

GSA/RP/17/14

"Maintenance of security systems of GSA premises in Prague"

Annex I.H- COMPLIANCE MATRIX for the SECURITY ASPECTS LETTER

Participants:

[Name of Company]

GSA	Contractor
-----	------------



Compliance matrix to the requirements of the Security Aspects Letter

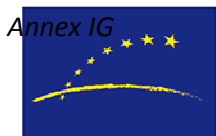
1 Introduction

The tenderers are required to submit the present compliance matrix to the requirements of the Security Aspects Letter (SAL) indicated below as part of their request to participate. This compliance matrix may require when necessary the provision of supporting data or information relating to the necessary security measures for the exchange of classified information.

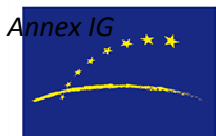
Please Note

The Compliance Matrix forms part of the selection criteria – only candidates compliant with all requirements of the Matrix may be further considered regarding eligibility for participation in the tender process.

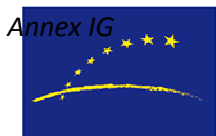
You are therefore kindly asked to carefully read and answer truthfully all the requested requirements. Also submit attachments / supporting documents where requested. Untruthful answering of the requirements will result in exclusion from the tendering process and may be subject to further legal procedures.



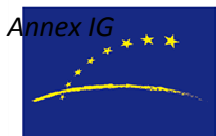
Compliance matrix to the core requirements of the Security Aspects Letter for Contract X	Declaration of Compliance of the tenderer		
	YES	PARTIALLY (please comment)	NO (please comment)
SAL Requirement			
- [REQ 1] The contractor and sub-contractor shall be registered in an EU Member State.			
- [REQ 2] All Contractor's personnel as well as subcontractors' personnel involved in work under this Contract shall be nationals of an European GNSS PSI Participant unless otherwise agreed in advance and in writing with the GSA.			
- [REQ 3] All Contractor's personnel as well as subcontractors' personnel involved in work under this contract shall hold an appropriate valid Personnel Security Clearance (PSC) for accessing EU and, national classified information at the level of Secret UE, should the need arise to access such national classified information.			
- [REQ 4] All industrial or other entities participating in classified contracts which involve access to information classified UE CONFIDENTIEL or above shall hold a Facility Security Clearance (FSC) at the appropriate classification level. The FSC is granted by the NSA/DSA of the participating State in which it is located to confirm that a facility can afford and guarantee adequate security protection of classified information to the appropriate classification level.			
- [REQ 5] The documents referenced in section 1, Applicable Documents, in their latest version shall be applicable to the contractor and subcontractors and the security principles they contain shall govern the execution of the contract.			
- [REQ 6] Information generated by the contractor or any subcontractor which requires classification shall be marked using the EU security classification markings.			
- [REQ 7] When a doubt arises about the classification level of information generated under contractual activity, the contractor or subcontractor(s) involved shall ask the GSA in writing about the classification level to adopt. While waiting for the reply of the GSA, the information shall be classified Confidential UE and all parties shall handle it accordingly until the GSA has decided on the actual classification level and communicated it in writing to the contractor and/or subcontractor(s).			



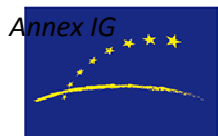
- [REQ 8] The contractor shall handle and protect classified information or material provided to them or generated by the contractor pursuant to this Contract in accordance with its classification as described in AD2, The European GNSS PSI or, provided they are no less stringent, in accordance with national regulations.			
- [REQ 9] In situations where provisions in national legislation and regulations differ from the provisions in this SAL, the provisions in national legislation and regulations may be applied provided that they are not less stringent than the provisions set out in this SAL. In all such cases the contractor shall inform in writing the GSA of the revised security procedures.			
- [REQ 10] If the contractor's responsible NSA/DSA identifies a failure by the contractor to observe the security provisions described and Regulations referred to under this SAL, it shall inform the GSA. If this failure is of such a nature as to result in the withdrawal of the contractor's Facility Security Clearance (FSC) to handle classified documents as necessary for the execution of the Contract, the GSA shall have the right to terminate the Contract with immediate effect in accordance with the relevant provisions of the General Terms and Conditions for Contracts awarded by the GSA, without prejudice to criminal and civil proceedings against the contractor.			
- [REQ 11] If the responsible NSA/DSA has identified such a failure to comply with the relevant security Regulations by any subcontractor resulting in the withdrawal of the subcontractor's FSC, the GSA shall be entitled to require the contractor to terminate the sub-contract with immediate effect, without prejudice to the GSA's right to terminate the contract with immediate effect and/or to initiate criminal and/or civil proceedings against the subcontractor.			
- [REQ 12] For work performed on the GSA's premises, the contractor and its personnel shall comply with the the local safety and security rules provided they are not less stringent than those of AD 2 the European GNSS PSI.			
- [REQ 13] For work performed on other locations than the GSA and the contractor's premises, the contractor and its personnel shall comply with the local safety and security rules provided they are not less stringent than those of AD 2 the European GNSS PSI.			
- [REQ 14] Procedures for international visits contained in AD2 The European GNSS PSI shall be applied to all visits necessary in the performance of this contract.			
- [REQ 15] The contractor shall not transmit any classified information or material to a subcontractor without the prior written consent of the originator and the GSA.			
- [REQ 16] The ultimate responsibility for protecting classified information within industrial or other entities rests with the management of those entities.			



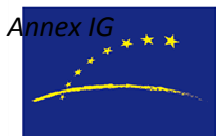
- [REQ 17] It may be necessary for the contractor to negotiate classified subcontracts with subcontractors at various levels. The contractor is responsible for ensuring that all subcontracting activities are undertaken in accordance with the common minimum standards contained in this SAL. The procedures for subcontracting in AD 2, The European GNSS PSI will be applied to all potential subcontracts.			
- [REQ 18] Classified information released to the contractor or subcontractor or generated under contractual activity shall not be used for purposes other than those defined by the classified contract and shall not be disclosed to third parties without the prior written consent of the originator and of the GSA.			
- [REQ 19] If changes to the security requirements emerge during the performance of the contract and if such changes significantly deviate from the initial arrangements, the contract shall be amended accordingly or terminated, as appropriate.			
- [REQ 20] Where changes of security requirements result in additional security measures to be taken or investments to be made by the contractor, a contract amendment shall be negotiated on a fair and reasonable basis.			
- [REQ 21] In case the contractor cannot comply with increased security requirements, the contract shall be terminated. However, any contract termination resulting from changes of the security requirements shall not be by default the responsibility of the contractor, and the contractor may be entitled to compensation by the GSA.			
- [REQ 22] In the event of the contract terminated by either party, the procedures described in AD, The European GNSS PSO for the disposal of classified information shall be implemented;			
- [REQ 23] The NSA/DSA of the participant in which the contractor is registered shall be informed by the contractor and by the GSA Local Security Officer separately of the award of a classified contract.			
- [REQ 24] When a classified contract or a classified subcontract is terminated, the contractor and the GSA Local Security Officer shall notify separately this termination in less than one month to the NSA/DSA of the participants in which the contractor and subcontractors are registered.			
- [REQ 25] Throughout the life of the classified contract, compliance with all its security provisions shall be monitored by the GSA, in conjunction with the relevant NSA/DSA. Any security incidents shall be reported, in accordance with the provisions laid down in the European GNSS PSI. Any change to or withdrawal of a Facility Security Clearance shall immediately be communicated to the GSA Local Security Officer.			
- [REQ 26] The contractor shall - under penalty of termination of the contract - comply with any security requirements prescribed by the Contracting Authority as detailed in this Security Aspects Letter.			
- [REQ 27] The Contractor shall uphold and describe its security organisation in its bid and provide the identification and contact details of the Contract Manager and the company Security Officer.			
- [REQ 28] Any subsequent changes shall be communicated in writing to the GSA using NSA/DSA's channels within 30 days of their occurrence.			



- [REQ 29] The procedures for transmission of classified information contained in AD2, The European GNSS PSI, shall be applied to any transmission of classified information as a result of contractual activities.			
- [REQ 30] In addition to the prescriptions of AD2, The European GNSS PSI, classified information, whenever stored on a digital media for transmission and whatever its classification level, will be encrypted.			
- [REQ 31] Any sensitive information related to the contract execution will be encrypted before transmission.			
- [REQ 32] Details of transmission arrangements when information classified at the level UE CONFIDENTIEL or above is exchanged are considered as sensitive and shall be encrypted when sent by e-mail.			
- [REQ 33] Unless otherwise agreed in writing, the tool 'Chiasmus for Windows' developed by the BSI shall be used for encryption.			
- [REQ 34] The Contractor shall ensure they are licensed by the BSI to use the tool. BSI's details: Bundesamt für Sicherheit in der Informationstechnik (BSI) Refereat Z5 / Vertrieb Postfach 20 03 63 53133 Bonn GERMANY Phone: +49 228 9582 281 or 212 Fax: +49 228 9582 4430 E-mail: vertrieb@bsi.bund.de			
- [REQ 35] All parties involved in contractual activities shall handle the encryption tool and the generated encrypted documents in accordance with the Security Operating Procedures (SecOPS) of the Authority providing the encryption tool or, provided they are not less stringent, in accordance with national regulations.			
- [REQ 42] Security violations shall be handled as prescribed in in AD 2, The European GNSS PSI.			
- [REQ 43] Reports of security violations shall be sent to the GSA Local Security Officer.			
- [REQ 44] Reports of security violations shall be classified as appropriate and transmitted accordingly. Should the classification of the report be higher than UE RESTREINT UE (or equivalent), a sanitized report allowing a classification at the level UE RESTREINT of lower shall be established in order to allow a quick transmission of it using appropriate channels and tools.			



<p>- [REQ 45] Any security-related notices or communication to the GSA shall be addressed to: European GNSS Agency (GSA), Security Department for the attention of the Local Security Officer, Janovskeho 438/2, 170 00 Prague 7, Czech Republic Email: Iso@gsa.europa.eu</p>			
--	--	--	--



1 Applicable documents

- AD 1 Regulation (EU) n° 912/2010 of the European Parliament and of the Council, setting up the European GNSS Agency, as amended by Regulation (EU) No 512/2014.
- AD 2 The European GNSS PSI, latest version
- AD 3 Commission Decision No 2001/844/EC, ECSC, Euratom published in OJ L 317 of 3.12.2001 as last amended by Commission Decision 2006/548/EC, Euratom published in OJ L 215 p.38 of 5.8.2006, amending its internal Rules of Procedure (COMMISSION PROVISIONS ON SECURITY), as last amended
- AD 4 Decision No 1104/2011/EU of the European Parliament and of the Council of 25 October 2011 on the rules of access to the public regulated service provided by the global navigation satellite system established under the Galileo Programme

GSA	Contractor
-----	------------