ANNEX I

Provision of consultancy services in the areas of security, business continuity and data protection for the Agency for the Cooperation of Energy Regulators

Lot 1: Consultancy services in the areas of Physical Security and Information Security

Lot 2: Consultancy services in the area of Business Continuity

Lot 3: Consultancy services in the area of Privacy and Personal Data Protection

Single Framework Contracts

TENDER SPECIFICATIONS

OPEN CALL FOR TENDERS

ACER/OP/DO/11/2017

List of Annexes

TABLE OF CONTENTS

1. TITLE OF THE INVITATION TO TENDER

Provision of consultancy services in the areas of security, business continuity and data protection for the Agency for the Cooperation of Energy Regulators, tender no. ACER/OP/DO/11/2017.

The tender is divided into three (3) lots:

- Lot 1: Consultancy services in the areas of Physical Security and Information Security

- Lot 2: Consultancy services in the area of Business Continuity

- Lot 3: Consultancy services in the area of Privacy and Personal Data Protection

Tenderers may submit offers for one or several lots. Tenderers wishing to apply for more than one lot must submit **a separate tender for each lot**.

2. BACKGROUND INFORMATION

The Agency for the Cooperation of Energy Regulators ('the Agency') is a European Union body, established in 2009 by Regulation (EC) No 713/2009[1] and operational since 2010. Based in Ljubljana, Slovenia, the Agency is central to the liberalisation of the EU's electricity and natural gas markets.

The Agency works towards a competitive, sustainable, secure and transparent Internal Energy Market for the benefit of all consumers in the European Union (EU). Its overall mission is to assist National Regulatory Authorities (NRAs) to perform their duties at the EU level and to coordinate their actions whenever necessary. The Agency thus cooperates closely with NRAs, but also with EU institutions, European associations of stakeholders and market participants, especially the European Networks of Transmission System Operators (ENTSOs), to deliver a series of instruments for the completion of a single EU energy market.

The main areas on which the Agency's activities focus are:

- supporting the European market integration: this is mainly done through the development of common network and market rules, as well as through the coordination of regional initiatives which are concrete efforts from market participants to work towards greater integration;

- advising the EU institutions on trans-European energy infrastructure issues: the Agency issues opinions on the ten-year network development plans with a view to making sure that these are in line with the priorities set at EU level. Additional tasks in this area have been assigned to the Agency by Regulation (EU) No 347/2013[2] on guidelines for trans-European energy infrastructure;

[1] Regulation (EC) No 713/2009 of the European Parliament and of the Council of 13 July 2009 establishing the Agency for the Cooperation of Energy Regulators, OJ L 211/1, 14.8.2009.
[2] Regulation (EC) No 347/2013 of the European Parliament and of the Council of 17 April 2013 on guidelines for trans-European energy infrastructure and repealing Decision No 1364/2006/EC and amending Regulations (EC) No 713/2009, (EC) No 714/2009 and (EC) No 715/2009, OJ L 115, 25.04.2013, p.39.

- energy market monitoring: the Agency has a general mission in terms of market monitoring at the EU level and has, since the end of 2011, a very specific responsibility when it comes to monitoring wholesale energy trading under Regulation (EU) No 1227/2011[3] on wholesale energy market integrity and transparency ('REMIT').

More information on the Agency can be found on its website: www.acer.europa.eu.

3. OBJECTIVES OF THE FRAMEWORK CONTRACT(S)

The Agency intends to enter into one or more Framework Contracts (hereinafter referred as the 'FWC') according to which the Contractor(s) shall provide the Agency with highly qualified external expertise to ensure that all required aspects and impacts, in the areas of physical and information security, business continuity and privacy and personal Data Protection, and arising from the applicable relevant legal framework will be properly assessed and implemented.

4. PURPOSE OF THE FRAMEWORK CONTRACT(S)

When performing its tasks stemming from the EU legislation, the Agency is required properly to assess, analyse and implement complex technical and legal aspects in order to ensure physical and information security, business continuity of its operations, as well as to implement appropriate legal, technical and organisational measures ensuring that the Agency is able to demonstrate its adherence to data protection principles such as fairness, transparency, lawfulness, accuracy, data minimisation and security (in terms of integrity and confidentiality) of personal data processing.

The services covered under the FWC(s) should provide the Agency with information and assistance required to prepare for different aspects of internal policy development in the above-mentioned areas, and in particular, but not limited to:

- preparation of drafts and revision of existing or new policies and/or manuals addressed to experts, staff, external stakeholders and/or management;

- establishment of technical, organisational and operational measures for the implementation of policies;

- definition and documentation of technical standards required for the efficient and sustainable establishment of policies;

- definition and documentation of working instructions required for the efficient and sustainable establishment of policies;

- monitoring and assessment of the effectiveness of the current and future implementation of policies, proposing working instructions;

- preparation and execution of regular exercises to verify the preparedness of staff of the Agency and the correctness of the policies and the procedures/working instructions, including updates of the documentation;

- conducting audits and compliance checks;

[3] Regulation (EU) No 1227/2011 of the European Parliament and the Council on wholesale energy market integrity and transparency, OJ L 326, 08.12.2011, p.1

- conducting penetration tests;

- defining and proposing master plans or short/medium term remediation plans, with the aim to reduce the risks and to remove threats also in the event of predictable changes in the existing legislation and standards;

- organisation and delivery of training and awareness raising actions for staff of the Agency.

5. DESCRIPTION OF SERVICES

For each lot separately, the selected Contractor(s) (hereinafter referred as 'the Contractor') shall be able to provide services as listed below.

5.1. Lot 1: Consultancy services in the areas of Physical Security and Information Security

5.1.1. Consultancy in the field of Physical Security

The Agency has needs similar to those of the European Commission, as specified in the provisions of Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission[4], which regulates security and physical security of the European Commission.

The Administrative Board of the Agency adopted a Security Policy and an operational Security Manual (hereinafter referred to 'the Security Policy'), establishing provisions for the implementation of security at the Agency premises (located at Trg republike 3, 1000 Ljubljana, Slovenia), and tailored to its specific needs, effectively to manage security; namely Decision AB No 13/2015 of 17.09.2015 establishing security measures and procedures in the form of a Security Policy and an operational Security Manual, which will be available to the tenderers upon the signature of the non-disclosure agreement (hereinafter referred to 'the NDA') - see Section 10 for further information.

The Agency's Security Officer will be the main contact point between the Agency and the Contractor. However, depending on the nature of the tasks other staff of the Agency may be the designated contact point as well.

In view of the above decisions, the scope of any Specific Contract(s) may include, without limitation, one or more of the following tasks:

- Perform Risk and Threat Assessments to identify areas not covered or only partially covered under the Security Policy and by its actual implementation. If threats arise, the Contractor may be asked to propose additional security measures to overcome the new emerging threats and to reduce the risk to an acceptable level for the Agency;

- Perform Impact Assessments to identify areas not covered or partially covered under the Security Policy, but which may require the introduction of new elements of physical security, due to the possible impact on the Agency's standard operations;

[4] OJ L 72, 17.03.2015, p.41

- Support the Agency in drafting fit-for-purpose policy documentation related to physical security, and ensure that documents related to operational, technical and performance aspects of physical security, are in place, up to date and communicated and shared with the audience proposed by the Contractor and/or specified by the Agency;

- Define an implementation strategy and an implementation plan underlining the organisational processes or modifications to the existing processes, in order to establish a Physical Security Compliance System with the aim to achieve an efficient, sustainable and integrated approach towards its implementation. The strategy and the plan need to respect and take into consideration all other legal frameworks which have been set and which may have an effect on decisions about the establishment of such processes (e.g. Information Security, Business Continuity and Privacy and Data Protection);

- Support and advise the Agency in the rolling-out of sustainable and efficient implementation of all policies, procedures and standards, taking into consideration financial and human resources constraints, and trying to adhere as close as possible to the literal interpretation of the proposed texts;

- Suggest any technical and/or organisational measures to improve preparedness in case of physical security incidents and to reduce the impact on people and assets following such incidents;

- Perform independent audits or support the Agency's staff when performing audits to identify potential issues related to the existing Security Policy and the rules therein;

- Provide advice to the Agency's Security Officer on technical measures and procedures to be introduced in order effectively and efficiently to implement the existing policies and manuals, taking into account and respecting all existing Information Security, Business Continuity, and Privacy and Data Protection policies;

- Design, prepare and deliver training and awareness raising campaigns to pre-defined audiences, tailored on their level of involvement with physical security and for their specific skills, roles and needs;

- Assist in the preparation and/or execution of penetration tests with the aim to verify the preparedness of the Agency staff, the level of compliance with the existing rules and procedures, and the suitability of the policies in line with the Agency's specific environment and specific physical security needs;

- Provide the Agency with notifications of changes to relevant and applicable current EU and/or local (e.g. Slovenian) legislation;

- Provide advice and develop strategies for the implementation of recent or forthcoming legislative changes;

- Assist the Agency in re-drafting and implementing policies in the case of changes to the applicable legislation;

- Monitor the legal compliance of the Security Policy, advise the Agency on efficient ways and practical measures to re-tailor the processes in order to comply with security legislation and/or best practices and/or internationally accepted standards, having as a driving principle the "duty of care" towards the Agency staff (which must be read as a "duty to safeguard the lives and the well-being of the Agency staff and Agency's visitors");

- Support the Agency's staff in the analysis of compliance with newly introduced rules. Propose, where needed and applicable, the introduction of elements of physical security which may be necessary in order to comply with existing policies or to improve current practices;

- Support, coach and advice the Agency and key stakeholders involved in the physical security implementation, on effective ways to establish a functioning security system in compliance with existing regulation(s) and policies, and following the most recent trends and technological standards.

5.1.2. Consultancy in the field of Information Security

The Agency applies, by analogy, similar provisions on information and physical security as those specified in Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 regulating these areas in the European Commission.

Regarding European Union Classified Information (EUCI), the Agency uses as a reference the principles defined in Commission Decision (EU, Euratom) 2015/444 of 13 March 2015[5] on the security rules for protecting EU classified information.

In addition, the Administrative Board of the Agency adopted a Security Policy and an operational Security Manual (hereinafter referred to 'the Security Policy'), establishing provisions for the implementation of security at the Agency premises (located at Trg republike 3, 1000 Ljubljana, Slovenia (Decision AB No 13/2015 which will be available to the tenderers upon the signature of the NDA.

By the end of 2017, the Agency plans to establish an Information Security Policy mainly based on the ISO 27000 Standards.

The Security Manual, incorporated in the Security Policy, includes further elements on Information Security.

The Administrative Board of the Agency in Decision AB No 13/2015 established clear rules for the handling of EUCI (Decision AB No 13/2015 which will be which will be available to the tenderers upon the signature of the NDA – see Section 10 for further information).

At the same time, the REMIT Information Security Policy, which regulates only specific information and activities under Article 12 of Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency (REMIT), is in place and was adopted by Decision of the Agency for the Cooperation of Energy Regulators No 01/2015 of 10 February 2015 which will be available to the tenderers upon the signature of the NDA - see Section 10 for further information.

The Agency Security Officer and the Agency Local Information Security Officer will be the main contact points between the Agency and the Contractor. However, depending on the nature of the task other staff of the Agency may be the designated contact point as well.

Having this in mind, the scope of any Specific Contract(s) may include, without limitation, one or more of the following tasks:

- Perform Risk and Threat Assessments to identify areas not covered or only partially covered under the adopted Information Security Policies. If threats arise, the Contractor

[5] OJ L 72, 17.03.2015, p. 53

may be asked to propose additional security measures to overcome the new emerging threats and to reduce the risk to an acceptable level for the Agency or for any affected Department of the Agency;

– Perform Impact Assessment(s) to identify areas not covered or partially covered under the applicable Information Security Policies, but which may require the introduction of new elements of Information Security, due to the possible impact on the Agency's operations;

- Support the Agency in ensuring that the policy documentation related to Information Security is in place and fit-for-purpose, and that documents related to operational, technical and implementation aspects of the Information Security are in place and are communicated and shared with the audience proposed by the Contractor and/or specified by the Agency;

- Define an implementation strategy and an implementation plan underlining the organisational processes and/or modifications to the existing processes, in order to establish an Information Security Compliance System with the aim to achieve an efficient, sustainable and integrated approach towards its implementation. The strategy and the plan need to respect and to take into consideration all other legal frameworks which have been set and which may have an effect on decisions about the establishment of such processes (e.g. Physical Security, Business Continuity and Security and Privacy and Data Protection);

- Support and advice the Agency in rolling-out a sustainable and efficient implementation of all policies, procedures and standards as described below, taking into consideration financial and human constraints, and trying to adhere as close as possible to the literal interpretation of the texts;

- Suggest any technical and/or organisational measures to improve preparedness in case of information security incidents and to reduce the impact on both assets and people, deriving from such incidents;

- Advise the Agency in implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk, for example, *inter alia* as appropriate:
  (a) pseudonymisation and encryption of personal data;
  (b) ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  (c) ensuring that the Agency is able to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
  (d) defining processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing
  (e) other privacy enhancing-technologies that will allow protection of personal data.

- Perform independent audits and/or support the Agency's staff when performing audits to identify potential issues related to the performance of the existing Information Security framework;

- Advise and assist the Agency in ensuring Privacy and Data Protection by design and by default is implemented in line with Article 25 of General Data Protection Regulation (hereinafter referred to 'GDPR')[6];

[6] Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, p. 1 of 4.5.2016.

- Provide advice to the Agency about technical measures and/or organisational procedures to be introduced in order to effectively and efficiently implement the Information Security Policies, taking into account and respecting all existing Physical Security, Business Continuity and Privacy and Data Protection and privacy policies;

- Design, prepare and deliver training and awareness raising campaigns to pre-defined audiences, tailored to their level of involvement with Information Security and to their specific role, skills and needs;

- Assist in the preparation and/or execution of penetration tests with the aim to verify the preparedness of staff, the level of compliance of technical measures with the existing rules and procedures, and the suitability of the policies in respect to the optimal implementation of Information Security framework;

- Provide the Agency with notifications of changes to current EU and/or local legislation;

- Provide advice in strategies for the implementation of recent or forthcoming legislative changes;

- Assist the Agency in re-drafting and implementing policies in the case of changes to the applicable legislation;

- Monitor the legal compliance with the Information Security policies, advise the Agency on efficient ways and practical measures to re-tailor the organisational processes in order to comply with Information Security legislation and/or best practices and/or standards, having as driving principles the “duty to care” and the “need to know” principles;

- Support the Agency’s staff in the analysis of compliance with newly introduced rules. Propose, where needed and applicable, the introduction of elements of Information Security which may be necessary in order to comply with existing policies or to improve current practices;

- Support, coach and advice the Agency’s staff and key stakeholders involved in the Information Security implementation, on effective ways to establish a functioning Information Security System in compliance with existing regulation(s) and policies, and following the most updated trends and technological standards;

- Consult and coordinate with other contractors which may be involved in delivery of other related services (i.e. arising from services to be procured under Lot 2 and Lot 3) which may have an impact or an influence on the final deliverables of the assigned tasks.

5.2. Lot 2: Consultancy services in the area of Business Continuity

The Agency has adopted and is implementing its Business Continuity Plan (‘BCP’); Director Decision 2016-06 of 23 March 2016 on the adoption of the Business Continuity Plan of the Agency for the Cooperation of Energy Regulators, which will be available to the tenderers upon the signature of the NDA - see Section 10 for further information.

The Business Continuity Coordinator will be the main contact point between the Agency and the Contractor. However, depending on the nature of the task other staff of the Agency may be the designated contact point as well.

In view of the above decision, the scope of any Specific Contract(s) may include, without limitation, one or more of the following tasks:

- Perform Risk Assessments and identify any risk areas only partially covered or not covered under the established Business Continuity Plan. Re-assess areas covered by previous risk assessments (i.e. those identified in the BCP). Suggest risk management strategies and action plans;

- Perform Impact Assessments on the Agency's operations and identify areas not covered or only partially covered under the established Business Continuity Plan, which may require additional attention due to their critical role for the Agency operations;

- Support the Agency to ensure policy documentation related to Business Continuity is in place and fit-for-purpose, and that documents related to operational, technical and implementation aspects of Business Continuity are up to date and communicated to the relevant audience (including also revision and/or update of the Business Continuity Plan);

- Suggest any activity which may improve prevention, detection, preparedness, reaction and response in case of an incident or crisis, and which may boost restoration and recovery of the Agency's critical and essential services, potentially interrupted following a crisis;

- Perform independent audits or support the Agency's staff when performing audits to identify potential issues related to the existing Business Continuity plan and procedures of the Agency;

- Advise the Agency about technical measures and procedures to be introduced in order effectively to implement business continuity, taking into account all the necessary elements of existing Physical Security, Information Security, Privacy and Data Protection or any other relevant polices of the Agency;

- Design, prepare and deliver training and awareness raising campaigns to pre-defined audiences, tailored to their level of involvement in the execution of the Business Continuity Plan and to their specific roles, skills and needs. Support the Agency's staff and key stakeholders in performing their duties in compliance with the rules in place.

- Assist in the preparation and execution of regular exercises with the aim to verify the preparedness of staff, the suitability and efficiency of the Business Continuity Plan in times of crises, as well as the compliance of the Plan with existing rules and procedures;

- Provide the Agency with notifications of changes to current EU and/or local legislation;

- Advise the Agency on and develop strategies for the implementation of recent or forthcoming legislative changes;

- Assist the Agency in re-drafting and in the implementation of policies in the case of changes to the applicable legislation;

- Advise the Agency on efficient ways and practical measures to improve the existing processes in order to comply with current Business Continuity policies and needs and/or best practices and standards. Propose, where appropriate, the addition of elements of Business Continuity which may be necessary in order to comply with existing policies or improve preparedness and the continuity of operations;

– Consult and coordinate with other Contractors which may be involved in the delivery of other related services (i.e. arising from services to be procured under Lot 1 and Lot 3) which may have an impact or an influence on the final deliverables of the assigned tasks.

5.3. Lot 3: Consultancy in the field of Privacy and Personal Data Protection

When processing personal data, the Agency is currently subject to the provisions set in Regulation (EC) No 45/2001 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[7] (hereinafter referred to 'Regulation (EC) No 45/2001').

Regulation (EC) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation[8] (further 'GDPR') entered into force on 25 May 2016 and shall apply from 25 May 2018.

Regulation (EC) No 45/2001 will soon be repealed by means of a new Regulation[9] to align the provisions of Regulation (EC) No 45/2001 with the principles and rules laid down in Regulation (EU) 2016/679. The new regulation replacing Regulation (EC) No 45/2001 will become applicable to the Agency as of 25 May 2018.

The European Data Protection Supervisor[10] (EDPS), the European Union's (EU) independent data protection authority monitors and ensures the protection of personal data at the Agency.

In accordance with Article 24 of Regulation (EC) No 45/2001, one (1) Data Protection Officer (DPO) and two (2) Data Protection Coordinators (DPC) have been appointed at the Agency. Furthermore, the Agency adopted internal implementing rules based on Article 24(8) of Regulation (EC) No 45/2001, namely Director Decision 2017-08 of 30 March 2017 on the adoption of Implementing Rules concerning the Data Protection Officer and repealing Decision No 2015-24 of the Director of the Agency for the Cooperation of Energy Regulators of 6 November 2015, which will be available to the tenderers upon the signature of the NDA - see Section 10 for further information.

The DPO and/or DPCs will be the main contact points between the Agency and the Contractor. However, depending on the nature of the task other staff of the Agency may be the designated contact point as well.

The Agency's processes or may process personal data mainly in the area of:

- Human Resources in the area of EU civil law (e.g. staff appraisal and promotions),
- Information and Physical Security (e.g. security analytics, internet traffic, system logs, e-traffic data, CCTV camera systems, data breaches,),
- IT and communications (e.g. web services, e-mail services, network, active directory services, mobile device management, cloud computing contracts, electronic contracts),
- General Administration (e.g. finance, budget, procurement and facility management),

[7] OJ L 8, p.1 of 12.1.2011.
[8] OJ L 119, p. 1 of 4.5.2016
[9] See Commission Proposal for a Regulation on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, COM(2017) 8 final, of 10 January 2017.
[10] https://edps.europa.eu/edps-homepage_en?lang=en

- Monitoring the EU internal energy market for gas and electricity and cooperation with European energy regulators and other stakeholders (e.g. stakeholder meetings and communication, market monitoring).

Depending on the specificities of a processing activity involving personal data in the Agency, the following EU legal framework, among else, may also apply**:**

- Privacy shield as a replacement scheme for the invalidated Safe Harbor decision, available at: http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm

- 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, OJ L 281, p. 31 of 23.11.1995, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, p. 37 of 31.7.2002, soon to be replaced by the new e-Privacy Regulation, available at: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

- Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) (Text with EEA relevance). OJ L 39, p. 5 of 12.2.2010, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&from=en

- Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ L 385, p. 74 of 29.12.2004, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0915:EN:HTML

- 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. OJ L 145, p. 43 of 31.5.2001, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001R1049&from=EN

Having the above in mind, the scope of any Specific Contracts) may include, without limitation, one or more of the following specific legal services, taking into account the current and future legal framework on personal data protection applicable to the Agency:

- Advise in defining a general implementation strategy and compliance plan to allow for transition to new Regulation repealing Regulation (EC) No 45/2001, taking into consideration personal data processing activities in the Agency and other processes and activities in place,

- Advice in establishing a Privacy and Personal Data Protection Compliance System that will be integrated in respect to legal and operational frameworks which have been set within the Agency (in particular, Information Security and Physical Security Systems);

- Design, prepare and deliver training and awareness-raising campaign(s) on privacy and personal data protection to pre-defined audiences (mostly consisting of Agency's staff members), tailored to their level of involvement with the obligations in terms of Personal Privacy and Data Protection and to their specific roles, skills and needs;

- Support drafting and implementing adequate personal data protection policies in the areas by which the Agency, as the data controller, will be able to demonstrate accountability and compliance with Privacy and Personal Data Protection principles;

- Advise the Agency in which cases Security Risk Assessments ('SRA') are appropriate, assist and advise in performing the SRA or advise on updates in line with the new GDPR and the new Regulation repealing Regulation (EC) No 45/2001 on previously completed SRA;

- Assist the Agency in performing Privacy and Data Protection Impact Assessment in accordance with Article 35 of GDPR, for example prior to entering into cloud computing and/or other electronic contracts;

- Draft and/or assist the Agency in drafting templates and 'fit-for-purpose' forms for carrying out Privacy and Data Protection Impact Assessments and Security Risk assessments;

- Support the Agency in drafting and implementing transparent information, communication and other modalities (i.e. privacy statements and policies) and procedures for the exercise of the rights of data subjects, as well as 'fit-for-purpose' consent forms;

- Provide an on-site and/or off-site audit capacity to ensure continued compliance in the area of Privacy and Personal Data Protection;

- Assist in drafting appropriate audit standards and perform independent Privacy and Data Protection Compliance Assessments and Audits and/or support the staff of the Agency in performing compliance audits to verify that all procedures are followed and controls are in place and performed in a consistent and systematic manner;

- Draft policies and processes or advise and assist in drafting policies and processes to identify potential personal data breaches, evaluate its likely consequences for the rights of data subjects and establish internal procedures in the event of a breach;

- In accordance with Article 33 of GDPR, in the event of data breach, advise the Agency in data breach management (e.g. by drafting information to data subjects and supervisory authority, where appropriate, and in documenting the breach);

- Assist and advise the Agency in the case of data transfers, particularly in trans-border data transfer agreements, clauses and in contracts with processors and joint-controllers;

- Assist and advise the Agency on enforcement of data handling instructions prior to procuring online products or services that involve personal data transfers to external processor(s);

- Advise and monitor legally-compliant use of personal data processing procedures, IT software and devices that are in operation or planned to be purchased, specifically advising the Agency on appropriate ways to tailor the related processes in order to comply with applicable Privacy and Personal Data Protection legislation;

- Assist and advise the Agency in case of any disputes or requests with data subjects;

- Notify in a timely manner to the Agency any case law and other changes to applicable legislation and provide state of the art legal advice and strategies for the implementation of such changes;

- Support and advise the Agency staff in the analysis of documents (for example procurement documents) drafted by the Agency to ensure their compliance with the applicable Privacy and Personal Data Protection legislative framework, and propose, as appropriate, the Privacy and Data Protection clauses in order to comply with existing policies and applicable legislative framework;

- Provide general support and advice to Agency on effective ways to process personal data in compliance with existing regulation(s) and policies;

- Provide legal advice on relevant state-of-the-art privacy enhancing-technologies that allow appropriate protection of personal data;

- Consult and coordinate with other contractors which may be involved in delivery of other related services, as appropriate (i.e. arising from services to be procured under lot 1 and lot 2) which may have an impact or influence the final deliverables of the assigned tasks.

6. DOCUMENTATION AND REPORTING

Except where the Specific Contracts provides for otherwise, the Contractor(s) must report in English on the services rendered in performance of each Specific Contract in a proper literate manner and must be fully comprehensive in terms of grammatical structure (e.g. complete sentences, punctuation, explanation of abbreviations, etc.).

The quantity of the reports and the forms in which they shall be submitted will be specified in each Specific Contract.

Contractor can usually expect the following to be delivered:

a) an inception report;

b) a progress report (another type of report might be defined in a Specific Contract);

c) a final report (another type of report might be defined in a Specific Contract);

d) an annotated power-point presentation and an executive summary.

The request for services will specify the expected deliverables, the layout requirements and the deadlines for the submission to the Agency.

All reports shall be delivered in an electronic version (USB flash drive or by e-mail) in PDF format and MS Word format and in case of data also in MS Excel format. In addition, the final report shall be delivered in a hard copy version, if not specified otherwise in the Specific Contract. The number of hard copies of the final report to be delivered will be defined in the Specific Contract but shall not exceed five (5) copies.

The Agency may make the reports public and may reproduce or use all documentation and reports in full or in part.

7. PARTICIPATION IN THE CALL FOR TENDER

Participation in the Agency's procurement procedure is open on equal terms to all natural and legal persons or groupings of such persons (consortia) falling within the scope of the Treaties. It includes all economic operators registered in the EU and all EU citizens.

Pursuant to Article 119 of the Financial Regulation, the participation is also open to all natural and legal persons from non-EU countries that have a ratified agreement with the European Union in the field of public procurement on the conditions laid down in that agreement. The Agency can therefore accept offers from and sign contracts with tenderers from 36 countries, namely: the 28 EU Member States, 3 European Economic Area (EEA) Countries (Lichtenstein, Norway, Iceland) and 5 Stabilisation and Associations Agreements (SAA) Countries (the Former Yugoslav Republic of Macedonia, Albania, Montenegro, Serbia and Bosnia and Herzegovina). The Agency's procurement procedures are not open to tenderers from other countries covered by the Agreement on Government Procurement (GPA).

8. VARIANTS

No variants are permitted.

9. DURATION AND SIZE OF THE FRAMEWORK CONTRACT(S)

The FWC(s) shall have an initial duration of one (1) year as from date of signature and may be renewed up to three (3) times, each time for an additional period of one (1) year. The total duration of the FWC(s) shall not exceed four (4) years. The Agency reserves the right to cancel the FWC(s) with the Contractor(s) whose services are deemed to be of a quality below the required standards and procedures.

The total maximum value of the services per lot for the total duration of the FWC(s) (up to four (4) years) is as follows:

- **For Lot 1**: Consultancy services in the areas of Physical Security and Information Security: **225,000.00 EUR**, excluding VAT.
  Specific contracts will not be signed once the budget is consumed.

- **For Lot 2**: Consultancy services in the area of Business Continuity: **85,000.00 EUR**, excluding VAT.
  Specific contracts will not be signed once the budget is consumed.

- **For Lot 3**: Consultancy services in the area of Privacy and Personal Data Protection: **150,000.00 EUR**, excluding VAT.
  Specific contracts will not be signed once the budget is consumed.

The estimated date for signature of the FWC(s) is August 2017.

10. DOCUMENTS AVAILABLE TO THE TENDERER

(a) Contract notice published in the Official Journal of the European Union (OJ EU) 101 on 27.05.2017.

(b) Invitation to tender and annexes.

(c) Internal Agency sensitive documents related to Information Security, Business Continuity and Privacy and Data Protection as listed in Annex I.G to these tender specifications.

> **IMPORTANT**:
>
> Annex I.G, including internal Agency sensitive documents related to Information Security, Business Continuity and Privacy and Data Protection as listed above will be provided by the Agency by e-mail upon request by potential tenderers. The request shall be submitted to ACERProcurement@acer.europa.eu and shall be accompanied by a non-disclosure agreement drafted in accordance with the template contained in Annex I.F and duly signed by the potential tenderer or its legal representative.
>
> The information and the documents included in Annex I.G are the sole property of the Agency (unless otherwise specified) and are provided without prejudice and for the exclusive use of the tenderer.

(d) Other documents, as mentioned in these tender specifications.

11. CONTRACTUAL FRAMEWORK

11.1. Type of Contract

For each lot the services described above will be the subject of a single Framework Contract ('FWC').

The FWC(s) will lay down the legal, financial, administrative and technical conditions applicable throughout its period of validity, including price indexation.

The draft FWC is attached as Annex III to this invitation to tender. Signature of the FWC(s) does not commit the Agency to placing orders and does not give the Contractor(s) any exclusive rights regarding the services covered by the FWC(s).

In any case, the Agency reserves the right, at any time during the validity of the FWC(s), to cease placing orders, without the Contractor(s) having the right to any compensation.

11.2. Ordering procedure

Ordering is the process through which the Agency acquires services. It starts with the request for services and ends with the signature of a Specific Contract. Specific Contracts shall be used to order services under the FWC(s).

The Agency initiates the order process by issuing a request for services to the Contractor.

Within two (2) working days of a request for services being sent by the Agency to the Contractor by e-mail, the Agency shall receive a notification from the Contractor confirming that the request has been received and is readable.

Within ten (10) working days of a request for services being sent by the Agency to the Contractor, the Agency shall receive, by e-mail, an offer.

The offer shall include all the details as specified in the request for services, namely:

(a) **The technical offer** which shall detail the methodology, the composition and skills of the team and the responsible team leader for the specific assignment;

(b) **The financial offer** which shall detail the resources to be allocated for the execution of the specific assignment; i.e. the number of person/days per the expert level and the price per person-day as defined in the FWC, the price per person-day per the expert level can be lower than the one in the Framework Contract but it cannot exceed it.

Within seven (7) working days of receiving the offer the Agency shall evaluate the compliance of the submitted offer and inform the Contractor whether the offer: (a) is accepted, (b) needs to be revised or (c) is rejected, providing details for options (b) and (c).

In case the offer needs to be revised, the Contractor shall have five (5) working days to revise the offer according to the Agency's guidelines and re-submit it to the Agency by e-mail. The Agency shall inform the Contractor within five (5) working days after receiving the revised offer whether the offer is accepted or rejected, providing reasons for the decision.

For each specific request, the Contractor will calculate his/her price on the basis of the prices quoted in the financial offer, Annex II to this invitation to tender (which forms an integral part of the FWC(s)).

Once the offer is accepted by the Agency, the Agency shall forward the Specific Contract to the Contractor for signature.

Performance of the tasks starts from the date on which the Contract is signed by the last party.

In the event of failure to observe any of the above-mentioned deadlines or disagreement on the allocation of resources, the Contractor shall be considered unavailable.

The Contractor must work in close and regular cooperation with the responsible units within the Agency. The Contractor works under his/her own capacity and responsibility and does not represent the Agency. The Contractor's staff works under the instructions of the Contractor.

11.3. Changes in the team

For the specific contracts, changes or additions to the team initially proposed must be notified to the Agency in writing.

The Contractor is obliged to provide the team with an equivalent level of qualification and experience, as defined in these tender specifications.

The Agency will have the right to object to any changes of members of the team from those initially proposed.

In case the original team is no longer available, the Agency will have the right to cancel a specific contract.

11.4. Joint tender

A joint tender is a situation where a tender is submitted by a group of economic operators (natural or legal persons). The FWC shall be signed by one of them which has been duly authorised by the others (in this case a power of attorney (see Annex I.H to these tender specifications) shall be attached to the FWC). Each legal entity of the group shall assume joint

and several liability towards the contracting authority for the fulfilment of the terms and conditions of the contract.

Any change in the composition of the group during the procurement procedure may lead to the rejection of the tender. Any change in the composition of the group after the signature of the contract may lead to the termination of the contract.

The group shall nominate one legal entity ('the leader') who will have full authority to bind the group and each of its members, and will be responsible for the administrative management of the contract (invoicing, receiving payments, etc.) on behalf of all other entities.

11.5. Subcontracting

Special attention will be paid to the approach proposed by the Contractor for managing its subcontractors. Tenderers will be required to indicate the kind of work which they plan to subcontract and the name of any companies to which they are intending to subcontract part of the work.

In case of subcontracting the contractor shall retain full liability towards the contracting authority for implementation of the FWC.

Any change in subcontracting during the procurement procedure may lead to the rejection of the tender.

Any change in subcontracting after the signature of the FWC is permitted only with the prior written consent of the Agency and may lead to the termination of the contract.

12. CONTRACTOR'S OBLIGATIONS

12.1. Compliance with applicable law

The tenderers must comply with applicable environmental, social and labour law obligations established by Union law, national legislation, collective agreements or the international environmental, social and labour conventions listed in Annex X to Directive 2014/24/EU of the European Parliament and Council of 26 February 2014 on public procurement and repealing Directive 2014/18/EC [11].

Further, the tenderers are reminded that their offer must be established in conformity with the applicable national and European employment legislation regarding the transfer of undertakings, and specifically Directive 2001/23/EC[12] and its national implementing measures. In particular, the Contractor should take note of the provisions on safeguarding employees' rights in the event of a change of employer as a result of a legal transfer.

12.2. Copyright and other intellectual property rights

Copyright and other intellectual or industrial property rights and any other right of ownership related to the products provided and services performed by the Contractor will be vested in the

[11] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).
[12] Council Directive 2001/23/EC of 12 March 2001 on the approximation of the laws of the Member States relating to the safeguarding of employees' rights in the event of transfers of undertakings, businesses or part of undertakings or businesses, OJ L 82 of 22.03.2001, p. 16.

Agency, except where one or more of these rights already exists.

The Contractor must specify any parts of the products provided and services performed that are covered by copyright or any other rights of ownership prior to the execution of each specific contract. The Contractor must confirm that it has obtained the authorisation of the holder of these rights to use these parts. Any costs arising from obtaining this authorisation will be borne by the Contractor and clearly identified on his invoice.

Any results or rights thereon, including copyright and other intellectual or industrial property rights, obtained in performance of the FWC and specific contracts, shall be owned solely by the Agency, which may use, publish, assign or transfer them as it sees fit, without geographical or other limitation, except where industrial or intellectual property rights exist prior to the FWC being entered into force.

Should the title of the copyright or intellectual property rights belong to a third party, the Contractor shall guarantee that it has requested and obtained those third parties' written authorisation to grant a license or assign to the Agency their copyright or intellectual property rights to the extent necessary for performing the services under the FWC and the specific contracts, and to the extent where the results/works obtained under the FWC are to be re-used in the context of another Agency's project with another Contractor(s) working under a FWC or specific contracts. Costs will be covered by the Contractor.

This applies to all products, documentation, distribution media and methods.

If subcontractors are used, the Contractor will be required to obtain a guarantee from them on this point.

12.3. Confidentiality – personal data

While implementing the services, and especially when data is electronically processed, the Contractor shall respect the applicable legislation concerning data protection as stated in 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[13].

13. PLACE OF PERFORMANCE OF THE SERVICES AND WORKING HOURS

13.1. Place of work

The principle place of performance of the FWC(s) shall be at the Contractor’s premises (working *off-site*).

The principal place of performance of Specific Contract(s) shall depend on each specific contract and shall be indicated in the relevant request for services (the place may either be at the Agency’s premises in Ljubljana, Slovenia or at the Contractor’s premises).

In cases where the performance of a specific contract shall take place at the Agency’s premises, this shall be considered as working *on-site*.

Working *on-site* includes also participation in meetings, presentations, awareness raising campaign(s) etc. organised at the Agency’s premises in Ljubljana, Slovenia

[13] OJ L 8/1, 12.1.2001

13.2. Meetings

Meetings between the Agency's staff and the Contractor shall take place at the Agency's premises in Ljubljana, Slovenia, and only exceptionally and with the agreement of the Agency, at the Contractor's premises.

If deemed appropriate and at the sole discretion of the Agency, meetings between the Agency and the Contractor could be organised using a video-conference system, telephone conferences and/or any other communication means.

Meetings between the Agency and third parties (NRAs, EU institutions and other stakeholders), to which the Contractor may be invited, will be mainly organised in Ljubljana, Slovenia, but may take place also in other EU Member States.

All meetings will be notified to the Contractor, by e-mail, in reasonable time and in any case at least five (5) calendar days prior to the meeting, or at least two (2) calendar days prior to the meeting if video/telephone conferencing systems are used. The Contractor shall confirm by e-mail the attendance to the meeting.
The Contractor shall prepare minutes of these meetings, indicating the participants, agenda, and main issues of discussion and action points.

Any expenses incurred by the Contractor within the framework of these meetings (i.e. travel costs, subsistence allowance or any other related costs) shall not be reimbursed separately by the Agency.

Within twenty (20) calendar days following the entry into force of the FWC(s) **a kick-off meeting** with the Agency shall take place via video-conference/teleconference.

13.3. Working time of the Agency

The normal working time of the Agency is between 8:00 am and 20:00 with core hours from 9:30 to 12:00 and from 14:00 to 16:00.

The Agency's public holidays are published on the Agency's website and are updated yearly.

The information for the public holidays of the Agency in 2017 is available at:
http://www.acer.europa.eu/Official_documents/Director/Directors%20Decision/18_Director%20Decision%202016-18.pdf.

14. LANGUAGE

The working language of the Agency is English. All communication, all the required services and all documentation must be provided in English. All meetings shall be held in English.

All documentation (e.g. reports, presentation, etc.) must be provided in English in the highest drafting quality.

15. PAYMENT METHODS

Except where the specific contracts provides for otherwise, provisions related to payment are laid down in the draft FWC (Annex III to the Invitation to Tender). Payments will be made exclusive of VAT, as the Agency is exempt from all duties and taxes, including value added tax (VAT), under Articles 3 and 4 of the Protocol on the Privileges and Immunities of the

European Union. Invoice(s) presented by the Contractor must specify the amount(s) exclusive of VAT.

Interim payment(s) will take place upon the delivery and approval of intermediary deliverables by the Agency accompanied by invoice(s).

16. PRICES

- The prices should be quoted in euro.
- Under Articles 3 and 4 of the Protocol on the Privileges and Immunities of the European Union the Agency is exempt from all duties and taxes, including value added tax (VAT). VAT can be indicated separately but will not be taken into account when considering prices.
- The unit prices quoted must be firm and not subject to revision for the first year of the FWC.
- From the beginning of the second year prices may be revised upwards or downwards according to monetary union index of consumer prices (MUICP index) for Eurozone and the method laid down in the FWC.
- The prices quoted shall be all inclusive and shall include all charges and all administrative costs (such as but not limited to backstopping costs, insurance, reports, communication costs, any travel and/or subsistence expenses, etc.).

No expenses incurred in relation to the preparation of the offer will be reimbursed.

17. SUBMISSION OF TENDERS

The tenderer's offer should include:

A. **A dated cover letter signed by the tenderer.**

B. **A duly completed reference table** related to the exclusion and selection criteria (see Annex I.A of these tender specifications).

C. **A duly filled in, signed and dated declaration on honour on exclusion criteria** listed in Section 18 of these tender specifications (form provided in Annex I.C to these tender specifications).

D. All the **documents relating to the selection criteria** listed in Section 19 of these tender specifications.

E. **The technical tender**, as described in Section 20 of these tender specifications;

F. **The financial offer** based on the model in Annex II to the invitation to tender, signed and dated by the tenderer.

Tenders may be drafted in any of the official languages of the European Union.

The working language of the Agency is English.

In case the offer involves subcontracting or the tender is submitted by a consortium or grouping of service providers, the tender must contain additional information as specified in Sections 18 and 19 of these tender specifications.

18. EXCLUSION CRITERIA

Tenderers must prove that they are not in one of the situations giving rise to exclusion as in Annex I.C (situation of exclusion concerning the legal person, situations of exclusion concerning natural persons with power of representation, decision-making or control over the legal person and situations of exclusion concerning natural or legal persons assuming unlimited liability for the debts of the legal person).

18.1. Exclusion from participation

The tenderer must prove that he/she is not in one of the situations giving ground to rejection from this procedure as listed in Annex I.C – Declaration on honour on exclusion criteria.

18.2. Exclusion from award of contracts

The FWC shall not be awarded to tenderers who, during the procurement procedure for this FWC:

(a) has misrepresented the information required as a condition for participating in the procedure or has failed to supply that information;

(b) was previously involved in the preparation of procurement documents where this entails a distortion of competition that cannot be remedied otherwise.

Evidence

1. Tenderers shall provide a declaration on their honour, **duly signed** and **dated**, stating that they are not in one of the situations referred to in points 18.1 and 18.2 of the present tender specifications using the form provided in Annex I.C – Declaration on honour on exclusion criteria – to these tender specifications.

2. The tenderer to whom the FWC is to be awarded shall provide, within a time-limit specified by the Contracting Authority and prior to the signature of the FWC, the following evidence in support of their declarations:

   The contracting authority shall accept as satisfactory evidence that the tenderer to whom the contract is to be awarded is not in one of the situations described in (a), (c), (d) or (f) of Annex I.C – Declaration on honour on exclusion criteria, a **recent extract from the judicial record** or, failing that, an equivalent document recently issued by a judicial or administrative authority in the country of establishment showing that those requirements are satisfied. The contracting authority shall accept, as satisfactory evidence that the tenderer is not in the situation described in point (a) or (d) of Annex I.C – Declaration on honour on exclusion criteria a **recent certificate issued by the competent authority of the State concerned**.

   The extract from the judicial record and administrative certificates can be regarded as recent if they are not more than one (1) year old starting from their issuing date and are still valid at the date of their request by the contracting authority.

Where the document or certificate referred to in the paragraph above is not issued in the country concerned the tenderer, may provide a sworn statement made before a judicial authority or notary or, failing that, a solemn statement made before an administrative authority or a qualified professional body in its country of establishment.

The tenderer is not required to submit the evidence if it has already been submitted for another procurement procedure. The documents must have been issued no more than one year before the date of their request by the contracting authority and must still be valid at that date.

3. Depending on the national legislation of the country in which the tenderer is established, the documents referred to in in the paragraph above shall relate to legal persons and/or natural persons including, where considered necessary by the contracting authority, company directors or any person with powers of representation, decision-making or control in relation to the tenderer.

The Agency reserves the right to check the information provided by tenderers.

18.3. Tenders submitted by consortia or groups of service providers – tenders involving subcontracting

In the case of tenders submitted by consortia or groups of service providers, each of the economic operators involved in the tender must provide a dated and signed declaration on honour, based on the model provided in Annex I.C – Declaration on honour on exclusion criteria – to these tender specifications, confirming that none of the exclusion criteria for participation in or award of the FWC apply to them.

The tenderers proposed for award of the FWC must furnish, within the time-limit specified by the awarding authority and prior to the signature of the FWC, the evidence listed above, corroborating the declaration on their honour, in respect of each economic operator forming part of their consortium or group of service providers.

In the case of tenders involving subcontracting, the tenderer proposed for award of the FWC must furnish, within the time-limit specified by the awarding authority and prior to the signature of the FWC, the declaration on their honour and/or the evidence listed above regarding exclusion criteria for participation in or award of the FWC, in respect of each of the subcontractors in respect of whom the Agency requests such evidence.

The Agency reserves the right to check the information provided by tenderers.

19. SELECTION CRITERIA

Tenderers must demonstrate that they have the necessary economic, financial, technical and professional capacity to perform the tasks described in these tender specifications in accordance with the payment schedule specified in the draft FWC at Annex III to the Invitation to Tender.

If any selection criterion is fulfilled by relying on the capacity of a third party (regardless of the link it has with the tenderer), the tenderer must prove to the contracting authority that it will have at its disposal the resources necessary for performance of the FWC by producing a commitment on the part of those entities to this effect.

If the tenderer relies on the capacity of a third party for economic and financial capacity, the contracting authority may require that the third party be jointly liable for performance of the FWC.

If the tenderer relies on the capacity of a third party for technical and professional capacity, it can only do so for the tasks for which this particular capacity is required, for example by providing a document stating clearly the allocation of tasks between entities.

Tenderers must provide proof of their legal, economic, financial technical and professional capacity by enclosing with their tender the following information and documents, accompanied by the reference table shown in Annex I.A to these tender specifications.

19.1. Legal capacity

FOR EACH LOT

- Duly completed and signed identification form (see Annex I.B to these tender specifications);

- Duly completed and signed financial identification form (see Annex I.D to these tender specifications) – the form can be downloaded from: http://ec.europa.eu/budget/contracts_grants/info_contracts/financial_id/financial_id_en.cfm;
- Duly completed and signed legal entity form (see Annex I.E to these tender specifications) – the form can be downloaded from: http://ec.europa.eu/budget/contracts_grants/info_contracts/legal_entities/legal_entities_en.cfm;

- Certificate of enrolment on the professional or trade register in accordance with the legislation of the Member State in which the tenderer is established.

19.2. Economic and financial capacity

Evidence of economic and financial capacity must be provided by means of the following documents:

19.2.1. FOR LOT 1 - Consultancy services in the areas of Physical Security and Information Security

The turnover concerning the services covered by the FWC should amount to **at least EUR 150,000.00** for the years 2015 and 2016 combined.

Evidence to be provided: A statement of overall turnover and a statement of turnover concerning the services covered by the FWC during the last two (2) years.

19.2.2. FOR LOT 2 - Consultancy services in the area of Business Continuity

The turnover concerning the services covered by the FWC should amount to **at least EUR 55,000.00** for the years 2015 and 2016 combined.

Evidence to be provided: A statement of overall turnover and a statement of turnover concerning the services covered by the FWC during the last two (2) years.

19.2.3. FOR LOT 3 - Consultancy services in the area of Privacy and Personal Data Protection

The turnover concerning the services covered by the FWC should amount to **at least EUR 100,000.00** for the years 2015 and 2016 combined.

Evidence to be provided: A statement of overall turnover and a statement of turnover concerning the services covered by the FWC during the last two (2) years.

19.3. Technical and professional capacity

Proof of the technical and professional capacity of the tenderers shall be furnished on the basis of the documents listed below (for joint applications, the capacities of all members of the joint application, including subcontractors, shall be taken into account).

The tenderer must prove that he/she fulfils the following criteria:

19.3.1. FOR LOT 1 – Consultancy services in the areas of Physical Security and Information Security

- Provision of services of the type as requested in this Lot, and covering the areas of policy and legislation analysis, technical analysis, and drafting reports and recommendations, for a total invoiced amount (i.e. total amount effectively invoiced to the customer(s)) of **at least EUR 150,000.00 in the last two (2) years combined**.

  This shall include at least:

  - **three (3) projects** in the field related to this lot,
  - **at least four (4) projects** where the services have been delivered in English and
  - **at least two (2) projects** which included organising workshops and stakeholders' consultations, within or outside the EU.

  Evidence to be provided: Name(s) of customer(s), a description of services undertaken (indicating the area as mentioned above, the language used and specifying whether this included organisation of workshops and/or stakeholders' consultations), starting and ending date(s) of each project listed, total financial volume of the contract(s) effectively delivered (i.e. total amount effectively invoiced to the customers) in 2015 and 2016 combined.

- The team delivering the services shall include as a minimum at least one (1) expert for each profile as defined below. Each of the proposed experts[14] must fulfil the minimum levels of qualifications and professional experience applicable for a respective profile as described below.

  Each member of the proposed team must have the following minimum levels of qualification:

[14] Each expert not employed by the tenderer has to provide a declaration that she/he is willing to participate in the team of the tenderer in the execution of the tasks defined in this FWC.

Minimum levels of qualification for the **Senior expert and Team Leader in the area of Physical Security**:

- Completed university studies of at least three (3) years attested by a diploma in the area of law, military or law enforcement studies, social studies or information security
- A least seven (7) years' professional experience in physical security or any related field (i.e. law enforcement and/or close protection, armed forces and/or private armed guards companies);
- At least three (3) years' professional experience covering the European Union and/or EU National regulatory frameworks related to security;
- At least four (4) years' professional experience covering the implementation aspects of physical security and its interactions and links with Information Security, Business Continuity and Privacy and Personal Data Protection;
- At least four (4) years' professional experience covering technical aspects of the implementation of physical security in complex environments;
- Excellent knowledge of English (at least level B2 according to the Common European Framework of Reference for Languages);
- Very good writing and communication skills.

Minimum levels of qualification for the **Junior expert in the area of Physical Security**:

- Completed university studies of at least three (3) years attested by a diploma.
- At least four (4) years' professional experience in physical security or any related field (i.e. law enforcement and/or close protection, and/or armed forces and/or private armed guards companies);
- At least two (2) years' professional experience covering the European Union and/or EU National regulatory frameworks related to security;
- At least two (2) years' professional experience covering the implementation aspects of physical security and its interactions and links with Information Security, Business Continuity and Privacy and Data Protection;
- At least two (2) years' professional experience covering technical aspects of the implementation of physical security in complex environments;
- Excellent knowledge of English (at least level B2 according to the Common European Framework of Reference for Languages);
- Very good writing and communication skills.

Minimum levels of qualification for the **Senior expert and Team Leader in the area of Information Security:**

- Completed university studies of at least three (3) years attested by a diploma
- At least seven (7) years' professional experience in information security or any related field (e.g. audit of information security systems, working in IT companies with specific focus on security);
- At least three (3) years' professional experience covering the European Union and/or EU National regulatory frameworks related to information security and/or EUCI;
- At least four (4) years' professional experience covering of the implementation aspects of information security and its interactions and links with Physical Security, Business Continuity and Privacy and Personal Data Protection;
- At least four (4) years' professional experience covering technical aspects of the implementation of information security in complex environments;
- Excellent knowledge of English (at least level B2 according to the Common European Framework of Reference for Languages);
- Very good writing and communication skills.

Minimum levels of qualification for the **Junior expert in the area of Information Security:**

- Completed university studies of at least three (3) years attested by a diploma;
- At least four (4) years' professional experience in information security or any related field (e.g. auditing information security systems, and/or working in IT companies with specific focus on security);
- At least two (2) years' professional experience covering the European Union and/or EU National regulatory frameworks related to information security and/or EUCI;
- At least two (2)years' professional experience covering the implementation aspects of information security and its interactions and links with Physical Security, Business Continuity and Privacy and Personal Data Protection;
- At least two (2)years' professional experience covering technical aspects of the implementation of information security in complex environments;
- Excellent knowledge of English (at least level B2 according to the Common European Framework of Reference for Languages);
- Very good writing and communication skills.

Evidence to be provided: The tenderer shall include Curricula Vitae (CVs)[15] showing clearly their qualifications and professional experience within the relevant business area. The tenderer shall provide **at least one (1) CV for each profile** as described above, clearly indicating the profile on each CV.

19.3.2. FOR LOT 2 - Consultancy services in the area of Business Continuity

– Provision of services of the type as requested in this Lot, and covering the areas of policy and legislation analysis, technical analysis, and drafting reports and recommendations, for a total invoiced amount (i.e. total amount effectively invoiced to the customer(s)) of **at least EUR 55,000.00 in the last two (2) years combined**.

This shall include **at least:**

- **three (3) projects** in the field related to this lot,
- **at least four (4) projects** where the services have been delivered in English and
- **at least two (2) projects** which included organising workshops and stakeholders' consultations, within or outside the EU.

Evidence to be provided: Name(s) of customer(s), a description of services undertaken (indicating the area as mentioned above, the language used and specifying whether this included organisation of workshops and/or stakeholders' consultations), starting and ending date(s) of each project listed, total financial volume of the contract(s) effectively delivered (i.e. total amount effectively invoiced to the customers) in 2015 and 2016 combined.

– The team delivering the services shall include as a minimum **at least one (1) Senior expert and at least two (2) Junior experts as defined below**. Each of the proposed experts[16] must fulfil the minimum levels of qualifications and professional experience applicable for a respective profile as described below.

[15] Preferably, in accordance with the European CV format: http://europass.cedefop.europa.eu/en/documents/curriculum-vitae/templates-instructions

[16] Each expert not employed by the tenderer has to provide a declaration that she/he is willing to participate in the team of the tenderer in the execution of the tasks defined in this FWC.

Each member of the proposed team must have the following minimum levels of qualification:

Minimum levels of qualification for the **Senior expert and Team Leader in the area of Business Continuity:**

- Completed university studies of at least three (3) years attested by a diploma;
- At least seven (7) years' professional experience in business continuity matters or any field related to business continuity, proven preparedness and reaction (prior experience as crises manager and/or working in civil protection and/or complex and/or hostile environments);
- At least three (3) years' professional experience covering the European Union and/or EU National regulatory frameworks and/or any relevant recognised international standards related to business continuity (in particular ISO 22301);
- At least four (4) years' professional experience covering the implementation aspects of Business Continuity;
- At least four (4) years' professional experience with technical aspects of business continuity in complex and difficult environments;
- Excellent knowledge of English (at least level B2 according to the Common European Framework of Reference for Languages);
- Very good writing and communication skills.

Minimum levels of qualification for the **Junior expert in the area of Business Continuity**:

- completed university studies of at least three (3) years attested by a diploma;
- At least four (4) years' professional experience in business continuity matters or any field related to business continuity – preparedness and reaction (prior experience as crises manager and/or working in civil protection and/or complex and/or hostile environments);
- At least two (2) years' professional experience covering the European Union and/or EU National regulatory frameworks and/or any relevant recognised international standards related to business continuity (in particular ISO 22301);
- At least two (2) years' professional experience covering the implementation aspects of Business Continuity and its interactions and links with Physical Security, Information Security and Privacy and Personal Data Protection;
- At least two (2) years' professional experience covering technical aspects of the implementation of business continuity in complex and difficult environments;
- Excellent knowledge of English (at least level B2 according to the Common European Framework of Reference for Languages);
- Very good writing and communication skills.

Evidence to be provided: The tenderer shall include Curricula Vitae (CVs)[17] showing clearly their qualifications and professional experience within the relevant business area. The tenderer shall provide **at least one (1) CV for the profile Senior expert** and **at least two (2) CVs for the profile Junior expert** as described above, clearly indicating the profile on each CV.

[17] Preferably, in accordance with the European CV format: http://europass.cedefop.europa.eu/en/documents/curriculum-vitae/templates-instructions

19.3.3. FOR LOT 3 - Consultancy services in the area of Privacy and Personal Data Protection

– Provision of services of the type as requested in this Lot, and covering the areas of policy and legislation analysis, technical analysis, and drafting reports and recommendations, for a total invoiced amount (i.e. total amount effectively invoiced to the customer(s)) of **at least EUR 100,000.00 in the last two (2) years combined**.

This provision of services shall include:
- **at least three (3) projects** in the field related to this Lot,
- **at least four (4) projects** where the services have been delivered in English and
- **at least two (2) projects** which included organising workshops and stakeholders' consultations, within or outside the EU.

Evidence to be provided: Name(s) of customer(s), a description of services undertaken (indicating the area as mentioned above, the language used and specifying whether this included organisation of workshops and/or stakeholders' consultations), starting and ending date(s) of each project listed, total financial volume of the contract(s) effectively delivered (i.e. total amount effectively invoiced to the customers) in 2015 and 2016 combined.

– The team delivering the services shall include as a minimum **at least one (1) Senior expert and at least two (2) Junior experts as defined below**. Each of the proposed experts[18] must fulfil the minimum levels of qualifications and professional experience applicable for a respective profile as described below.

Each member of the proposed team must have the following minimum levels of qualification:

Minimum levels of qualification for the **Senior expert and Team Leader in the area of Privacy and Personal Data Protection:**
- Completed university studies of at least three (3) years attested by a diploma (in law or law and ICT[19])
- At least seven (7) years' professional experience in Privacy and Personal Data Protection matters which shall include experience with technical aspects of its implementation;
- Excellent knowledge of English (at least level C1 according to the Common European Framework of Reference for Languages);
- Very good writing and communication skills.

Minimum levels of qualification for the **Junior expert in the area of Privacy and Personal Data Protection:**
- Completed university studies of at least three (3) years attested by a diploma (in law or law and ICT);
- At least three (3) years' professional experience in Privacy and Personal Data Protection matters which shall include experience with technical aspects of its implementation;
- Excellent knowledge of English (at least level C1 according to the Common European Framework of Reference for Languages);
- Very good writing and communication skills.

[18] Each expert not employed by the tenderer has to provide a declaration that she/he is willing to participate in the team of the tenderer in the execution of the tasks defined in this FWC.
[19] Information and Communication Technologies.

Evidence to be provided: The tenderer shall include Curricula Vitae (CVs)[20] showing clearly their qualifications and professional experience within the relevant business area. The tenderer shall provide **at least one (1) CV for the profile Senior expert** and **at least two (2) CVs for the profile Junior expert** as described above, clearly indicating the profile on each CV.

19.4. Subcontracting

FOR EACH LOT

For those tenders including subcontracting, the tenderer must submit:

- A declaration of the tenderer, duly signed and dated, stating clearly the identity and roles of the subcontractor(s) as well as the description of the quality control measures the tenderer intends to apply on the tasks to be carried out by (each of) the subcontractor(s).

- A letter of intent by (each of) the subcontractor(s), duly signed and dated, stating the unambiguous undertaking to collaborate with the tenderer if the latter wins the FWC and the extent of the resources that it will put at the tenderer's disposal for the performance of the FWC.

In the absence of subcontracting:

- A declaration of the tenderer, **duly signed and dated**, stating that he does not intend to subcontract and that he will inform the Agency about any change in this situation. The Agency reserves the right to judge if such change would be acceptable.

Offers involving subcontracting will be assessed as follows:

- Where the tenderer relies on the economic, financial, technical and professional capacity of the subcontractor(s) to meet the selection criteria, subcontractors shall be treated as if they were partners in a consortium or a group of companies for the purposes of the evaluation of the selection criteria, and therefore, they shall provide proof of economic, financial, technical and professional capacity as well.

19.5. Tenders submitted by a consortium or grouping of service providers

FOR EACH LOT

For those tenders submitted by a consortium or grouping of service providers, the tender must contain:

- A document stating clearly the composition and constitution of the grouping or similar entity (company/temporary association/…), or the legal form their cooperation will take, should they be awarded the FWC;

- A letter **dated and signed** by each member stating its commitment to execute the services in the tender clearly indicating its role, qualifications and experience;

[20] Preferably, in accordance with the European CV format:
http://europass.cedefop.europa.eu/en/documents/curriculum-vitae/templates-instructions

- A document **dated and signed** by all members specifying the lead of the consortium or grouping of service providers and authorising the appointed lead of the consortium or grouping of service providers to submit the offer.

Joint tenders will be assessed as follows:

- The exclusion criteria will be assessed in relation to each company individually. The declaration on honour on exclusion criteria included in Annex I.C, duly signed and dated, stating that the tenderer is not in one of the exclusion situations, must be provided by each member of the consortium or the group.

- The selection criteria for technical and professional capacity will be assessed in relation to the consortium or group of companies as a whole.

Tenders which do not meet the exclusion and/or selection criteria will not be considered.

Tenderers who do not provide the documents required in these tender specifications with regard to the exclusion and/or selection criteria may be excluded.

The Agency will decide whether the substantiating documents provided constitute compliance with the exclusion and/or selection criteria.

20. TECHNICAL TENDER

Tenderers should include in their offer a technical tender detailing how they intend to perform the tasks covered by the FWC(s), in compliance with all the requirements of these tender specifications. Tenders that fail to comply with this requirement may be rejected.

The technical tender should not include any of the documents referred to under the exclusion and/or selection criteria, nor should it refer to matters already covered by the exclusion and/or selection criteria.

20.1. FOR LOT 1 - Consultancy services in the areas of Physical Security and Information Security

The technical tender shall, in the line with the requirements of as described in Sections 3, 4 and 5, include:

(a) Standard project management methodology proposed for the implementation of the FWC.

(b) The tenderer shall submit a proposal, in writing, **for the following questions 1, 2, 3 and 4** as described below.

The questions do not reflect the reality, they are based on assumptions, and sometimes information given is partial in order to allow the tenderer to analyse different scenarios. **A reply to each question shall not exceed 750 words.**

- **Question 1 (Physical Security)**

  During a recent security incident, an external visitor was able to introduce a gun inside the Agency's premises. The external visitor, who appears to be a Security Officer from another EU Institution, wanted to check preparedness of the armed guards and effective use of the existing security devices (X-Ray scanner for visitors' belongings and metal detector portal for visitors).

The incident ended with no consequence, but the Agency management wants to assess if this issue may have been prevented.

What would you advice the Agency in a similar event, and which would be the first actions you would suggest to take in order to prevent a similar incident?

- **Question 2 (Physical Security)**

Which are the physical security aspects to take into consideration when applying security in a multi-tenant building, in comparison to the standard security principles applicable to a single tenant building? Please explain also your reasoning.

- **Question 3 (Information Security)**

The Agency has a draft Information Security Policy. The Agency would like to proceed with its implementation, starting with a risk assessment and an impact assessment. Nevertheless, while you, as a consultant, would prefer to perform all this on your own in order to gain some knowledge of your customer, the Agency wants you, as a Contractor, to just act as a coach for staff in order to enable staff performing it in an autonomous but controlled way. Which strategy would you propose to achieve this task, what would be your approach and how would you structure your work?

- **Question 4 (Information Security)**

How would you structure an awareness campaign which should have as a main purpose the need to enhance awareness, knowledge and compliance of staff members with Information Security, having in mind that the staff members are all coming from companies where they were free to share information also with stakeholders in an uncontrolled way, and where the value of information was relatively very low?

How would you justify the introduction of the “need to know” principle?

20.2. FOR LOT 2 - Consultancy services in the area of Business Continuity

The technical tender shall, in the line with the requirements of as described in Sections 3, 4 and 5, include:

(a) Standard project management methodology proposed for the implementation of the FWC.

(b) The tenderer shall submit a proposal, in writing, **for the following questions 1 and 2** as described below.

The questions do not reflect the reality: they are based on assumptions, and sometimes information given is partial in order to allow the tenderer to analyse different scenarios**. A reply to each question shall <u>not exceed 750 words</u>.**

- **Question 1 (Business Continuity)**

Which are the ten (10) main questions you may use to evaluate the level of understanding of Business Continuity by one of your customers?

- **Question 2 (Business Continuity)**

  During a recent Business Continuity simulation exercise, a number of issues were highlighted, which, in a real situation, may have prevented the company you observed from running their critical and essential business processes.

  Which would be the strategy/approach you would use to convey the right message to the management on the need to improve the existing Business Continuity Plan? Which would be the strategy you would use towards its staff, in order to tell to each actor what they did right and wrong, avoiding any misunderstanding?

20.3. FOR LOT 3 - Consultancy services in the area of Privacy and Personal Data Protection

The technical tender shall include a detailed proposal, in writing, **for the questions 1, 2, 3 and 4** as described below.

The questions do not reflect the reality: they are based on assumptions, and sometimes information given is partial in order to allow the tenderers to analyse different scenarios. **A reply to each question shall not exceed 750 words.**

(a) Question 1 (Privacy and Personal Data Protection)

During your first visit to a customer's premises, you notice an extremely low level of attention with regard to Privacy and Personal Data Protection matters; e.g. screens are left open with sensitive information displayed; personal documents are left on tables unattended; you notice that people speak openly without paying much attention to the fact that the information they give to you is private information of other colleagues.

How would you use these observations in order to convince your customer that some actions are needed in the short term, and which actions would you suggest?

(b) Question 2 (Privacy and Personal Data Protection)

A customer is planning to conclude a cloud computing contract (software as a service (SaaS) with US-based cloud service provider that will involve transfer of certain confidential and other data of the customer to the cloud providers' data centres in the EU. Which aspects of the contractual terms would you advise your customer to focus on in carrying out data protection impact assessment and security risk assessment? Which standard contractual clauses usually used by cloud computing providers would most likely have to be tailor-made to comply with EU legal framework on data protection?

(c) Question 3 (Privacy and Personal Data Protection)

Describe a data protection policy you would propose on staff monitoring tools (e.g. CCTV cameras), email and internet use in the organisation of the customer. What would you consider justified and what not?

(d) Question 4 (Privacy and Personal Data Protection)

Customer contacts you explaining it discovered a data breach. What actions would you propose in short term and in long term? What methodology would you use to evaluate the severity of the breach? What strategy would you propose to mitigate risks to the reputation of the customer?

21. AWARD CRITERIA

For each lot, the FWC will be awarded to the tender offering the best value for money on the basis of the criteria specified below.

21.1. Technical quality with 60% weighting

Tenders scoring less than 60 overall points will be excluded from further evaluation. Tenders scoring less than 60% of the points awarded for each of the single criterion will be excluded from further evaluation.

The technical quality criteria, their importance factor and system of scoring are presented in detail below:

FOR LOT 1 - Consultancy services in the areas of Physical Security and Information Security

No	Technical quality criteria	Maximum points available	Threshold
1.	Completeness, appropriateness, relevance and consistency of the standard project management methodology	40	24
2.	Completeness, appropriateness, relevance and consistency of the reply to Question 1	15	9
3.	Completeness, appropriateness, relevance and consistency of the reply to Question 2	15	9
4.	Completeness, appropriateness, relevance and consistency of the reply to Question 3	15	9
5.	Completeness, appropriateness, relevance and consistency of the reply to Question 4	15	9
	TOTAL	**100.00**	**60.00**

FOR LOT 2 - Consultancy services in the area of Business Continuity

No	Technical quality criteria	Maximum points available	Threshold
1.	Completeness, appropriateness, relevance and consistency of the standard project management methodology	50	30
2.	Completeness, appropriateness, relevance and consistency of the reply to Question 1	25	15
3.	Completeness, appropriateness, relevance and consistency of the reply to Question 2	25	15
	TOTAL	**100.00**	**60.00**

FOR LOT 3 - Consultancy services in the area of Privacy and Personal Data Protection

No	Technical quality criteria	Maximum points available	Threshold
1.	Completeness, appropriateness, relevance and consistency of the reply to Question 1	25	15
2.	Completeness, appropriateness, relevance and consistency of the reply to Question 2	25	15
3.	Completeness, appropriateness, relevance and consistency of the reply to Question 3	25	15
4.	Completeness, appropriateness, relevance and consistency of the reply to Question 4	25	15
	TOTAL	**100.00**	**60.00**

21.2. Price with 40% weighting

In order to evaluate the offers, the Agency will calculate for each lot separately a total reference price, based on the financial offer submitted by the tenderer in Annex II to the invitation to tender.

The total reference price has no contractual value and will be used solely for the purpose of the evaluation.

IMPORTANT:

The unit prices quoted shall include all services as described in Section 17, including any charges and all administrative costs (such as but not limited to backstopping costs, insurance, reports, communication costs, any travel and/or subsistence expenses, etc.), and shall specify the cost of person/day per expert as indicated in the table below:

FOR LOT 1 (Consultancy services in the areas of Physical Security and Information Security) - FORMULA FOR CALCULATING the total reference price:

	TEAM MEMBER	UNIT	Cost per unit in EUR	QUANTITY	VALUE
A	**B**	**C**	**D**	**E**	**G = D * E**
1.	Senior expert and Team Leader in the area of Physical Security working off-site	person/ day		15	
2.	Senior expert and Team Leader in the area of Physical Security working on-site	person/ day		15	
3.	Junior expert in the area of Physical Security working off-site	person/ day		40	
4.	Junior expert in the area of Physical Security working on-site	person/ day		40	
5.	Senior expert and Team Leader in the area of Information Security working off-site	person/ day		15	
6.	Senior expert and Team Leader in the area of Information Security working on-site	person/ day		15	
7.	Junior expert in the area of Information Security working off-site	person/ day		40	
8.	Junior expert in the area of Information Security working on-site	person/ day		40	
	TOTAL REFERENCE PRICE = VALUES 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8				

FOR LOT 2 (Consultancy services in the area of Business Continuity) - FORMULA FOR CALCULATING the total reference price:

	TEAM MEMBER	UNIT	Cost per unit in EUR	QUANTITY	VALUE
A	**B**	**C**	**D**	**E**	**G = D * E**
1.	Senior expert and Team Leader in the area of Business Continuity working off-site	person/ day		20	
2.	Senior expert and Team Leader in the area of Business Continuity working on-site	person/ day		20	
3.	Junior expert in the area of Business Continuity working off-site	person/ day		60	
4.	Junior expert in the area of Business Continuity working on-site	person/ day		60	
	TOTAL REFERENCE PRICE = VALUES 1 + 2 + 3 + 4				

FOR LOT 3 (Consultancy services in the area of Privacy and Personal Data Protection) - FORMULA FOR CALCULATING the total reference price:

	TEAM MEMBER	UNIT	Cost per unit in EUR	QUANTITY	VALUE
A	**B**	**C**	**D**	**E**	**G = D * E**
1.	Senior expert and Team Leader in the area of Privacy and Personal Data Protection working off-site	person/ day		30	
2.	Senior expert and Team Leader in the area of Privacy and Personal Data Protection working on-site	person/ day		15	
3.	Junior expert in the area of Privacy and Personal Data Protection working off-site	person/ day		30	
4.	Junior expert in the area of Privacy and Personal Data Protection working on-site	person/ day		15	
	TOTAL REFERENCE PRICE = VALUES 1 + 2 + 3 + 4				

21.3. Final evaluation

FOR EACH LOT

The Contract will be awarded to the tenderer who has submitted the economically most advantageous offer, according to the following formula:

$$\text{Final score for tender X} = \frac{\text{cheapest total reference price}}{\text{total reference price of tender X}} * 40 + \frac{\text{total technical quality of tenderer X}}{100} * 60$$

Tenderers will be ranked according to the criterion of the economically most advantageous tender, i.e. starting from the tender achieving the highest technical quality/price combination, obtained on the basis of the formula indicated above.

The tenderer with the highest mark for the final score will be awarded the FWC.