

Privacy statement related to EIOPA's procurement procedures and the implementation of related contracts

► Introduction

1. EIOPA, as a European Authority, is committed to protect individuals with regard to the processing of their personal data in accordance with Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (further referred as "the Regulation").

► Purpose of the processing of personal data

2. Personal data are processed for the management and administration of procurement procedures by EIOPA. Such a processing is also necessary for the implementation of the contracts resulting from these procedures.

More specifically, personal data is processed to assess eligibility and capacity of potential contractors; to select the best tender and to decide to which economic operator a contract will be awarded; to subsequently manage the contracts awarded and obtain the services, supplies, and works required. Personal data received and processed depends on the relevant procurement procedure: in some cases, only contact details of an individual are needed to make a procurement or a purchase possible; in other cases personal data needed is more comprehensive (like financial statements in case of a self-employed professional, criminal records extract of managers, or profiles of staff of a tenderer) and is key to conclude that the tenderer is not in a situation of exclusion, fulfils the selection criteria, and/or has submitted the best tender. The latter is often the case in procurement and always the case for selection of experts.

Personal data of data subjects internal to EIOPA is processed when included in documents and platforms required to carry out procurement procedures such as: procurement approval documents; committees appointment documents; procurement evaluation documents; contracts; advanced electronic signature platform EU Sign, the EC's qualified electronic signature; PPMT; eSubmission; CIRCABC Fundings&Tenders Portal.

As regards the processing within the PPMT and eSubmission, identification data of persons internal to EIOPA is added to PPMT and eSubmission for the opening of tenders and for evaluation committees. Identification data of external persons included in tenders and other documents as well as profiles of tenderers' staff are contained in the tenders submitted by tenderers via eSubmission.

3. Your personal data will not be used for any purposes other than the performance of the activities specified above. Otherwise, you will be informed accordingly.
4. The legal basis for this processing operation comprises of:
 - Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing the European Insurance and Occupational Pensions Authority (EIOPA);
 - 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;
EIOPA's Financial Regulation of 6 June 2019, as this has been revised on 11 October 2019 (EIOPA-MB-19-057_rev1).
5. In accordance with Article 5(1)(a) of the Regulation processing is lawful as it is necessary for the performance of a task carried out in the public interest.
6. Personal data collected are processed according to the conditions set out in the above-mentioned Regulation.
7. Data will not be used for any purposes other than the performance of the activities specified above.

► **Controller of the personal data processing**

8. The controller responsible for processing your data is EIOPA's Executive Director.
9. Address and email address of the controller:

Westhafen Tower, Westhafenplatz 1
60327 Frankfurt am Main
Germany
fausto.parente@eiopa.europa.eu

► **Personal data collected**

10. The following personal data may be collected and processed:

Regarding data subjects internal to EIOPA:

- Identification data: name, surname, title, signature;
- Contact details: business email address, business phone number;

Regarding data subjects external to EIOPA (tenderer(s) and/or contractor(s) (in case s/he is a natural person), and potentially their staff or subcontractors (if natural persons):

- Identification data: name, surname, place and date of birth, passport number, ID number (including identification data of tenderers' clients from which information regarding tenderers might be sought); title, signature, function;

- Contact details: business email address, business telephone numbers, fax number, postal address, company and department, country of residence (including contact details of tenderers' clients from which information regarding tenderers might be sought);
- Criminal records extract of potential contractor's managers/owners, as some offences are considered exclusion criteria based on Articles 136 and 137 of Regulation (EU, Euratom) 2018/1046;
- Information for evaluation of selection criteria of tenderers and experts: professional profiles with identification data and information on educational background, professional experience and skills relevant to the selection or award phases of the procurement procedure, including details on current and past employment, other personal data contained in CVs;
- Financial data: Bank account reference (IBAN and BIC codes), VAT number, etc;
- Certificates for social security contributions and taxes paid; extracts from judicial records;
- Declaration on honour or equivalent concerning exclusion criteria, selection criteria and/or eligibility criteria;
- IP address.

Regarding data subjects, both internal and external to EIOPA, while using the following systems:

- ABAC: Legal Entity Form (LEF) and Bank Account identification Form (BAF) for self-employed contractors and experts: identification data as defined above, contact details as defined above, address, VAT number and bank account details. LEF and BAF for companies: name and signature of the representative of the contractor.
- PPMT: Personal details: name and surname.
- eSubmission: Personal details and contact information: name, surname and work email address.
- CIRCABC: Personal details and contact information: username, first name, surname, email address, title, organisation, phone number, postal address, fax, URL address, open text/description.
- EU Sign: Personal details and contact information: name, surname, User ID of the requestor, professional email address, data present on the signing certificate for remote signing functionality (name, surname, date of birth, ID number, membership, title/role). Technical data: type of operation requested (sign/seal, verify, extend), date and time of the operation, target of the operation (EC internal, Seal, Qualified Electronic Signature).
- European Commission Authentication Service (EU Login) login name and password (only stored in EU Login), security data/log files (for audit trails).

In addition to the above, in order to verify whether a tenderer is in one of the situations mentioned in Article 136 of Regulation (EU, Euratom) 2018/1046, EIOPA will check whether it has been registered in the Early Detection and Exclusion System (EDES) managed by the European Commission. For more information, see (http://ec.europa.eu/budget/explained/management/protecting/protect_en.cfm).

► To whom are your data disclosed?

11. Your data may be disclosed to the following recipients:

- Designated EIOPA staff members, e.g Procurement Experts and Specialists in the Finance and Corporate Services Unit, members of the Evaluation Committee, Authorising Officer, the initiating unit (the contract owner) and other units in case they need to use the awarded contract, financial actors (e. g. OIAs/OVAs) for data entered into e-finance workflows;

- Other EU institutions'/agencies' staff in case of inter-agency/inter-institutional (joint) procurement procedures;
- External experts and contractors working on behalf of EIOPA for the purposes of tender evaluation;
- The EC: DG BUDGET for ABAC, PMO for ABAC (LEF and BAF); DG DIGIT for eSubmission, PPMT, Fundings and Tenders Portal, CIRCABC, EU Sign.
- Bodies in charge of monitoring, audit or inspection tasks in application of European Union law such as OLAF, European Court of Auditors and Internal Audit Service of the European Commission; the EDPS, Court of Justice of the EU;
- Public: in case of contract award notices published in the Official Journal of the European Union or on EIOPA's website (in particular your name and address, the amount awarded and the name of the project or programme for which you are awarded a contract); and in case of publications in the Official Journal of the European Union of contract award notices in case a self-employed contractor or an expert are awarded a contract above the relevant financial threshold;

12. Personal data are transmitted in accordance with the relevant provisions of Regulation.

► How long are your data kept?

13. Personal data are kept in EIOPA's internal shared drive ERIS, in the systems of the EC (PPMT, eSubmission):
- Files relating to successful tenderers, including personal data, are retained for a period of 10 years following the procedure's closure.
 - Files relating to unsuccessful tenderers are kept for 5 years following the procedure's closure.
 - For unsuccessful candidates in response to an invitation to request to participate or successful candidates who did not subsequently tender, data specific to the candidate are retained for 5 years following the closure of the procedure, that is following the signature of the contract with awarded tenderer(s).
 - Criminal records extracts (requested only to awarded tenderers) are kept for 2 years following the signature of the contract with awarded tenderer(s).
 - For procurement contracts and framework contracts, personal data written on them and acquired during the management of the contract are kept by the EIOPA Unit responsible for the contract in ERIS for a period of 10 years following the budget discharge of the year when the (framework) contract terminates.
 - For candidates to a Call for Expressions of Interest, data specific to the candidate are retained for 5 years following the closure of the relevant procedure.
 - Data collected when managing the execution of the contract are retained for 10 years following last payment made under the contract.
 - For the purpose of a possible audit, the above-mentioned personal data are kept until the end of such audit if started before the end of the above-mentioned retention periods.

If a relevant case is brought before the EU Courts or an investigation/audit is initiated, the personal data will be kept for a period of up to 2 years following the conclusion of the respective proceedings. Further retention periods:

- ABAC: personal data per data category mentioned above is kept for a maximum of 10 years after the last transaction for data related to natural persons other than the EIUs staff and a maximum of 100 years after the date of recruitment for the EIUs staff.
- CIRCABC: identity and contact information are kept for 1 year after the user stops belonging to any active group. The user account is then deleted.
- EU Sign: personal data, administrative data related to the user of the electronic signature service, technical data related to the usage events of electronic signature service is kept 25 months.

14. Files will not be kept beyond the periods specified above unless the personal data XX is rendered anonymous.

► **Transfer of personal data to a third country or international organisation**

15. No personal data will be transferred to a third country or international organisation.

► **Profiling**

16. No profiling is performed in the context of this processing operation.

► **How can you have access to your data, verify their accuracy, rectify them or object to their processing?**

17. In general, you have the right to access their data, obtain from the controller a copy of your personal data in order to check the accuracy of the data held, and/or to obtain rectification or update of these data (facts) if necessary.
18. You may also ask for erasure of your data if the processing thereof is unlawful, or to have your data blocked for a period enabling the data controller to verify the accuracy, including the completeness, of the data.
19. You may object to or obtain the restriction of the processing of your personal data.
20. Where processing is based solely on your consent, you have the right to withdraw your consent to the processing of your personal data at any time.
21. 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.

22. In case of rejecting of access to their personal data, data subjects can file a complaint with the EDPS.

► **Whom can you contact if you have questions or complaints with regard to data protection?**

23. Should you wish to obtain access to or receive a copy of your personal data, their rectification, or deletion or to object, please contact:

- Procurement@eiopa.europa.eu, or
- the Data Protection Officer at EIOPA at DPO@eiopa.europa.eu or by letter:

EIOPA Data Protection Officer (Confidential)
Westhafen Tower, Westhafenplatz 1
60327 Frankfurt am Main
Germany

24. All questions or complaints concerning the processing of your personal data can be addressed to EIOPA's Data Protection Officer (DPO@eiopa.europa.eu).

25. Alternatively, you can also have recourse at any time to the European Data Protection Supervisor (www.edps.europa.eu).