| Category | | Title of the processing operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | 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<br>Service Level Agreement EIF - EIB | EIF HR Staff<br>EIB HR Staff<br>Chief Executive and Deputy Chief Executive<br>Members of Selection Panel<br>Requesters | *Electronic application: indefinitely (for statistical and resource planning purposes)<br>*Application after first selection: 2 years<br>*Psychological tests: 18 months | n/a | Access to applicants' personal data is restricted exclusively to HR Staff, requesters and members of the selection panel<br>IT access to applicants' personal data restricted to HR Staff<br>Personal data communicated outside HR for recruitment purposes is |
| | 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) | interim staff, trainees, students for summer jobs, secondees | Name etc, CVs and similar data | EIF Statutes, Staff Rules and Staff Regulations<br>HR Manual of Procedures<br>SLA EIF - EIB<br>EIB guidelines for in-house training, Luxembourg law (for interim staff) | EIF HR Staff<br>EIB HR Staff<br>Chief Executive and Deputy Chief Executive<br>Requesters | Data is retained for the periods indicated below following departure:<br>*Trainees: (paper files) three years (for reasons of establishing working certificates): indefinite for statistical purposes in PeopleSoft | n/a | Access to applicants' personal data is restricted exclusively to HR Staff, requesters and interviewers during selection process.<br>IT access to applicants' personal data restricted to HR Staff<br>Personal data communicated outside HR for recruitment purposes is |
| | 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<br>Hiring managers and EIF HR staff within the hiring team | All candidates for interim positions<br>20-Oct-20<br>- Curriculum vitae (that contains only name and surname). Purpose: To identify the most suitable interim staff via Beeline.<br>2) Selected interim staff<br>- "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<br>- 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<br>3) Hiring managers and/or HR Staff<br>Last name, first name, department, role in Beeline<br>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 | 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.<br>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.<br>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.<br>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.<br>4) Satisfaction surveys: EIF HR Staff dedicated to the administration of interim | Personal data of all candidates (selected and non-selected): 3 years in Beeline and GED<br>Paper documents related to the interim staff recruitment campaign are destroyed at the end of the selection process.<br>"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.<br>20-Oct-20<br>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.<br>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.<br>ManpowerGroup Solution teams servicing EIF off-site are located in Brussels and Woluwe (Belgium).<br>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.<br>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** | | EIF | Collect, analyse and process applications for the EIF GRAD Programme, as part of the EIF e-recruitment process.<br>The GRAD Programme aims to offer new and recently qualified graduates the opportunity to acquire professional | Applicants to the EIF GRAD Programme | During the online application process the candidate will upload the following personal data:<br>□ Personal data: name, first name, date and place of birth, nationality and second nationality (if applicable), | 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 | 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 |
| | 1.1.5 | **Recruitment of Trainees** | | EIF | Recruitment of trainees as part of the EIF internship programme | Candidates applying for EIF internship programme and selected candidates | During online application: :<br>• name, first name, date and place of birth, nationality (ies), gender, contact details<br>• Qualifications<br>For selected candidates:<br>• traineeship contract, copy of the passport, copy of the last | 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 operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | 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 possible to invite EIB colleagues to participate as panel members. | Internal and external candidates | The application form, and CV of external candidates, are circulated to the panel members. The application form contains the following data:<br>• Personal data: first name, date and place of birth, nationality (and second nationality if applicable), gender, contact details (telephone, email, address)<br>• Qualifications: higher education and professional qualifications<br>• Professional experience: current and former employers, date of employment, description of key responsibilities<br>The recruitment panel members take notes on the individual candidates and complete a scoring sheet which is returned to EIF HR. | • Compliance with EIF Statutes, Staff Rules and Staff Regulations, EIF HR Manual of Procedures, EIB Group "Guidelines on Internal Mobility and Promotions".<br>• 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. | 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.<br>In terms of the candidates other documentation, the retention is as follows:<br>• Motivation letters of candidates are kept in PeopleSoft for the entire period of employment of the applicants.<br>• External candidates: on-line data is retained indefinitely for statistical purposes.<br>• Personality tests: 18 months<br>• Candidates' electronic profile : 3 years from application date for each application<br>• Statistical data (such as number/nationality/gender split of applications per recruitment campaign) are retained indefinitely. | n/a | 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.<br>IT access to applicants' personal data is restricted to HR Staff, the panel members do not have access to the HR IT system.<br>Personal data communicated outside HR for recruitment purposes is destroyed immediately following the closure of the selection process |

| Category | | Title of the processing operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | Technical & Organizational Security Measures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1.2 - Human Resources - Evaluation and | 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 | All new EIF recruits subject to a probationary period, as stipulated in their letter of appointment | Individual online probation documents, with the following sections:<br>o Staff Member Information<br>• First name<br>• Last name<br>• Middle name<br>• Job Title (Generic Role title) | 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), | Probation documents are stored electronically and may be printed if required.<br>After decision by the Head of Human and Resources Management of EIF regarding the confirmation, extension, or non-confirmation of | 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 | Article 22 of the EIF Staff Regulations<br>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 |
| 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).<br>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).<br>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).<br>To allow EIF HR to review the presence and absence of EIF | 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:<br>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).<br>Time event data visible in TiM and Peoplesoft Absence & Time Management<br>□ 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.<br>□ 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.<br>□ Staff member’s requests for parental leave.<br>□ Registration of automatic and | EIF Staff Regulations Articles 25-28, 30 and 31<br>EIF Staff Rules chapters 3 to 5 and Annex VI concerning part-time working arrangements<br>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 | 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).<br>21 October 2020<br>A staff member may correct their time registration data for the current month and those going back over the past 12 months.<br>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.<br>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:<br>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.<br>PeopleSoft also leaves an audit trail recording all actions on data.<br>Data is stored in Oracle 12c database.<br>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 operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | Technical & Organizational Security Measures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1.3 - Human | 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.<br>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.<br>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.<br>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.<br>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.<br>In the above cases, the disclosure will be done in the presence of a representative from EIF HR and the EIF DPO.<br><br>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:<br>- Personal electronic data kept 3 months before deletion<br>- Personal belongings/physical data may be retrieved within 1 month<br>b) in the event of death:<br>- Close relatives may request to retrieve any personal physical data or personal electronic data within 3 months following the death.<br>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.<br>The assistance of EIB IT-SEC may be requested to access electronic documentation in order to separate professional/personal electronic data.<br>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'.<br>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 operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | 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<br>Date at which the relevant sanction is enforced<br>Details of the incident leading to the sanction<br>Term of sanction | EIF Staff Regulations (Art. 38)<br>Service Level Agreement EIF - EIB for HR administrative measures | EIF HR Staff<br>EIF Compliance<br>EIF Legal Services<br>EIF Board of Directors<br>EIB Personnel Staff | Personal data concerning sanctions is retained until termination of the employment contract.<br>information remains part of the personal file of the staff member concerned | n/a | Access to personal data is restricted exclusively to HR Staff.<br>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<br>2) EIF Dignity at Work policy<br>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 Resourc | 1.5.1 | **Accident Insurance** | HR | Third party provider<br>----------<br>EIF | Processing of insurance claims linked to: *the accident of an EIF staff member or family member<br>*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<br>*Data related to luggage | EIF Insurance contracts | Insurers, medical examiners | Five years in central EIB Group archives | n/a | Information and personal data is known, nanaged and filed by the specific responsible for the relevant file |

| Category | | Title of the processing operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | Technical & Organizational Security Measures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 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".<br>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.<br>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 operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | 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.<br>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<br>training courses | EIF HR extract lists of registered participants per training course (including the name and<br>date of the training course, with a full list of the name and first name of participants) and signatures are gathered to document attendance.<br>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<br>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<br>& Development Portfolio) | The Chief Executive, Deputy Chief Executive, Compliance Department, HR and linemanagers.<br>Data subjects may request proof of attendance to training sessions. For example, staff<br>members may need to provide such information to external companies (ACCA, CFA etc.)<br>when they are required to attend a certain amount of courses per year to adhere to their<br>membership rules.<br>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<br>is no longer an active member of staff.<br>The attendance lists for registered participants are retained as per the established retention<br>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;<br><br>- 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 | 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).<br>Participation is voluntary and anonymity guaranteed by secure data processing. In particular:<br>- 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<br>- survey outputs: survey answers and results will be anonymous and it will not be possible for | Personal data shared with PwC/Qualtrics: first name, last name and recipients' e-mail addresses<br><br>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.<br><br>Art. 23 from Rules of Procedure of the EIF.<br><br>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. | • 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.<br>• 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.<br>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:<br>• 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 | 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<br><br>Separation of security functions: 1) EIB Group - ITadministrator 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.<br>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, and has legal responsibility to do so, and 3) |

| Category | | Title of the processing operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | Technical & Organizational Security Measures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1.6.3 | **Recruitment Tools** | | External providers: Le consortium "Deloitte Tax & Consulting sàrl et SHL Belgium sa" | Using state of the art tools throughout:<br>• Recruitment process for external and internal candidates in addition to standard selection tools (such as interviews and professional tests)<br>• Development Centres for EIF staff members<br>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:<br>• Internal and external candidates may be subject to psychometric tests and filling the personality questionnaire.<br>• EIF staff members identified for Development Centres may be subject to psychometric tests and filling the personality questionnaire.<br>To be sent to Deloitte Tax & Consulting sàrl:<br>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).<br>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 | • Relevant staff at the service providers,<br>• Recruiters, assistants and managers/panel members participating in the recruitment processes, other HR staff members when managing Development Centres,<br>• 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.<br>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. |
| | 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:<br>□ They are not Luxembourg nationals<br>□ They reside in Luxembourg (a hotel address is not acceptable)<br>□ They do not already hold a Luxembourg residency permit (an attestation d'enregistrement) 21-Oct-20<br>□ For a partner/spouse or dependent child – they are registered at the same address as the staff member, and | □ Employer name and type of Institution (Embassy or EU Institution/International Organisation)<br>□ Description of status (Person with diplomatic status, Official, Administrative and technical staff, Family member)<br>□ Date of arrival in Luxembourg<br>□ Work start date<br>□ Likely duration of stay (number of years or permanent contract)<br>□ Name and surname<br>□ Date and place of birth<br>□ Nationality<br>□ ID type and number<br>□ Civil status<br>□ 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.<br>Appointed EIB PERS staff members dealing with the administration linked to CdLs (cartedelegitimation@eib.org)<br>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.<br>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.<br>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.<br>The details of the eventual CdLs issued to eligible family members are also stored in the same PeopleSoft screen.<br>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.<br>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 |

| Category | | Title of the processing operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | Technical & Organizational Security Measures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1.6 - Human Resources - Other | 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).  Name, address, date of birth, address, civil status, entry date at EIF, employee ID number, nationality, of staff | Luxembourg law on VAT Protocol on Privileges and Immunities of the European Communities as implemented by Luxembourg Directive 2006/112/EC – Article 151 | Competent Luxembourg Tax Authorities: Administration de l'Enregistrement et des Domaines Office address: Bureau d'imposition 11 – département franchises, 67- | 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 | n/a | Data is based on the invoices scanned by the Scanning team and stored 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 |
| | 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 to submit supporting documentation (for example their marriage certificate) to EIF HR, who in turn validate the change in the system. As the personal data listed below (see section d) can impact individual rights and benefits, it | 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 | 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 Artcile 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 | 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 |
| | 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 | All EIF staff members | After selection the successful candidate will be asked to upload copies of the following personal documentation onto the newcomers portal: o Passport or identity card o Birth certificate, including, where applicable, those of the | 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). | With HC: 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 | 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. Staff members may consult the entirety of their own personal file. |

| Category | | Title of the processing operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | Technical & Organizational Security Measures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 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 | No special security of processing (except for photo and date of birth – see below) as all data are public.<br><br>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). |
| | 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 | Information about reasons to leave and potential improvements suggestions are gathered in a word report, stored within HR. These reports remain undisclosed.<br>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.<br>Identification data : name, first name; ID number; date of the interview<br>Professional data: work location, job title;<br>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. | 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 | 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 | 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 | 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 |

| Category | | Title of the processing operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | 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.<br>Biometric features (facial image and fingerprints).<br>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.<br>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.<br>The EU laissez-passer is a travel document governed by Council Regulation 1417/2013.<br>Authorities in EU Member States must recognise it as a valid document.<br>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 | European Commission LP Services.<br>The data subject retains the LPData may be disclosed, at the request of the data subject, to embassies in order to obtain travel visas.<br>14-Oct-20<br>EIF Staff (for business purposes only) | Information stored electronically in PeopleSoft is kept for the full length of service of the staff member.<br>The physical LP is destroyed when the staff member leaves service or the LP expires.<br>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<br>under the data subjects Staff ID (LP issue date, status, expiry date and LP number)<br>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 | **EDGE gender survey** | HR | EDGE Strategy AG, Vorstadt 2, 6300 Zug, Switzerland | In line with the 2018 Diversity and Inclusion Policy at EIF, the EIF has contracted EDGE as a service provider to provide an independent assessment and a third-party certification (EDGE certification) on the EIF's gender balance. The certification process will be repeated every two years. This will allow EIF to receive feedback on its gender data and the EIF inclusion policy and recommendations on how the EIF's practices can be improved. This follows the same assessment and certification process carried out on the EIB side.<br>Part of the assessment includes a survey to assess the inclusiveness of the EIF culture. The survey will be carried out in Q1 2021. Participation will be voluntary and the survey will consist of 22 questions covering the perceptions and experience of gender equality on topics such as recruitment & promotion, pay, training & leadership development, flexible working and organisational culture. The questionnaire contains 21 multiple-choice | All EIF staff with at least 6 months of service will be the data subjects in the gender survey | No personal data will be gathered in the context of the survey, instead staff members will be asked about their eexperience of gender equality at the EIF. | The 2018 Diversity and Inclusion Policy at EIF and the staff member's consent (shown be clicking on the link to participate in the survey as participation is on a voluntary basis) | The Chief Executive, the Deputy Chief Executive, the Head of Human & Resources Management, the Head of Division of Human Resources (HRD) and the officers of the Performance Management Unit of HRD will have access to the aggregated data from the survey.<br>In addition, any stakeholders involved in the implementation of recommendations aimed at achieving EDGE certification such as the Resources Management Unit (RMU) of HRD, the EIF College of Staff Representation and the hierarchy of the data subject, may also have access to the aggregated survey data. The employees of the processor (EDGE) based in Switzerland will have access to the list of email addresses, the raw survey data provided by participants individually and anonymously and to | The Processor will delete the list of email addresses once the survey has closed. Aggregated data: historical (i.e. no personal data present; the aggregated data will be used for benchmarking purposes in the re-certification process). f the reply to the open ended question reveals or enables an identification of a data subject then this data will be immediately anonymized (i.e. the identification data will be immediately deleted) by the Processor | n/a | Participation in the survey is voluntary. Anonymity and confidentiality are guaranteed via the following measures:<br>The survey is completely anonymous, no personal data will be shared.<br>The service provider will provide an open link to the survey, identical for all employees. This will not require the sharing of email addresses. The link will be shared with the data subjects via a generic email to all staff to launch the survey.<br>There will be no questions on age and participants will not be requested to identify themselves. Data will be aggregated to prevent the attribution of responses to individuals, i.e. there is no way for the processor to trace back responses to individual employees.<br>Once the survey is closed the processor will delete any uniquely identifiable answers from the replies to the open-ended question that would allow the identification of data subjects prior to the analysis of the data and sending it back to the EIF.<br>The Processor is compliant with EU data protection regulation. The Processor is based in Switzerland and its servers and services are located exclusively in Switzerland. The Processor has signed the necessary |

| Category | | Title of the processing operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | Technical & Organizational Security Measures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1.6.14 | **Elections of EIF Staff Representatives** | HR | | Organising and carrying out elections of the EIF Staff Representatives in line with the EIF Election Guidelines. For this purpose the EIB online voting platform is used. This involves steps such as the creation of the list of electors, verification of | All EIF staff eligible to stand and vote in the elections are the data subjects in this processing | name, ID number, length of service, data relating to status of active service, date of entry into service, date of the end of the employment contract. | Annex III of the Staff Rules 'Convention governing Staff Representation at the EIF' and the Guidelines for the Election of Staff Representation at the EIF | All EIF staff for the list of colleagues standing for elections and the published results. The EIF Election Committee for manual voting. The EIB IT team for assistance with the voting platform. | The documents relating to elections shall be stored for two months on the voting platform following the elections and the published results shall be stored for an indefinite period.<br>The time limit for blocking or erasure is 5 working days. | n/a | Prior to launching any EIF elections, EIF HR reach out to the Chairman of the EIB Election Committee to formally request the use of the platform and to notify them of the dates of the election. The EIB IT Identity & Access Management Team (IAM) manage the accesses to the online voting platform, |
| | 1.6.15 | **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 set out above. | 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".<br>• 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.<br>• 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.<br>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.<br>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:<br>- Outlook shared mailbox (only area where personal data is persistently kept by SRs)<br>- G:drive folder<br>- Individual mailboxes<br>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 operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | Technical & Organizational Security Measures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2.1 - Compliance - Governance | 2.1.1 | **Declaration of Interest** | Compliance | EIF | Ensuring conformity with the EIB Group Conflict of Interests (CoI) Guidelines and the EIF Implementing Rules to the CoI Guidelines (both approved by the EIF CE on 16/10/2018) and alignment with the EIB regarding para. 2.3.2.3 of the | • EIF Heads of Departments (HoDs) and staff members nominated to a governing body of an investment structure,<br>• HoDs spouses' (professional | • For HoDs and staff members: (i) outside activities, (ii) financial interests, (iii) assets, (iv) major liabilities;<br>• For HoDs spouses': professional activities. | EIF Implementing Rules to the EIB Group Conflict of Interests Guidelines (approved by the EIF CE on 16/10/2018) | Declaration forms are sent in sealed envelopes by the required staff to attention to the Chief Compliance Officer (CCO).<br>CCO reviews them, obtains scanned copies and stores them in a secured | Declarations are reviewed on an annual basis and data are deleted after five years following the date of the termination of the external activity. | n/a | Declaration forms (only on paper) are kept in a secured cupboard, with access based on need-to-know basis to CCO and Corporate Compliance officers |
| | 2.1.2 | **Investigations** | Compliance | EIB Inspectorate General – Investigations Division (IG/IN) | Preventing and investigating cases of prohibited conduct. | As per EIF Anti-fraud Policy (of 9 March 2015):<br>• EIF members of governing bodies and staff,<br>• Financial intermediaries, | • Identification data,(name, surname, address, date of birth, nationality …)<br>• Behavioral data | • EIF Anti-fraud Policy and EIB Group Investigation Procedures, as amended from time to time,<br>• Regulation (EU) No 883/2013 of the European Parliament and of the Council of 11 September | • OLAF for pursuing a case whenever (i) suspicious of misconduct of staff, (ii) illegal activity affecting the financial interests of the EU,<br>• Other EU bodies ( EPO or CJEU),<br>• National authorities, both | Aligned with the IG/IN retention periods: documentation and information for cases shall be retained for at least five years and up to ten years maximum from the date of closure of the case (i.e. five years for cases deemed inadmissible and ten | Transfers must be processed by the processor in line with the Data Processing Agreement | Data are kept strictly confidential and disclosed only to persons or entities authorized to receive them or otherwise on a need-to-know basis |
| | 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 | 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), | EIF Statutes, Art.2(1): The task of the Fund shall be to contribute to the pursuit of the objectives of the European Union.<br>According to Internal Audit Charter, Internal Audit can process personal data in | In no circumstance, Personal Data are ever disclosed in audit reports in any member state, third country or international organization.<br>However, OLAF – in the course of an investigation - | All audit files (audit working papers with potential personal data) saved in electronic version are stored permanently in TeamMate.<br>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:<br>"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 |
| 2.2 - Compliance - Conduct | 2.2.1 | **External Activities** | Compliance | | Compliance with the EIB Group Staff Code of conduct. | EIF staff, for all cases related to outside professional activities, as per Art. 5.8 of the EIB Group Staff Code of Conduct. | The Declaration form on External Activities requires:<br>• Identification data,<br>• Outside professional activity,<br>• Financial data (remuneration).<br>A register is kept in order to track the declarations. | Art. 5.8 of the EIB Group Staff Code of Conduct | • RM COMPL,<br>• EIF H&RM. | Declaration are reviewed on an annual basis and data are deleted after five years following the date of the termination of the external activity. | n/a | Hard copy declarations are kept in a secured physical environment, while the electronic versions and the register are stored in a restricted folder. Access to the information is granted, on need-to-know basis only, to RM-COMPL staff. |
| | 2.2.2 | **Gifts and advantages** | Compliance | | Compliance with provisions of the EIB Group Staff Code of Conduct | Members of staff of the EIF, as per para. 5.4 of the EIB Group Staff Code of Conduct Members of staff may include third parties (such as consultants). | Identification data | • EIB Group Staff Code of Conduct.<br>• The above-mentioned codes of conduct and the Staff Regulations | RM COMPL | 5 years following the date of declaration | n/a | Declarations are stored in a secured physical environment; the electronic versions and the register are stored in a restricted folder |
| | 2.2.3 | **Whistleblowing Policy** | Compliance | | handling reports regarding alleged serious misconduct within the EIF | "EIF staff members and everyone working for the EIB Group" (as per the EIB Group Whistleblowing Policy, hereafter "EIBG WBP"; potentially third parties | contact data, behavioral data | EIB Group Whistleblowing Policy (2019) | EIF services on a need to know basis, e.g Compliance, H&RM, EIB IG/IN | Aligned with the IG/IN retention periods: documentation and information for cases shall be retained for at least five years and up to ten years maximum from the date of closure of the case (i.e. five years for cases deemed inadmissible and ten | n/a | data is stored in a secured electronic environment |
| | 2.2.4 | **Complaints** | Compliance | EIB Inspectorate General / Complaints Mechanism (IG/CM) | Information received as a result of lodged external complaints.<br>In the context of the Complaints Mechanism Policy dated November 2018, EIF may be in charge of processing personal Data in order to manage an external complaint of alleged | Individuals working at Financial institutions and EIB staff members | • Identification data name, surname, address, date of birth, nationality …)<br>• Behavioral data (same as for investigations) | The legal bases for this processing are:<br>(i) 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). | • Relevant EIF services – in order to assist the inquiry by providing information.<br>• EIB IG/CM – which handles complaints on behalf of the EIF as per the framework agreement signed between the EIF and | Aligned with the IG/IN retention periods i.e. five years for cases deemed inadmissible and ten years for the admissible ones. | n/a | All cases are handled as strictly confidential and electronic data are stored in restricted areas, in line with the need-to-know principle |
| | 2.2.5 | **Conflict of Interest** | Compliance | | Assessing personal and organizational conflicts of interest, potential and actual, of EIF staff members | EIF staff members, potentially third party individuals | contact data, financial data, behavioral data | compliance with the relevant provisions of the codes of conduct and conflict of interest guidelines | EIF services (H&RM and RM COMPL), EIB IG/IN in case of an investigation | five years after the conflict of interest has ended | n/a | Hard copy declarations are kept in a secured physical environment, while the electronic versions and the register are stored in a restricted folder. Access to the information is granted, on need-to-know basis only, to RM-COMPL staff. |

| Category | | Title of the processing operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | Technical & Organizational Security Measures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2. | 2.2.6 | **Insider lists** | Compliance | | keeping audit trail for potential investigation of market abuse, as required by Art. 18 Regulation (EU) No 596/2014 | CE, DCE and EIF staff members | contact information, date of birth, address, in accordance with Article 18 of Regulation (EU) No 596/2014 and as per format required by the Commission Implementing Regulation (EU) 2016/347 of 10 March 2016 laying down implementing technical standards with regard to the precise format of insider lists and for updating insider lists in accordance with Regulation (EU) No 596/2014 of the European Parliament and of the Council; potentially family members and close associates. | Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC, EIB Group Guidelines for the Prevention of sider Dealing and Market Manipulation entered into force on the 3rd of July 2016 and EIF Procedures concerning Market Abuse adopted in December 2017 | EIF Compliance, relevant competent authorities having jurisdiction to investigate market abuse and EIB services in charges of GED. | five years after the insider list has been drawn up or updated (as per Art. 18 (5) Regulation (EU) No 596/2014 | n/a | data is stored in a “central register” (shared with and maintained by the EIB) in GED |
| 2.3 - Compliance - Transactions | 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:<br>- financial intermediary and shareholders and<br>- 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.<br>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:<br>EIF staff members/consultants of<br>a. transactional services,<br>b. the Compliance Division,<br>c. Risk and Portfolio Management,<br>d. OIM,<br>e. internal audit, and<br>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. |
| | 2.3.2 | **SAR-STR Reporting** | Compliance | EIF | 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 | Personal data may be processed in relation to:<br>- EIF counterparties and their key persons<br>- EIF employees | 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 | The Legal basis are the 4th and the 5th AML Directives requirements. | The personal data are processed by:<br>• EIF staff members/consultants of<br>o transactional services,<br>o the Compliance Division,<br>o Risk and Portfolio Management, | 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 | No Transfers | Data is stored in corporate systems, which are password protected in order to ensure security and data privacy.<br>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 |
| | 2.3.3 | **Register of Natural Persons (incl. PEPs)** | Compliance | EIF | 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 | Personal data may be processed in relation to:<br>- financial intermediary and shareholders and<br>- Individuals (UBO, key persons, PEPs and Bas | 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 | The legal basis are the 4th and 5th AML directives requirements.<br>EIF Statutes express the basic mission of EIF and decisions of its General Meeting and its Board of Directors. Furthermore, EIF | The personal data are processed by:<br>EIF staff members/consultants of<br>a. transactional services,<br>b. the Compliance Division,<br>c. Risk and Portfolio Management, | | 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 | 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 operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | Technical & Organizational Security Measures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 - Corporate Governace - EIF Statuory 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 Audti Board's approval and the signature fo 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 | 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 | 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 | 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 |
| | 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 | 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 | □ 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 | Members and alternate members of the Board of Directors and Audit Board. | □ CVs containing personal and professional details as disclosed by the individual<br>□ 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. | □ 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.<br>□ Accounting details for | □ Data made available on the Portals and the EIB website is removed with immediate effect following the member's departure from office.<br>□ Personal declarations concerning access to information and remuneration shall be | The General Meeting includes representatives of financial institutions outside the European Economic Area. Therefore in this context some transfer of personal data outside | □ 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 |
| | 3.1.6 | **Personal information of EIF shareholder representatives** | Governing Bodies | EIF | □ Maintaining contacts database and distribution mailing lists for decision-making and information-sharing purposes with the representatives of the EIF shareholders.<br>□ Maintaining proof of the | 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 | Name, title, email, phone, address, signatures | EIF Statutes (Articles 10–12) and EIF Rules of Procedure (Chapter II) | □ 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.<br>□ In addition, contact | □ Mailing lists are updated immediately upon receipt by the Secretary (Secretary@eif.org) of relevant changes.<br>□ Personal data collected and processed in this context, including voting forms and powers of attorney submitted in | The General Meeting includes representatives of financial institutions outside the European Economic Area. Therefore in this context some transfer of personal data outside | Shareholder information sheets and supporting information provided in hard copy are stored in 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 |
| | 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 documents on behalf of the EIF and in connection with the EIF's banking operations | 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 | 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 | | □ 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 | Members of the Audit Board | Individual's signature specimen | Prior consent of the data subject according to Regulation (EU) 2018/1725 (Article 5.d) | □ The signature specimens are accessible by GBU staff and CIA assistant.<br>□ Documents containing the Audit Board members' signatures may be made available on the Audit Board Portal, in which case | 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 operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | Technical & Organizational Security Measures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3.1 | 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 | 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 th eend of the respective contractual relationship | n/a | Contractual and related documentation is stored on secure corporate drives and in DLM/M-Files where adequate access rights are properly set up to ensure strict confidentiality (if need be). Original documents are kept are kept in dedicated cupboards/binders on EIF's premises and, in the case of |
| | 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. | • Audio and video recordings of the persons to be identified<br>• Surname, Name<br>• Address<br>• Phone number<br>• E-mail address<br>• 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, Bahrein, Brunei, Kuwait, China / Hong Kong, Oman, Japan, Qatar, Korea, Saudi Arabia, Malaysia, UAE, New Zeeland, 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-decision- making bodies in EIF investees. | 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 | Collected data is stored in EIF system (eFront) which is password protected |

| Category | | Title of the processing operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | Technical & Organizational Security Measures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Governace - MIBO & Other | 3.2.3 | **Tax reporting to fund managers** | OIM | | Purposes related to:<br>Tax administration<br>FATCA / CRS<br>Withholding tax | Chief Executive of EIF, EIF employees that sign the relevant 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:<br>- Tax administration procedure (M-Files ID 151336);<br>- FATCA / CRS procedure (M-Files ID 151579); and<br>- Withholding tax procedure (M- | 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 |
| | 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:<br>- legal representatives of the respective applicant, financial intermediary and/or<br>- 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 needs to have the emails as they are used as logins. EIF needs the IP to make sure that | 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 | Link to the survey will be sent through a dedicated EIF-NPI Equity Platform outbox in Outlook which is routinely used |

| Category | | Title of the processing operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | Technical & Organizational Security Measures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3.2 - Corporate Gov | 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 Mfiles, 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:<br>• Name;<br>• Surname;<br>• Professional email address;<br>• Phone number;<br>• Date of birth;<br>(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).<br>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<br>• Legal representative of counterparties | • Name<br>• Surname<br>• 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<br>• Legal representative of counterparties | • Name<br>• Surname<br>• 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. |
| | 3.2.11 | **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, …<br>In respect with the above, eFront is storing personal data | Data concerned are linked to :<br>• EIF counter-parties, as legal representatives<br>• EIF sub-contractors staff as eFront users<br>• EIF staff as eFront | Contacts: salutation, first name, last name, date of birth, nationality(ies), Phone number (including mobile), email addresses, standard mail addresses, social network<br>• 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 | 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 | **Scan of Network Drive part of End User Computing (EUC) Governance** | OIM | | Read metadata information from MS Excel and Access files saved on the departmental network drives (G-Disk) for EIF Directorates as part of a requested scan to identify potential End User Computing tools and their owners. | EIF Staff username listed under FileAuthor metadata field files scanned under the following formats: xls, .xlsx, .xlsm, .xlsb, .xla, .xlt, .xlam, .xlw, .xltx, .xltm, .ACCDB, | The dedicated software application will only read the departmental network drives for the Fund's Directorates of this document, coming out from the file extension at the point c) of this document, the following file data: | Specific Contract No. 9112 signed by the EIB the 10/05/2019, under the Framework Agreement signed by EIB and D-fine GmbH, on the performance of consultancy services to provide support to the EUC | External consultants selected by EIB, and including EIF, in accordance with the Bank's internal procurement rules and having signed the EIB's General Terms and Conditions and Rules for | Data part of the scan will archived and uploaded ClusterSeven Inventory Management Systems, as check evidence of scan execution and respective results assessment. Those evidences are indeed required for any potential internal | There will be no transfers of data outside of the EIB Group. | EIB IT Security Clearance based on the agreement that for the execution of the Scan with Cluster Seven will be used a service account and IAM will be responsible for the password retention |

| Category | | Title of the processing operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | Technical & Organizational Security Measures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 3.2.13 | **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 | Final recipients, i.e. individuals benefitting from EIF financial guarantees or other debt instruments provided to financial intermediaries ("EIF Products"), are | 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 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 | 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 | 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 | 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 | 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 |
| | 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 operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | Technical & Organizational Security Measures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 4.1.8 | **Annual Report 2021 staff photos demand** | Marketing | Blossom (design agency) | Creating a visual collage of staff photos for the EIF Annual Report 2021. The Annual Report is published online and printed. | EIF staff | Photos of staff at their desk and photos of staff's desks. They will be used to create a visual collage for one of the chapters of the Annual Report. | Consent of the data subjects | General public, EIF's service provider: Blossom (design agency) | he data will be publicly available in the design form (collage) indefinitely. The original photos will be deleted after 1 year. | n/a | The photos will be stored on the G drive, with limited access to the Marketing division of the EIF. The transfer to the service provider will be made using SmartShare, the EIB Group's secure transfer platform. |

| Category | | Title of the processing operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | 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:<br>• potential freelancing provider(s) of services or supplies;<br>• team member(s) proposed by legal persons acting as potential providers of services or supplies, in the context of their tender;<br>• legal representatives of the tenderers/candidates and/or<br>• individuals in the context of the tender process for individual external advice | Name, telephone, e-mail address<br>Passport or ID (in case of freelancing)<br>Technical and professional ability, incl. qualifications, experience and academic background (CV)<br>Evidence of fiscal status or otherwise commercial registration, incl. bank account<br>Fiscal and social security obligations, absence of bankruptcy, fraud, conflict of interest<br>Evidence of recent turnover<br>Extract from the judicial record | Directive 2014/24/EU being the legal basis of the EIF Procurement Guide<br>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<br>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<br>* Nationality<br>* Date of birth<br>* ID or passport number<br>* Other ID or passport data (because copy of document is provided)<br>* Residential address<br>* Marital status Tax ID number Position in EIF<br>* Business Email<br>* 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.<br>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<br>ii. Expense Report: Employee | i. Travel policy<br>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<br>• 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<br>Manual processing – scanning the Reimbursement by Scanning team, control of the file before payment |

| Category | | Title of the processing operation | Controller EIF Service | Processor | Purpose(s) of the processing | Category of Data subjects | Category of data | Legal basis | Recipients | Retention Period | Transfer to third countries or international organisations | Technical & Organizational Security Measures |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 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 | AAll 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. |
| **6.1 RM - Information Security** | 6.1.1 | **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:<br>1) information or cyber security incidents<br>2) non-compliance with information security regulations (internal & external)<br>3) security testing, and<br>4) results of security awareness campaigns.<br>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 | 1. EIF user names<br>2. EIF user contact details such as business email and business phone number<br>3. EIF user functional/ organization association<br>4. EIF user data specific and relevant to the security incident | Article 5.1(b) Compliance with a lLegal 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.<br>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. | Data will only be retained by the EIF ISO function and its organizational unit and stored securely on a storage only accessible to the EIF ISO function and organizational unit. |