



## **OPEN CALL FOR TENDERS**

### ***Tender Specifications***

# **“Enabling the information society - Securing personal data in online environments”**

## **ENISA P/18/12/TCD**

**LOT 1** – Identifying security best practices for privacy protection purposes

**LOT 2** – Securing personal data in online environments

- Part 1**      **Introduction to ENISA**
- Part 2**      **Technical Description**
- Part 3**      **Administrative Details**

- Annex I      Legal Entity Form
- Annex II      Financial Identification Form
- Annex III      Declaration of Honour for exclusion criteria & absence of conflict of interest
- Annex IV      Financial Offer form
- Annex V      Draft Service contract
- Annex VI      Declaration by Authorised Representative
- Annex VII      Consortium Form
- Annex VIII      Sub-Contractors Form
- Annex IX      Document Checklist

## CONTENTS

<b>PART 1 INTRODUCTION TO ENISA</b> .....	<b>4</b>
<b>1. CONTEXT</b> .....	<b>4</b>
1.1 Introduction .....	4
1.2 Scope .....	4
1.3 Objectives .....	4
<b>2. ADDITIONAL INFORMATION</b> .....	<b>4</b>
<b>PART 2 TECHNICAL DESCRIPTION</b> .....	<b>5</b>
<b>A. SCOPE OF THIS TENDER</b> .....	<b>5</b>
<b>1. LOT 1: IDENTIFYING SECURITY BEST PRACTICES FOR PRIVACY PROTECTION PURPOSES</b> .....	<b>6</b>
1.1 GENERAL DESCRIPTION OF THE REQUIRED SERVICES .....	6
1.2 OBJECTIVES AND TASKS.....	7
1.2.1 TASK 1: Scope definition and data gathering .....	8
1.2.2 TASK 2: Survey on IT security certification among Member States .....	9
1.2.3 TASK 3: Existing implementations of the data security principles under the Data Retention Directive.....	10
1.2.4 TASK 4: Compilation of the two survey reports.....	11
1.2.5 Task (on-going) Project management.....	11
1.3 EXPECTED SKILLS.....	12
1.4 DURATION .....	13
1.5 LIST OF DELIVERABLES.....	13
1.6 DURATION OF THE SERVICE.....	14
1.7 PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATIONS .....	14
1.8 TENDER RESULT AND ESTIMATED CONTRACT VALUE .....	15
1.9 CONTENT AND PRESENTATION OF THE TECHNICAL OFFER.....	15
<b>2. LOT 2 - SECURING PERSONAL DATA IN ONLINE ENVIRONMENTS</b> .....	<b>16</b>
2.1 GENERAL DESCRIPTION OF THE REQUIRED SERVICES .....	16
2.2 OBJECTIVES AND TASKS.....	17
2.2.1 TASK 1: Setting methodology, requirements and the minimum objectives while securing personal data.....	17
2.2.2 TASK 2: Provide recommendations for 3 case studies, selected based on task 1 ...	18
2.2.3 TASK 3: Preparing the report on algorithms and recommended key sizes and other parameter settings .....	18
2.2.4 TASK (on-going): Project management .....	18
2.3 EXPECTED SKILLS.....	19
2.4 DURATION .....	20
2.5 DELIVERABLES.....	20
2.6 DURATION OF THE SERVICE.....	21
2.7 PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATIONS .....	21
2.8 TENDER RESULT AND ESTIMATED CONTRACT VALUE .....	21
2.9 CONTENT AND PRESENTATION OF THE TECHNICAL OFFER.....	21
<b>4. CONTENT AND PRESENTATION OF THE PRICE OFFER</b> .....	<b>23</b>
<b>5. PRICE</b> .....	<b>23</b>
<b>6. PRICE REVISION</b> .....	<b>23</b>
<b>7. COSTS INVOLVED IN PREPARING AND SUBMITTING A TENDER</b> .....	<b>23</b>
<b>8. PERIOD OF VALIDITY OF THE TENDER</b> .....	<b>23</b>
<b>9. PROTOCOL ON PRIVILEGES AND IMMUNITIES OF THE EUROPEAN COMMUNITIES</b> ..	<b>23</b>
<b>10. PAYMENT ARRANGEMENTS</b> .....	<b>23</b>
<b>11. CONTRACTUAL DETAILS</b> .....	<b>23</b>

<b>PART 3 ADMINISTRATIVE DETAILS.....</b>	<b>24</b>
<b>1. FORMAL REQUIREMENTS .....</b>	<b>24</b>
1.1 Address and deadline for submission of the Tender:.....	24
1.2 Presentation of the Offer and Packaging.....	25
1.3 Identification of the Tenderer.....	25
1.4 Participation of consortia.....	27
1.5 Subcontracting.....	27
1.4 Signatures of the Tender.....	28
1.5 Total fixed price.....	28
1.6 Language.....	28
1.7 Opening of the Tenders .....	28
<b>2. GROUNDS FOR EXCLUSION OF TENDERERS .....</b>	<b>28</b>
2.1 Reasons for Exclusion .....	28
2.2 Other reasons for not awarding the Contract.....	29
2.3 Confidentiality and Public Access to Documents.....	29
<b>3. SELECTION CRITERIA.....</b>	<b>30</b>
3.1 Professional Information .....	30
3.2 Financial and Economic Capacity .....	30
3.3 Technical and professional capacity.....	30
<b>4. AWARD CRITERIA .....</b>	<b>31</b>
4.1 Quality of the Offer.....	31
4.2 Price of the Offer.....	32
<b>5. AWARD OF THE CONTRACT .....</b>	<b>32</b>
<b>6. PAYMENT AND STANDARD CONTRACT .....</b>	<b>33</b>
<b>7. VALIDITY.....</b>	<b>33</b>
<b>8. LOTS .....</b>	<b>33</b>
<b>9. ADDITIONAL PROVISIONS .....</b>	<b>33</b>
<b>10. NO OBLIGATION TO AWARD THE CONTRACT .....</b>	<b>33</b>
<b>11. DRAFT CONTRACT .....</b>	<b>33</b>
<b>12. SPECIFIC INFORMATION.....</b>	<b>34</b>
12.1 Timetable .....	34
<b>ANNEX I.....</b>	<b>35</b>
<b>ANNEX II.....</b>	<b>36</b>
<b>ANNEX III.....</b>	<b>37</b>
<b>ANNEX IV .....</b>	<b>39</b>
<b>ANNEX V .....</b>	<b>40</b>
<b>ANNEX VI .....</b>	<b>41</b>
<b>ANNEX VII .....</b>	<b>42</b>
<b>ANNEX VIII .....</b>	<b>43</b>
<b>ANNEX IX Document CHECKLIST .....</b>	<b>44</b>

# PART 1 INTRODUCTION TO ENISA

## 1. CONTEXT

### 1.1 Introduction

ENISA, the European Network and Information Security Agency, is an Agency of the European Union (EU). It was set up to strengthen the capacity of the European Union, its Member States and the business community to prevent, address and respond to network and information security threats.

Computers and other information technology devices, such as smart phones, are now central to how Europe's citizens live their lives. Therefore, protecting digital information and networks is crucial, for society and the European economy.

In order to achieve this goal, ENISA acts as a centre of expertise in network and information security and facilitates cooperation between the public and private sectors. The Agency's mission is to support a high and effective level of Network and Information Security within the EU. Together with the EU-institutions and the Member States, ENISA seeks to develop a culture of Network and Information Security for the benefit of citizens, consumers, business and public sector organizations in the European Union.

### 1.2 Scope

The Agency assists the Commission and the EU Member States, and cooperates with the business community in order to help them to meet the requirements of network and information security. This work supports the smooth functioning of the EU's internal market.

### 1.3 Objectives

The Agency's objectives are as follows:

- Advising and assisting the European Commission and the Member States on information security and in their dialogue with industry to address security in hardware and software products.
- Collecting and analysing data on security incidents in Europe and emerging risks.
- Promoting risk assessment and risk management methods to enhance the Agency's capability to deal with information security threats.
- Awareness-raising and co-operation between different actors in the information security field, notably developing public and private sector partnerships with industry.

## 2. ADDITIONAL INFORMATION

Further information about ENISA can be obtained on its website: [www.enisa.europa.eu](http://www.enisa.europa.eu)

## PART 2 TECHNICAL DESCRIPTION

### A. SCOPE OF THIS TENDER

Within the framework of this Open tender procedure, ENISA would like to find suitably qualified contractors to provide the services as stipulated in the technical specifications outlined below. The tender has been split into 2 standalone projects defined as LOTS.

A tenderer may bid for **one or both LOTS**. The projects are outlined below:

LOT No	Subject of the tender	Maximum budget
LOT 1	Identifying security best practices for privacy protection purposes	€ 60,000.00
LOT 2	Securing personal data in online environments	€ 60,000.00

If bidding for more than one LOT, the tenderer is required to provide completely separate technical bids for each LOT.

If a tenderer decides to bid for more than one LOT, then the *administrative documentation* required to be provided (as outlined in PART 3 - Section 3: SELECTION CRITERIA and Annexes) only needs to be provided once.

## 1. LOT 1: IDENTIFYING SECURITY BEST PRACTICES FOR PRIVACY PROTECTION PURPOSES.

### 1.1 GENERAL DESCRIPTION OF THE REQUIRED SERVICES

ENISA has been contributing to the area of privacy and trust in online environment for several years. During 2013, ENISA will continue its work by providing recommendations on the protection of personal data of EU citizens, based on its information security expertise, in the context of its Work programme (WP<sup>1</sup>), work package “WPK 3.3 Enabling the Information Society”, “Deliverable D1: Supporting EC activities in the implementation of trustmarks. Identifying best practice from security certification that could be deployed for privacy certification and trustmark”.

Within this project, ENISA intends to conduct two activities:

- Survey of existing information technology security certification schemes across EU Member States for supporting the activities of the European Commission DG JUST and JRC<sup>2</sup> on developing recommendations for a pan-European privacy certification approach.
- Identifying the relevant data security specifications/standards used for securing personal data in the framework of Data Retention Directive in EU MS.

The first activity will explore the area of information technology security certification. Certification consists of the attestation, by an independent third party assessment, that certain requirements and best practices are being observed. Several certification schemes to accredit the security of information technology products and services (hereinafter IT security) are currently in place in EU Member States. However, the fields of privacy certification and eGovernment services security certification and have been until now largely unexplored.

The proposal for review of data protection<sup>3</sup> legislation (published by the European Commission in January 2012 and which will replace the existing Data Protection Directive) contains specific provisions relevant to certification, data protection seals and marks. The proposal foresees encouraging the adoption of data protection certification mechanisms in order to enhance transparency and compliance.

In order to provide guidance for the adoption of a framework on privacy certifications, as well as for eGovernment services certification, ENISA will contribute by conducting a survey on existing IT security certification schemes across EU Member State. The final aim of this survey will be to provide a set of recommendations on aspects of security certification that could be applied to privacy and eGovernment services certification.

---

<sup>1</sup> ENISA WP 2013 available at <http://www.enisa.europa.eu/publications/programmes-reports/work-programme-2013>

<sup>2</sup> JRC launched a project to propose a pan-European approach for privacy certification in the EU in collaboration with EC DGJUST.

<sup>3</sup> European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012, available at:

[http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_11\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf)

The second survey will explore implementations of the data security principles under the Data Retention Directive across EU Member States. The Data Retention Directive<sup>4</sup> lays down the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime. This retention of users' data should be conducted following certain data security principles as to guarantee that it is only accessed by authorized personnel in the cases foreseen by the law. To ensure this provision, the Directive lays down in its article 7 that technical and organizational security measures should be in place to protect data against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure; and to ensure that they can be accessed by specially authorized personnel only.

Members States must implement provisions in their national legislation for guarantying the correct application of the art 7 of the Directive. ENISA will conduct a survey on how technical and organisational security measures to protect retained users' data have been implemented across couple of Member States. The aim of this survey will be to provide a set of recommendations for a common European approach based on best practices among Member States. With this activity, ENISA aims to contribute to its objective of increasing users' the trust in the online services.

In conclusion, the expected deliverables from this activity are:

- A survey report on IT security certification across Member States. The report will outline the most relevant IT security regulations, standards and industry specifications which serve as a base for existing certification schemes; describe implemented certification schemes in Member States; and provide recommendations for privacy certification.
- A survey report on existing implementations of the data security principles under the Data Retention Directive across EU Member States. The report will describe the existing provisions on Member States for the implementation of security measures to protect retained users' data, and provide recommendations for a common European approach based on identified best practices.

## 1.2 OBJECTIVES AND TASKS

With this Call for Tenders ENISA aims to collect and analyse data concerning the topics described above.

ENISA expects from the tenderer to include in the offer a project plan and a description of the methods proposed to achieve these expected results. The project plan requires a description of tasks to be carried out, a timeline with clear deadlines and frames for delivery of drafts and review, a description of deliverables, a list of potential parties to contact in order to collect ground information, a methodology for analysing data, a methodology for legal and regulatory research, a Gantt chart, and a quality assurance plan.

---

<sup>4</sup> Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:en:NOT>

ENISA expects the tenderer to perform at least the tasks listed below. Details should be included as part of the offer. However, ENISA would consider any other proposal that adequately corresponds to the requested services.

**Task 1: Scope definition and data gathering for two activities**

- a) Gather information to obtain a general characterization of the domains covered in the surveys.
- b) Rationale for the selection of the Member States and selection of the Member States to be included in the surveys.
- c) Identification of methodology and stakeholders for collecting information

**Task 2: Survey on IT security certification schemes across EU Member State**

- d) Prepare the questionnaires.
- e) Conduct the interviews and gather the data.
- f) Compile, normalize and analyse the information obtained in the surveys.
- g) Develop recommendations.

**Task 3: Survey on the existing implementations of the data security principles under the Data Retention Directive across EU Member States**

- h) Prepare the questionnaires.
- i) Conduct the interviews and gather the data.
- j) Compile, normalize and analyse the information obtained in the surveys.
- k) Develop recommendations.

**Task 4: Compilation of two survey reports**

- l) Compilation of the two survey reports.
- m) Review cycle as agreed with ENISA.
- n) Presentation of the results.

**Task 5: Project management**

- o) Timelines, deliverables, resources, quality assurance, Gantt chart, methodology etc.

Details of each task as it is expected by ENISA are given below.

**1.2.1 TASK 1: Scope definition and data gathering**

The first task of the project covers the preparatory activities aimed to obtaining the relevant information expected from the survey results.

The following activities are to be conducted by the Contractor:

1) Scope definition and data collection

The Contractor should conduct independent research in order to obtain a general overview of the domains covered in the two surveys.



## 2) Selection of the countries to be included in the surveys

The next activity to be conducted is the choice of the EU Member States to be included in the surveys. The selection must cover:

- Survey on IT security certification: at least half of the MSs should be surveyed or a number of member states that would account for at least 50% of the EU population.
- Survey on the implementation of data security principles of the Data Retention Directive: 5- to 7 countries.

A choice of a representative sample of member states covering different cultures and with adequate population/geographic coverage is recommended. Additionally, selection of countries with a wide implementation of the domains covered in the respective survey will be preferred. In the project proposal a clear argumentation should be provided for the choice including the rationale for their selection.

The list of countries to be included in the surveys must be validated by ENISA, who may propose changes to the Contractor.

## 3) Identification of methodology and stakeholders for collecting information

The Contractor should provide ENISA a description of methodology to be used for approaching and obtaining the engagement of the stakeholders. The list of interview candidates must be validated by ENISA, who may propose changes to the Contractor.

The Contractor is encouraged to provide in the project proposal a rationale for selection of the countries and briefly described the proposed methodology for collecting data for the two surveys

### **1.2.2 TASK 2: Survey on IT security certification among Member States**

The first activity within this task consists on the preparation of the questionnaires for the different stakeholders. The results of the previous activities should be used as an input for identifying the key questions, in order to obtain the relevant information for the survey results.

The Contractor is expected to gather information regarding the following aspects:

- 1) Analysis of the IT security certification framework in the Member State: Identification of the existing IT security certification schemes at the national level. A characterization is to be conducted of each scheme which should include the following information:
  - Certification criteria: description of the regulation, standard or industry specification that serves as the base for the certification criteria and identification of the responsible body.
  - Certification enforcement: voluntary or mandatory certification.
  - Certification scheme: self-regulated or publicly regulated certification.
  - Certification domain: addressing specifications of products, management policies, service provision, professional qualifications, etc.

- The certification scheme: description of the accreditation and certification bodies.
- The certification process: brief description of required documentation and the audit or self-assessment process.
- Description of the target sector certification candidates.
- Description of the target sector of certification demanders.
- Maturity of the certification program: Volume of awarded certifications, level of penetration in different markets.

2) Stakeholders' recommendations regarding:

- Approaches for extending the current framework to eGovernment services security certification.
- Approaches for extending the current framework to eGovernment services security certification and to privacy certification.

Following the conduction of the interviews and the collection the data from the replies to the questionnaires and the opinions expressed by key interviewees, the Contractor is expected to carry out qualitative analysis of the data. The objectives of the analysis will be:

- Identify best practices on IT security certification across in EU Member States.
- Provide recommendations for the extension of the IT security certification framework to eGovernment services security certification and to privacy certification

### **1.2.3 TASK 3: Existing implementations of the data security principles under the Data Retention Directive**

The first activity within this task consists on the preparation of the questionnaire. The results of the previous activities should be used as an input for identifying the key questions, in order to obtain the relevant information for the survey results.

The Contractor is expected to gather information regarding the following aspects:

- Legal framework: identification of the existing legal framework on data retention on the telecommunications sector at the national level and of the provisions for technical and organisational security measures for retained users' data.
- Identification of the designated body responsible for the supervision of correct implementation the security measures to protect retained users' data.
- Existence of additional self-promoted industry codes of practice.

1) Description of security measures applied to protect users' data.

The Directive foresees that technical and organisational security measures should be in place to protect data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure; and to ensure that they can be accessed by specially authorised personnel only. The requirements for security measures to guarantee the former should be explored, in particular: organizational and technical measures.

## 2) Audit provisions:

Description of existing provisions regarding the conduction of audits to verify implemented security measures and procedures are compliant with the applicable regulation.

Following the collection the data, the Contractor is expected to carry out qualitative analysis of the data. The objectives of the analysis will be:

1. Outline the main elements of the existing implementations of security measures at a national level in EU Member States.
2. Identify best practices on the existing security measures across countries and provide recommendations for a single European approach by taking into account the best practices in Member States.

### **1.2.4 TASK 4: Compilation of the two survey reports**

The Contractor will produce two final deliverables, one for Task 2 and one for Task 3.

Each report should include:

- A description of the domain covered in the survey, based on the research carried out by the Contractor
- The key findings from the conducted interviews and from the informal discussions with stakeholders
- The main conclusions from the analysis of the results
- The proposed recommendations

The reports will be reviewed and validated by the Contractor in coordination with ENISA. After this, the Contractor is expected to update the survey report with the comments, suggestions and recommendations of ENISA before issuing a final version.

### **1.2.5 Task (on-going) Project management**

The main objective of this task is to define and implement appropriate management mechanisms, sound planning and resource allocation according to proven expertise and prior knowledge of the subject.

As part of this task the Contractor should also provide justification for subcontracting, interact with ENISA staff and external experts, and provide regular management reporting. This will ensure the punctual delivery of good quality results of this report on budget.

The Contractor is expected to submit to the Agency, prior to the kick off meeting, detailed Gantt Charts and accompanying documentation with sufficient details. These will be negotiated with ENISA and be confirmed as final.

The Gantt charts and related documentation should include:

- Scheduling of all tasks and activities within the tasks
- Identification of 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
- Detailed information on the expertise of the contractors on the tasks and topics of this tender including references to previous, relevant projects,
- Detailed CVs of experts proposed to be involved in all the tasks of the project
- Detailed justification for subcontracting tasks or parts of them. In that case, ENISA requires additional information on the
  - Tasks undertaken by the sub-contractor
  - Expertise of the contractor and its experts
  - Resources allocated to him/her
  - Co-ordination mechanisms among the prime and the sub-contractors
  - Risk management method in case of delayed and/or low quality delivery of sub-contractor's outcomes
  - Official statement of overall responsibility for the whole project and its results by the prime contractor

Based on the Gantt chart, the contractor is expected to deliver the following documents regularly:

- Brief weekly progress report on current activities (as they defined in the Gantt chart) information on the progress achieved, next steps, possible risks affecting project, and risk mitigation measures.
- Early warning reports, at any time, if emerging risks threaten key milestones of the project and when the Agency needs to either be informed or take a decision.
- Minutes from the two-weekly teleconferences with ENISA staff on the progress of the project and its tasks.
- Intermediates and final reports on peer-review progress and quality assurance.

In addition and on demand, the Contractor should be able to provide ENISA with a draft or snapshot of the results produced so far for the deliverables.

### **1.3 EXPECTED SKILLS**

The performance of the above mentioned activities requires professionals that have good academic, professional legal and multi-disciplinary knowledge on all of the following fields:

- Proven solid knowledge and experience in the area of IT security certification schemes, of IT security at the national, European, and international level.

- Previous publications (articles, studies, reports) addressing the areas. List(s) of publications should be included in the proposal; at least 2 experts from the proposer's team should fulfil this requirement;
- Very good understanding of existing international and industry standards in the field of IT security and IT security certification schemes and processes at the national, European, and international level,
- Good understanding of existing legal and regulatory as well as policy aspects in the field of IT security at the national, European, and international level;
- Excellent oral and written language skills in English.

It is expected that possible tenderer may need to use the services of a subcontractor or to form a consortium in order to adequately cover all the specialised areas.

If external experts are considered for certain tasks, their CVs as well as time and budget allocations should be reflected in the proposal

#### 1.4 DURATION

The duration of this work is for around 4.5 months in the period 15<sup>th</sup> March 2013 to 31<sup>st</sup> of July 2013. The Contractor should provide a timeline of the project depicting milestones and interim deliverables. The deadlines should be equated to the following:

(where X = contract signature date):

- Task 1: (Scope definition and data collection) should be finalised not later than X + 1 months.
- Task 2: (Survey) should be finalised by X + 3 months.
- Task 3: (Survey) should be finalised by X + 3 months. (In parallel with task 2).
- Task 4: (Survey reports) should be finalised not later than X + 4.5 months.
- Task 5: (Project Management) is an on-going task throughout this project.

ENISA will provide comments for each stage within a maximum of 2 weeks. The comments from ENISA should be processed by the contractor within a maximum period of 2 weeks.

ENISA may additionally invite external experts to provide feedback and/or recommendations during all stages of the project. The contractor should take into consideration and incorporate the recommendations received by experts in the same previous time frames.

#### 1.5 LIST OF DELIVERABLES

The following deliverables are required from the Contractor:

- **D1:** A list of proposed EU Member States, stakeholders and interview candidates for the IT security certification survey; (linked to **Task 1**);
- **D2:** A list of proposed EU Member States, stakeholders and interview candidates for the retained data security principles survey; (linked to **Task 1**);

- **D3:** The questionnaires for the IT security certification survey (linked to **Task 2**);
- **D4:** A compilation of the interviews responses to the questionnaires and of the informal discussions with stakeholders for the IT security certification survey; (linked to **Task 2**);
- **D5:** The questionnaires for the retained data security principles survey (linked to **Task 3**);
- **D6:** A compilation of the interviews responses to the questionnaires and of the informal discussions with stakeholders for the retained data security principles survey; (linked to **Task 3**);
- **D7:** The draft survey report on IT security certification (linked to **Task 4**)
- **D8:** The draft survey report on retained data security principles (linked to **Task 4**)
- **D9:** The final survey report on IT security certification (linked to **Task 4**)
- **D10:** The final survey report on retained data security principles (linked to **Task 4**)
- **D11:** Project plan and progress reports on predefined milestones (linked to **Task 5**)

The working language of the Agency is English. All documentation related to this activity is expected to be drafted in English, professionally proofread and presented by using the layout indicated by ENISA.

## 1.6 DURATION OF THE SERVICE

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). In its offer the Tenderer should indicate the estimated amount of person days required to accomplish all tasks associated with this procurement.

## 1.7 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 present at ENISA premises for all necessary meetings and for collecting all relevant information to conduct the analysis. For this purpose network based collaborative tools (i.e. videoconferencing) could also be used.

At least the following communication with the Contractor is expected.

- One kick-off meeting to be organised at the ENISA Branch Office in Athens
- Regular video or teleconferences on the progress achieved (every two weeks or at more frequent intervals to be agreed upon).

It should be mentioned that the costs of necessary business trips should be included in the Financial Offer (Annex IV). ENISA will not additionally reimburse the Contractor for taking part in meetings or other events as outlined above.

Informal and regular contacts should be maintained by telephone / Skype / Lync / video conferencing and e-mail.

## 1.8 TENDER RESULT AND ESTIMATED CONTRACT VALUE

The result of the evaluation of tenders will be the awarding of a Service Contract for LOT 1. The total estimated budget cannot exceed **60,000.00 Euros (sixty thousand Euros)**<sup>5</sup> covering all tasks executed and including all costs (e.g. travelling expenses of the contractor etc.).

## 1.9 CONTENT AND PRESENTATION OF THE TECHNICAL OFFER

The Tenderer shall enclose with the **Technical Offer** all documents and information that will enable its offers 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 must address each of the following elements as A MINIMUM in order to be considered to be a valid and conforming offer:

- Description of the skills of the expected contractor
  - The Tenderer will have to present its compliance with the expected skills as described in the relevant section.
- Description of the deliverables
  - The deliverables must be presented as requested in section entitled “Deliverables”
  - The requested proposals and additional details (see section “Deliverables”) must be included in the offer
  - The prospective Contractor is expected to provide insights in the methodology chosen in order to produce 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 prospected contractor must also identify possible risks to the project and propose mitigation measures.

In addition the Contractor is expected to highlight / explain:

- Availability and ability of the Contractor to respond to ENISA request: 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.
- If applicable, ability of the Contractor to manage services of a subcontractor or to work as a consortium in order to adequately cover all the specialised areas.
- 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 call

---

<sup>5</sup> Please note that following implementation of the contract with the successful contractor and depending on the further needs of the contracting authority specifically in the field of endeavour the subject of this contract, the maximum amount contracted may be increased by up to 50% - subject to budget availability.

## 2. LOT 2 - SECURING PERSONAL DATA IN ONLINE ENVIRONMENTS

### 2.1 GENERAL DESCRIPTION OF THE REQUIRED SERVICES

ENISA has been contributing to the area of privacy and trust in online environment for several years. During 2013, ENISA will continue its work by providing recommendations on technological measures to protect and secure personal data of EU citizens in the context of its Work programme (WP<sup>6</sup>), work package “WPK 3.3 Enabling the Information Society”, “Deliverable 2: Recommendations for best practice on data security of personal data/the use of cryptographic techniques for eGov services in Europe”.

One of the main objectives of ENISA, as stated in Article 3 of its Regulation is to assist and support the European Commission and the Member States in their dialogue with industry to address security-related problems, as well as to collect appropriate information and analyse current and emerging risks and, in particular at the European level, those which could produce an impact on the authenticity, integrity and confidentiality of the information accessed and transmitted through electronic communications networks.

The agency launched a study on the use of cryptographic techniques in the EU in 2011<sup>7</sup> in order to identify the relevant documents setting requirements/specifications related to authentication, integrity and confidentiality of information at national and international levels (even beyond EU).

Between the recommendations of the study were:

- Benefits are expected from an EU-wide initiative to specify a common minimum standard for cryptography of unclassified data in e-government services. From a long-term perspective this would not only ensure a certain level of protection for all EU citizens, but also would simplify the exchange of government data between MS – which becomes increasingly important with the increasing mobility of citizens. Providing these guidelines publicly, other stakeholders will benefit from such an initiative, for instance could bring economies of scale to the commercial market outside e-government services.
- Organizations must pro-actively review their encryption documents and solutions, updating them in line with the changing circumstances. Clear processes for withdrawal of compromised or algorithms, or those that are too weak, must be included in the policies.

During 2013, ENISA will work towards creating the framework for a multiannual activity in the area of cryptography with an emphasis on providing revised recommendations and technical specifications for protecting personal data in eGov services. In this area, the recommendations for the use of algorithms, parameters and key lengths need to be updated<sup>8</sup> based on the new discovered vulnerabilities. This project will address these issues.

<sup>6</sup> ENISA WP 2013 available at <http://www.enisa.europa.eu/publications/programmes-reports/work-programme-2013>

<sup>7</sup> ENISA study on the use of Cryptographic Techniques in Europe, available at:

<http://www.enisa.europa.eu/activities/identity-and-trust/library/the-use-of-cryptographic-techniques-in-europe>

<sup>8</sup> ECRYPT NoE, more exactly the review of the report on algorithms and key lengths, was one of the reference sources for a large number of MSs according to our previous study. ECRYPT just published its final update (“ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012)” <http://www.ecrypt.eu.org/documents/D.SPA.20.pdf>) and there is no clear follow up activity in the field in Europe.



Technical protection measures, specified in legal documents, need to be matched with technical specifications in order to secure personal data. For instance EU-wide data security best practice guide should be developed in the context of preventing and minimizing the effect of data breaches.

Article 4 of ePrivacy directive and Article 29 of the proposed data protection regulation<sup>9</sup> also mention technical measures, which have an impact on the notification procedure in the case of data breaches. Further technical description is needed to translate the legal provisions i.e. “[...] *technological protection measures shall render the data unintelligible to any person who is not authorised to access it.*” and to provide a common understanding across the EU. Such work is useful also in the context of secure electronic signatures<sup>10</sup>. Personal data retained for the purpose of data retention directive<sup>11</sup> needs to be secured as well and the technical measures mentioned in legal documents need to be clearly mapped to existing techniques and minimum security requirements.

In conclusion, the expected deliverables from this activity are:

- Recommendations addressing technical measures for securing personal data;
- Report on algorithms and recommended key sizes and other parameter settings.

## 2.2 OBJECTIVES AND TASKS

With this Call for Tenders ENISA aims to set a methodology and the structure for a multiannual activity addressing review and update of security and cryptographic recommendations.

ENISA expects from the tenderer to include in the offer a project plan and a description of the methods proposed to achieve these expected results. The project plan requires a description of tasks to be carried out, a timeline with clear deadlines and frames for delivery of drafts and review, a description of deliverables, a Gantt chart, and a quality assurance plan.

ENISA expects the tenderer to perform at least the tasks listed below. Details should be included as part of the offer. However, ENISA would consider any other proposal that adequately corresponds to the requested services.

### 2.2.1 TASK 1: Setting methodology, requirements and the minimum objectives while securing personal data

- a) Gather the information and the requirements from different legal documents (ePrivacy directive, data protection proposed regulation, data retention directive) that include securing personal data; this activity should be in close collaboration with ENISA.

---

<sup>9</sup> European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012, available at:

[http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_11\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf)

<sup>10</sup> In the CROBIES study reference is made to possible involvement of ENISA in the process of establishing the Lists of algorithms and parameters for secure electronic signatures. *CROBIES : Study on Cross-Border Interoperability of eSignatures*, last version July 2010, available at: [http://ec.europa.eu/information\\_society/policy/esignature/crobies\\_study/index\\_en.htm](http://ec.europa.eu/information_society/policy/esignature/crobies_study/index_en.htm) and see also: *Note on the “Algo Paper” issue*, CROBIES deliverable, July 2010, available at: [http://ec.europa.eu/information\\_society/policy/esignature/docs/crobies\\_deliverables/crobiesd5.3.pdf](http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd5.3.pdf)

<sup>11</sup> Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:en:NOT>

- b) Identify the relevant objectives (i.e. confidentiality, integrity, authentication and non-repudiation while data is stored, transferred etc.) to be achieved while protecting/securing personal data; Provide a structure for these objectives and matching them with relevant requirements i.e. cryptographic techniques.
- c) Prepare a general framework for recommendations (for task 2) and the structure for the list of recommended cryptographic algorithms, to be used for 3.

### **2.2.2 TASK 2: Provide recommendations for 3 case studies, selected based on task 1**

- a) Prepare recommendations for 3 case studies, agreed with ENISA based on the work carried out at Task 1. (i.e. for technological protection measures mentioned/identified at task 1.a);
- b) Identify challenges, threats, and research requirements in the field.

### **2.2.3 TASK 3: Preparing the report on algorithms and recommended key sizes and other parameter settings**

- a) Compilation of recommendations. This report should provide a list of recommended cryptographic algorithms (e.g. block ciphers, hash functions, signature schemes, etc.) and recommended key sizes and other parameter settings (where applicable) to reach specified security objectives.
- b) The focus should be on algorithms with reasonable practical use, mature, which are part of standards or are implemented in services and applications

### **2.2.4 TASK (on-going): Project management**

The main objective of this task is to define and implement appropriate management mechanisms, sound planning and resource allocation according to proven expertise and prior knowledge of the subject.

As part of this task the Contractor should also provide justification for subcontracting, interact with ENISA staff and external experts, and provide regular management reporting. This will ensure the punctual delivery of good quality results of this report on budget.

The Contractor is expected to submit to the Agency, prior to the kick off meeting, detailed Gantt Charts and accompanying documentation with sufficient details. These will be negotiated with ENISA and be confirmed as final.

The Gantt charts and related documentation should include:

- Scheduling of all tasks and activities within the tasks
- Identification of 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
- Detailed information on the expertise of the contractors on the tasks and topics of this tender including references to previous, relevant projects,
- Detailed CVs of experts proposed to be involved in all the tasks of the project
- Detailed justification for subcontracting tasks or parts of them. In that case, ENISA requires additional information on the
  - Tasks undertaken by the sub-contractor
  - Expertise of the contractor and its experts
  - Resources allocated to him/her
  - Co-ordination mechanisms among the prime and the sub-contractors
  - Risk management method in case of delayed and/or low quality delivery of sub-contractor's outcomes
  - Official statement of overall responsibility for the whole project and its results by the prime contractor

Based on the Gantt chart, the contractor is expected to deliver the following documents regularly:

- Brief weekly progress report on current activities (as they defined in the Gantt chart) information on the progress achieved, next steps, possible risks affecting project, and risk mitigation measures.
- Early warning reports, at any time, if emerging risks threaten key milestones of the project and when the Agency needs to either be informed or take a decision.
- Minutes from the bi-weekly teleconferences with ENISA staff on the progress of the project and its tasks.
- Intermediates and final reports on peer-review progress and quality assurance.

In addition and on demand, the Contractor should be able to provide ENISA with a draft or snapshot of the results produced so far for the deliverables

### **2.3 EXPECTED SKILLS**

The performance of the above mentioned activities requires professionals that have good academic and professional knowledge on the following fields:

- Proven knowledge and experience in the areas of security, authenticity, integrity and confidentiality of the information and cryptography;
- Previous publications (articles, studies, reports) addressing cryptography and security. List(s) of publications should be included in the proposal; at least 4 experts from the proposer's team should fulfil this requirement;
- Previous involvement in projects addressing the above mentioned topics;
- Excellent Project Management skills;

- Experience in writing reports on technical issues for non-technical audience;
- Excellent communication skills;
- English as working language.

It is expected that possible tenderer may need to use the services of a subcontractor or to form a consortium in order to adequately cover all the specialised areas.

If external experts are considered for certain tasks, their CVs as well as time and budget allocations should be reflected in the proposal

## 2.4 DURATION

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). In its offer the Tenderer should indicate the estimated amount of person days required to accomplish all tasks associated with this Call for Tenders.

The successful contractor should cooperate with relevant ENISA experts throughout the whole process of preparation of the report; progress reports should be provided and conference calls agreed on at least a two weekly basis.

The tasks should be accomplished, with the correspondent deliverables, within the following deadlines:

- Task 1: 5<sup>th</sup> of April 2013
- Task 2: 31<sup>th</sup> of May 2013
- Task 3: 31<sup>th</sup> of August 2013
- Task 4: on-going throughout the project.

ENISA will provide comments for each stage within a maximum of 2 weeks. The comments from ENISA (or external experts) should be processed within a maximum period of 2 weeks.

The final recommendation report should be finalized and presented to ENISA not later than the 31<sup>st</sup> of August, 2013. The comments from ENISA (or external experts) on the final recommendations report should be processed until the 30<sup>th</sup> of September 2013 at the latest.

ENISA may additionally invite external experts to provide feedback and/or recommendations during all stages of the project. The contractor should take into consideration and incorporate the recommendations received by experts in the same time frames

## 2.5 DELIVERABLES

The following deliverables are required from the Contractor:

- **D1:** Methodology and security measures for securing personal data; (linked to **Task 1**);
- **D2-D4:** Recommendations for the agreed case studies (linked to **Task 2**);

- **D5:** Report on algorithms and recommended key sizes and other parameter settings (linked to **Task 3**);
- **D6:** Project plan and progress reports on predefined milestones (linked to **Task 4**)

The working language of the Agency is English. All documentation related to this activity is expected to be drafted in English, professionally proofread and presented by using the layout indicated by ENISA.

## 2.6 DURATION OF THE SERVICE

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). In its offer the Tenderer should indicate the estimated amount of person days required to accomplish all tasks associated with this procurement.

## 2.7 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 present at ENISA premises for all necessary meetings and for collecting all relevant information to conduct the analysis. For this purpose network based collaborative tools (i.e. videoconferencing) could also be used.

At least the following communication with the Contractor is expected.

- One kick-off meeting to be organised at ENISA Branch Office in Athens
- Regular video or teleconferences on the progress achieved (every two weeks or at more frequent intervals to be agreed upon).

It should be mentioned that the costs of necessary business trips should be included in the Financial Offer (Annex I). ENISA will not additionally reimburse the Contractor for taking part in meetings or other events as outlined above.

Informal and regular contacts should be maintained by telephone / Skype / Lync / video conferencing and e-mail.

## 2.8 TENDER RESULT AND ESTIMATED CONTRACT VALUE

The result of the evaluation of tenders will be the awarding of a Service Contract for Lot 2. The total estimated budget cannot exceed **60,000.00 Euros (sixty thousand Euros)**<sup>12</sup> covering all tasks executed and including all costs (e.g. travelling expenses of the contractor etc.).

## 2.9 CONTENT AND PRESENTATION OF THE TECHNICAL OFFER

The Tenderer shall enclose with the **Technical Offer** all documents and information that will enable its offers to be assessed in terms of quality and of compliance with the Specifications. An

---

<sup>12</sup> Please note that following implementation of the contract with the successful contractor and depending on the further needs of the contracting authority specifically in the field of endeavour the subject of this contract, the maximum amount contracted may be increased by up to 50% - subject to budget availability.

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 must address each of the following elements as A MINIMUM in order to be considered to be a valid and conforming offer:

- Description of the skills of the expected contactor
  - The Tenderer will have to present its compliance with the expected skills as described in the relevant section.
- Description of the deliverables
  - The deliverables must be presented as requested in section entitled “Deliverables”
  - The requested proposals and additional details (see section “Deliverables”) must be included in the offer
  - The prospective Contractor is expected to provide insights in the methodology chosen in order to produce 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 prospected contactor must also identify possible risks to the project and propose mitigation measures.
- In addition the Contractor is expected to highlight / explain
  - Availability and ability of the Contractor to respond to ENISA request: 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.
  - If applicable, ability of the Contractor to manage services of a subcontractor or to work as a consortium in order to adequately cover all the specialised areas.
- 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 call.

## **The following specifications are common to BOTH LOTS:**

### **4. CONTENT AND PRESENTATION OF THE PRICE OFFER**

The Price offer(s) must be drawn up using the Financial Offer template provided (see Annex IV).

### **5. 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.

### **6. PRICE REVISION**

Prices submitted in response to this Tender shall be fixed and not subject to revision.

### **7. COSTS INVOLVED IN PREPARING AND SUBMITTING A TENDER**

ENISA will not reimburse any costs incurred in the preparation and submission of a Tender. Any such costs must be paid by the Tenderer.

### **8. PERIOD OF VALIDITY OF THE TENDER**

Tenderers must enclose a confirmation that the prices given are valid for (90) ninety days from the date of submission of the tender.

### **9. 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.

### **10. PAYMENT ARRANGEMENTS**

Payments under the Contract shall be carried out subject to prior approval of the Services by ENISA within 30 days after an invoice is submitted to ENISA. 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.

### **11. CONTRACTUAL DETAILS**

A model of the Service Contract is proposed to the successful candidate(s) - see Annex V.

***Please note that the general conditions of our standard service contract cannot be modified. Submission of a tender by a potential contractor implies acceptance of this contract and all of the terms and conditions contained therein. It is strongly recommended that you have this draft contract checked and passed by your legal section before committing to submitting an offer.***

## PART 3 ADMINISTRATIVE DETAILS

### 1. FORMAL REQUIREMENTS

#### 1.1 Address and deadline for submission of the Tender:

You are invited to tender for this project and requested to submit your tender no later than **28 January 2013** either by:

- a) **Registered post or express courier**. The postal service's dated stamp or the courier company's printed delivery slip and stamp will constitute proof of compliance with the deadline given above:

or

- b) **Hand-delivery** (direct or through any authorised representative of the Tenderer) by 17.00 hours on **28 January 2013** at the latest to the address shown below (please, be informed that only delivery during working hours 09:00-17:00 hrs. is accepted). In the case of hand-delivery, in order to establish proof of the date of deposit, the depositor will receive from an official at the below-mentioned address, a receipt which will be signed by both parties, dated and time stamped.

Please note that in this case it is the date and time actually received at the ENISA premises that will count.

**Please Note:** Due to frequent delays encountered with the postal services in Europe, we would ***strongly suggest that you use a courier service***. It is important to avoid delays to the programmed Opening and Evaluation dates as this will in turn delay the contract award, thereby affecting project completion dates.

The offer must be sent to one of the following addresses:

Postal Address		Express Courier & Hand Delivery
European Network and Information Security Agency (ENISA)  For the attention of: The Procurement Officer PO Box 1309 71001 Heraklion Greece	or	European Network and Information Security Agency (ENISA)  For the attention of The Procurement Officer Science and Technology Park of Crete (ITE) Vassilika Vouton 700 13 Heraklion Greece

Please note that late despatch will lead to exclusion from the award procedure for this Contract.



## 1.2 Presentation of the Offer and Packaging

The offer (consisting of one original and two copies) should be enclosed in two envelopes, both of which should be sealed. If self-adhesive envelopes are used, they should be further sealed with adhesive tape, upon which the Tenderer's signature must appear.

The **outer envelope**, in addition to the above-mentioned ENISA address, should be addressed as follows:

<p>OPEN CALL FOR TENDER NO.      <b>ENISA P/18/12/TCD</b></p> <p><b>“ Enabling the information society - Securing personal data in online environments ”</b></p> <p>NOT TO BE OPENED BY THE MESSENGER/COURIER SERVICE</p> <p>NOT TO BE OPENED BY THE OPENING COMMITTEE BEFORE <b>8<sup>th</sup> FEB 2013</b> TENDERED BY THE FIRM: &lt;PLEASE INSERT NAME OF THE TENDERER/COMPANY&gt;</p>
---

The **inner envelope** should be addressed as follows:

<p>OPEN CALL FOR TENDER NO.      <b>ENISA P/18/12/TCD</b></p> <p><b>“ Enabling the information society - Securing personal data in online environments ”</b></p> <p>NOT TO BE OPENED BY THE OPENING COMMITTEE BEFORE <b>8<sup>th</sup> FEB 2013</b> TENDERED BY THE FIRM: &lt;PLEASE INSERT NAME OF THE TENDERER/COMPANY&gt;</p>
--

## 1.3 Identification of the Tenderer

Tenderers are required to complete the **Legal Entity Form (Annex I)** which must be signed by a representative of the Tenderer authorised to sign contracts with third parties. There is one form for 'individuals', one for 'private entities' and one for 'public entities'. A standard form is provided for each category - please choose whichever is applicable. In addition to the above, a **Financial Identification Form** must be filled in and signed by an authorised representative of the Tenderer and his/her bank (or a copy of the bank account statement instead of bank's signature). A specimen form is provided in **Annex II**. Finally a **Declaration by Authorised Representative (Annex VI)** must also be completed for internal administrative purposes.

The **Legal Entity Form** must be supported by the following documents relating to each Tenderer in order to show its name, address and official registration number:

**a) For private entities:**

- A legible copy of the instrument of incorporation or constitution, and a copy of the statutes, if they are contained in a separate instrument, or a copy of the notices of such constitution or incorporation published in the national or other official journal, if the legislation which applies to the Tenderer requires such publication.
- If the instruments mentioned in the above paragraph have been amended, a legible copy of the most recent amendment to the instruments mentioned in the previous indent, including that involving any transfer of the registered office of the legal entity, or a copy of the notice published in the relevant national or other official journal of such amendment, if the legislation which applies to the Tenderer requires such publication.
- If the instruments mentioned in the first paragraph have not been amended since incorporation and the Tenderer's registered office has not been transferred since then, a written confirmation, signed by an authorised representative of the Tenderer, that there has been no such amendment or transfer.
- 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.
- If the above documents do not show the registration number, a proof of registration, as prescribed in their country of establishment, on one of the professional or trade registers or any other official document showing the registration number.
- If the above documents do not show the VAT number, a copy of the VAT registration document, where applicable.

**b) For Individuals:**

- A legible copy of their identity card or passport.
- Where applicable, a proof of registration, as prescribed in their country of establishment, on one of the professional or trade registers or any other official document showing the registration number.
- If the above documents do not show the VAT number, a copy of the VAT registration document, where applicable.

**c) For Public Entities:**

- A copy of the resolution decree, law, or decision establishing the entity in question or failing that, any other official document attesting to the establishment of the entity.

**All tenderers must provide their Legal Entity Form (Annex I) as well as the evidence mentioned above.**

**In case of a joint bid, only the co-ordinator must return the Financial Identification form (Annex II).**

The Tenderer must be clearly identified, and where the Tender is submitted by an organisation or a company, the following administrative information and documents must be provided:

Full name of organisation/company, copy of legal status, registration number, address, person to contact, person authorised to sign on behalf of the organisation (copy of the official mandate must be produced), telephone number, facsimile number, VAT number, banking details: bank name, account name and number, branch address, sort code, IBAN and SWIFT address of bank: a bank identification form must be filled in and signed by an authorised representative of each Tenderer and his banker.

Tenders must be submitted individually. If two or more applicants submit a joint bid, one must be designated as the lead Contractor and agent responsible.

#### **1.4 Participation of consortia**

Consortia, may submit a tender on condition that it complies with the rules of competition. The 'Consortium Form' (Annex VII) must be completed and submitted with your offer.

A consortium may be a permanent, legally-established grouping or a grouping which has been constituted informally for a specific tender procedure. Such a grouping (or consortia) must specify the company or person heading the project (the leader) and must also submit a copy of the document authorising this company or person to submit a tender. All members of a consortium (i.e., the leader and all other members) are jointly and severally liable to the Contracting Authority.

In addition, each member of the consortium must provide the required evidence for the exclusion and selection criteria (*Articles 2 and 3 below*). Concerning the selection criteria "technical and professional capacity", the evidence provided by each member of the consortium will be checked to ensure that the consortium as a whole fulfils the criteria.

The participation of an ineligible person will result in the automatic exclusion of that person. In particular, if that ineligible person belongs to a consortium, the whole consortium will be excluded.

#### **1.5 Subcontracting**

In well justified cases and subject to approval by ENISA, a contractor may subcontract parts of the services. The 'Sub-contractors Form' (Annex VIII) must be completed and submitted with your offer.

Contractors must state in their offers what parts of the work, if any, they intend to subcontract, and to what extent (% of the total contract value), specifying the names, addresses and legal status of the subcontractors.

The sub-contractor must not sub-contract further.

Sub-contractors must satisfy the eligibility criteria applicable to the award of the contract. If the identity of the intended sub-contractor(s) is already known at the time of submitting the tender, all sub-contractors must provide the required evidence for the exclusion and selection criteria.

If the identity of the sub-contractor is not known at the time of submitting the tender, the tenderer who is awarded the contract will have to seek ENISA's prior written authorisation before entering into a sub-contract.

Where no sub-contractor is given, the work will be assumed to be carried out directly by the bidder.

#### **1.4 Signatures of the Tender**

Both the technical and the financial offer must be signed by the Tenderer's authorised representative or representatives (preferably in blue ink).

#### **1.5 Total fixed price**

A total fixed price expressed in Euro must be included for each LOT in the Tender. The contract prices shall be firm and not subject to revision.

#### **1.6 Language**

Offers shall be submitted in one of the official languages of the European Union (preferably in English).

#### **1.7 Opening of the Tenders**

The public opening of received tenders will take place on **8<sup>th</sup> February 2013 at 10:00am** 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, at least 48 hours prior to the opening session.

## **2. GROUNDS FOR EXCLUSION OF TENDERERS**

### **2.1 Reasons for Exclusion**

Pursuant to Article 29 of Council Directive 92/50/EC relating to Public Service Contracts and to Article 93 of the Financial Regulation, ENISA will exclude Tenderers from participation in the procurement procedure if:

- They are bankrupt or being wound up, are having their affairs administered by the courts, have entered into an arrangement with creditors, have suspended business activities, are the subject of proceedings concerning those matters, or
- Are in any analogous situation arising from a similar procedure provided for in national legislation or regulations;
- They have been convicted of an offence concerning their professional conduct by a judgement which has the force of res judicata;

- They have been guilty of grave professional misconduct proven by any means which the contracting authority can justify;
- They have not fulfilled obligations relating to the payment of social security contributions or the payment of taxes in accordance with the legal provisions of the country in which they are established or with those of the country of the contracting authority or those of the country where the contract is to be performed;
- They have been the subject of a judgement which has the force of *res judicata* for fraud, corruption, involvement in a criminal organisation or any other illegal activity detrimental to the Communities' financial interests;
- Following another procurement procedure or grant award procedure financed by the Community budget, they have been declared to be in serious breach of contract for failure to comply with their contractual obligations.

Tenderers must certify that they are not in one of the situations listed in sub-article 2.1 (see Annex III: Exclusion criteria and non-conflict of interest form). If the tender is proposed by a consortium this form must be submitted by each partner.

## **2.2 Other reasons for not awarding the Contract**

Contracts may not be awarded to Candidates or Tenderers who, during the procurement procedure:

- a. Are subject to a conflict of interest;
- b. Are guilty of misrepresentation in supplying the information required by the contracting authority as a condition of participation in the contract procedure or fail to supply this information;
- c. Any attempt by a Tenderer to obtain confidential information, enter into unlawful agreements with competitors or influence the evaluation committee or ENISA during the process of examining, clarifying, evaluating and comparing tenders will lead to the rejection of his offer and may result in administrative penalties.

See last paragraph point 2.1.

## **2.3 Confidentiality and Public Access to Documents**

In the general implementation of its activities and for the processing of tendering procedures in particular, ENISA observes the following EU regulations:

- 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;
- 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;

- 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.

### 3. 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.

#### 3.1 Professional Information

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

#### 3.2 Financial and Economic Capacity

Proof of financial and economic standing may be furnished by one or more of the following references:

- a) Annual accounts, balance sheet or extracts from balance sheets for at least the last 2 years for which accounts have been closed, shall be presented where publication of the balance sheet is required under company law of the country in which the economic operator is established;

It is necessary that the extracts from balance sheets be dated, signed and stamped by the authorised representatives of the tenderer.

- b) Statement of the undertaking's overall turnover and its turnover in respect of the services to which the contract relates for the previous two financial years.
- c) If tenderers will call on the competences of another entity (for example, a parent company), a written undertaking by the said entity certifying that it will make available to the tenderers the resources required to implement the contract.

If, for any valid reason, the service provider is unable to provide the references requested by the contracting authority, he may prove his economic and financial standing by any other document which the contracting authority considers appropriate, following a request for clarification before the tender expiry date.

#### 3.3 Technical and professional capacity

**The following applies to LOTS 1 and 2 identically:**

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, has to be included, in which the Tenderer has to make statements about (in line with Part 2 – Art 1.3 for LOT 1, Art 2.3 for LOT 2 - Expected Skills):

- His technical knowledge and experience in the relevant technical areas (including references to projects similar to the one proposed by this tender);
- His management capability (including, but not limited to, project management in a European context and quality assurance).

#### 4. AWARD CRITERIA

The following applies to LOTS 1 and 2 identically:

##### 4.1 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.	<b>Technical compliance</b>	Compliance with the technical descriptions (part 2 of this document)	30/100
2.	<b>Quality and accuracy of content and structure</b>	Quality of the proposal and accuracy of the description to provide the requested services	25/100
3.	<b>Project Team</b>	Composition of project team, direct involvement of senior staff, and distributions of tasks amongst experts; proposed workflows and quality review cycles	20/100
4.	<b>Methodology</b>	Selected methodology and project management	25/100
<b>Total Qualitative Points (QP)</b>			<b>100</b>

##### 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.

#### 4.2 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; Article 1.8 for LOT 1 and Article 2.8 for LOT 2 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

$$PP = (PC / PB) \times 100$$

Where;

- PP** = Weighted price points  
**PC** = Cheapest bid price received  
**PB** = Bid price being evaluated

#### 5. AWARD OF THE CONTRACT

The contract for each Lot 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:

$$TWP = (QP \times 0.7) + (PP \times 0.3)$$

Where;

- QP** = Qualitative points  
**PP** = Weighted 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.

## 6. PAYMENT AND STANDARD CONTRACT

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 V)

In drawing up their bid, the Tenderer should take into account the provisions of the standard contract which include the “General terms and conditions applicable to contracts”

## 7. VALIDITY

Period of validity of the Tender: 90 days from the closing date given above. The successful Tenderer must maintain its Offer for a further 220 days from the notification of the award.

## 8. LOTS

This Tender is divided into two Lots.

- LOT 1 – Identifying security best practices for privacy protection purposes
- LOT 2 – Securing personal data in online environments

## 9. ADDITIONAL PROVISIONS

- Changes to tenders will be accepted only if they are received on or before the final date 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.

## 10. 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.

## 11. DRAFT CONTRACT

A Service Contract will be proposed to the selected candidate for each LOT. A draft copy of which is included as Annex V to this tender.

***Please note that the general conditions of our standard service contract cannot be modified. Submission of a tender by a potential contractor implies acceptance of this contract and all of the terms and conditions contained therein. It is strongly recommended that you have this draft contract checked and passed by your legal section before committing to submitting an offer.***

## 12. SPECIFIC INFORMATION

### 12.1 Timetable

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

Title: **“Enabling the information society - Securing personal data in online environments”**

**ENISA P/18/12/TCD**

#### Summary timetable comments

Launch of tender - Contract notice to the Official Journal of the European Union (OJEU)	<b>6 December 2012</b>	
Deadline for request of information from ENISA	<b>22 January 2013</b>	
Last date on which clarifications are issued by ENISA	<b>24 January 2013</b>	
Deadline for submission of offers	<b>28 January 2013</b>	in case of hand-delivery (05:00 pm local time. This deadline is fixed for the receipt of the tender in ENISA's premises)
Opening of offers	<b>8 February 2013</b>	At 10:00 Greek time
Date for evaluation of offers	<b>8 February 2013</b>	At 11:00 Greek time
Notification of award to the selected candidate	Mid February 2013	Estimated
14 day standstill period commences	Mid February 2013	Estimated
Contract signature	Early March 2013	Estimated
Commencement date of activities	As per tender	Estimated
Completion date of activities	As per tender	Estimated

# ANNEX I

## Legal Entity Form

The specific form, for either a;

- c) public entity,
- d) private entity or
- e) individual entity,

is available for download in each of the 22 official languages at the following address: [http://ec.europa.eu/budget/execution/legal\\_entities\\_en.htm](http://ec.europa.eu/budget/execution/legal_entities_en.htm)

*Please download the appropriate form, complete the details requested and include in your tender offer documentation.*

## ANNEX II

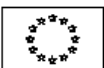
### FINANCIAL IDENTIFICATION FORM

- SPECIMEN FOR THE TENDERER -

(to be completed by the Tenderer and his financial institution)

The Tenderer's attention is drawn to the fact that this document is a sample only, and a specific form in each of the 22 official languages is available for download at the following address:

[http://ec.europa.eu/budget/execution/ftiers\\_en.htm](http://ec.europa.eu/budget/execution/ftiers_en.htm)

	<b>FINANCIAL IDENTIFICATION</b>
PRIVACY STATEMENT	<a href="http://ec.europa.eu/budget/execution/ftiers_fr.htm">http://ec.europa.eu/budget/execution/ftiers_fr.htm</a>
<b>ACCOUNT NAME</b>	
ACCOUNT NAME <sup>(1)</sup>	<input type="text"/>
	<input type="text"/>
ADDRESS	<input type="text"/>
	<input type="text"/>
TOWN/CITY	<input type="text"/>
POSTCODE	<input type="text"/>
COUNTRY	<input type="text"/>
<b>CONTACT</b>	
CONTACT	<input type="text"/>
TELEPHONE	<input type="text"/>
FAX	<input type="text"/>
E - MAIL	<input type="text"/>
<b>BANK</b>	
BANK NAME	<input type="text"/>
	<input type="text"/>
BRANCH ADDRESS	<input type="text"/>
	<input type="text"/>
TOWN/CITY	<input type="text"/>
POSTCODE	<input type="text"/>
COUNTRY	<input type="text"/>
ACCOUNT NUMBER	<input type="text"/>
IBAN <sup>(2)</sup>	<input type="text"/>
REMARKS:	<input type="text"/>
<b>BANK STAMP + SIGNATURE OF BANK REPRESENTATIVE</b> (Both Obligatory) <sup>(3)</sup>	<b>DATE + SIGNATURE ACCOUNT HOLDER :</b> (Obligatory)
<input type="text"/>	<input type="text"/>
	DATE <input type="text"/>
<small>(1) The name or title under which the account has been opened and not the name of the authorized agent (2) If the IBAN Code (International Bank account number) is applied in the country where your bank is situated (3) It is preferable to attach a copy of recent bank statement, in which event the stamp of the bank and the signature of the bank's representative are not required. The signature of the account-holder is obligatory in all cases.</small>	

## ANNEX III

### DECLARATION OF HONOUR

WITH RESPECT TO THE

### EXCLUSION CRITERIA AND ABSENCE OF CONFLICT OF INTEREST

The undersigned: ..... (Please print name)

in his/her own name (if the economic operator is a natural person)

or

representing (if the economic operator is a legal entity)

Official name of the company/organisation: .....

.....

Official legal form: .....

Official address in full: .....

.....

.....

VAT (Tax) registration number:

.....

**Declares that the company or organisation that he/she represents:**

- is not bankrupt or being wound up, is not having its affairs administered by the courts, has not entered into an arrangement with creditors, has not suspended business activities, is not the subject of proceedings concerning those matters, and is not in any analogous situation arising from a similar procedure provided for in national legislation or regulations;
- has not been convicted of an offence concerning professional conduct by a judgment which has the force of res judicata;
- has not been guilty of grave professional misconduct proven by any means which the contracting authorities can justify;
- has fulfilled obligations relating to the payment of social security contributions or the payment of taxes in accordance with the legal provisions of the country in which it is established or with those of the country of the contracting authority or those of the country where the contract is to be performed;

- has not been the subject of a judgement which has the force of res judicata for fraud, corruption, involvement in a criminal organisation or any other illegal activity detrimental to the Communities' financial interests;
- has not been declared to be in serious breach of contract for failure to comply with his contractual obligations subsequent to another procurement procedure or grant award procedure financed by the Community budget.

In addition, the undersigned declares on his honour:

- that on the date of submission of the tender, the company or organisation he represents and the staff proposed for this tender are not subject to a conflict of interests in the context of this invitation to tender; he undertakes to inform the ENISA Agency without delay of any change in this situation which might occur after the date of submission of the tender;
- that the information provided to the ENISA Agency within the context of this invitation to tender is accurate, truthful and complete.

By signing this form, the undersigned acknowledges that they have been acquainted with the administrative and financial penalties described under art 133 and 134 b of the Implementing Rules (Commission Regulation 2342/2002 of 23/12/02), which may be applied if any of the declarations or information provided prove to be false

.....  
Full name

.....  
Signature

.....  
Date

## ANNEX IV

### FINANCIAL OFFER:

### “Enabling the information society - Securing personal data in online environments”

#### ENISA P/18/12/TCD

Please provide your financial lump sum offer for **LOT 1 and/or LOT 2**

<b>LOT Description:</b>	Number of 'Person days' required for completion of project.	<b>Your OFFER</b>
<b>LOT 1 - Identifying security best practices for privacy protection purposes.</b> <i>Please provide your lump sum price for the total deliverables.</i>	P/Days	€
<b>LOT 2 – Securing personal data in online environments</b> <i>Please provide your lump sum price for the total deliverables.</i>	P/Days	€

<b>Print name:</b> <i>(of the Tenderer or authorised representative)</i>	<b>Signature:</b>	<b>Date:</b>
---	-------------------	--------------

# **ANNEX V**

## **Model Service Contract template**

**(See attached file)**



## ANNEX VI

### DECLARATION BY THE AUTHORISED REPRESENTATIVE(S):

<b>NAME OF LEGAL REPRESENTATIVE</b>	
<i>I, the undersigned, certify that the information given in this tender is correct and that the tender is valid.</i>	
First name	
Last name	
Title (e.g. Dr, Mr, Mrs)	
Position (e.g. Manager, Director)	
Telephone number	
Fax number	
e-mail address	
Website	
<b>NAME OF 2<sup>nd</sup> LEGAL REPRESENTATIVE (if applicable)</b>	
<i>I, the undersigned, certify that the information given in this tender is correct and that the tender is valid.</i>	
First name	
Last name	
Title (e.g. Dr, Mr, Mrs)	
Position (e.g. Manager, Director)	
Telephone number	
Fax number	
e-mail address	
Website	

**SIGNATURE:** ..... **DATE:** .....

## ANNEX VII Consortium form

Name of tenderer:

Form of the Consortium: (Please cross the relevant box)

Permanent:  Legally established:  Specifically for this tender:

	Name(s)	Address
<b>Leader of the Consortium</b> <i>(person authorised to conclude contract)</i>		
<b>Partner 1*</b>		
<b>Partner 2*</b>		

\* add additional lines for partners if required. **Note that a subcontractor is not considered to be a partner.**

We confirm, as a partner in the consortium, that all partners are jointly and severally liable by law for the performance of the contract, that the leader is authorised to bind, and receive instructions for and on behalf of, each partner, that the performance of the contract, including payments, is the responsibility of the leader, and that all partners in the consortium are bound to remain in the consortia for the entire period of the contract's performance.

<b>Signature:</b> <i>Leader of consortium</i>	
<b>Date:</b>	
<b>Signature:</b> <i>Partner 1</i>	
<b>Date:</b>	
<b>Signature:</b> <i>Partner 2...etc</i>	
<b>Date:</b>	

## ANNEX VIII Sub-contractors form

	Name(s)	Address
<b>Tenderer</b> (person authorised to sign contract)		
<b>Sub-contractor 1*</b>		
<b>Sub-contractor 2*</b>		

\* add additional lines for subcontractors if required.

As subcontractors for this tender, we confirm that we are willing to perform the tasks as specified in the tender documentation.

<b>Signature:</b> <i>Tenderer</i>	
<b>Date:</b>	
<b>Signature:</b> <i>Subcontractor 1</i>	
<b>Date:</b>	
<b>Signature:</b> <i>Subcontractor 2</i>	
<b>Date:</b>	

## ANNEX IX Document CHECKLIST

### WHAT MUST BE INCLUDED IN THE TENDER SUBMISSION:

PLEASE TICK EACH BOX  AND RETURN THIS CHECKLIST

TOGETHER WITH YOUR OFFER

- 1 **Technical Offer (for each LOT you bid for)**
- 2 **Professional information** (*see Part 3 – Article 3.1*)
- 3 **Proof of financial and economic capacity** (*see Part 3 – Article 3.2*)
- 4 **Proof of technical and professional capacity** (*see Part 3 – Article 3.3*)
- 5 **Legal Entity Form**<sup>13</sup> (*Annex I*) signed and dated
- 6 **Financial Identification Form**<sup>14</sup> (*Annex II*) signed and dated
- 7 **Declaration on Honour on exclusion criteria** (*Annex III*) signed and dated
- 8 **Financial Offer** (*Annex IV*) signed and dated
- 9 **Declaration by Authorised Representative** (*Annex VI*) signed and dated
- 10 **Consortium form** (*Annex VII*) signed and dated - if applicable
- 11 **Sub-Contractors form** (*Annex VIII*) signed and dated - if applicable

***\*The tenderers' attention is drawn to the fact that any total or partial omission of documentation requested may lead the Contracting Authority to exclude the tender from the rest of the procedure.***

**Print name:**

**Signature:**

**Date:**

*(of the Tenderer or authorised representative)*

<sup>13</sup> If you have provided a Legal Entity form to ENISA within the previous 12 months maximum and no details have changed in the meantime, then you may provide a photocopy of this previous form.

<sup>14</sup> If you have provided a Financial Identification form to ENISA within the previous 12 months maximum and no details have changed in the meantime, then you may provide a photocopy of this previous form.