in TeamMate. Should there be any paper document the retention period is 10 years	In no circumstance, Personal Data are ever transferred in any member state, third country or international organization	Internal Audit applies the IIA Code of Ethics which includes a confidentiality clause: "Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so". The data are stored in Internal Audit Document Management system TeamMate, where access is restricted to Internal Audit staff members and consultants. For staff members and consultants access is restricted to the files of assignments they have worked on. Also for consultants, access is restricted to the duration of the assignment. For every audit assignment, only the specific team involved in the audit has access
2.2 - Compliance - Conduct	2.2.1	Staff External Activities	Compliance		Process to ensure compliance of EIF Staff with limits based on the Code of Conduct for authorised activities external to EIF employment	EIF Staff members, Chief Executive and Deputy Chief Executive	Identity of the beneficiary, Type of activity, Remuneration, Employer/beneficiary, Duration, Estimated time consumption	Paragraph 2.2 of the EIF Staff Code of Conduct.	EIF Staff members of EIF Compliance	The data is deleted after ten years following the date of the termination of the external activity.	n/a	Requests are only received and processed electronically, no hard copies are held. Access to the electronic file and to the register of declarations is limited to the to EIF Staff members in EIF COR
	2.2.2	Gifts and advantages	Compliance	EIF	Process relating to the rules under which gifts and direct or indirect advantages may be accepted by EIF Staff from EIF business partners	Chief Executive, Deputy Chief Executive, EIF Staff	Identity of beneficiary, Type of gift or advantage, Identity of the donor, Estimated value of the gift or advantage, Circumstances in which the gift or advantage was received	Paragraph 2.4.3 EIF Staff Code of Conduct, Paragraph 2.4.3 of the Code of Conduct for the Chief Executive and the Deputy Chief Executive	EIF Staff members of EIF Compliance	The data is deleted after five years following the issue of the position of EIF COR to the EIF Staff member concerned	n/a	Requests are only received and processed electronically, no hard copies are held. Access to the electronic file and to the register of declarations is limited to the respective EIF Staff member concerned and to EIF Staff members in EIF COR
	2.2.3	Whistleblowing Policy	Compliance	EIF	Reporting of process deficiencies, which could create a financial or reputation risk to EIF to an independent internal service within the organisation and disregarding usual hierarchical reporting lines	EIF Staff, Temporary Staff, Consultants	Name of the data subject and information on his/her situation within the organisation, any document or other evidence of efforts to address and/or resolve the identified issue	EIF Statutes, EIF Staff Code of Conduct, EIF Whistleblowing Policy, Art. 22a-c of the Staff Regulations of the Officials of the European Communities.	EIF Compliance	Personal data will only retained if the data subject concerned so consents and then for the customary period of five years after the closure of the file	n/a	Electronic data received by EIF Compliance, from which an identification of the data subject concerned could be derived is only accessible by the Head of EIF Compliance. The hard copies of documentation are stored securely into a dedicated locked cabinet with access only by the Head of EIF Compliance
ons	2.3.1	Transactional Integrity DD	Compliance	EIF	The EIF AML/CFT standards follow the EIB Group AML/CFT framework. EIF proceeds systematically to a detailed due diligence on the integrity of EIF counterparts. The level of due diligence depends on potential red flags identified during the on-boarding process of the financial intermediary. The ML/FT risk attributed determine the frequency of the review of the financial intermediary (cf. EIF AML/CFT Procedures).	Personal data may be processed in relation to: - financial intermediary and shareholders and - Individuals (UBO and key persons), who are identified to be relevant for the proposed transaction.	Personal data stored in the g:/drive and eFront data base are the name, ID number, company registration number, date of birth, address, phone number, bank account number of the key person(s) or company(ies) involved in the EIF transactions;	The legal basis are the 4th and 5th AML directives requirements. EIF Statutes express the basic mission of EIF and decisions of its General Meeting and its Board of Directors. Furthermore, EIF acts as advisor to a variety of incorporated and non-incorporated third party mandates, to which the EIF due diligence process applies. The due diligence process is described in the procedures that apply to EIF transactions (cf. EIF AML/CFT Procedures).	The personal data are processed by: EIF staff members/consultants of a. transactional services, b. the Compliance Division, c. Risk and Portfolio Management, d. OIM, e. internal audit, and the Chief Executive and the Deputy Chief Executive and members of the Board of Directors of EIF. For specific due-diligence purposes, the aforementioned personal data may be shared with the EIB Group relevant services.	Any personal data collected and processed in the context herein will be retained by the EIF, as the case may be, for a maximum period of 5 years as from the date of the termination of the business relationship with the financial intermediary or the rejection of the application.	No transfers	Data is stored in corporate systems, which follows the EIF IT standards and are password protected in order to ensure security and data privacy.

Category		Title of the processing	Controller EIF / EIB	Processor	Purpose(s) of the processing	Category of Data subjects	Category of data	Legal basis	Recipients	Retention Period	Transfer to third countries or	Technical & Organizational Security Measures
2.3 - Compliance - Transactional	2.3.2	SAR-STR Reporting	Compliance	EIF	<p>The purpose of this SAR/STR procedure is to document roles and responsibilities between EIF COMPL and IG/IN, as well as the practical modalities (such as information flows) to be able to declare any potential case of ML/FT suspicions to the FIU without delay.</p> <p>A suspicious activity report or a suspicious transaction report is a document that EIF must file with the Luxembourgish FIU whenever there is a suspected case of money laundering, an associated predicate offences and/or financing of terrorism. These reports are tools to help monitor any activity/transaction within finance-related industries.</p>	<p>Personal data may be processed in relation to:</p> <ul style="list-style-type: none"> - EIF counterparties and their key persons - EIF employees 	<p>The MLRO should assess the activity or transaction deemed suspicious, he/she has the obligation to file a SAR or STR as soon as possible. The filing of a report is done through the registration of EIF in the "goAML system", which is a secured virtual platform used to submit SARs and STRs to the Luxembourgish FIU.</p> <p>An SAR/STR should include the following details:</p> <ul style="list-style-type: none"> - Personal data (name, ID number or company registration number, date of birth, address, telephone number, bank account number) of the person(s) or company(ies) involved in the suspicious transaction/activity; - The explanation, if any, given by the person or the company about the transaction/activity. 	<p>The Legal basis are the 4th and the 5th AML Directives requirements.</p>	<p>The personal data are processed by:</p> <ul style="list-style-type: none"> • EIF staff members/consultants of <ul style="list-style-type: none"> o transactional services, o the Compliance Division, o Risk and Portfolio Management, o MIBO, o internal audit, and the Chief Executive and the Deputy Chief Executive and members of the Board of Directors of EIF. For common counterparties, the aforementioned personal data may be shared with the EIB Group relevant services 	<p>Any personal data collected and processed in the context herein will be retained by the EIF, as the case may be, for a maximum period of 5 years as from the date of the termination of the business relationship with the financial intermediary or the rejection of the application.</p>	<p>No Transfers</p>	<p>Data is stored in corporate systems, which are password protected in order to ensure security and data privacy. A dedicated folder in M-files with restricted accesses shall be maintained by the FIU Officer to keep a copy of the communication/documents that may pertain to both the external and internal communication. The folder in M-files with restricted access shall also contain a register of cases. The difference with the register in M-files will include the name of the parties concerned, which is not stored on GoAML's register.</p>
	2.3.3	Register of Natural Persons (incl. PEPs)	Compliance	EIF	<p>EIF applies Enhanced Due Diligence in case the Relevant Counterparties following the analysis of Preliminary Integrity Questionnaire information. Criteria such as jurisdiction, entity type, listing or level of regulation are taken into account when determining the level of due diligence applied. Until automated Screening Tool is implemented, EIF COMPL has defined an enhanced manual monitoring process for Politically Exposed Persons. The update of the register is performed based on the results of the Preliminary Integrity Checks and the ongoing</p>	<p>Personal data may be processed in relation to:</p> <ul style="list-style-type: none"> - financial intermediary and shareholders and - Individuals (UBO, key persons, PEPs and Bas 	<p>Personal data stored in the g:/drive within the BA and Natural Persons registers and eFront data base are the name, ID number, date of birth, address, phone number. Identification data can also be data related to offences, public criminal records, investigation and prosecution, business relationships. An assessment is performed on a yearly basis at least on publicly available sources (World Check and Google search) and public sanctions lists (OFAC, EU) as BA and PEPs are under enhanced Due diligence process.</p>	<p>The legal basis are the 4th and 5th AML directives requirements. EIF Statutes express the basic mission of EIF and decisions of its General Meeting and its Board of Directors. Furthermore, EIF acts as advisor to a variety of incorporated and non-incorporated third party mandates, to which the EIF due diligence process applies. The due diligence process is described in the procedures that apply to EIF transactions (cf. EIF AML/CFT Procedures).</p>	<p>The personal data are processed by:</p> <ul style="list-style-type: none"> EIF staff members/consultants of <ul style="list-style-type: none"> a. transactional services, b. the Compliance Division, c. Risk and Portfolio Management, d. MIBO, e. internal audit, and the Chief Executive and the Deputy Chief Executive and members of the Board of Directors of EIF. For specific due-diligence purposes, the aforementioned personal data may be shared with the EIB Group relevant services. 		<p>Personal data collected, is, in principle, not disclosed to third parties with the exception of EIB IG/IN on the basis of a service level agreement pursuant to which IG/IN proceeds to internal and external investigations for EIF. For investigation purposes and under the terms and conditions of EIF investigations data may be transferred to OLAF.</p>	<p>Data is stored in corporate systems, which follows the EIF IT standards and are password protected in order to ensure security and data privacy</p>

Category		Title of the processing	Controller EIF / EIB	Processor	Purpose(s) of the processing	Category of Data subjects	Category of data	Legal basis	Recipients	Retention Period	Transfer to third countries or	Technical & Organizational Security Measures
3.1 - Corporate Governance - EIF Statutory Bodies	3.1.1	Audio recording of Board meetings	Governing Bodies	SEC	Audio recording of meetings of the EIF Board of Directors to support the minutes	Participants at meetings of the BoD	Electronic audio recordings of the meetings of the BoD	EIF Statutes, EIF Rules of Procedures, Decision of the EIF Board of Directors	Upon request, participants at meetings of the Board of Directors. Beyond meeting participants, disclosure of data only on the basis of a legitimate need	from the end of the Board meeting until the Board's approval and the signature of the minutes to which the recording relates	n/a	
	3.1.2	Audio recording of Audit Board sessions	Governing Bodies	EIF	Preparation of minutes of the corresponding meeting of the Audit Board	Participants of Audit Board meetings	Electronic audio recordings of the meetings of Audit Board	Audit Board Charter	Audit Board meetings participants	From the end of the Audit Board meeting until the Audit Board's approval and the signature of the minutes to which the recording relates	n/a	Recordings are accessible by the Head of the Governing Bodies Unit and Audit Board Liaison Officer, with strictly limited access to the Secretary of the Fund if necessary
	3.1.3	Authorised signatories of the EIF	Governing Bodies	EIF	Maintaining a list of authorised signatories as proof of the authority to sign correspondence and documents on behalf of the EIF and in connection with the EIF's activities	EIF staff members eligible for inclusion on the list of authorised signatories	Name, title (where relevant) and specimen signature of the eligible staff members. The GBU continues to maintain a full list of authorised signatories (per signature category), however the signature specimens are now stored by the Data Protection Officer	EIF Statutes (Article 21), Rules for Internal Authorisation and Signature, Rules for the Signature of Written Instruments	The list is accessible to EIF staff members and is also provided to third parties on request and on a confidential basis, solely for the purposes of the recipients' internal control procedures with respect to the EIF's authorised signatories.	Historical versions of the authorised signatories list will be stored for audit purposes for a period of up to 15 years.	Personal data may be transferred to recipients established outside of the European Economic Area to the extent adequate protection, equivalent to the standards of the Regulation (EU) 201 8/1 725, can be ascertained or adequate safeguards are applied	The list is maintained by the GBU. A secured pdf file is stored in M-Files with read-only access to EIF staff and made available on the EIF's intranet for business purposes. Signature specimens are stored by the DPO on the G-drive with restricted access only to the DPO office (Word documents for internal use and pdf password-protected files for external recipients) and are shared with authorised staff on request
	3.1.4	Confidentiality declarations by Board assisting persons	Governing Bodies	EIF	Administering access to information relating to the Board of Directors, including the Board Portal	Assisting persons to members and alternate members of the Board of Directors (applicable to individuals external to the EIB Group, not covered by common Group provisions)	Each individual designated as assisting person by a Board member is required to sign a confidentiality declaration which may contain their name, title, organisation, telephone number, email and signature	Audit recommendation (ref. IA-2017-EIF-01), Board of Directors Code of Conduct	As a general rule, the above-mentioned personal information is accessible to GBU staff for day to day administration of the EIF's governing bodies and for audit purposes. Contact details for access administration are disclosed to EIB Identity and Access Management.	The data will be stored by the GBU for audit purposes for a period of up to five years after the person's access to Board-related information has ceased		
	3.1.5	Personal information of Board and Audit Board members	Governing Bodies	EIF	<ul style="list-style-type: none"> As members of the EIF's governing bodies, and thus public figures, certain personal information of the members and alternate members (collectively the "members") of the Board of Directors and Audit Board is stored and processed by the GBU for corporate and legal purposes. Upon designation, each shareholder group provides the CV of their nominated member(s), which is annexed to the proposal for their appointment to the General Meeting. Upon taking function, each member is requested to return a signed Code of Conduct (which entails obligations during and after term of office) and personal declarations with details pertaining to the administration of access to information and remuneration. Subject to explicit authorisation from the individual, certain personal details are made available online on the EIF Board Portal or Audit Board Portals 	Members and alternate members of the Board of Directors and Audit Board.	<ul style="list-style-type: none"> CVs containing personal and professional details as disclosed by the individual Individual's name / title / organisation / email / telephone / signature / bank account 	EIF Statutes, EIF Rules of Procedure, Audit Board Charter, Policy for the remuneration of members and alternate members of the Board of Directors, Policy for the remuneration of Audit Board members. Where applicable, prior consent of the data subject according to Regulation (EU) 2018/1725 (Article 5.d).	<ul style="list-style-type: none"> As a general rule, the above-mentioned personal information is accessible to GBU staff for day to day administration of the EIF's governing bodies and for audit purposes. Accounting details for expenses processing are disclosed to Financial Control. Contact details for access administration are disclosed to EIB Identity and Access Management. Data authorised by the data subjects for publication on the Portals is accessible to other Portal users. Data authorised by the data subjects for publication on the EIF website is publicly available. 	<ul style="list-style-type: none"> Data made available on the Portals and the EIB website is removed with immediate effect following the member's departure from office. Personal declarations concerning access to information and remuneration shall be retained for audit purposes for a period of up to 10 years following the member's departure from office. The same approach shall apply to documents supporting expenses claims, in line with Financial Control retention period of invoices. CVs provided in nomination letters or annexed to General Meeting proposals shall be retained for corporate archiving purposes for a period of up to 15 years following the member's departure from office. Signed Codes of Conduct shall be retained for legal and corporate archiving purposes for a period of up to 15 years following the member's departure from office. 	The General Meeting includes representatives of financial institutions outside the European Economic Area. Therefore in this context some transfer of personal data outside the European Economic Area may occur as part of the General Meeting governance decision-making process	<ul style="list-style-type: none"> Paper originals of Codes of Conduct and personal declarations are stored by GBU staff in key-protected drawers at the EIF's premises. Electronic copies are stored on G-drive (GBU staff and Head of Compliance access only) and in the shared Secretary and Audit Board functional mailboxes (GBU staff and CIA assistant access only). Paper originals of nomination letters containing CVs are stored by GBU staff in key-protected drawers at the EIF's premises. Electronic copies are stored in the shared Secretary and Audit Board functional mailboxes (GBU staff and CIA assistant access only). Proposals submitted to the General Meeting are stored in M-Files with access to GBU M Files group and archived in the shared Secretary and Audit Board functional mailboxes (GBU staff and CIA assistant access only). The documents are also made available for information on the Portals, which are secure online platforms accessible by authorised users only (members of the Board and Audit Board, designated assisting persons and authorised EIF and EIB staff).
	3.1.6	Personal information of EIF shareholder representatives	Governing Bodies	EIF	<ul style="list-style-type: none"> Maintaining contacts database and distribution mailing lists for decision-making and information-sharing purposes with the representatives of the EIF shareholders. Maintaining proof of the signature authority of designated "official representatives" of the EIF shareholders with respect to the decision-making of the General Meeting. Maintaining voting registers (on the basis of submitted voting forms and powers of attorney where relevant) in connection with the decision-making 	Individuals designated by their respective institution as official representatives with voting authority with respect to the General Meeting and/or as points of contact for EIF shareholder-related matters.	Name, title, email, phone, address, signatures	EIF Statutes (Articles 10–12) and EIF Rules of Procedure (Chapter II)	<ul style="list-style-type: none"> As a general rule, the above-mentioned personal information is accessible to GBU staff for day to day administration of the EIF's governing bodies and for audit purposes. In addition, contact details are accessible internally to the Secretary General's office, the Corporate Relations team, and a limited number of other authorised EIF staff. Certain contact details may be accessible to other shareholder representatives in the General Meeting. 	<ul style="list-style-type: none"> Mailing lists are updated immediately upon receipt by the Secretary (Secretary@eif.org) of relevant changes. Personal data collected and processed in this context, including voting forms and powers of attorney submitted in the context of the General Meeting decision-making, shall be retained for a period of up to 5 years. 	The General Meeting includes representatives of financial institutions outside the European Economic Area. Therefore in this context some transfer of personal data outside the European Economic Area may occur as part of the General Meeting governance decision-making process, as well as in connection with shareholder-related communications and information exchanges	Shareholder information sheets and supporting information provided in hard copy are stored in key-protected drawers at the EIF's premises. Electronic copies are stored in the shared Secretary functional mailbox (GBU staff and CIA assistant access only). A shared contacts directory in the Secretary mailbox is accessible to GBU staff and a limited number of authorised EIF staff.
	3.1.7	EIF signature list for banking operations	Governing Bodies		Maintaining a list of authorised signatories and corresponding specimen signatures as proof of the authority to sign correspondence and	EIF staff members eligible for inclusion on the list of authorised signatures for banking operations	Name, title (where relevant) and specimen signature of the eligible staff members	Article 21 of the EIF Statutes and Rules of Signature for Written Instruments	The list is accessible to EIF Financial Control ("FC") and is also provided to third parties on request and on a confidential basis, solely for the purposes of the recipients' internal control procedures with respect to the EIF's authorised signatories	Historical versions of the authorised signatures list for banking operations will be stored for audit purposes for a period of up to 15 years	n/a	The list is maintained by the GBU and a secured pdf file is stored in M-Files with read-only access restricted to FC for business purposes
	3.1.8	Signature samples of Audit Board members	Governing Bodies		<ul style="list-style-type: none"> In the course of the mandate of a member of the Audit Board, each member shall be required to evidence their approval, with their signature, of certain reports and, when holding the position of Chair of the Audit Board, their approval of the minutes of Audit Board meetings. For practical purposes, when 	Members of the Audit Board	Individual's signature specimen	Prior consent of the data subject according to Regulation (EU) 2018/1725 (Article 5.d)	<ul style="list-style-type: none"> The signature specimens are accessible by GBU staff and CIA assistant. Documents containing the Audit Board members' signatures may be made available on the Audit Board Portal, in which case these documents are accessible to other Portal users. 	The individual's signature specimen is deleted immediately upon them leaving their position on the Audit Board or upon individual request of the respective Audit Board member	n/a	The signature samples are stored in M-Files with access restricted to GS/CIA/Govern. Bodies

Category		Title of the processing	Controller EIF / EIB	Processor	Purpose(s) of the processing	Category of Data subjects	Category of data	Legal basis	Recipients	Retention Period	Transfer to third countries or	Technical & Organizational Security Measures
	3.1.9	Storage/use/archiving of contractual and related documentation	General Secretariat	EIF	Storage/use/archiving of contractual and related documentation (online and offline)	i) in majority of cases, natural persons acting as legal representatives of EIF's counterparties, (ii) external consultants, (iii) other third party data subjects depending on contractual arrangements	Names, contact details and signatures of natural persons legally representing EIF's counterparties for the purposes of executing contracts/contractual documentation	Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract	EIF staff members and/or third parties such as EC, EIB and external advisors (depending on mandate and legal/regulatory requirements)	Depending on the specific legal/regulatory and mandate requirements. In principle up to 10 years following the end of the respective contractual relationship	n/a	Contractual and related documentation is stored on secure corporate drives and in DLM/Files where adequate access rights are properly set up to ensure strict confidentiality (if need be). Original documents are kept in dedicated cupboards/binders on EIF's premises and, in the case of electronic signatures, on EIF's secure corporate drives.
	3.1.10	E-signing project	Legal Services	IDnow	Providing selected EIF staff members and selected authorized signatories of EIF's clients with qualified electronic signature in order to sign contracts electronically following their identification via video transmission	Selected EIF staff members with authority to sign contracts on behalf of EIF. Selected authorized signatories of EIF's clients.	<ul style="list-style-type: none"> • Audio and video recordings of the persons to be identified • Surname, Name • Address • Phone number • E-mail address • Data of personal identity documents (in particular, passport number, type of identification document and the country which issued the document) 	Explicit consent captured through an ad hoc document to be signed by the concerned individuals	IDnow	The recordings will be kept for five years	n/a	If the reference to the data subject is not absolutely necessary for the result achievement, data analyses will be pseudonymised. All personal data transferred between the Ident Centre and the data centre are sent via IPsec VPN and additionally SSL encrypted. The network for processing identification data is physically separated from the network of the office. Data transfer to the Customer is always encrypted (TLS, SFTP, S/MIME). Data transfer between the user and IDnow during the identification process is also carried out in an encrypted form (TLS, DTLS for video). In this case, the encryption standard BSI TR 02102 "Cryptographic methods: Recommendations and Key Lengths" is used. The data are not sent physically.
	3.1.11	Due Diligence and Monitoring activities of Equity fund investments	EIG		Screening, Appraisal, Due Diligence of fund investment opportunities or Monitoring of existing funds, Fund Managers and Investee Companies	Investment team of the fund manager, CFO of fund manager, other LPs	Analysis of investment strategy, Team composition (CVs of Fund managers, title, age, tenure, office location; incentive schemes of current and previous funds, i.e. salary/bonus, shareholdings, team investment; FM track record and reputation), fund structure/governance	i) Public interest (art. 5.1.a) Regulation (EU) 2018/1725, ii) Contract with the counterparty, iii) EIF statutes	EIF staff, EIF board, IRC distribution list, AMUF/SDUF IRC, auditor, mandator	As per relevant mandate documentation (maximum data retention period 30 years)	Only in case of AMUF funds used: non-EU investors potentially based world-wide (Australia, Bahrain, Brunei, Kuwait, China / Hong Kong, Oman, Japan, Qatar, Korea, Saudi Arabia, Malaysia, UAE, New Zealand, Singapore, Kazakhstan, Taiwan, UK, Thailand)	Filing and confidentiality in line with internal procedure
	3.2.1	LMM Monitoring allocation	EIG	EIF	Process to propose for allocation of a monitoring team in EIF investees including nomination, dismissal or replacement of members of non-	EIF Staff members	Data collected is the name of LMM officers. Names are collected in order to identify the team member in charge of monitoring each EIF investee	Art. 2 of the EIF Statutes, Equity procedures	EIF internal services to the extent required	As per e-front, 20 years	n/a	Personal data relating to monitoring tasks are kept in the EIF transactional data base e-Front and are on a restricted access (LMM only) folder on the G drive
	3.2.2	Sharing of fund managers' quarterly reports with the Service provider	OIM	Numen Europe	Fund managers' quarterly reports are shared with the service provider (Numen Europe) that has been engaged by EIF to provide data input services	fund manager's team and portfolio company employees	Contact details, key men event triggered by personal situation e.g. new CEOs appointed, names of portfolio company employees engaged in criminal activities etc.	The outsourcing process is explained in OIM/DH/DI&V procedures.	Service provider (Numen Europe)	OIM/DH/DI&V stores contact details (name and business email address) of people responsible for reporting in the management company. These personal data are stored for a maximum period of 20 years.	Numen Europe stores reports received from EIF in its own application. Such reports are available to Numen team, based in Madagascar, which performs data input. In addition, Numen Madagascar is following up with fund managers for missing reports. Standard Contractual Clauses have been set up with the Service Provider in order to cover the transfer of data to a third country as foreseen by article 16(1)(f) of EUDPR	Collected data is stored in EIF system (eFront) which is password protected
	3.2.3	Tax reporting to fund managers	OIM		Purposes related to: Tax administration FATCA / CRS Withholding tax	Chief Executive of EIF, EIF employees that sign the relevant tax forms according to EIF's internal signature rules and similar individuals at EIF's mandators.	On an exceptional basis, this would include personal data such as name, national ID number, place of birth and date of birth of EIF's CE and the name and signature of two EIF employees that can sign the relevant tax forms according to EIF's internal signature rules. It could include similar information from EIF's mandators (e.g., name and signature on FATCA / CRS forms of mandators).	The legal basis for this processing is the public interest in line with the EIF's mission to "contribute to the pursuit of the objectives of the European Union" (Art. 2 of the EIF Statutes). I.e., the sharing of the data is meant for EIF and its counterparts to comply with applicable tax legislation.	Fund managers, external service providers and tax authorities (as applicable).	Time limits will differ from country to country and are mainly dependent on the type of distributions and applicable statute of limitations / audit rights of tax authorities. For a detailed overview of the applicable deletion date of the relevant tax documents, reference is made to the "document management" appendix in the following EIF procedures: <ul style="list-style-type: none"> - Tax administration procedure (M-Files ID 151336); - FATCA / CRS procedure (M-Files ID 151579); and - Withholding tax procedure (M-Files ID 152001). The relevant appendixes of the three tax procedures (as approved in October 2019 and subject to review) have been copied at the end of this document.	Tax related information might be shared with i.a. fund managers, mandators and FoF investors. This includes organizations such as the European Commission and the EIB. Moreover, information might need to be shared with tax authorities outside of the EU (e.g., U.S., Norway, Switzerland, U.K. and Israel).	Tax related information is typically only accessible to the relevant teams within EIF. This can vary on a case-by-case basis but typically that would include LS, OIM-TMT (Operational tax) and EI. Appropriate restrictions are typically applied when filing tax related information in MFiles and the EIF-VC-Administration mail folder

Category		Title of the processing	Controller EIF / EIB	Processor	Purpose(s) of the processing	Category of Data subjects	Category of data	Legal basis	Recipients	Retention Period	Transfer to third countries or	Technical & Organizational Security Measures
3.2 - Corporate Governance - MIBO & Other	3.2.4	KYC Process	FOBS / KYC Unit		The personal data referred to herein will be collected for the purpose of implementing the “Know-Your-Customer” process in compliance with the Directive (EU) 2018/843 of the European Parliament and Council of 30 May 2018 amending Directive (EU) 2015/849 (“AML Directive”) on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, as amended and supplemented from time to time	Personal data may be processed in relation to: - legal representatives of the respective applicant, financial intermediary and/or - individuals, who are identified to be instrumental for the commercial success of the proposed transaction or otherwise described as key persons of the relevant counterparty	The personal data comprise essential information on the identity, address, the professional education and curriculum vitae, as such data are provided by the Data Subject. Such data may be completed by publicly (media) available information	The legal basis for this processing is the AML Directive, based on the requirement “compliance with a legal obligation to which the controller is subject” in accordance with Article 5.1.(b) of the Regulation (EU) 2018/1725	The aforementioned personal data will be processed only by the EIF relevant services and may also be shared with the European Investment Bank in case of a common counterparty in line with the Addendum to the Convention between the European investment Bank and the European Investment Fund on the exchange of information and documents of 14 April 2020, or with other mandators (e.g. European Commission) under relevant audits and controls.	Any personal data collected and processed in the context herein will be retained by the EIF, as the case may be, for a maximum period of 5 years as from the date of the termination of the business relationship with the financial intermediary or the rejection of the application without prejudice to any other (legal) document retention requirements EIF is subject to	Personal data may be transferred to EIF, EIB, Mandators/funding providers established outside of the European Economic Area to the extent adequate protection equivalent to the standards of the Regulation (EU) 2018/1725 can be ascertained.	Data is stored in corporate systems, which are password protected in order to ensure security and data privacy
	3.2.5	The Bench Website	EIG		EIG is planning to launch a new website “The Bench” which will collect from the users their emails for login and IP addresses for traffic check. EIF	emails and IP addresses of the users of the platform	emails and IP addresses of the users of the platform. The emails are needed as those are the logins, and the IP addresses are to check compliance with the not sharing logins policy.	consent by the user of the “term of use” as a pop up at first login.	EIF business owner of the digital platform only. This is solely to manage logins and ensure not sharing of logins.	as long as the user has an active account.	n/a	the logins and IP addresses will be kept in a secure protected location.
	3.2.6	EIF-NPI Equity Platform Survey	MM		Facilitate administration of EIF-NPI Equity Platform Secretariat correspondence on certain topics	Data subjects are professionals and other individuals acting as contact persons of NPIs and NPBs, the European Commission, and any other relevant stakeholders	Contact person data (name, surname, e-mail) is required to facilitate follow-up on routine administrative or logistics queries concerning meetings of the platform and/or occasional surveys of Platform members related to NPI business/operational activity and/or opinions concerning the workings of the Platform	The legal basis for this processing is the consent expressed by the Data Subjects	the European Commission, or other relevant stakeholders formally associated with the Platform as members or as guest participants/contributors/observers	Data Subjects’ personal data will be retained up to ten (10) years after the termination of each processing operation	Could occur if other future Aligned Members join which are associated with third countries outside the EU (e.g. Innovation Israel) or international organisations (e.g. Black Sea Trade and Development Bank). At present no aligned members are associated with third countries (outside the EEA). According to the current terms of the Charter, full NPI members must necessarily be from EU Member States	Link to the survey will be sent through a dedicated EIF-NPI Equity Platform outbox in Outlook which is routinely used
	3.2.7	EU Microfinance Platform FCP	MM		Responsibilities linked to tasks related to the role of EIF as the Management Company of the FCP.	Members and Observers of the Decision Making Bodies of the FCP (General meeting of investors, Sub fund(s) meeting of Investors)	Name and Surname, professional address, role, date of designation, date of resignation/ replacement, justification for replacement or resignation, attendance(s) in meetings, minutes; recording of meetings (audio and/ or video)	In accordance with the Article 5(1)(c) of the Regulation 2018/1725, processing is necessary for the performance of a contract to which the data subject is party	“Unitholders” of the FCP and/or “Lenders” in the Facility, internal EIF officers part of the secretariat, EIB, auditor of the Facility, internal and external Auditors (where required by Law or Regulatory Reason, (e.g. by the European Court of Auditors or by OLAF, CSSF etc.), and Ernest & Young, the appointed service provider fro compliance with GPDR.	Personal data are kept up to 15 years after the expiration of the agreement	No transfer to third countries	Personal data flag is marked in Miles, documents intended for internal (corporate) use, general retention EIF policy applies.
	3.2.8	M-Files	OIM		M-Files is the content management platform that encompasses the management of the complete lifecycle of EIF corporate documents. The purpose of processing personal data is determined by the type and content of each document stored in the platform falling under the responsibility of the document originator/owner.	Nearly any personal data subject that may be covered by an official/corporate EIF document. In addition, all the user administration may contain personal data.	The most common refer to: • Name; • Surname; • Professional email address; • Phone number; • Date of birth; (CVs/Passports should be included as separate documents)	Framework Agreement	EIF internal services. Exceptionally the access to specific documents may be granted to admin users for well-defined interventions upon authorization from the EIF controlling service.	20 years as a principle, however there is an ongoing initiative trying to reach a comprehensive retention plan/schedule for EIF records (focused on documents).	Services are provided by M-Files in other regions than EU to ensure 24/7 support. This is governed by the framework agreement and in particular the “clauses for personal data transfer processors” according to Article 26(2) of Directive 95/46/EC.	Several certifications in the domain of information security (ISO 27001/27002, SOC 1/SSAE 16, SOC 2, amongst other). Data centres (primary and secondary) are located in the EU (Western Europe). File storage and database are encrypted at rest through AES-256 and Transparent Database Encryption respectively. Network connections are encrypted, client-server connections use SHA-256 encryption. Access to the application will be limited to listed fixed IP addresses after 31/03/2019.
	3.2.9	Tableau	OIM		Data visualisation and dashboard platform based on Tableau to cover EIF dashboards and reporting needs. The platform is fed with data available in source application in eFront and SAS.	• Counter parties • Legal representative of counterparties	• Name • Surname • Email	The legal basis for this processing is the public interest pursued by the OIM Department supporting EIF’s mission to “contribute to the pursuit of the objectives of the European Union” (Art. 2 of the EIF Statutes)	n/a	20 years as a principle, however there is an ongoing initiative trying to reach a comprehensive retention plan/schedule for EIF records (focused on documents).	n/a	Data and services are kept with EU. Data is encrypted at rest and during transit. The application access is limited to a limited number of fixed IP addresses approved by EIF. Access to the application is protected by strong password method or 2-factor authentication process.
	3.2.10	SAS	OIM		Analytical platform on SAS used to monitor Guarantees deals underlying portfolios and third-parties mandates treasury	• Counter parties • Legal representative of counterparties	• Name • Surname • Email	The legal basis for this processing is the public interest pursued by the OIM Department supporting EIF’s mission to “contribute to the pursuit of the objectives of the European Union” (Art. 2 of the EIF Statutes)	n/a	20 years as a principle, however there is an ongoing initiative trying to reach a comprehensive retention plan/schedule for EIF records (focused on documents).	n/a	Data and services are kept with EU. Data is encrypted at rest and during transit. The application access is limited to a limited number of fixed IP addresses approved by EIF. Access to the application is protected by strong password method or 2-factor authentication process. Access to the application is limited to some listed fixed IP addresses after validation of EIF.

Category		Title of the processing	Controller EIF / EIB	Processor	Purpose(s) of the processing	Category of Data subjects	Category of data	Legal basis	Recipients	Retention Period	Transfer to third countries or	Technical & Organizational Security Measures
	3.2.11	e-Front	OIM		It is reminded that the scope, in term of data to be considered, is related to any data allowing to identify a living natural person, such email, lastname, firstname, ... In respect with the above, eFront is storing personal data in the context of : • Customer Relation Management (CRM) • Compliance/KYC • Portfolio input and inclusion • Reporting to mandators • Users administration	Data concerned are linked to : • EIF counter-parties, as legal representatives • EIF sub-contractors staff as eFront users • EIF staff as eFront users	• Contacts: salutation, first name, last name, date of birth, nationality(ies), Phone number (including mobile), email addresses, standard mail addresses, social network • Users: salutation, first name, last name, professional email	The legal basis for this processing is the public interest pursued by the OIM Department supporting EIF's mission to "contribute to the pursuit of the objectives of the European Union" (Art. 2 of the EIF Statutes)	Personal data captured within eFront are disclosed to EIF internal services only	20 years as a principle, however there is an ongoing initiative trying to reach a comprehensive retention plan/schedule for EIF records (focused on documents).	Data are currently transferred to eFront d.o.o. Beograd, in the context of processing activities for Maintenance and Support purposes, as well as for the purposes of occasionally providing Professional Services. This transfer is covered through suitable SCC eFront{EIF_Standard Contractual Clauses.docx (Desktop, Web, Mobile). Another transfer to Numen Madagascar – SA, in the context of processing NAV and portfolio input, is currently being studied.	Data and services are kept with EU. Data is encrypted at rest and during transit. The application access is limited to a limited number of fixed IP addresses approved by EIF. Access to the application is protected by strong password method or 2-factor authentication process.
	3.2.12	Processing of Final Recipients' Personal Data for monitoring purposes	OIM		In order to monitor that the deployment of the EIF Products is made by the financial intermediaries towards eligible final recipients in accordance with the applicable investment strategy, EIF may performs certain monitoring activities in the context of which personal data of sampled final recipients are collected and processed.	Final recipients, i.e. individuals benefitting from EIF financial guarantees or other debt instruments provided to financial intermediaries ("EIF Products"), are the data subjects whose personal data may be shared by the financial intermediaries with (i) the EIF, (ii) its mandators/funding providers, (iii) EIF's outsourcers and service providers and (iv) external auditors having the right to control the use of funds within EIF Products in accordance with applicable legal and/or contractual base.	The referred personal data include the name, address and other personal data of the final recipients collected by the financial intermediaries and transmitted to the EIF. Such personal data are collected by EIF within the ongoing reports provided by the financial intermediaries to EIF and/or within the exchange of the contractual and/or supporting documentation related to the transaction signed between the financial intermediaries and the final recipients (loan/lease/guarantee, including any relevant application forms, self-declaration, documents used for credit assessment purposes and all documentation exchanged between the financial intermediaries and the final recipients) in the context of the deployment by the financial intermediaries of the EIF Products.	The legal bases for this processing include: -Article 5(1)(a) of the Regulation, pursuant to which processing is necessary for the performance of a task carried out by the controller in the public interest; -Article 2 of the EIF Statutes, which obliges the EIF to "contribute to the pursuit of the objectives of the European Union". In pursuing its statutory objectives, the EIF provides financial guarantees or other debt instruments or equity investments to financial intermediaries for the final benefit of f inal 7/22/2020 recipients. In this context, the EIF - has developed a framework of policies, published on its website1, which provide general guidance to EIF transactions; -is entrusted with a variety of mandates from third parties, i.e. mandators/funding providers, which may contain specific policy guidelines to the transactions funded out of such mandates.	The aforementioned personal data are processed by the EIF relevant services and may also be shared with the European Investment Bank, the EIF mandators/funding providers, EIF outsources/service providers and external auditors having the right to control the use of funds within EIF Products in accordance with applicable legal and/or contractual base.	Any personal data collected and processed in the context herein may be retained by the EIF for a maximum period of seven years following the end of the implementation period of the mandate or termination of the agreement concluded by the EIF with the financial intermediary or the agreement concluded by the financial intermediary with the final recipient or the closure of operations under the mandate, as applicable.	Personal data may be transferred to third Countries in compliance with the Regulation, i.e. upon adoption of appropriate safeguards such as standard contractual clauses	Personal data are stored in corporate systems, which are password protected in order to ensure security and data privacy
4.1 - Legal Department	4.1.1	Publication of EIF Working Papers on EIF's website (and elsewhere)	RMA		Publishing EIF Working Papers on EIF's website (and elsewhere)	EIF staff members/consultants/other co-authors of EIF Working Papers	Names, photos, email addresses, telephone numbers and job titles	The legal basis for this processing is the public interest pursued by the RMA Division supporting EIF's mission to "contribute to the pursuit of the objectives of the European Union" (Art. 2 of the EIF Statutes).	General public (documents are publicly available)	Considering the nature of the means used, the data will be kept until a potential request from the concerned data subject "to be forgotten" (Ar. 19 of Regulation (EU) N° 2018/1725)	n/a	Pictures are stored on the g-drive, in the section accessible only to RMA.
	4.1.2	Distribution list of subscribers to EIF Working Papers	RMA		Distribution of RMA's publications to subscribers	Natural persons – subscribers to the mailing list for RMA's publications	Names, email addresses	The legal basis for this processing is the public interest pursued by the RMA Division supporting EIF's mission to "contribute to the pursuit of the objectives of the European Union" (Art. 2 of the EIF Statutes).	None	The distribution list is kept for 10 years and at the end of this period it is subject to review	n/a	The data is stored in M-files with restricted access to RMA team.
	4.1.3	Event Organization	Marketing		Registration to EIF events	Participants (natural persons) attending events	Name, Company/organisation name and geographical location, Position, E-mail address	The legal basis for this processing is the consent expressed by the Data Subjects	The aforementioned personal data will be processed by the Marketing Division and/or any other EIF Divisions in charge of organising the event and also by service providers in charge of providing event related services such as e-mail campaign systems (e.g. mailjet), app developers, event agencies and organisers.	Up to 10 years after the end of the event	n/a	The list of attendees is uploaded in M-files with restricted access to Marketing Division and EIG users
	4.1.4	Video & written case-studies	Marketing		Development of case-studies in written or video format	Natural persons representing Small Medium Enterprises ("SMEs")	Name, email address, telephone number (contact details) & potentially photos (used in order to contact the SMEs and conduct a telephone interview to develop the case-study story)	Consent of the concerned data subjects (Article 5.d of Regulation 2018/1725)	Contact details are not passed on to any recipients out of the EIF. Photos are passed on to the EIB and EC with the consent of the SME, who agrees by email	10 years	n/a	Data is stored on secure corporate drives and processing is done through secure, password-protected internal communication channels. Both are secured by password-protected access limited only to EIF staff
	4.1.5	Print material	Marketing		Development of print material for marketing purposes	Natural persons representing SMEs/public authorities/contractors, EIF staff members	Images (photos) and occasionally names	Consent of the concerned data subjects (Article 5.d of Regulation 2018/1725)	General public (documentation is publicly available)	10 years	n/a	Data is stored on secure corporate drives and processing is done through secure, password-protected internal communication channels. Both are secured by password-protected access limited only to EIF staff.
	4.1.6	Social Media	Marketing		Posting on social media (Youtube, Instagram, LinkedIn, Facebook, Twitter etc) for marketing purposes	Natural person representing SMEs/public authorities, EIF staff members	Images (photos), videos and occasionally names	The legal basis for this processing is the consent expressed by the Data Subjects	General public	Considering the nature of the means used, the data will be kept until a potential request from the concerned data subject "to be forgotten" (Ar. 19 of Regulation (EU) N° 2018/1725)	n/a	Security measures adopted by providers/platforms selected from time to time

Category		Title of the processing	Controller EIF / EIB	Processor	Purpose(s) of the processing	Category of Data subjects	Category of data	Legal basis	Recipients	Retention Period	Transfer to third countries or	Technical & Organizational Security Measures
	4.1.7	Management of EIF Infodesk	Marketing, on a basis of the EIB-SLA Framework Agreement (Chapter III)		Responding to the public inquiries submitted through the online form on EIF's website	General public (natural persons using the EIF contact form)	Name, contact details	f) The legal basis for this processing is the consent expressed by the Data Subjects	EIF Marketing team, EIB Infodesk	10 years	n/a	Data is stored on secure corporate drives and processing is done through secure, password-protected internal communication channels. Both are secured by password-protected access limited only to EIF staff

Category		Title of the processing	Controller EIF / EIB	Processor	Purpose(s) of the processing	Category of Data subjects	Category of data	Legal basis	Recipients	Retention Period	Transfer to third countries or	Technical & Organizational Security Measures
5.1 - Finance & Accounting - HR Payment Processes	5.1.1	Procurement	SPA	EIF	The personal data referred to herein may be collected with a view to evaluate the tenderers/candidates and their offers with regard to the exclusion, selection and award criteria in the context of the relevant procurement procedure.	Natural person(s) as: • potential freelancing provider(s) of services or supplies; • team member(s) proposed by legal persons acting as potential providers of services or supplies, in the context of their tender; • legal representatives of the tenderers/candidates and/or • individuals in the context of the tender process for individual external advice	Name, telephone, e-mail address Passport or ID (in case of freelancing) Technical and professional ability, incl. qualifications, experience and academic background (CV) Evidence of fiscal status or otherwise commercial registration, incl. bank account Fiscal and social security obligations, absence of bankruptcy, fraud, conflict of interest Evidence of recent turnover Extract from the judicial record	Directive 2014/24/EU being the legal basis of the EIF Procurement Guide EIF Statutes	EIF Procurement Officer, EIF staff members evaluating the tenders, Compliance officers, Legal officers, Auditors and EIF Management	No more than 5 years following the termination of (i) the contract for the successful tenderers and (ii) the award procedure for the unsuccessful tenderers. The extracts from the judicial records will be kept up to two years after the accomplishment of the particular procedure.	n/a	Hard copies are stored in locked cupboards with limited access Electronic copies are stored on a Data Management system, where the access rights are limited to the staff members listed under section f) above
	5.1.2	External Banking Operations	Financial Control		Collect and transfer personal data of employees of Financial Control Division for the purpose of opening of bank accounts	Employees of Financial Control Division who in course of their duties have to get access to the bank accounts to view account movements or to manage bank accounts(input or sign payment instructions)	* Full name * Nationality * Date of birth * ID or passport number * Other ID or passport data (because copy of document is provided) * Residential address * Marital status Tax ID number Position in EIF * Business Email * Office Telephone number	The legal basis for this processing is Article 2 of the EIF Statutes, which obliges EIF to "contribute to the pursuit of the objectives of the European Union". Article 5(b) of the Regulation (EU) 2018/1725	Relevant staff of the Financial Institutions with which EIF requests to open accounts	Personal data (pdf files of copies of ID) is kept on file as long as the person is employed by EIF Then files are deleted within one month from the departure of the data subject.	n/a	Electronic copies of the collected personal data are saved in dedicated folders accessible only by authorized staff of the Financial Control Division. Paper versions are not stored. If signed paper copies of IDs are required to be sent to the Financial Institutions they are sent by registered mail of DHL directly addressed to the authorized person in the Financial Institutions.
	5.1.3	Recording of ALC Meetings	Financial Control		Audio recording of the meeting in order to facilitate the drafting of the minutes	ALC Members. Only voice recording, members don't mention their names when intervening.	Audio file	The legal basis for this processing is the consent expressed by the Data Subjects	Only ALC coordinator and Liquidity Management Unit	1 Year	n/a	Audio recording file is provided to ALC Coordinator and saved in our G drive with access to limited staff.
	5.1.4	Missions Expenses supporting documents submitted for reimbursement	Financial Control		Reimbursement of mission expenses is done upon presentation of relevant supporting documents (hotel invoice, airfare, taxi receipts etc.)	EIF employees	i. Travel Authorization : Employee ID, description of mission, business purpose, expense type, service provider, amount, total authorized amount, location, status of approval, comments on trip ii. Expense Report: Employee ID, description of mission, business purpose, expense type, transaction amount, payment type, exchange rate, total amount, location, description, other additional information iii. Hotel invoice iv. Boarding pass v. Taxi/train receipts vi. Parking receipt vii. Tolls receipts viii. Bank / credit statements ix. Training/conference programmes x. Derogation(s) xi. Other documents	i. Travel policy ii. FC mission expenses procedure	i. EIF and EIB employees who are involved in processing and payment of travel expenses	30 years	n.a,	• Automated processing via PPSofT application • Manual processing – scanning the expense report by Scanning team, control of the file before payment
	5.1.5	Membership fees supporting documents submitted for reimbursement	Financial Control		Reimbursement of membership fees is done upon presentation of relevant supporting documents (reimbursement form, proof of payment)	EIF employees	Reimbursement form including staff name, bank account details, description of payment, receipt of payment	FC internal procedures	EIF employees, EIB employees (Scanning team)	30 years	n.a,	Automated processing via PPSofT application Manual processing – scanning the Reimbursement by Scanning team, control of the file before payment
	5.1.6	Timesheet	Financial Control	EIF	The timesheet collection is strictly aimed at the computation of EIF mandates' profitability, namely the allocation of staff costs in the interest of the EIF and its Mandators, and the collection of data for invoicing purposes. The Timesheet tool has been developed by EIB through PeopleSoft HR and is hosted on premises. Data saved in PeopleSoft HR systems (i.e. Time Management) are used to populate the timesheets entry page and facilitate staff's input. This includes worked-hours (for clockers staff members) and off days (the "OFF" labels is covering all kinds of leaves)	All staff with EIF indefinite or fixed term contracts will be requested to submit their timesheet, excluding administrative assistants who may opt-out and temporary workforce such as consultants, trainees, temps.	first name, last name, employee ID, hours allocated to any specific mandate/activity, "off" days.	Public interest (art. 5.1.a) Regulation (EU) 2018/1725.	SPA and timesheet approvers (for invoice-related timesheets only). On an aggregated basis (provided that no identification per person is possible), data may be shared with management, PMC members, relevant mandate managers and all staff.	The same retention policy as per Time Management data applies. The current timesheet tool used at EIB has a 15+ years retention.	n/a	AAAll data are saved in PeopleSoft, same security measures apply as MyPortal, i.e. EIB Group credentials (User ID and password). Data aggregation takes place in Tableau Prep. Processing will happen in a secured folder of the G:\ drive.

Category		Title of the processing	Controller EIF / EIB	Processor	Purpose(s) of the processing	Category of Data subjects	Category of data	Legal basis	Recipients	Retention Period	Transfer to third countries or	Technical & Organizational Security Measures
6.1 RM - Information Security		Information Security	Risk Management		Processing of EIF user data for the purpose of executing security risk assessments, conducting awareness campaigns, and identifying, analysing and remediating information security incidents. Security incidents may fall into any of the following categories: 1) information or cyber security incidents 2) non-compliance with information security regulations (internal & external) 3) security testing, and 4) results of security awareness campaigns. Furthermore, the data is processed to allow evaluations of the effectiveness of the EIF information security controls framework and to perform required risk reporting to EIF (senior) management and information security governing bodies.	EIF users which comprise Chief Executive, Deputy Chief Executive, staff members, irrespective of rank of functional role in the organization as well as external users working on behalf of EIF, such as interns, contractors, and consultants						
	6.1.1							1. EIF user names 2. EIF user contact details such as business email and business phone number 3. EIF user functional/ organization association 4. EIF user data specific and relevant to the security incident	Article 5.1(b) Compliance with a legal obligation: EIF Statutes Article 2.3 – Tasks and Activities – The activities of the Fund shall be based on sound banking principles(...)	The gathered personal data will solely be used by the EIF ISO function for the purpose(s) described above. Whenever possible, EIF user data will be processed in aggregated form, to prevent identification of individuals, e.g. for information security reporting	The personal data will be stored for a maximum of 5 years, to allow for year-to-year comparison of security incidents, performance, or compliance involving EIF users. After this period, only aggregated statistical data will be retained and the individual data records will be deleted.	No transfer of EIF user data to third countries or international organisations.