

RECORD OF PERSONAL DATA PROCESSING ACTIVITY according to Article 31 of Regulation (EU) 2018/1725

► E-finance workflows

Contents

General information.....	1
Description and Purpose of the Processing	2
Data Subject's Rights.....	3
Categories of Data Subjects & Personal Data	3
Categories of Recipients & Data Transfers.....	4
Automated Decision Making.....	5
Retention Period & Security Measures	5

General information

Introduction
EIOPA, as a European Authority, is committed to protect individuals with regard to the processing of their personal data in accordance with Regulation (EU) No 2018/1725 (further referred as the Regulation) ¹ .
Contact Details of Data Controller(s)
Fausto Parente, Executive Director Westhafenplatz 1, 60327 Frankfurt am Main, Germany fausto.parente@eiopa.europa.eu
Contact Details of the Data Protection Officer
Eleni Karatza Westhafenplatz 1, 60327 Frankfurt am Main, Germany dpo@eiopa.europa.eu
Contact Details of Processor
EIOPA's Team/Unit/Department responsible for the processing: Corporate Support Department, Finance & Corporate Services Unit, efinance@eiopa.europa.eu

¹ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

Description and Purpose of the Processing

Description of Processing
The e-finance is used for the process of financial and procurement transactions. Depending on the type of transaction the data collected are related to internal or external data subjects (see note 9); personal data are collected and retained for staff administration, relations with external parties, procurement and accounting, auditing and information administration in the framework of the e-finance workflow. Audit information containing names, User IDs, and other information about users (department, line manager, contact details) may be captured in EIOPA internal shared drive ERIS in the following scenarios: - Staff member being assigned a workflow task or completing a workflow task. - Being added to a security group, and thereby granted access to a site, document library or document. The supporting documents processed in the Nintex workflows are covered by the separate record for ERIS and fall under the responsibility of the Document Management System (in efinance no documents are stored, only links to ERIS)
Purpose (s) of the processing
☒ Staff administration ☒ Relations with external parties ☒ Procurement and accounting ☐ Administration of membership records ☒ Auditing ☒ Information administration ☐ Other (please give details):
Lawfulness of Processing
- Legal Basis justifying the processing: - EIOPA’s Financial Regulation of 6 June 2019, as revised on 11 October 2019 (EIOPA-MB-19-057_rev1) - Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union - Processing is necessary: ☒ for the performance of a task carried out in the public interest -Article 5(1)(a) of the Regulation ☐ for compliance with a legal obligation to which the Controller is subject ☐ 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 ☐ in order to protect the vital interests of the data subject or of another natural person Or ☐ Data subject has given his/her unambiguous, free, specific and informed consent

Data Subject’s Rights

Information on how to exercise data subject’s rights
Data subjects may exercise their data privacy rights provided in Articles 17 to 24 of the Regulation (EU) 1725/2018. Data subjects have the right to: • access their personal data, receive a copy of them in a structured and machine-readable format or have them directly transmitted to another controller, as well as request their rectification or update in case they are not accurate. • request the erasure of their personal data, as well as object to or obtain the restriction of their processing. • withdraw their consent to the processing of their personal data at any time in case such processing is based solely on their consent. For the protection of the data subjects’ privacy and security, every reasonable step shall be taken to ensure that their identity is verified before granting access, or rectification, or deletion. Should data subjects wish to access/rectify/delete their personal data, or receive a copy of them/have it transmitted to another controller, or object to/restrict their processing, please contact efinance@eiopa.europa.eu or DPO@eiopa.europa.eu. <u>Complaint:</u> Any complaint concerning the processing of the data subjects’ personal data can be addressed to EIOPA’s Data Protection Officer (DPO@eiopa.europa.eu). Alternatively, data subjects can also have at any time recourse to the European Data Protection Supervisor (www.edps.europa.eu).

Categories of Data Subjects & Personal Data

Categories of Data Subjects
☒ EIOPA permanent staff, Temporary or Contract Agents ☒ SNEs or trainees ☒ Visitors to EIOPA (BOS, MB, WG, Seminars, Events, other) If selected, please specify: Board of Appeal members, stakeholders, external experts for OPSG and IRSG meetings, event and seminar speakers entitled to a financial reimbursement. ☒ Providers of good or services ☐ Complainants, correspondents and enquirers ☒ Relatives and associates of data subjects

☒ Other (please specify): Board of Appeal members, stakeholders, external experts for OPSG and IRSG online meetings, event, and speakers entitled to a financial reimbursement.
Categories of personal data
(a) General personal data: The personal data contains: ☒ Personal details (name, address etc) ☒ Education & Training details ☒ Employment details ☒ Financial details ☒ Family, lifestyle and social circumstances ☐ Other (please give details): (b) Special categories of personal data The personal data reveals: ☐ Racial or ethnic origin ☐ Political opinions ☐ Religious or philosophical beliefs ☐ Trade union membership ☐ Genetic or Biometric data ☐ Data concerning health, sex life or sexual orientation

Categories of Recipients & Data Transfers

Recipient(s) of the data
☒ Managers of data subjects ☒ Designated EIOPA staff members If selected, please specify: Operational Initiating Agents, Financial Initiating Agents, Financial Verifying Agents, Operational Verifying Agents, Workflow Authorising Officers, Accounting Officer, and Accounting Specialist who have received a delegation by the Executive Director to carry out this task, IT administrators. ☐ Relatives or others associated with data subjects ☐ Current, past or prospective employers ☐ Healthcare practitioners ☐ Education/training establishments ☐ Financial organisations ☒ External contractor: Nintex (developer), for the purpose of maintenance and other technical assistance

☐ Other (please specify):
Data transfer(s)
☒ Within EIOPA or to other EU Institutions/Agencies/Bodies If selected, please specify: all departments and units within EIOPA, as required (on need-to-know basis each workflow has own actors based on permissions), internal and external auditors on request when an audit is performed. ☐ To other recipients within the EU (e.g. NCAs) ☒ To third countries If selected, please specify: Whether suitable safeguards have been adopted: ☒ Adequacy Decision of the European Commission ² (UK) ☐ Standard Contractual Clauses (SCC) ☐ Binding Corporate Rules (BCR) ☐ Administrative Arrangements between public Authorities (AA) ☐ To international organisations If selected, please specify the organisation and whether suitable safeguards have been adopted:
Data subjects could obtain a copy of SCC, BCR or AA here:

Automated Decision Making

Automated Decision-making, including profiling
A decision is taken in the context of this processing operation solely on the basis of automated means or profiling: ☒ No ☐ Yes In case of an automated decision-making or profiling, please explain:

Retention Period & Security Measures

Retention period
How long will the data be retained?

² Third countries for which the European Commission has issued adequacy decisions are the following: [Adequacy decisions \(europa.eu\)](https://eudataprotection.eu/adequacy-decisions).

• Nintex workflow data (stored in SharePoint) – the retention period applicable to financial documents shall apply (depending by the financial document 5 or 10 years from the date of discharge for the financial year concerned). Workflow data are purged on an annual basis³. • Nintex workflow outputs (stored in SharePoint lists in the eFinance site) - the retention period applicable to financial documents shall apply (depending by the financial document, 5 or 10 years from the date of discharge for the financial year concerned). The applicable retention policy shall be applied to each list⁴. • Nintex workflow history (recording all actions performed by users in relation to e-finance) – 5 years.
For further processing envisaged beyond the original retention period for historical, statistical or scientific purposes, please specify whether the personal data will be anonymised: ☒ No ☐ Yes
Technical & organisational security measures taken
Several technical and organisational measures have been adopted in order to ensure the optimum security of the documents and personal data collected in the context of the procedures described under section ‘Description and Purpose of the Processing’.

³ “Purge Workflow Data” action shall be performed in SharePoint Central Administration under the Nintex Workflow Management section.
⁴ An Information Management Policy shall be applied to each eFinance list, under List Settings.