European Parliament

PUBLIC PROCUREMENT FORUM

Guidelines

MANAGEMENT OF CYBERSECURITY-SENSITIVE TENDERS AND CONTRACTS: GOOD PRACTICE AND RECOMMENDATIONS

1. Introduction

The objective of these guidelines is to raise awareness and provide a tool for the European Parliament to mitigate security risks of connected or connectable devices, data processing and network services as well as infrastructure works it purchases. To this end, these guidelines:

- reflect the targets for public procurement in order to continuously protect Parliament against possible attempt to disrupt its activities and to protect all data stored and processed by or on behalf of Parliament while ensuring business continuity,
- define a set of good practices in order to facilitate the drafting of the tender documents;
- make recommendations to integrate security considerations in the planning of public procurement, in tender documents, in selection and award criteria as well as in contracts dealing with sensitive information and in contract execution.

These guidelines also apply to concession contracts and should be the base of interinstitutional tenders.

2. Definitions and legal framework

Given the widespread reality of cyber-attacks and data theft, cybersecurity has to be mainstreamed into public procurement procedures **for all devices, services and works that involve possible connections, networks or infrastructure**. The authorising officer responsible has to determine whether a specific procedure is security-sensitive. Potentially a wide array of tenders that in the past may have been regarded as non-sensitive will in future be regarded as sensitive.
Therefore, it is important that all staff of Parliament involved in procurement procedures develop an appropriate awareness concerning security-related aspects and how to mitigate security risks in procurement through choosing the right options in procurement procedures.

It is important to note that security-sensitive issues may concern any supplies, intellectual or non-intellectual services or works.

One situation could be, for instance, the presence of spy hardware or software in ITC devices, or seemingly innocuous devices which are so widespread throughout the house that their collective undermining could disrupt Parliament's normal functioning

A part from the choice of procedure and contract options, the information put into the market also deserves attention: in particular, as a general measure, building plans of Parliament buildings should not be published to the whole market. A tender which implies the renewal of a contract with *intra muros* consultants or, if necessary, access to IT system from outside the Parliament premises, could also be regarded as sensitive.

The development of an IT application managing data should be regarded as sensitive.

The present guidelines are aimed at providing good practices for the management of security-sensitive tenders as defined by the competent authorising officer.

The management of security-sensitive tenders should be dealt with under full respect of the Financial Regulation and its Annex I.

3. Choice of the most appropriate procurement procedures

The Financial Regulation offers several procedures for launching a tender.

Considering the security-sensitivity of a tender, the following aspects should be taken into consideration when choosing the most appropriate procedure for launching the tender:

- Based on exclusion and selection criteria, the **restricted procedure** allows to select a limited number of tenderers. Only the selected tenderers will be provided with the procurement documents. If the procurement documents contain confidential information, that information will not be made available to other economic operators on the market than the selected tenderers (Article 164 of the Financial Regulation and Point 25 of Annex I to the Financial Regulation).

- The authorising officer may exceptionally choose a **negotiated procedure** without prior publication of a contract notice in the event of a monopoly for technical reasons or exclusive rights (Point 11.1 (b) of Annex I to the Financial Regulation[1]) or for contracts declared to be secret or for contracts whose performance must be accompanied by special security measures (Point 11.1 (i) of Annex I to the Financial Regulation). The authorising officer may contact one or more economic operators and then negotiate the offer. The case-law of the Court of Justice is rather strict when it comes to the use of procedures without competition (see C-337/05 or C-187/16). If the authorising officer exceptionally chooses such a procedure, a duly motivated justification is essential. A mere reference to the security aspects of a tender procedure is not enough.

- An innovation partnership allows the acquisition of innovative products, innovative services and innovative works under the condition that they do not exist on the market (Point 7 of Annex I to the Financial Regulation). That procedure implies a mandatory preliminary consultation of the market. The procedure is time-consuming and costly and not usual in Parliament.

- A competitive procedure with negotiation or the competitive dialogue may be used, among others, if the "contract cannot be awarded without prior negotiations because of specific circumstances related to the nature, complexity or the legal and financial make-up of the contract or the risks attached to the subject matter of the contract. It may also be used in case the "the technical specifications cannot be established with sufficient precision (..)". It should be noted that this

[1] If Point 11.1 (b) of Annex I to the Financial Regulation is used, the tender may only be launched after a prior opinion of the Public Procurement Forum.

procedure/dialogue can last several months and is thus rather time-consuming procedure (see points 10 and 12 of Annex I to the Financial Regulation);

- Should the value of the contract be below the threshold of the EU Directive 2014/24/EU, the authorising officer may develop a list of preselected vendors following a call for expression of interest (Point 13 of Annex I to the Financial Regulation).

The choice of any other procedure than the open procedure has to be duly justified.

4. Specifications in procurement documents

4.1 Minimum requirements

The tender could contain minimum requirements specified in the procurement documents which require that the services, supplies or works have a minimum level of quality linked to the security-sensitivity of the tender or conform to existing security standards.

One of possible requirements could be related to the data security for tenders potentially involving communication with an outside server (to be inserted in the technical specifications):

'Where the purchase of a product is inseparably bound up with data storage services, the relevant servers or other data storage facilities shall be located on European Union territory.'

or

'Where the purchase of a product is inseparably bound up with data storage services, the relevant servers or other data storage facilities shall be located on European Union territory or in the territory of a third country which, as established by decision of the Commission in accordance with Article 45 of Regulation (EU) 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, ensures an adequate level of protection.'

The second draft relies on an application in analogy of the system of authorisation by the Commission, provided in GDPR for personal data. That option may be considered if restricting the territory of storage exclusively to the European Union was not be compatible with the object of the tender or deprived the authorising officer of any potential tenderers.

4.2 Exclusion criteria

The authorising officer responsible shall exclude a person or entity from participating in award procedures governed by the Financial Regulation where that person or entity is in an exclusion situation.

Article 136(1)(c) and (e) of the Financial Regulation can be of a greater use for the purposes of ensuring the cyber-security of tenders. Firstly, in application of Article 136(1)(c) of the FR, the authorising officer shall exclude a person or entity that was found by a final judgement or a final administrative decision guilty of grave professional misconduct, under the conditions listed in this provision. Secondly, according to Article 136(1)(e), the deficiencies in complying with main obligations in the implementation of a contract that have led to the early termination, the application of liquidated damages or have been

discovered in a formal investigation, place a person or entity that is responsible for them in an exclusion situation.

The authorising officer is invited to extend the application of these provisions, to any subcontractor or any entity on whose capacity a tenderer intends to rely (Article 137(2) of the Financial Regulation).

It should be kept in mind that if an exclusion situation is created or noticed during the execution of the contract, Parliament has the possibility to terminate the contract according to its general terms and conditions.

4.3 Selection criteria

The selection criteria should be defined according to the object of the contract. The following proposals could help the authorising officer in drafting the selection criteria for security-sensitive tenders.

Tenderers should be required to execute security-sensitive parts of a contract themselves in accordance with Point 18.8 of Annex I to the Financial Regulation. Thus, the risk linked to the sub-contracting of the security-sensitive part is avoided. It may be a significant or sometimes even impossible burden for Parliament to control a sub-contractor who manages the security-sensitive part of a contract.

On the legal capacity:

The authoring officer may require the tenderer to "hold a particular authorisation proving that it is authorised to perform the contract in its country of establishment or be a member of a specific professional organisation" (Point 18.3 of Annex I to the Financial Regulation).

On the technical and professional capacity:

1. The authorising officer should search for possible certifications. An admissible reliable certification should be drawn up by independent bodies attesting the compliance of the economic operator with certain quality assurance standards. It shall refer to quality assurance systems based on the relevant European standards series certified by accredited bodies (Point 20.4 of Annex I to the Financial Regulation).

Security certificates are not always available but should be used where it makes sense.

2. As provided for under Point 20.3 of Annex I to the Financial Regulation, "evidence of technical and professional capacity may be secured by means of a check carried out by the contracting authority or on its behalf by a competent official body of the country in which the economic operator is established, subject to that body's agreement. Such checks shall concern the supplier's technical capacity and production capacity and, if necessary, its study and research facilities and quality control measures".

This possibility is only valid for complex services or supplies.

As for the selection criteria, a tenderer may rely on the capacities of other entities (for instance, the parent company). In such cases, the authorising officer may verify the respect of the exclusion criteria by these entities (see section 3.2).

4.4 Award criteria (Article 167 of the Financial Regulation)

The award method and the award criteria are defined by the authorising officer in the framework of the Financial Regulation.
When using the best price-quality ratio method, the authorising officer should think about having a qualitative criterion related to the security-sensitivity of the tender.

For procurement procedures linked to ICT products, the following clause could be added to the award criteria:

1. Cybersecurity certification

A [to be completed] certificate shall be issued by [to be completed] for the equipment to which the contract relates. It is the responsibility of the tenderer/candidate to provide proof thereof. Tenders proposing non-certified equipment shall be excluded. Where a certificate has been issued for the equipment proposed, the contracting authority shall award points for this subcriterion on the basis of the guaranteed level of protection.

2. Security-related equipment tests and analyses

The tenderer/candidate shall provide the contracting authority with specimens of the equipment covered by the contract so that it can conduct tests and analyses as to their conformity with the relevant security standards [give details as to what the tests and analyses will involve and who will conduct them]. Depending on the outcome of the tests and analyses in relation to the level of security afforded, the contracting authority shall award points for this subcriterion.

3. Manufacturing procedure

The tenderer/candidate shall explain the measures taken by it, by its subcontractors or by the equipment manufacturers so as to ensure that the equipment complies with the highest security standards, in particular in connection with the manufacture of the equipment.

4. Cyberespionage and sabotage risk assessment

An assessment shall be carried out of the cyberespionage and sabotage risks specific to the products or services proposed. That assessment may be based on, in particular, information available from credible sources, the cybersecurity reputation of the tenderer/candidate or the opinions of relevant specialists.

Criterion	*Subcriterion*	*Maximum points*		*Relevant section of questionnaire*
Cybersecurity	*National or European product/service security certification*	*...*	*...*	*...*
	Outcome of the equipment tests and analyses	*...*		*...*
	Manufacturing procedure	*...*		
	Cyberespionage and sabotage risk assessment	*...*		*...*

To be inserted into the technical evaluation tables

The authorising officer should particularly bear in mind that the principles of equal treatment and of transparency as well as the obligation to state reasons have to be respected while applying these award criteria.

5. Contractual clauses

Two alternative clauses could be inserted in contracts involving cyber-security issues.

The more restrictive version of the clause (5.1) for the cases where the event triggering the clause occurs in the context of the execution of the contract concluded with the EP. In such cases, a provision on damages is included and the EP has the possibility to terminate the contract without giving the contractor the opportunity to present their observations, since in such a situation it may be crucial to terminate immediately the contract in order to avoid further damages. Since the situations described in paragraph 2, points (a)-(d), of this clause constitute criminal offences, it is advised to notify the competent national authorities before terminating the contract.

The larger clause (5.2) for the cases where the event triggering the clause occurs in the context of the execution of any contract signed by the EP's contractor. In such cases, as the clause is really large, the EP has to pay particular attention to assessing the risks and it has to duly verify the necessity of inserting such a clause in the contract according to the principle of proportionality. In addition, in order to comply with this principle and to ensure the balance of the contract, the contractor should be granted the possibility to submit explanations.

On the one hand, the proposed clauses can lead to higher prices, significantly limit the number of tenderers or even discourage all of them from submitting offers. On the other hand, cybersecurity risks can be present in everyday applications, services and devices and can lead to significant disruptions of Parliament's functions and procedures. Before inserting the clauses into draft contracts or in the tender specifications, the authorising officer shall assess the cybersecurity risks in relation to the contract and the necessity to confer to the EP the solutions proposed in those clauses.

5.1 Proposed security clause covering any incident or situation having a negative impact on the European Parliament's information networks and systems

1. The Contractor shall undertake to provide the European Parliament with all relevant security-related information in connection with risks and potential or actual incidents and with the corrective measures it proposes to take.

2. In view of the subject matter of the contract and the importance that the European Parliament attaches to the security of its information networks and systems, the following shall in particular be regarded as breaches of contractual obligations:

(a) any instance where, during performance of the contract, the Contractor, any of its subcontractors or suppliers or any of the manufacturers of the equipment proposed by them has accessed or accesses intentionally, without right, the whole or any part of the European Parliament's information system by infringing a security measure;[2]

(b) any instance where, during performance of the contract, the Contractor, any of its subcontractors or suppliers or any of the manufacturers of the equipment proposed by them has seriously hindered or interrupted, or seriously hinders or interrupts, the functioning of the European Parliament's information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible, intentionally and without right;[3]

(c) any instance where, during performance of the contract, the Contractor, any of its subcontractors or suppliers or any of the manufacturers of the equipment proposed by

[2] Cf. Article 3 of Directive 2013/40/EU.
[3] Cf. Article 4 of Directive 2013/40/EU.

them deletes, damages, deteriorates, alters or suppresses European Parliament computer data, or renders such data inaccessible, or has previously done so, intentionally and without right;[4]

(d) any instance where, during performance of the contract, the Contractor, any of its subcontractors or suppliers or any of the manufacturers of the equipment proposed by them has intercepted or intercepts, by technical means, non-public transmissions of computer data to, from or within the European Parliament's information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right;[5]

(e) any instance where, during performance of the contract, the Contractor, any of its subcontractors or suppliers or any of the manufacturers of the equipment proposed by them is the cause of any reasonably identifiable situation or event having a potential negative impact on the security of the European Parliament's information networks and systems.

3. In all the instances described in paragraph 2, without prejudice to other provisions of this contract on termination, the European Parliament may immediately terminate the contract as of right, without recourse to legal proceedings, without compensation and without notice, by registered letter with acknowledgement of receipt.
Termination shall take effect on the date of receipt of the registered letter with acknowledgement of receipt terminating the contract, or on any other date referred to in the letter of termination.
The effects of termination provided for in paragraph 5 of Article II.16 hereof shall apply.

4. In all the instances described in paragraph 2, the European Parliament may require the Contractor to replace the equipment on which an illegal act within the meaning of paragraph 2 has been committed, or which was or is the cause of such an act, by equipment from a different manufacturer.
The European Parliament may also require the Contractor to replace the subcontractor, supplier or manufacturer involved in the incident.
In all the instances described in paragraph 2, the European Parliament may also require the Contractor to take all other possible corrective measures.

5. Should the Contractor fail to rectify the situations described in paragraph 2 or replace the equipment, subcontractor, supplier or manufacturer concerned by the set deadline, the European Parliament may apply a flat-rate penalty for each day of delay as from the first day of delay in accordance with the modalities laid down in this contract concerning flat-rate penalties.

6. The Contractor shall be liable for any direct or consequential damage suffered by the European Parliament as a result of the actions described in paragraphs 1 and 2.

7. In this connection, the European Parliament acts on the basis of objective elements and may rely on any form of proof, prima facie evidence, court judgment or ongoing court proceedings in a European Union Member State or third state, or administrative decision by a European Union Member State or institution.

[4] Cf. Article 5 of Directive 2013/40/EU.
[5] Cf. Article 6 of Directive 2013/40/EU.

5.2 Proposed security clause covering any incident or situation having a negative impact on other information networks and systems

1. The Contractor shall undertake to provide the European Parliament with all relevant security-related information in connection with risks and potential or actual incidents and with the corrective measures it proposes to take.

2. In view of the subject matter of the contract and the importance that the European Parliament attaches to the security of its information networks and systems, the following shall in particular be regarded as breaches of contractual obligations:

(a) any instance where the Contractor, any of its subcontractors or suppliers or any of the manufacturers of the equipment proposed by them has accessed or accesses intentionally, without right, the whole or any part of an information system by infringing a security measure;[6]

(b) any instance where the Contractor, any of its subcontractors or suppliers or any of the manufacturers of the equipment proposed by them has seriously hindered or interrupted, or seriously hinders or interrupts, the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible, intentionally and without right;[7]

(c) any instance where the Contractor, any of its subcontractors or suppliers or any of the manufacturers of the equipment proposed by them deletes, damages, deteriorates, alters or suppresses computer data, or renders such data inaccessible, or has previously done so, intentionally and without right;[8]

(d) any instance where the Contractor, any of its subcontractors or suppliers or any of the manufacturers of the equipment proposed by them has intercepted or intercepts, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right;[9]

(e) any instance where the Contractor, any of its subcontractors or suppliers or any of the manufacturers of the equipment proposed by them is the cause of any reasonably identifiable situation or event having a potential negative impact on the security of an information network or system.

3. In all the instances described in paragraph 2, without prejudice to other provisions of this contract on termination, the European Parliament may terminate the contract as of right, without recourse to legal proceedings, without compensation and with prior notice, by registered letter with acknowledgement of receipt.
Termination shall take effect on the date of receipt of the registered letter with acknowledgement of receipt terminating the contract, or on any other date referred to in the letter of termination.
The effects of termination provided for in paragraph 5 of Article II.16 hereof shall apply to the instances of termination laid down in paragraph 2.

4. In all the instances described in paragraph 2, the European Parliament may require the Contractor to replace the equipment on which an illegal act within the meaning of paragraph 2 has been committed, or which was or is the cause of such an act, by equipment from a different manufacturer.

[6] Cf. Article 3 of Directive 2013/40/EU.
[7] Cf. Article 4 of Directive 2013/40/EU.
[8] Cf. Article 5 of Directive 2013/40/EU.
[9] Cf. Article 6 of Directive 2013/40/EU.

The European Parliament may also require the Contractor to replace the subcontractor, supplier or manufacturer involved in the incident and participating in the execution of this contract.
In all the instances described in paragraph 2, the European Parliament may also require the Contractor to take all other measures to ensure the security of European Parliament equipment.

5. Should the Contractor fail to rectify the situations described in paragraph 2 or replace the equipment, subcontractor, supplier or manufacturer concerned by the set deadline, the European Parliament may apply a flat-rate penalty for each day of delay as from the first day of delay in accordance with the modalities laid down in this contract concerning flat-rate penalties.

6. Before the application of the measures foreseen in paragraphs 3, 4 and 5 above by the European Parliament, the Contractor shall have an opportunity to present his observations within a period not exceeding 15 calendar days with effect from the date of dispatch of the notice by registered letter with acknowledgement of receipt.

7. In this connection, the European Parliament acts on the basis of objective elements and may rely on any form of proof, prima facie evidence, court judgment or ongoing court proceedings in a European Union Member State or third state, or administrative decision by a European Union Member State or institution.

6 Access to procurement only for EU-based economic operators

In accordance with Article 176 of the Financial Regulation, access to Parliament's procurement procedures is limited to economic operators based in Member States. Only on an exceptional basis, economic operators from countries with which the EU has a special agreement in the field of public procurement can be allowed to participate in Parliament's tenders. If a tender procedure concerns security-sensitive goods, services or works, any opening of the tendering procedure to non-EU economic operators should be very well justified and the protection of data in accordance with applicable EU law should be ensured for non-EU operators.