Scan to verify source & version of document.

OPEN CALL FOR TENDERS

"A framework on appropriate security measures for the processing of personal data"

ENISA D-COD-16-T09

Part 1 **Introduction to ENISA**

Part 2 **Terms of Reference**

Part 3 **Tender Specifications**

Annex I	Legal Entity & Financial ID Forms
Annex II	Declaration of Honour for exclusion criteria & absence of conflict of interest
Annex III	Financial Offer form
Annex IV	Draft Service contract
Annex V	Power of Attorney for Consortium Form
Annex VI	Sub-Contractors Form
Annex VII	Checklist of documents to be submitted in the e-Submission application
Annex VIII	e-Submission Quick Guide for Tenderers
Annex IX	Guide to creating an ECAS account

e-Submission

*Offers via e-Submission portal **ONLY***

CONTENTS

PART 1 INTRODUCTION TO ENISA

1. Background on ENISA

1.1 Introduction

Electronic communications, infrastructure and services are essential factors, both directly and indirectly, in economic and societal development. They play a vital role for society and have in themselves become ubiquitous utilities in the same way as electricity or water supplies, and also constitute vital factors in the delivery of electricity, water and other critical services. Communications networks function as social and innovation catalysts, multiplying the impact of technology and shaping consumer behaviours, business models, industries, as well as citizenship and political participation. Their disruption has the potential to cause considerable physical, social and economic damage, underlining the importance of measures to increase protection and resilience aimed at ensuring continuity of critical services. The security of electronic communications, infrastructure and services, in particular their integrity, availability and confidentiality, faces continuously expanding challenges which relate, inter alia, to the individual components of the communications infrastructure and the software controlling those components, the infrastructure overall and the services provided through that infrastructure. This is of increasing concern to society not least because of the possibility of problems due to system complexity, malfunctions, systemic failures, accidents, mistakes and attacks that may have consequences for the electronic and physical infrastructure which delivers services critical to the well- being of European citizens.

1.2 Scope

The European Union Agency for Network and Information Security (ENISA, hereinafter 'the Agency') was established in order to undertake the tasks assigned to it for the purpose of contributing to a high level of network and information security within the Union and in order to raise awareness of network and information security and to develop and promote a culture, of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organisations in the Union, thus contributing to the establishment and proper functioning of the internal market.[1]

1.3 Objectives

The Agency's objectives are as follows:

- The Agency shall develop and maintain a high level of expertise.
- The Agency shall assist the Union institutions, bodies, offices and agencies in developing policies in network and information security.
- The Agency shall assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union, thus contributing to the proper functioning of the internal market.
- The Agency shall assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents.
- The Agency shall use its expertise to stimulate broad cooperation between actors from the public and private sectors.

2. Additional Information

Further information about ENISA can be obtained on its website: www.enisa.europa.eu.

[1] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

PART 2 TERMS OF REFERENCE

I. SCOPE OF THIS TENDER

Within the framework of this Open tender procedure, ENISA would like to find a suitably qualified contractor to provide the services as stipulated in the Terms of Reference outlined below.

Subject of the tender	Maximum budget
A framework on appropriate security measures for the processing of personal data	**€ 55,000.00**
PLEASE NOTE: *This tender procedure is limited to tenderers which are legally incorporated in a member state of the European Union/EEA, or which have an incorporated subsidiary in one of the EU/EEA member states. (The Agreement on Government Procurement (GPA) does not apply to EU Regulatory Agencies.)*	

Method of submitting tenders:	***e-Submission portal***	***YES***
	Courier or postal service	*NO*
	By hand	*NO*
	By email	*NO*

II. ELECTRONIC SUBMISSION OF OFFERS

*Please see **ANNEX VIII** of this Tender for a quick description of the e-Submission application.*

Access to the e-Submission application

If you are accessing a tender procedure linked to e-Submission via the e-Tendering platform *for the first time*, you will need to create a user account in the Commission system (**European Commission Authentication Service - ECAS**): https://webgate.ec.europa.eu/cas/

A ***'Guide to creating an ECAS account'*** is provided as Annex IX to this Tender.

A button "Submit your Tender" will be then displayed and you will be able to access the e-Submission application.

Before proceeding to fill in the tender details in the system, you need to accept the Terms & Conditions and acknowledge the Privacy Statement of the e-Submission application.

On-time submission of tenders

You are ***strongly advised*** not to wait until the last moment before the deadline to submit your tender. The process of uploading your documents and entering required data may take longer than anticipated.

It is highly recommended to give yourself a MINIMUM of 24 hours before the stated expiry date and time to upload your tender to e-Submission!

In case of any problems with the submission of your electronic tender, we recommend that you call the helpdesk in reasonable time before the time limit for receipt.

After submitting a tender, but within the time limit for receipt, you may still submit a new (updated) version of your tender. To do this, you should upload a new consolidated tender package containing corrected tender documents together with formal notification by email that the previous tender is withdrawn (to procurement@enisa.europa.eu).

Late receipt of your tender will lead to its exclusion from the award procedure for this contract.

Proof of receipt

You will receive a tender receipt confirmation in your e-Submission mailbox, including information about the timestamp put on your tender by the e-Submission system. This is considered as the official time of receipt and will constitute proof of compliance with the tender deadline.

Withdrawal of tender

If, after submission, you wish to withdraw your tender, you must send a duly signed letter, firstly by email to procurement@enisa.europa.eu as well as by registered post to the address below identifying the name and reference of the tender you wish to withdraw. This notification must be signed by the same authorised legal representative(s) who previously signed the tender in question.

Address
[*Insert tender title and reference*]
ENISA
For the attention of the Procurement Officer
PO Box 1309,
Heraklion 710 01,
Greece

Get to know the e-Submission application

On the ***'Help for e-Submission'*** page of the application a detailed *User Manual,* in each of the 23 languages of the European Union, is available that elaborates the system requirements and a step by step procedure to successfully submit a tender.

A ***Quick Guide*** can also be found on this Help page, summarising the User Manual (*the English version is included as Annex VIII of this tender*).

The 'Help for e-Submission' page is available at:
https://webgate.ec.europa.eu/supplier_portal_toolbox/esubmissionFileProject/files/BT3/spotsHelpPage_en.html

TEST environment for e-Submission application

In order to familiarise yourself with the system and to test whether your workstation configuration is working correctly with our environment, you are invited to access the ***test environment***:

Select the first link if the Call for Tenders has NO LOTS, or the second link for a tender with LOTS.

For a tender with **NO** LOTS:
https://webgate.ec.europa.eu/supplier_portal_toolbox/spots/openSpots.do?CFTUUID=TEST_CFT-NO_LOTS&VERSION=1&CAID=5790001791483&screenWidth=1000&screenHeight=850

For a tender **WITH** LOTS:
https://webgate.ec.europa.eu/supplier_portal_toolbox/spots/openSpots.do?CFTUUID=TEST_CFT-3_LOTS_3&VERSION=1&CAID=5790001791483&screenWidth=1000&screenHeight=850

1. GENERAL DESCRIPTION OF THE REQUIRED SERVICES

1.1 BACKGROUND

Information risk management is an integral part of an organization's management process that deals with the identification, treatment, communication and acceptance of IT security risks. It involves the selection and implementation of measures justified by the identified risks and the reduction of those risks to acceptable levels. It also comprises continuous monitoring of risks and risk communication. Several methodologies and frameworks have been proposed and have been adopted by organizations during the last decade but none of them was oriented on the protection of personal data.

Under the European legal framework, personal data can only be collected under specific conditions, for a legitimate purpose. Furthermore, organisations which collect, process and store personal data must protect it from misuse and they are obliged to ensure that technical and organisational measures are undertaken so as to protect the personal data with an appropriate level of security. Data subjects should have the same level of protection, regardless of the size of the organisation or the amount of personal data it processes. In 2014, Article 29 Data Protection Working Party[2] has acknowledged that this protection can be done on in a scalable manner and has issued a statement on the role of a risk-based approach in data protection legal frameworks.

Such a risk-based approach should enable organizations to identify and assess the risks, likelihood and impact, and prioritize the events that could compromise the integrity and confidentiality of personal data. Following the risk assessment, it should also support organizations to select appropriate security and organizational measures and control to mitigate the identified risks, the potential impact and reduce the probability of occurrence.

In line with the above, the Proposal for a General Data Protection Regulation[3], sets in its Article 30, about security of processing, the following obligations for organizations acting as data controllers or processors:

1. *The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.*
2. *The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.*

Against this background, ENISA has undertaken this project, under its Work Program 2016[4], in order to provide guidelines for small and medium organizations acting as data controllers or processors on (i) how to perform a security risk assessment and (ii) implement appropriate organizational and security measures to protect personal data that are adequate to the level of risk.

[2] http://ec.europa.eu/justice/data-protection/article-29/index_en.htm
[3] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2012:0011:FIN
[4] https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2016

1.2 Goal of the Study

The goal of this study is to design and propose a framework that will support small and medium organizations to implement appropriate security measures for the processing of personal data.

More specifically the objectives of this study are:

- Provide guidelines on how to perform security risk assessment for the electronic processing of personal data.
- Propose possible organizational and technical security measures for different information security domains based classified based on the level of risk.
- Provide use cases as guidance on how to apply to proposed framework.

1.3. Target Audience and Validation

The target audience of this study comprises small and medium organizations across Europe, coming from all activity sectors, acting as personal data controllers or processors.

Validation of the results of the study will be performed throughout one workshop organised by ENISA during the course of the project. The workshop is expected to gather stakeholders in the areas of information security and data protection to debate about the results.

2. OBJECTIVES AND TASKS

The objectives of this tender are organised into the following tasks:

2.1 TASK 1: Risk assessment

The tenderer should produce a set of guidelines to support organizations in determining the level of risk in the electronic processing of personal data. The guidelines should meet the following requirements:

- They should follow the methodology and nomenclature of the ISO/IEC 27005:2008 (Information technology - Security techniques - Information security risk management)[5].
- They should take into account different types of organizations, distinct categories of personal data assets (e.g. identification, financial, health data, etc.) and threats (human made, unintentional, etc.).
- They should be scalable and easy to apply for small and medium organizations.
- They should focus exclusively on the ICT security risks arising from the processing of personal data.

This task results in a deliverable (D1).

2.2 TASK 2: Organizational security measures

The tenderer should produce a set of guidelines to support organizations in selecting appropriate organizational security measures to protect personal data.

[5] http://www.iso.org/iso/catalogue_detail?csnumber=42107

The proposed organizational security measures should cover the most relevant information security areas, employing for this purpose widely known classifications (e.g. ISO/IEC 27001:2013[6], NIST Special Publication SP 800-53[7], etc.).
The final collection of areas will be agreed with ENISA. An indicative, but non-exhaustive list, is the following:

- Personal data security policy
- Allocation of responsibilities
- Personnel security
- Awareness and training programs
- Personal data asset management
- Incident management procedures
- Third party processing services management
- System acquisition and support

Each proposed organizational security measure should be associated with a specific level of risk (i.e. the list of measures in each area should be divided on those appropriate to all levels of risks or only for a certain level risk).
The proposed organizational security measures should be scalable for small and medium organizations.
This task results in a deliverable (D2).

2.3 TASK 3: Technical security measures

The tenderer should produce a set of guidelines to support organizations in selecting appropriate technical security measures to protect personal data.

The proposed technical security measures should cover the most relevant information security areas, employing for this purpose widely known classifications (e.g. ISO/IEC 27001:2013[6], NIST Special Publication SP 800-53[7], etc.).

The final collection of areas will be agreed with ENISA. An indicative, but non-exhaustive list, is the following:

- User access management
- Network and communications security management
- Audit and traceability management.
- ICT infrastructure configuration management
- Cryptography management
- Data preservation and business continuity
- Web applications security
- Vulnerability assessment
- Media protection
- Physical security

[6] http://www.iso.org/iso/catalogue_detail?csnumber=54534
[7] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Each proposed technical security measure should be associated with a specific level of risk (i.e. the list of measures in each area should be divided on those appropriate to all levels of risks or only for a certain level risk).

The proposed technical security measures should be scalable for small and medium organizations.

This task results in a deliverable (D3).

2.4 TASK 4: Use cases

The tenderer should prepare at least FOUR use cases depicting fictional organizations processing personal data, in order to present practical examples on how to apply the framework.

The examples selected should try to cover diverse organizations, in terms of:

- Activity sector (e.g. educational, medical, retail, etc.).
- Categories of personal data processed (e.g. identification, financial, health, etc.).
- Size (small/medium organization).
- Nature (public/private organization).

Each use case should present:

- A brief description of the organization and its data processing activities.
- An explanatory risk assessment of the data processing activities.
- A selection of proposed possible organizational and technical security measures (adequate to the level of risk calculated).

This task should results in a deliverable (D4).

2.5 TASK 5: Presentation material

The tenderer should prepare FOUR power point presentations, one for each of the previous deliverables. The material should be sufficient to thoroughly introduce the framework to an organization wishing to apply it. Each presentation should conclude with at least TEN multiple choice questions summarizing the content of the deliverable.

This task should results in a deliverable (D5).

2.6 TASK (on-going) Project management

The contractor should implement an appropriate and efficient project management method.

The contractor is expected to submit to the agency, prior to the Kick Off meeting, detailed planning (e.g. a Gantt chart). These will be reviewed by ENISA.

The planning should address:

- Scheduling of tasks and activities within tasks
- Milestones and critical activities
- Assignment of experts and person days to tasks and activities
- Identification of possible risks and suggestions to mitigate them
- Quality assurance and peer review measures to ensure high quality results

The contractor is expected to send two-weekly progress reports using the ENISA template to the ENISA project manager(s) about the project and to schedule bi-weekly videoconference meetings about the progress. The progress reports should include (in bullets) what has been done the previous two weeks, the status, what is planned for the next two weeks, the risks and suggested solutions and finally, points to take decisions upon.

After every meeting (progress meetings, or project meetings), the contractor should take minutes and send them to the ENISA project manager(s) using the ENISA template

3. EXPECTED SKILLS

The performance of the above mentioned activities requires professionals that have broad experience with related tasks, and at least:

- Sound knowledge and professional experience on security aspects of personal data processing, both at policy and technical level.
- Sound knowledge and professional experience in the area of information security risk assessment and management (methodologies, tools and applications).
- Sound knowledge and professional experience in analysing, proposing and/or implementing organizational and technical controls to address information security risks and/or achieve compliance with data protection regulations.
- Professional experience on advising and/or implementing security measures in different types of organizations (in terms of sector and size).
- Excellent knowledge of data collection, analysis and validation methods including the ability to produce clear and understandable text.
- Excellent project management skills including quality assurance.
- Very good communication skills.

4. DURATION AND DEADLINES

The duration of this work is foreseen from April 2016 until October 2016.

- Kick of meeting – no later than 1st of April 2016.
- Delivery of D1– no later than 30th of May 2016.
- Delivery of D2– no later than 30th of June 2016.
- Delivery of D3– no later than 30th of July 2016.
- Delivery of D4– no later than 30th of September 2016.
- Validation workshop - no later than 30th of September 2016.
- Delivery of D5– no later than 30th of October 2016.

The Tenderer is required to make a proposal in their tender for the time schedule of the activities in order to carry out the project (e.g. including a Gantt chart). The tenderer may propose to carry out different activities in parallel. In its offer the Tenderer should indicate the estimated amount of person days required to accomplish all tasks associated with this procurement.

5. LIST OF DELIVERABLES

The contractor is expected to deliver five deliverables:

- **Deliverable 1** (D1): A document on guidelines for risk assessment on the processing of personal data.
- **Deliverable 2** (D2): A document on guidelines for appropriate organizational security measures for the processing of personal data.
- **Deliverable 3** (D3): A document on guidelines for appropriate technical security measures for the processing of personal data.
- **Deliverable 4** (D4): A document on use cases how to apply the proposed guidelines.
- **Deliverable 5** (D5): Presentations of all previous deliverables.

English is the language to be used for all the documents produced. The layout of the final report should be based on the templates provided by ENISA. The final report is expected to be proofread by a native English speaker. ENISA may edit the full report and publish it.

6. PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATIONS

The execution of the activities will take place at the Contractor's premises. The Contractor is required to be virtually present for all necessary meetings and for collecting all relevant information to conduct the analysis. For this purpose network based collaborative tools (i.e. videoconferencing) will be used.

The contractor will be required to conduct two business trips:

- A one day kick-off meeting
- A one day validation workshop

These meetings will take place at a location agreed with ENISA (within mainland Europe). The cost of these two business trips should be included in the total offer. ENISA will not additionally reimburse the contractor for taking part in these meetings.

The validation workshop for the study will be organized by ENISA and the Agency will cover all organizational costs (except for the business trip of the contractor).

7. TENDER RESULT AND ESTIMATED CONTRACT VALUE

The result of the evaluation of tenders will be the awarding of a Service Contract. The total estimated budget cannot exceed **55,000.00 Euros (fifty five thousand Euros)** covering all tasks executed and including all costs (e.g. travelling expenses of the contractor).

8. CONTENT AND PRESENTATION OF THE TECHNICAL OFFER

The Tenderer shall enclose with the **Technical Offer** all documents and information that will enable its offer to be assessed in terms of quality and of compliance with the Specifications. An Offer shall include a description of the operational means and procedures to be implemented to perform the Contract, supported where appropriate by related documents.

An Offer shall cover the following aspects:

- Skills and experience of the expected contactor
  - The Tenderer will have to present its compliance with the expected skills as described in the relevant section.

- The Tenderer will have to present its understanding of the topic.
- Examples of previous related works, a list of all related projects and activities that the contractor has undertaken in the past.

- Description of the deliverables
  - The proposed initial structure and contents of the deliverables listed in the section “List of deliverables”.
  - The approach and methodology used to perform the tasks and ensure the quality of the deliverables.
- Management of provision of services
  - Project Management: a close description of the project management method used including quality assurance is required. Breakdown of tasks; milestones definition; assignment of experts to tasks and person days to tasks should be presented in a Gantt chart, included in the offer.
  - At the kick off meeting, the project plans will be confirmed as final.
  - The prospective contactor must also identify possible risks to the project and propose mitigation measures.
- In addition the tenderer is expected to highlight / explain
  - Availability and ability of the tenderer to respond: prompt availability of resources is required within the specified delivery timeframes. Additionally, any ancillary or support resources, such as a network of associates to support the scope of this Call for Tenders must be clearly stated.
- Short CV’s of the experts that will be allocated in the project focussing on their experience and expertise on the areas covered by the study.
- If applicable, the contractor should also provide justification for subcontracting,

9. CONTENT AND PRESENTATION OF THE FINANCIAL OFFER

The Financial offer must be drawn up using the **Financial Offer form (see Annex III)**.

10. DATA PROTECTION

Personal contact information will normally be professional contact data only, so no special confidentiality requirements are envisaged.

Regarding personal data, the following EU data protection regulations have to be respected:

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
2. Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data;
3. Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

11. MARKING OF SUBMITTED DOCUMENTS

The tenderer SHOULD NOT mark tender documents (for e.g. the header or footer) with any of the following words: RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET. If the tenderer considers that such markings are required, a prior approval from the ENISA Procurement office should be attained BEFORE sending the tender documents. The tenderer should be aware that the information sent to ENISA for procurement purposes is handled in accordance with the governing rules for EU Public Procurement and the EU Financial Regulation framework.

12. PRICE

Prices submitted in response to this Tender must be inclusive of all costs involved in the performance of the contract. Prices shall be submitted only in Euro and VAT excluded.

13. PRICE REVISION

Price revision does not apply to this tender procedure.

14. PROTOCOL ON PRIVILEGES AND IMMUNITIES OF THE EUROPEAN COMMUNITIES

ENISA is exempt from all taxes and duties, including value added tax (VAT), pursuant to the provisions of Articles 3 and 4 of the Protocol on the Privileges and Immunities of the European Communities. Tenderers must therefore give prices which are exclusive of any taxes and duties and must indicate the amount of VAT separately.

15. PAYMENT ARRANGEMENTS

Payments under the Contract shall be carried out within 60 days of submission of an invoice accompanying the final report or deliverable based on the conditions set out in the draft contract. One single payment will be made after receipt and approval of the deliverables by ENISA. An invoice must specify the specific deliverables covered. A note that accompanies the final deliverables must present the resources used for each of the deliverables presented. Time sheets should be submitted as appropriate.

Payments under the Service Contract shall be made in accordance with article I.5 of the Special Conditions and article II.4.3 of the General Conditions (see Annex IV)

PART 3 TENDER SPECIFICATIONS

1. INFORMATION ON TENDERING

1.1 Contractual conditions

In drawing up their offer, the tenderer should bear in mind the provisions of the draft contract (Annex IV) attached to this invitation to tender particularly those on payments, performance of the contract, confidentiality, and checks and audits. Submission of a tender by a potential contractor implies acceptance of this contract and all of the terms and conditions contained therein. Any limitation, amendment or denial of the terms of contract will lead to automatic exclusion from the procurement procedure.

It is strongly recommended that you have this draft contract checked and passed by your legal representative before committing to submitting an offer.

The Agency may, before the contract is signed, either abandon the procurement procedure or cancel the award procedure without the tenderers being entitled to claim any compensation.

1.2 Joint Tenders (if applicable)

A joint tender is a situation where a tender is submitted by a 'group' of economic operators (consortium). Joint tenders may include subcontractors in addition to the joint tenderers.

Tenders can be submitted by groupings of service providers/suppliers who will not be required to adopt a particular legal form prior to the contract being awarded. However, the Agency will require the grouping:

- Either to have the contract sign by all members of the grouping. In this case, one of them will be responsible for the receipt and processing of payments for members of grouping, for managing the service administration and for coordination of the contract; or
- to have the contract sign by a team leader, which has been duly authorised by the other members to bind each of them (a power of attorney will be attached to the contract according to the template provided by the Agency).

In addition, the composition and constitution of the grouping, and the allocation of the scope of tasks amongst the members, shall not be altered without the prior written consent of the Agency which can be withheld at discretion.

In case of a joint offer, for each partner, except the LEAD partner:

- the **Legal Entities form** and the **Power of attorney of each partner**, must be filled in, signed by (an) authorised representative(s), scanned and uploaded in the corresponding section.

- the **Declaration of honour with respect to the Exclusion Criteria and absence of conflict of interest** must be filled in, signed by (an) authorised representative(s), scanned and uploaded in the corresponding section.

Hand written or electronic signature of the consortium leader who submits the tender is not required, since the signature of the *e-Submission 'Tender Preparation Report'* implies that all included documents are signed by this party.

More details about uploading the respective documents can be found in Annex VII.

1.3 Liability of members of a group

Partners in a joint offer assume **joint and several liability** towards the Agency for the performance of the contract as a whole.

Statements, saying for instance:

- That one of the partners of the joint offer will be responsible[8] for only one part of the contract and another one for the rest, or
- That more than one contract should be signed if the joint offer is successful

are thus incompatible with the principle of joint and several liability. The Agency will disregard any such statement contained in a joint offer, and reserves the right to reject such offers without further evaluation, on the grounds that they do not comply with the tendering specifications.

1.4 Subcontracting

Subcontracting is permitted in the tender but the contractor will retain full liability towards the Contracting Authority for performance of the contract as a whole.

If the tenderer intends to subcontract part of the service, they shall indicate in their offer which part will be subcontracted and to what extent (% of the total contract value).

Tenderers must ensure that Article II.7 of the contract (Annex IV) can be applied to subcontractors.

Tenderers must give an indication of the proportion of the contract that they intend to subcontract.

Tenderers are required to identify all subcontractors.

During contract execution, the change of any subcontractor identified in the tender will be subject to prior written approval of the Contracting Authority.

[8] not to be confused with distribution of tasks among the members of the grouping

2. STRUCTURE AND CONTENT OF THE TENDER

2.1 General

Tenders must be written in **one of the official languages** of the European Union. The working language of ENISA is English.

Tenders must be clear and concise, with continuous page numbering. Since tenderers will be judged on the content of their written bids, they must make it clear that they are able to meet the requirements of the specifications.

2.2 Structure of the tender

Based on the *e-Submission* environment, all tenders must include two sections:

1) Qualification data;
2) Tender data.

The 'Qualification data' consists of:
- Identification of the Tenderer;
- The lots the tender is applicable for;
- Information regarding exclusion and selection criteria.

The 'Tender data' consists of:
- The technical proposal;
- The financial proposal.

2.3 Qualification data

a) Identification of the Tenderer

The tenderer must fill in all required fields in the section:
"Qualification" → "Identification of the Tenderer" →"[Party Name]".

In case of a joint tender the consortium name has to be provided in the section:
"Qualification" → "Identification of the Tenderer" →"Consortium"

and an identification of every party in the consortium needs to be added in the section:
"Qualification" → "Identification of the Tenderer" →"Consortium Members".

The following information should also be provided:

(i) Legal Entities

In order to prove their legal capacity and their status, all tenderers and identified subcontractors must provide a Legal Entity Form with its supporting evidence. The Legal Entity Form needs to be signed by participating parties that are not signing the *'Tender Preparation Report'* (see Annex VII for an overview of required signatures.)

However, the subcontractor(s) shall not be required to fill in or provide those documents when the services represent less than 20% of the contract.

The Legal Entity Form can be generated via the e-Submission application from the section:
"Qualification" → "Identification of the Tenderer" → "[Party Name]" → "Documents"

Located under the sub-section:
"Generate pre-filled documents" button "Legal Entity form"

and uploaded under *"Documents"* in the same section.

Alternatively a standard template in each EU language is available at:
http://ec.europa.eu/budget/contracts_grants/info_contracts/legal_entities/legal_entities_en.cfm

Tenderers must provide the following information if it has not been included with the Legal Entity Form:

- For **legal persons**, a legible copy of the notice of appointment of the persons authorised to represent the tenderer in dealings with third parties and in legal proceedings, or a copy of the publication of such appointment if the legislation which applies to the legal entity concerned requires such publication. Any delegation of this authorisation to another representative not indicated in the official appointment must be evidenced.
- For **natural persons**, where applicable, a proof of registration on a professional or trade register or any other official document showing the registration number.

(ii) Financial identification

The tenderer (or the single point of contact in case of joint tender) must provide a Financial Identification Form and supporting documents. Only one form per offer should be submitted (no form is needed for subcontractors and other joint tenderers). The form is available on:
http://ec.europa.eu/budget/contracts_grants/info_contracts/financial_id/financial_id_en.cfm

Remark: Tenderers that are already registered in the Agency's accounting system (i.e. they have already been direct contractors) must provide the filled in form but are not obliged to provide the supporting evidence.

The form needs to be printed, filled in and then scanned and uploaded in the section:
"Qualification" -> "Identification of the tenderer" -> "[Party Name]" -> "Documents".
In case of a joint tender, it has to be uploaded in the *"Documents"* section of the Consortium Leader.

(iii) Power of Attorney

In case of a joint tender, an Agreement / Power of Attorney of each partner must be filled in, signed by (an) authorised representative(s), scanned and uploaded in section:
"Qualification" -> "Identification of the tenderer" -> "[Party Name]" -> "Documents"

Please choose 'Model A' for an ad hoc grouping or 'Model B' for a legally constituted consortium - see templates in Annex V (a) and (b)

(iv) Lots interested in *(only in case the tender has multiple lots)*

The tenderer must indicate for which lots the tender is applicable, by ticking the boxes in the section: *"Qualification" -> "Interest in the following lots" of the e-Submission application.*

b) Information regarding exclusion and selection criteria:

The tenderer is requested to submit the following documents:

1. Declaration by the Tenderer relating to the exclusion criteria (see 3.1 below)

   The filled-in Declaration form needs to be uploaded under:

   "Qualification" -> "Exclusion Criteria" -> "[Party name]"

   In case of a joint tender, each member of the consortium has to submit a declaration under the respective party name (see template in Annex II)

2. Documents certifying economic and financial capacity (see 3.2.2 below)

   The documents need to be uploaded under:

   "Qualification" -> "Selection Criteria" -> "Financial and Economic Capacity" -> "[Party name]"

   In case of a joint tender, each member of the consortium has to submit the documents under the respective party name.

3. Proof of technical and professional capacity (see 3.2.3 below)

   The documents need to be uploaded under:

   "Qualification" -> "Selection Criteria" -> "Technical and Professional Capacity" -> "[Party name]"

   In case of a joint tender, each member of the consortium has to submit the documents under the respective party name.

If any of the above documents are associated with a specific Lot, please indicate for which Lot it is applicable inside the document AND in the Description field of the attachment *(only in case the tender has multiple lots).*

2.4 Tender data

a) Technical proposal

The technical section is of great importance in the assessment of the bids, the award of the contract and the future execution of any resulting contract.

The technical offer must cover all aspects and tasks required in the technical specification and provide all the information needed to apply the award criteria. Offers deviating from the requirements or not covering all requirements may be excluded on the basis of non-conformity with the tender specifications and will not be evaluated.

The technical tender needs to be uploaded in the section:
"Tender" → *"[name of Call for Tender]"* in the e-Submission application.

The tenderer selects the "Technical Tender" document from the dropdown box ("Financial Tender or Technical Tender"). The e-Submission application allows attachment of as many documents as necessary.

b) Financial proposal

All tenders must contain a financial proposal to be submitted **using the form attached as Annex III.**

The tenderer's attention is drawn to the following points:

- Prices must be quoted in **euros**, including the countries which are not in the euro-zone. As far as the tenderers of those countries are concerned, they cannot change the amount of the bid because of the evolution of the exchange rate. The tenderers choose the exchange rate and assume all risks or opportunities relating to the rate fluctuation.
- **Prices must be fixed amounts** [and include all expenses, such as travel expenses and daily allowances etc.].
- **Estimated travel and daily subsistence allowance expenses must be indicated separately**. This estimate should be based on Articles I.4 and II.16 of the draft contract (Annex IV). This estimate will comprise all foreseen travel and will constitute the maximum amount of travel and daily subsistence allowance expenses to be paid for all tasks.
- **Prices must be quoted free of all duties**, taxes and other charges, including VAT, as the European Union is exempt from such charges under Articles 3 and 4 of the Protocol on the privileges and immunities of the European Union. The amount of VAT may be shown separately.
- Prices shall be fixed and not subject to revision during the performance of the contract.

The total price needs to be encoded in the e-Submission application. The completed Financial Offer form, ALSO needs to be uploaded in section:
"Tender" → "[name of Call for Tender]"

The tenderer selects the "Financial Tender" document from the dropdown box ("Financial Tender or Technical Tender"). The e-Submission application allows attachment of as many documents as necessary.

3. ASSESSMENT AND AWARD OF THE CONTRACT

The assessment will be based on each tenderer's bid. All the information will be assessed in the light of the criteria set out in these specifications. The procedure for the award of the contract, which will concern only admissible bids, will be carried out in three successive stages.

The aim of each of these stages is:

1) to check on the basis of the ***exclusion criteria***, whether tenderers can take part in the tendering procedure;
2) to check on the basis of the ***selection criteria***, the technical and professional capacity and economic and financial capacity of each tenderer;
3) to assess on the basis of the ***award criteria*** each bid which has passed the exclusion and selection stages.

Only tenders meeting the requirements of one step will pass on to the next step

3.1 EXCLUSION CRITERIA

All tenderers shall provide a declaration on their honour (see Annex II), stating that they are not in one of the situations of exclusion listed in Annex II.

The declaration on honour is also required for identified subcontractors whose intended share of the contract is above 20%.

The declaration on honour has to be duly signed by parties that are not signing the Tender Preparation Report in *e-Submission* (see Annex VII for an overview of required signatures.).

The successful tenderer shall be asked to provide the documents mentioned as supporting evidence in Annex II before signature of the contract and within a deadline given by the contracting authority. This requirement applies to all members of the consortium in case of joint tender

Remark:
The tenderers will be waived of the obligation to submit the documentary evidence mentioned above if such evidence has already been submitted for the purposes of another procurement procedure launched by ENISA, provided that the documents are not more than one year old starting from their issuing date and that they are still valid. In such a case, the tenderer shall declare on his honour that the documentary evidence has already been provided in a previous procurement procedure, specifying the reference of the call for tender for which the documents have been provided, and confirm that no changes in their situation has occurred.

3.2 SELECTION CRITERIA

The following criteria will be used to select the Tenderers. If the Tender is proposed by a consortium these criteria must be fulfilled by each partner.

Documentary evidence of the Tenderers' claims in respect of the below-mentioned criteria is required.

3.2.1 Professional Information

The Tenderer must provide evidence of enrolment (declaration or certificates) in one of the professional or trade registers, in the country of establishment.

3.2.2 Financial and Economic Capacity

Proof of financial and economic standing shall be furnished by the following documents and minimum requirements:

(a) Copy of the financial statements (balance sheets and profit and loss accounts) for the last two (2) financial years for which accounts have been closed, where publication of the accounts is required under the company law of the country in which the economic operator is established. In case of a consortium, each consortium member shall present their financial statements.

If the tenderer is not obliged to publish its accounts under the law of the state in which it is established, a copy of audited accounts for the last two (2) financial years should be presented. In case of a consortium, audited accounts for each consortium partner shall be presented.

(b) A statement of the average turnover of the last two (2) financial years for which accounts have been closed. In case of a consortium, the annual average turnover for each of the partners shall be presented.

If for some exceptional reason which the Contracting Authority considers justified, the tenderer is unable to provide the documentary evidence requested above, he may prove his economic and financial capacity by any other means which the Contracting Authority considers appropriate, but only following a request for clarification before the tender expiry date.

3.2.3 Technical and professional capacity

Evidence of the technical and professional capacity of the tenderers shall be furnished on the basis of the following documents:

- A curriculum vita of the Tenderer, as well as of all members of the Tenderer's team, shall be included, in which the Tenderer shall refer to the skills and experience required (in line with Part 2 – Section 3 - Expected Skills):
- Their technical knowledge and experience in the relevant technical areas (including references to projects similar to the one proposed in this tender);
- Their management capability (including, but not limited to, project management in a European context and quality assurance).

3.3 AWARD CRITERIA

3.3.1 Quality of the Offer

Once the Tenderer has demonstrated the appropriate capacity to perform the Contract on the grounds of the selection criteria, the offer will be assessed on the basis of the award criteria.

No	Qualitative award criteria		Weighting (max. points)
1.	Technical quality of the offer	Technical quality and accuracy of the services proposed to fulfil the requirements of the tender.	30/100
2.	Methodological quality of the offer	Quality, completeness, conciseness and clarity of the proposed methodology.	25/100
3.	Quality control measures	Quality control system applied to the deliverables, language quality check, and risk management measures.	15/100
	Relevant experience of the company	Relevant experience of the company in areas relevant to the project.	15/100
4.	Project Team	Composition of project team (ratio senior/juniors), relevant experience of the team, direct involvement of senior staff and distribution of tasks amongst experts.	15/100
Total Qualitative Points (QP)			**100**

Minimum attainment per criterion

Offers scoring less than 50% for any criterion will be deemed to be of insufficient quality and eliminated from further consideration.

Minimum attainment overall

Offers scoring less than 60% after the evaluation process will be considered to be of insufficient quality and eliminated from the following phase.

The sum of all criteria gives a total of 100 points. The respective weighting between the different awards criteria depends on the nature of the services required and is consequently closely related to the terms of reference. The award criteria are thus quantified parameters that the offer should comply with. The **qualitative award criteria** points will be weighted at **70%** in relation to the price.

3.3.2 Price of the Offer

Tenders must state a total fixed price in Euro. Prices quoted should be exclusive of all charges, taxes, dues including value added tax in accordance with Article 3 and 4 of the Protocol on the Privileges and Immunities of the European Communities. Such charges may not therefore be included in the calculation of the price quoted.

ENISA, in conformity with the Protocol on the Privileges and Immunities of the European Community annexed to the Treaty of April 8th, 1965, is exempt from all VAT.

Offers exceeding the maximum price set in Part 2; section 7 will be excluded. The cheapest offer will receive the maximum points and the rest of the candidate's offers will be awarded points in relation to the best offer as follows

$$P_P = (P_C / P_B) \times 100$$

where;

P_P = Weighted price points
P_C = Cheapest bid price received
P_B = Bid price being evaluated

3.3.3 Award of the contract

The contract will be awarded to the offer which is the most cost effective (offers the best value for money) which obtains the highest number of points after the final evaluation on the basis of the ratio between the **quality criteria (70%) and the price (30%).** The following formula will be used:

$$TWP = (Q_P \times 0.7) + (P_P \times 0.3)$$

where;

Q_P = Qualitative points
P_P = Price points
TWP = Total weighted points score

In case the successful tenderer is unable to sign the contract for any reasons, the Contracting Authority reserves the right to award the contract to other tenderers as per the ranking order established following the evaluation procedure.

4. TENDER OPENING

The public opening of received tenders will take place on **10th February 2016 at 10:30am EET** at ENISA Building, Science and Technology Park of Crete, GR - 70013 Heraklion, Greece.

A maximum of one legal representative per participating tenderer may attend the opening session. Tenderers shall inform the Agency in writing of their intention to attend by email to procurement@enisa.europa.eu **at least 48 hours** prior to the opening session.

5. OTHER CONDITIONS

5.1 Validity

Period of validity of the Tender: 90 days from the closing date stated in Invitation to Tender. The successful Tenderer must maintain its Offer for a further 120 days from the notification of the award.

5.2 Lots

This Tender is not divided into Lots.

5.3 Additional Provisions

- Changes to tenders will be accepted only if they are received on or before the final date and time set for the receipt of tenders.
- Expenses incurred in respect of the preparation and presentation of tenders cannot be refunded.
- No information of any kind will be given on the state of progress with regard to the evaluation of tenders.
- All documents submitted by Tenderers will become property of ENISA and will be regarded as confidential.

5.4 No obligation to award the contract

Initiation of a tendering procedure imposes no obligation on ENISA to award the contract. Should the invitation to tender cover several items or lots, ENISA reserves the right to award a contract for only some of them. ENISA shall not be liable for any compensation with respect to Tenderers who's Tenders have not been accepted. Nor shall it be so liable if it decides not to award the contract.

6. SPECIFIC INFORMATION

6.1 Timetable

The timetable for this tender and the resulting contract is as follows:

Title: **"A framework on appropriate security measures for the processing of personal data"**

ENISA D-COD-16-T09

Summary timetable comments

Launch of tender: Contract notice to the Official Journal of the European Union (OJEU) Uploaded to e-Tendering website Uploaded to ENISA website.	**18th December 2015**	
Deadline for request of information from ENISA	3rd February 2016	
Last date on which clarifications are issued by ENISA	4th February 2016	
Deadline for **electronic reception** of offers via ***e-Submission***	**9th February 2016**	**23:59 CET** (**Central** European time)
Opening of offers	10th February 2016	10:30 **EET** (**Eastern** European time)
Date for evaluation of offers	TBA	10:30 **EET** (**Eastern** European time)
Notification of award to the selected candidate + 10 day standstill period commences	late Feb 2016	Estimated
Contract signature	Mid - late March 2016	Estimated
Commencement date of activities	As per tender	Estimated
Completion date of activities	As per tender	Estimated