European Union Agency for Cybersecurity (ENISA)
Vasilissis Sofias 1, Maroussi 15 124, Attiki Greece,
Tel: +30 2814 40 9711,
www.enisa.europa.eu

Updated 1st December 2019

PRIVACY STATEMENT

for the processing of personal data related to

ENISA PROCUREMENT PROCEDURES

1. Context and Controller

The European Union Agency for Cybersecurity ("ENISA") is committed to respecting the privacy of natural persons participating in procurement procedures. Within the framework of the procurement process, the follow-up of tenderer's responses will require the recording and further processing of personal data by ENISA, all personal data are dealt with in accordance with Regulation (EU) 2018/1725, 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. The following Privacy statement outlines the policies by which ENISA collects, manages and uses the personal data provided by participants in procurement procedures.

ENISA (hereby known as the 'Controller'), is the controller of the procurement processing operation. The controller in practice is the Procurement Officer, as mentioned in the Invitation to Tender, who is responsible for the collection and processing of personal data.

2. What personal information do we collect, for what purpose, under which legal bases and through which technical means?

Types of personal data

Personal data collected and further processed concern the tenderer, its staff or subcontractors (natural persons).

Data relating to tenderers (legal persons):

- identification and contact details (official name, official legal form, abbreviation, name and first name of individual economic operators, place of registration, date of registration, VAT registration number, address, phone number, fax number, e-mail address, identity card number, date of birth, country of birth);
- proof of an independent worker status (if applicable) and extract from the trade register, bank certificate stating his/her financial situation; bank account number and bank's name;
- statement of the overall turnover for the services and/or supplies referred to in the procurement procedure;

- organisational chart of the tenderer and company profile;
- proof of having fulfilled all obligations to pay social-security contributions and taxes;
- certificate of clear criminal record or extract of judicial record (for individual economic operators);
- extract from the register of bankruptcy and reorganization procedures or extract from the register of debt regulations or a certificate given by a creditor, as applicable;
- documents attesting professional standing (curriculum vitae, copies of diplomas, certificates, references regarding professional activities);
- list of similar services provided by the tenderer and detailed information on three contracts considered similar in scope;

Please note that when using the European Commission's e-Submission portal for submitting tenders, the following data is also gathered by the European Commission: EU Login user account, eSignature (if used), type of web browser, type of Operating System, IP address used to download the Call For Tender and/or to submit the Tender Bundle. Please, refer to the relevant privacy statement of the European Commission for more information.

Data relating to the staff members of tenderers participating in the procurement procedure:

- identification and contact details only of the person authorised to sign the contract (first name, family name, function, e-mail address, business telephone number, mobile telephone number, fax number, postal address, company and department, country of residence, internet address);
- other data contained in the CVs (expertise, technical skills, educational background, languages, professional experience including details on current and past employment);
- extracts from judicial records only of the person authorised to sign the contract and for high-value contracts (above €144.000) before the award of the contract;
- Declaration of honour by the person authorised to sign the contract that they are not in one of the exclusion situations referred in Articles 136 and 137 of the Regulation (EU, Euratom) 2018/1046.

Data relating to the tenderers' subcontractors and consortium members:

- identification and contact details (official name, official legal form, address, VAT registration form);
- financial identification data (account name, address, city, country; bank name, branch address, account number, IBAN, name under which the account is opened and the telephone number, email address and fax number of the person concerned);
- data contained in the 'Declaration of absence of conflict of interest and of confidentiality';
- data contained in the documents proving the economic/financial and technical/professional capacity of the subcontractor;
- data contained in the 'Subcontractors form', stating unambiguous undertaking to collaborate with the tenderer if the latter wins the contract.
- data contained in the 'Consortium form', stating undertaking to be jointly and severally liable by law for the performance of the contract

Data relating to a natural person participating in the procurement procedure:

- identification and contact details (first name, family name, function, e-mail address, business telephone number, mobile telephone number, fax number, postal address, company and department, country of residence, internet address);
- other data contained in the CVs (expertise, technical skills, educational background, languages, professional experience including details on current and past employment);
- Bank account holders name, address, city, postcode and country. Contact name. Telephone and email address. Bank name, branch address, city, postcode and country. Bank account number, IBAN account number.
- extracts from judicial records for high-value contracts (over €144.000) before the award of the contract;
- Declaration of honour that they are not in one of the exclusion situations referred in Articles 136 and 137 of the Regulation (EU, Euratom) 2018/1046.

Depending on the value of the tender procedure, the following official documents may be requested from the legal entity/person:

  - Extracts from judicial records
  - Certificate attesting to Social Security contributions

Purpose

Upon reception of your tender or request to participate by ENISA, your personal data is collected and further processed for the purpose of the management and administration of the procurement procedures by ENISA services. The data is collected and processed with the purpose to evaluate the eligibility of economic operators to participate in the procurement procedure in accordance with exclusion and selection criteria as defined in articles 136 and 137 of the Regulation (EU, Euratom) 2018/1046 and to evaluate the content of tenders submitted during the procurement procedure with the view to awarding the contract, in accordance with award criteria as defined in article 167 of the Regulation (EU, Euratom) 2018/1046.

Legal basis

The processing is lawful under Article 5 (d) of Regulation (EU) 2018/1725: the data subject has unambiguously given his/her consent. The legal basis for the processing operations on personal data is:

The Financial Regulation applicable to the European Union Agency for Cybersecurity in conformity with the Commission Delegated Regulation (EU) No 2019/715 of 18 December 2018 on the framework financial regulation for the bodies set up under the TFEU and Euratom Treaty and referred to in Article 70 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council [1].

[1] http://www.enisa.europa.eu/about-enisa/accounting-finance/files/enisa-financial-regulation-1

Data processors

When the tender is submitted using the European Commission's e-Submission portal, the European Commission acts as a data processor for ENISA, in particular by facilitating the whole process and providing the storage of the data in encrypted form in its - specifically dedicated for this purpose – servers. The decryption of the tender files can only be performed locally at ENISA by the authorised ENISA staff. The European Commission has no access to the content of the tender files (and included personal data). ENISA has signed a Memorandum of Understanding (MOU) with the European Commission for the provision of this service.

Technical means

Personal data is provided by the submission of a tender. The information is collected in files stored on an isolated secure system. These tender files may either be received via electronic means, using digital portals provided by the European Commission such as '*e-Submission*' or '*e-Request*' (see section on data processors) or via a secured functional email account set up specifically for the procedure, or in the form of paper based documents received physically. The information is processed by ENISA and transferred to ENISA computer systems (as described in point 3), under the responsibility of the Procurement Officer mentioned in the Invitation to Tender or Request for Offers.

2. Who has access to your personal data and to whom is it disclosed?

For the purpose detailed above, access to your personal data may be given on a need-to know basis to the following persons:

- ENISA staff (the Procurement and Contract Team, the project manager of each tendering procedure, the members of the opening & evaluation committees, the DPO if needed) as well as external experts and contractor's staff who work for the purposes of management of the procurement procedure and tender evaluation;
- In case of control or dispute the bodies charged with a monitoring or inspection task in the application of Union law (e.g. Internal Audit Service, European Commission, OLAF, EU Courts etc.);
- Members of the public: In case you are awarded a contract by ENISA, limited personal data will be made public, in accordance with ENISA's obligation to publish information on the outcome of the procurement procedure and on the beneficiaries of funds deriving from the budget of the European Community. The information will concern in particular your name and address, the year, the amount awarded and the name of the project for which you are awarded a contract. These data may be published on a yearly basis on the website of ENISA, and/or in supplement S of the Official Journal of the European Union.

3. How do we protect and safeguard your information?

The collected personal data and all related information are stored after closure of the procurement procedure on the premises of ENISA and on servers of a computer centre of ENISA. The ENISA premises and operations of all computer centres abide by the Agency's

security decisions and provisions established by the ENISA's General Information Security Policy.

When using the European Commission's e-Submission portal, the personal data are stored in isolated servers of the European Commission in encrypted form (see also the section on data processors). Decryption of the data is only possible locally at ENISA by the authorised ENISA's staff.

4. How can you verify, modify or delete your information?

In case you wish to verify which personal data is stored on your behalf by the Controller, have it modified, corrected, or deleted, please make use of the contact information mentioned in the Invitation to tender, by explicitly describing your request. Usually this is done by sending an e-mail to procurement@enisa.europa.eu.

NB: Material data may not be updated or corrected after the deadline for submission of the tenders since elements that would change the nature of the offer cannot be changed after the offer has been received, as this would compromise the award procedure. In any case, such requests will be dealt with within 15 working days.

Special attention is drawn to the consequences of a request for deletion, as this may lead to an alteration of the terms of the tender and lead to exclusion as stated in Article 169 of the Regulation (EU, Euratom) 2018/1046[2].

However, the above-mentioned rights (access, update or correct, delete) may be restricted in case it is necessary to safeguard an important economic interest of the EU, including budgetary matters and the right of freedom of others. In this latter case, you will be duly informed on the main reasons for restrictions and of his right to recur to the EDPS.

5. How long do we keep your personal data?

- Files relating to tender procedures, including personal data, are to be retained by the service in charge of the procedure until it is finalised, and in the archives for a period of 5 years following budgetary discharge, correlating to a maximum of 7 years[3], while tenders from unsuccessful tenderers shall be kept for 5 years following signature of the contract.

[2] In line with Article 169 of the 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, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012

[3] In line with Article 75, subparagraph 1, and subparagraph 2, of the 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, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012

- Extracts of judicial records kept in the electronic form shall be retained for a maximum of 2 years following signature of the contract.
- Until the end of a possible audit, if one is commenced before the end of the abovementioned periods.
- After the periods mentioned above have elapsed, the tender files containing personal data from unsuccessful tenders and contractors are destroyed.

6. Contact information

For any questions on your rights and the exercise of your rights related to the processing of personal data (like access and rectification of your personal data), feel free to contact the Controller, by using the contact information mentioned in the Call for Tenders, and by explicitly specifying your request.

7. Recourse

In case of conflict on any Personal Data Protection issue, you can address yourself to the Controller at the address mentioned in the Call for tenders.

You can also contact ENISA's Data Protection Officer at the following email address: dataprotection@enisa.europa.eu

Should the conflict not be resolved by the Controller or the Data Protection Officer you may lodge a complaint with the European Data Protection Supervisor at any time:

Website http://www.edps.europa.eu ;

E-mail: edps@edps.europa.eu