
SCOTTISH STATUTORY INSTRUMENTS

2015 No. 446

The Public Contracts (Scotland) Regulations 2015

PART 2

RULES IMPLEMENTING THE PUBLIC CONTRACTS DIRECTIVE

CHAPTER 1

SCOPE AND GENERAL PRINCIPLES

SECTION 2

General Rules

Rules applicable to communication

23.—(1) Subject to paragraphs (3), (5) and (8), a contracting authority must ensure that all communication and information exchange, including submission, pursuant to these Regulations is performed using electronic means of communications in accordance with this Regulation.

(2) Subject to paragraph (13), the tools and devices to be used for electronic means of communication, and their technical characteristics, must—

- (a) be non-discriminatory;
- (b) be generally available;
- (c) be interoperable with the information and communication technology products in general use; and
- (d) not restrict economic operators' access to the procurement procedure.

(3) A contracting authority is not obliged to require electronic means of communication in the submission process where—

- (a) due to the specialised nature of the procurement, the use of electronic means of communication would require specific tools, devices or file formats that are not generally available or supported by generally available applications;
- (b) the applications supporting file formats that are suitable for the description of the tenders use file formats that cannot be handled by any other open or generally available applications or are under a proprietary licencing scheme and cannot be made available by the contracting authority for downloading or remote use;
- (c) the use of electronic means of communication would require specialised office equipment that is not generally available to the contracting authority; or
- (d) the procurement documents require the submission of physical or scale models which cannot be transmitted using electronic means.

(4) Where, in accordance with paragraph (3), electronic means of communication is not required, communication must be carried out—

- (a) by post or by other suitable carrier; or
 - (b) by a combination of post or other suitable carrier and, to the extent that electronic means of communication is possible, by such means.
- (5) A contracting authority is not obliged to require electronic means of communication in the submission process to the extent that the use of means of communication other than electronic means is necessary—
- (a) because of a breach of security of the electronic means of communication; or
 - (b) for the protection of information of a particularly sensitive nature which requires such a high level of protection that it cannot properly be ensured by using electronic tools and devices that are either generally available to economic operators or that can be made available to them by suitable alternative means of access in accordance with paragraph (14).
- (6) Where, in accordance with this regulation, a contracting authority requires means of communication in the submission process other than electronic means, the authority must state the reason for this in the individual report referred to in regulation 83 (reporting and documentation requirements).
- (7) Where electronic means of communication is not required for a reason referred to in paragraph (5), the contracting authority must state in the individual report the reasons why use of means of communication other than electronic means has been considered necessary under that paragraph.
- (8) Notwithstanding paragraph (1), oral communication may be used in respect of communications other than those concerning the essential elements of a procurement procedure, provided that the content of the oral communication is documented by the contracting authority.
- (9) In paragraph (8), reference to “the essential elements of a procurement procedure” includes the procurement documents, requests for participation, confirmations of interest and tenders.
- (10) A contracting authority must, to a sufficient extent and by appropriate means, document oral communications with tenderers which could have a substantial impact on the content and assessment of the tenders, in particular, by preparing written or audio records or summaries of the main elements of the communication.
- (11) In all communication, exchange and storage of information, a contracting authority must ensure that the integrity of data and the confidentiality of tenders and requests to participate are preserved.
- (12) A contracting authority must examine the content of tenders and requests to participate only after the time limit set for submitting them has expired.
- (13) A contracting authority may, where necessary, require the use of tools and devices which are not generally available, provided that the contracting authority offers suitable alternative means of access.
- (14) A contracting authority shall be deemed to offer suitable alternative means of access where the authority—
- (a) offers unrestricted and full direct access free of charge by electronic means to those tools and devices from the date of publication of the call for competition or from the date when the invitation to confirm interest is sent;
 - (b) ensures that tenderers having no access to the tools and devices concerned, or no possibility of obtaining them within the relevant time limits (provided that the lack of access is not attributable to the tenderer) may access the procurement procedure through the use of provisional tokens made available free of charge online; or
 - (c) supports an alternative channel for electronic submission of tenders.

(15) For the purpose of paragraph (14)(a) “date of publication of the call for competition” means the date of publication in the Official Journal after being sent in accordance with regulation 52 (form and manner of sending notices for publication at EU level).

(16) A contracting authority must specify in the call for competition or the invitation to confirm interest, referred to in paragraph (14)(a), the internet address at which those tools and devices are accessible.

(17) Tools and devices for the electronic receipt of tenders, requests to participate and, in design contests, plans and projects, must—

- (a) enable the precise determination of the exact time and date of the receipt of tenders, requests to participate and the submission of plans and projects;
- (b) to the extent reasonably possible, ensure that, before the time limit referred to in paragraph (12) has expired, no-one can have access to data transmitted to the authority using the tools and devices;
- (c) ensure that only authorised persons may set or change the dates for opening data received;
- (d) ensure that, during the different stages of the procurement procedure, only authorised persons may have access to data submitted or to part of such data;
- (e) ensure that only authorised persons may give access to data transmitted and only after the time limit referred to in paragraph (12) has expired;
- (f) ensure that data received and opened in accordance with the requirements in sub-paragraphs (a) to (e) remains accessible only to persons authorised to acquaint themselves with the data; and
- (g) to the extent reasonably possible, ensure that any infringement, or attempted infringement, of the conditions referred to in sub-paragraphs (b) to (f) is clearly detectable.

(18) In addition to the requirements set out in paragraph (17), a contracting authority must comply with all of the following requirements in relation to tools and devices for the electronic transmission and receipt of tenders and for the electronic receipt of requests to participate—

- (a) information on specifications for the electronic submission of tenders and requests to participate, including encryption and time-stamping, must be available to interested parties;
- (b) a contracting authority must specify the level of security required for the electronic means of communication in the various stages of the specific procurement procedure;
- (c) the level of security specified in accordance with sub-paragraph (b) must be proportionate to the risks attached;
- (d) where paragraph (19) applies, the contracting authority must accept advanced electronic signatures supported by a qualified certificate, created with or without a secure signature creation device, subject to compliance with all of the following conditions—
 - (i) the contracting authority must establish the required advanced electronic signature format on the basis of formats established in Commission Decision 2011/130/EU establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (notified under document C(2011) 1081)(1) and must put in place necessary measures to be able to process these formats technically;
 - (ii) where a different format of electronic signature is used, the electronic signature or the electronic document carrier must include information on existing validation possibilities;

(1) OJ L 53, 26.2.2011, p.66, amended by Commission Implementing Decision 2014/148/EU (OJ L 80, 19.3.2014, p.7).

- (iii) the validation possibilities must allow the contracting authority to validate the received electronic signature as an advanced electronic signature supported by a qualified certificate, such validation to be online, free of charge and in a way that is understandable for non-English speakers;
- (iv) where a tender is signed with an advanced electronic signature with the support of a qualified certificate from a provider that is included on a trusted list provided for in Commission Decision [2009/767/EC](#) setting out measures facilitating the use of procedures by electronic means through the points of single contact under Directive [2006/123/EC](#) of the European Parliament and of the Council on services in the internal market (notified under document C(2009) 7806)(2), as amended from time to time (in this regulation “the Commission Decision”), the contracting authority must not apply additional requirements that may hinder the use of the signature by the tenderer.

(19) This paragraph applies where a contracting authority concludes that the level of risk assessed in accordance with paragraphs (21) and (22) is such that advanced electronic signatures as defined by Directive [1999/93/EC](#) of the European Parliament and of the Council on a Community framework for electronic signatures(3) as amended from time to time, are required.

(20) A contracting authority shall assess the certificate referred to in paragraph (18)(d) by taking into account whether the certificate is provided by a certificate services provider, which is on a trusted list provided for in the Commission Decision.

(21) In deciding the level of security required at each stage of a procurement procedure, and in concluding whether the level of risk is such that advanced electronic signatures are required, a contracting authority must assess the risks having regard to—

- (a) the likelihood of particular risks materialising;
- (b) the potential adverse consequences if those risks materialise;
- (c) the need for consistency as between similar procurements performed by the same contracting authority; and
- (d) the need for proportionality between the expected benefits of any particular security requirements (in terms of eliminating or reducing any of the risks referred to in paragraph (22)), and the costs, burdens and obligations which those requirements may impose upon an economic operator.

(22) A contracting authority must assess all relevant risks, including, in particular, where applicable—

- (a) the risk to the proper functioning and integrity of the specific procurement process, including risks of breach of these Regulations;
- (b) risks to national security;
- (c) the risk of inadvertent or unauthorised disclosure of, or access to, any economic operator’s confidential information;
- (d) the risk of inadvertent or unauthorised disclosure of, or access to, information held by the contracting authority including information relating to the specific procurement;
- (e) the risk that use of electronic communications could provide opportunity for malicious attacks on the electronic systems of, or data held by, the authority, any economic operator or any other person, including introduction of malware or denial of service attacks; and
- (f) any other material risk relating to the procurement procedure in question.

(2) OJ L 274, 20.10.2009, p36, last amended by Commission Decision 2013/662/EU (OJ L 306, 16.11.2013, p.21).

(3) OJ L 13, 19.1.2000, p12, amended by Regulation (EC) No 1137/2008 (OJ L 311, 21.11.2008, p.1).

(23) Paragraph (24) applies where—

- (a) a competent authority of the United Kingdom located in Scotland; or
- (b) another issuing entity located in Scotland,

signs and issues a document for use in a procurement with the scope of the Directive, whether the procedure is under these Regulations or under the law of any member State.

(24) The competent authority or issuing entity may establish the required advanced signature format in accordance with the requirements set out in Article 1(2) of Commission Decision 2011/130/EU establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (notified under document C(2011) 1081)(4), as amended from time to time, and, where it does so—

- (a) it must put in place the necessary measures to be able to process that format technically by including the information required for the purpose of processing the signature in the document concerned; and
- (b) the documents must contain, in the electronic signature or in the electronic document carrier, information on existing validation possibilities that allow the validation of the received electronic signature online, free of charge and in a way that is understandable for non-English speakers.

(4) OJ L 53, 26.2.2011 p.66.