GSA/OP/25/20
" GRC Guarding, Security and Safety Monitoring Services "

Annex I to Invitation to Tender

“Tender Specifications"

Ref: GSA/OP/25/20/Annex I

Issue: 1 Rev 0

Date: 09/03/2021

Index

1 Overview

The present Tender Specifications, attached to the Invitation to Tender, complement the information contained in the Contract Notice with further information on the procurement procedure and scope.

1.1 Context of the tender: European GNSS Agency and GNSS Programmes

The European GNSS Agency (hereinafter referred to as 'the GSA', 'the Agency' or 'the Contracting Authority') is an agency formed by the European Union to accomplish specific tasks related to the European GNSS programmes (Galileo and EGNOS).

Further information can be found on the GSA's web site (http://www.gsa.europa.eu). This website contains also information about

- European GNSS programmes (https://www.gsa.europa.eu/european-gnss/what-gnss)
- Legal framework applicable to the GSA (https://www.gsa.europa.eu/register-of-documents)

Please note that in the financial perspective 2021-2027, a new regulation should be adopted foreseeing the start of the EU Space Programme Agency (EUSPA) as the successor to the GSA. EUSPA takes on increased responsibilities not only for Galileo and EGNOS, but also for the other EU space programmes, in particular Copernicus and GOVSATCOM.

1.2 Outline of the tender

Name: GRC Guarding, Security and Safety Monitoring Services

Procedure: **Open procedure** for the signature of a single framework contract in accordance with Article 164(1)(a) of Regulation 2018/1046 on the financial rules (hereafter 'Financial Regulation' or 'FR')[1] .

1.3 Principles

- Tenderers are required to accept all the terms and conditions set out in the Invitation to Tender, Tender Specifications and draft contract. Tenderers are required to waive their own general or specific terms and conditions. The terms and conditions set out in the Invitation to Tender, Tender Specifications and draft contract shall be binding on the tenderer to whom the contract is awarded for the duration of the contract.
- Any attempt by a tenderer to obtain confidential information, enter into unlawful agreements with competitors or influence the evaluation committee or the GSA during the process of examining, clarifying, evaluating and comparing tenders will lead to rejection of his tender and may result in administrative penalties.

[1] REGULATION (EU, Euratom) 2018/1046 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012

1.4 Purpose of the Invitation to Tender

The objective of this Invitation to Tender is to conclude one Framework contract (hereinafter referred to as "the Contract", "Framework Contract", or "FWC") for the provision of services described in present Tender Specifications.

1.5 Change of incumbent contractor

Tenderers are informed that the activities/services constituting the subject matter of this tender are currently performed by an incumbent Contractor. In case of a change of Contractor as a result of the present tender, the tenderers shall assess the applicability of the 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 parts of undertakings or businesses, as implemented in the relevant national legislation(s). Any risk or impact stemming from the application of the above-mentioned legislation shall be entirely allocated to the Contractor and shall be taken into consideration in the formulation of the offer.

1.6 Applicable legal acts and rules

It is the contractor's responsibility to comply with applicable laws in the execution of the awarded contract.

Applicable legal acts and rules include the following:

- Financial Regulation (FR);
- GNSS Regulation[2];
- GSA Regulation[3];
- GSA Financial Regulation[4];
- 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, and repealing Directive 95/46/EC (General Data Protection Regulation);
- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons 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;

[2] Regulation (EC) No 1285/2013 of the European Parliament and of the Council of 11 December 2013 on the implementation and exploitation of European satellite navigation systems and repealing Council Regulation (EC) No 876/2002 and Regulation (EC) No 683/2008 of the European Parliament and of the Council (hereinafter "GNSS Regulation").

[3] Regulation (EU) No 912/2010 of the European Parliament and of the Council of 22 September 2010 setting up the European GNSS Agency, repealing Council Regulation (EC) No 1321/2004 on the establishment of structures for the management of the European satellite radio navigation programmes and amending Regulation (EC) No 683/2008 of the European Parliament and of the Council, as amended by Regulation (EC) No 512/2014 of the European Parliament and of the Council of 16 April 2014.

[4] European GNSS Agency GSA Financial Regulation 2019 adopted by its Administrative Board on 16 August 2019.

- Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information;
- Regulation on public access to documents[5];
- The Programme Security Instruction (PSI) concerning European GNSS Programmes always in the latest version (current: Version 4.1 issued by the GNSS Security Board (GNSS SB) dated 26 September 2014).

1.7 Procurement schedule

Timetable	Date	Comments
Submission for publication of contract notice to the supplement to the Official Journal by the GSA.	02/03/2021	All documents of the Invitation to Tender available at: http://www.gsa.europa.eu/gsa/procurement
Deadline for submission of a non-disclosure undertaking (hereafter referred to as 'NDU') for access to Proprietary Information	30/03/2021 (advisable)	In accordance with section 1.8 below. The economic operators are advised to abide by the deadline specified herewith in order to have enough time for preparation of their tender.
Deadline for requests of clarifications.	20/04/2021	Requests to be sent in writing only to: tenders@gsa.europa.eu
Last date on which clarifications are issued by GSA.	23/04/2021	All clarifications will be published at the GSA's procurement website: http://www.gsa.europa.eu/gsa/procurement Tenderers are invited to check the GSA's procurement website on a regular basis.
Deadline for submission of tenders.	**30/04/2020**	**According to conditions of submissions set out in section 4.7 of these specifications.**
Opening session and start of evaluation session.	May 2021	

[5] Council Regulation (EC) No 1049/2001 of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

Completion of evaluation and award	June 2021	
Signature of contract and kick-off	June 2021	

1.8 Submission of Non-Disclosure Undertaking – access to proprietary information during the tender

Tenderers (including any consortium member and subcontractor) participating in this procurement procedure shall treat with confidentiality any information and documents, disclosed in any form, in writing or orally, in relation to the procurement procedure.

The economic operators participating in this procurement procedure are obliged to follow the Non-Disclosure Undertaking (NDU) signature procedure outlined below.

The NDU must be signed only by the prime Tenderer or the consortium coordinator. The prime Tenderer or consortium coordinator, with the signing of the NDU, further irrevocably and explicitly declares to ensure that the provisions under the NDU shall apply wholly and unconditionally to any members of the contractor's consortium and any of the subcontractors and any personnel he may draw on for the preparation of the tender.

Before the deadline indicated above in section 1.7, the prime Tenderer or the consortium coordinator may request access to the proprietary information [contained in Annex I.K] which is relevant for drafting the tender.

For this purpose, they shall each submit:

- NDU using the form attached in Annex I.;
- Legal Identification Form (the "LEF") and the supporting documents indicated in the LEF;
- proof that the person signing the NDU is authorised to represent the tenderer/consortium coordinator.

If possible, the Tenderer should submit the documentation only electronically to tenders@gsa.europa.eu. The documents must be signed electronically with a qualified electronic signature (QES) of the tenderer/applicant. This electronic signature must be provided by a provider which has a qualified status granted by a national competent authority of an EU Member State and which is listed in the national eIDAS Trusted Lists and the EU List of eIDAS Trusted Lists (LOTL) (available at https://webgate.ec.europa.eu/tl-browser/#/).

In case the Tenderer prefers to submit it on paper, all documentation shall be sent to the following address:

European GNSS Agency

Procurement and Legal Department
Non-Disclosure Undertaking under procurement procedure GSA/OP/25/20
Janovského 438/2
170 00 Prague 7
Holešovice, Czech Republic

In parallel, the tenderers shall send the scanned documents above to tenders@gsa.europa.eu to allow a faster treatment of the request. The subject of the email shall be: "GSA/OP/25/20: submission of NDU by *[insert name of legal entity / consortium]*" and it shall contain as attachment the relevant proof of submission.

Only entities which, according to the submitted Legal Identification Form and supporting documents, are established in a Member State of the European Union are eligible to receive proprietary information including any classified information. This does not prejudice the verification of the specific participation conditions under section 2.2.1 to be performed separately against the tenderers. In addition, the proprietary and/or classified information are only available to potential tenderers or subcontractors. The GSA reserves the right to refuse the access to the proprietary and/or classified information to entities which cannot provide sufficient evidence of capability to perform the contract(s).

Without prejudice to further legal measures, exchange of any proprietary and/or classified information subject to NDU with any person who has not previously signed the relevant NDU may lead to exclusion from the procurement procedure under the GSA's discretion.

Agreements previously signed by economic operators for access to the proprietary and/or classified information not related to this procurement are not regarded as fulfilling the present NDU's requirements.

Potential tenderers that decided not to submit a tender must return all classified information within 15 (fifteen) working days from the deadline for submission of tenders (see table in section 1.7). Likewise, an unsuccessful tenderer is required to return all classified information within 15 (fifteen) working days after publication of the relevant contract award notice in the Official Journal of the European Union.

2 Terms of reference

2.1 Technical terms of reference

The primary mission of the Galileo Reference Centre (GRC) is to perform independent monitoring of the Galileo Services and to report it to the relevant stakeholders. It provides the GSA, as the Galileo Service Provider, with an independent means of evaluating the performance of the Galileo Service Operator and the quality of the signals in space. It is fully independent of the system and the Galileo

Service Operator with respect to both the technical solution (hardware, software, reference products, etc.) and operations. The GRC also assesses the compatibility and interoperability between Galileo and other GNSS.

The GRC comprises a core facility, located in Noordwijk, the Netherlands, and integrates data and products from cooperating entities from the EU Member States (MS), Norway and Switzerland. The current version of the GRC operational infrastructure (GRC v1) is operational and MS contributions are being provided in the frame of Framework Partnership Agreements established between the GSA and respective MS.

The GRC building comprises of approximately 25% technical rooms (including laboratory), 15% operational rooms, 25% office space, 25% communal staff areas and reception facilities, and 10% meeting and conference facilities. In additional to the internal building facilities, the GRC also has a gated area of land that includes the moat around the building and on-site parking facilities that amounts to over 3000 square metres of space.

The scope of this procurement is the provision of:

- on-site guarding services during the nominal opening hours of the facility, between 07:00 and 20:00,
- on-site guarding services outside the nominal opening hours of the facility, following specific request of the GSA,
- 24/7 remote security and safety monitoring services of the facility.

In order to guarantee the security and safety inside the GRC premises, the Contractor is expected to provide:

- 24/7/365 security and safety monitoring services using the available facilities; available facilities at the GRC include:
    - Access Control System (ACS), including:
        - Checking of passports or identity documents,
    - Health Monitoring (HM) (non-contact) of employees and visitors during times of need (e.g. global pandemic),
    - Intrusion Detection System (IDS),
    - Safety Incident Detection (SID) to detect dangerous events (fire, water, heating, cooling, etc.),
    - On-site patrolling (using an Electronic Tagging System – see section 2.1.2.2.).
- 24/7/365 intervention and guarding service provided by:
    - On-Site Guarding and Intervention Service during opening hours (at the time of the tender the opening hours are between 07:00 and 20:00 (excluding weekends and national public holidays), however during the duration of the contract the opening hours could be extended up to 24 hours a day)
    - Security, Safety Monitoring, and Intervention Service outside of opening hours.

The services are further defined below. The roles of the Local Security Officer (LSO) and the Deputy LSO (DLSO) are appointed to GSA staff working at the GRC. Both of these roles will be referred to as D/LSO throughout this document.

2.1.1 General requirements

2.1.1.1 Work Organisation

The Contractor shall perform the work defined in the Tender Specifications in accordance with the Work Package Descriptions defined below.

2.1.1.2 Personnel Security Clearance

The Contractor shall ensure full compliance with all the requirements in the Security Aspects Letter (SAL) found in Annex I.H.

2.1.1.3 Security Tasks

The Contractor shall provide at least the following security tasks:

a) Conduct of applicable:
   i. on-site guarding and intervention services; and
   ii. security and safety monitoring services (monitoring and remote guarding of the GRC premises):
      - initialising and maintaining the connection between the GRC and their remote monitoring centre.

b) Contractual Reporting and coordination with the Contracting Authority;

c) Security Reporting and coordination with the DLSO;

d) Provision and maintenance of Security/safety incidents in the appropriate logbooks.

2.1.1.4 Contractor's Code of Conduct

The Contractor's on-site staff shall be the first point of contact with visitors to the GRC. Therefore, the appearance and attitude of the proposed staff must be impeccable. Politeness, discretion, and helpfulness will be required. In this regard, Tenderers must include an appropriate code of conduct in their tender.

2.1.1.5 Health, Safety, and the Environment

The Contractor is required to comply with the laws and regulations in force, particularly with regard to Health, Safety, and the Environment ("HSE"), and take all the measures necessary for the proper performance of the services covered by the Contract. To this end, the Contractor is required to implement health and safety protection measures in accordance with the laws and regulations in force.

2.1.2 Work packages (WP)

The work packages in Table 1 represent the activities foreseen under the framework contract. The Work Packages described in this section are transversal to all Specific Contracts (SCs) that may be concluded under this framework contract (FWC).

WP#	Work Package Title
WP.01	Management
WP.02	Security Guarding, Intervention, and Monitoring
WP.03	Contract Handover and Handback

2.1.2.1 WP.01: Management and Reporting

2.1.2.1.1 WP.01.01: Project Management

This Work Package comprises the project management activities necessary for successful execution of the contract.

Management Activities

The contractor shall perform the management activities as per the requirements in this Tender Specifications.

Project Management Organisation

The Contractor shall implement and maintain a project management organisation in order to manage and control adequately all the activities of the contract, to provide the proper control of the lower tier Subcontractors (if any) and ensure the required feedback and interface to the Contracting Authority.

Preparation of Plans

The Contractor shall prepare, for Contracting Authority's approval, the plans as required by the Specific Contracts. After approval, the plans shall be the baseline for the execution of the related work.

Table 1 – Reviews and Meetings of the Contract

Review / Meeting	Acronym	Major Outcomes
Kick-off Meeting	KOM	Kick-off of the activities of the Specific Contract to determine the terms of execution of the contract.
Monthly Status Meetings	MS#	Monthly meetings are organised between the GRC Deputy Local Security Officer (DLSO), the Contractor Guard Force Supervisor (GFS), and other participants to be delegated by the GSA as

Review / Meeting	Acronym	Major Outcomes
		needed.
Quarterly Review Meetings	QR#	Quarterly review meetings are to be combined with the third monthly status meeting of the period and are organised between the GRC Deputy Local Security Officer (DLSO), the Contractor Guard Force Supervisor (GFS), and other participants to be delegated by the GSA as needed.
Final Review	FR	Closure of the specific contract.

Kick-off Meeting (KOM) Organisation and Objectives

The Contractor shall organise the Kick-off Meeting (KOM) for each specific contract, after the signature of the respective specific contract. The main objectives of the KOM shall be:

a) the presentation of the contract major milestones and objectives;

b) the presentation of the Contractor Team and the Contracting Authority Team;

c) the closeout and agreement on open issues.

Monthly Status Meetings

The Contractor shall organise Monthly Status Meetings. These meetings shall be accompanied by a Monthly Report delivered a maximum of 7 working days after the end of the previous month, containing:

- the KPI calculations for the period;
- all relevant information pertaining to the events and incidents that have occurred in that month;
- the executed schedule (where applicable highlighting the discrepancies between the provisional and the executed schedule) in order to enable proper controlling of the hours worked and invoicing;
- filled-in time sheets for every day when services were provided;
- calculation of the price of services for the month;
- the provisional schedule for the following month.

Quarterly Review Meetings

The Contractor shall organise Quarterly Review Meetings. These meetings shall be accompanied by a Quarterly Report, delivered two weeks in advance of the meeting that shall contain:

- all relevant information pertaining to the events that have occurred during the quarter,

- a statistic report summarising the daily attendance and showing the actual hours worked by staff under the contract by name, type and quantity;
- timesheets justifying the amount of hours spent on performing the tasks which are charged as hourly rates, in accordance with Annex I.F (i.e. items CBS 06, 07, 08 and 09);
- updated certificates and movement of staff,
- a quality management report including:
    - a detailed presentation of the work carried out by Contractor's staff,
    - a thorough compilation of all unusual or unexpected events, discrepancies and abnormality in relation to the provided services;
    - a table of trainings, and certification (done, to be done, foreseen),
- a table of the status of actions and corrective measures agreed with GSA contract manager and/or his/her representative,
- all security reports of the quarter.

Format and Delivery of Reports and Logs

Reports and Logs templates shall be proposed by the Contractor and validated by the GSA. The Contractor shall get all templates validated before the end of the first month following the beginning of the contract. For operational needs, the GSA may at any time of the contract request from the Contractor changes in the templates. In such case, templates shall be validated again by the GSA before dissemination. All reports and logs shall be sent to the GRC DLSO or appointed contact in the event of the DLSO's unavailability.

Final Review

The Contractor shall organise a final review for each specific contract. This review shall aim at ensuring that all activities have been performed sufficiently. The review shall include a Lessons Learned section that can be implemented, where required, in the next specific contract with the aim of improving the services.

Review of Performance

The Contracting Authority will review the performance of the Contractor in the reviews defined in Table 1.

Replacement of Staff

The Contractor shall be responsible for replacement of its staff members in case of unavailability, thus ensuring uninterrupted and constant performance of all services as provided in this Tender.

2.1.2.1.2 WP.01.02: Reporting

Security Reports

The Contractor shall report on a weekly basis the logs of data concerning guarding, access control, video surveillance, anomalies including at least occurrences of the following:

a) GRC CCTV Monitoring Alarm: outside/inside, false/effective, time to detection,
b) Access Control System Alarm: outside/inside, false/effective, time to detection,
c) Intrusion Detection System Alarm: outside/inside, false/effective, time to detection,
d) Safety Incident Detection alarm: outside/inside, false/effective, time to detection,
e) Security & Safety Incident and Intervention: outside/inside, Intervention time,
f) Number of Visitors, vehicles and equipment (as detailed in the Security Operational Procedures, see Annex I.K),
g) Unavailability of guarding and monitoring systems,
h) Unusual events or observations on or around the GRC site.

These weekly logs shall be gathered into the Quarterly Report to be delivered to the Contracting Authority in the Quarterly review meeting.

KPIs for Guarding and Security Service

The Contractor shall continuously collect all the data required for the measurement of the key performance indicators (KPIs) and calculate and report their values to the Contracting Authority and to the DLSO on a monthly basis.

Security KPIs

The Contractor shall report following KPIs concerning guarding, access control, video surveillance, anomalies including at least occurrence of:

a) Timely Detection of Alarms, including:
    i) Monitoring Alarms,
    ii) Access Control System Alarms,
    iii) Intrusion Detection System Alarms,
    iv) Safety Incident Detection Alarms.
b) Timely Response to Security & Safety Incidents,
c) Availability of On-Site Guarding Service,
d) Availability of Remote Monitoring Service,
e) Timely provision of Security Logs,
f) Timely provision of Security Report and KPIs.

The calculation formulas and the target thresholds for the security KPIs and the calculation formulas for the related liquidated damages are provided in greater detail in Annex I.L

Weekly Delivery of Security Logs

The Contractor shall provide the Security Logs weekly to the contracting authority. In the event that the log contains a security incident, it shall be accompanied by a security report of the incident.

2.1.2.2 WP.02: Security Guarding, Intervention, and Monitoring

Security Organisation and Procedures

The Security organisation and related security procedures shall be put in place by the Contractor at the GRC site. The organisation and procedures shall be according to:

a) The local National Security Authority rules,

b) Commission decision 2015/444 on the security rules for protecting EU classified information,

c) The European GNSS Project Security Instruction – PSI (see Annex I.K);

d) GRC Security Operational Procedures (see Annex I.K),

e) GRC House Rules (Annex I.K).

Guards Force Supervisor (GFS)

The Guards shall be managed by a Guards Force Supervisor (GFS) of the contractor. GFS shall be the Point of contact for GRC DLSO and shall be responsible for coordination of all the security activities. The tasks of the GFS shall include:

- management of the equipment of the Contractor at different posts;
- controlling the duty performances of all Guards deployed at the GRC;
- ensuring the good functioning and the management of the entire Guard force by means of regular and traceable controls;
- planning of the duties of the Guards;
- ensuring proper and continuous coaching of the Guard force;
- inspecting all posts in unpredictable but routine manner;
- implementing the GRC security instructions and the follow up;
- ensuring training and coaching of the new Guards;
- Further details and description of other tasks will be provided in the GRC Security Operational Procedures (Annex I.K).

Guards Force Supervisor (GFS) Profile

The GFS shall have the following profile:

- Knowledge of English and Dutch, both at least equal to level B2;
- good computer skills relevant to the post;
- at least 5 years of proven general security experience;

- at least 2 years of proven experience in the management of security personnel;
- at least 2 years of proven experience in directing and training a guarding team.

Guards Profile

All Guards appointed to the GRC shall have at least the following profile:

- Knowledge of English and Dutch, both at least equal to level B2;
- Clean criminal record;
- good computer skills relevant to the post;
- at least 2 years of proven general security experience;
- at least 1 year of proven experience as a security guard.

The Guards and the Guards Force Supervisor may be required to handle classified information at CONFIDENTIEL UE/EU CONFIDENTIAL level or above. For such cases, they must comply with the relevant provisions of SAL, most notably having been granted a personal security clearance (PSC) within the meaning of Decision 2015/444 at the relevant level.

Guards Equipment

The Guards shall receive appropriate briefings and training, provided by the Contractor, prior to their employment at GRC premises. The contractor shall provide the guards with an individual uniform, which allows identifying them properly as guards at all times. Each guard shall carry on a visible place a badge of identification, displaying the name of the company, name of the individual, position and photograph of the individual. The contractor shall provide the guards with all necessary equipment to properly perform their functions.

Guards Training and Education

The Contractor shall ensure that all guards receive all training as required by national law related to private guarding. The training shall cover at least following areas:

a) first aid and Cardio-Pulmonary Resuscitation (CPR) training,
b) fire safety training (including fire drills, evacuation drills, fire prevention, fire awareness, use of fire extinguisher, etc.),
c) general security training,
d) training in the use of security systems,
e) General cyber security training.

The contractor shall prepare the internal Security Operation Procedures for guards, to be provided at the time of proposal and updated prior to the Contractor taking up responsibilities of guarding, and to be followed by guards during performance of their duties in GRC premises.

Personnel Requirements

The Contractor shall provide the GRC DLSO, at least five working days before the start of each month, with the planning of the personnel to be assigned for all the posts in the month to follow. Every change on the above-mentioned planning of personnel shall be notified sufficiently in advance and approved by the GRC DLSO.

Substitution of Guarding Personnel

A sufficient number of substitute guards shall be foreseen by the Contractor in order to cover leave or sickness or other absence.

Guarding Cover During Unexpected Unavailability

In case of unexpected unavailability, the Contractor shall be responsible for replacement of its staff in such a way that the uninterrupted and constant performance of all services is ensured.

Increased Guarding Presence

In case of emergency, increased threat level, etc. the Contractor shall provide upon request additional Guards and Security Centre Operators within five hours from the request.

Replacement of Personnel

GSA reserves the right to demand replacement of the GFS or Guards in case of underperformance, misbehaviour or due to the breach of internal security policies and procedures. The replacement must be done within five working days following the request in such a way that the uninterrupted and constant performance of all services is ensured.

Compliance with the GRC Internal Guidelines

All guarding procedures shall comply with Commission decision 2015/444 on the security rules for protecting EU classified information, the GRC Security Operational Procedures (see Annex I.K) and the instructions given by GRC DLSO.

Monitoring and Reporting of Security and Safety Events

All security and safety incidents shall be reported immediately to the Contracting Authority and the GRC DLSO.

Monitoring and Reporting of Security Intervention

In case of any security intervention, the Contractor shall report this to the Contracting Authority and to the GRC DLSO as soon as possible.

Logbooks

All Guards are requested to maintain logbooks (these can be in electronic format). The following logbooks (at least) shall be maintained:

a) general guards' logbook, containing:
    a. records of patrols,
    b. records of incident reporting,
    c. records of inspections,
    d. records of goods-in/goods-out,
    e. records of staff requests,
    f. other relevant information.
b) logbook for visitors and visitors' cars, containing the information detailed in the Security Operational Procedures (see Annex I.K).
c) logbook to record activation / deactivation of security monitoring equipment / alarm system as well as maintenance work on security equipment.

The logbooks shall be delivered to the Contracting authority together with the weekly security logs (section 2.1.2.1.2.).

Continuity of Service

The guards shall inform the Hosting Service Provider (HSP), using the ticketing tool provided (see Security Operational Procedures in Annex I.K), in case of unavailability or failure of utility services (electricity, water, internet connection, building alarms coming from the Building Management System (BMS), etc.). The guards shall also coordinate with HSP on suitable mitigation actions and inform GRC DLSO.

Security and Safety Incident Intervention

The Contractor shall be able to provide security incidents intervention on the basis of security and safety monitoring and on the basis of guarding.

Incident Detection Time

The Contractor shall take an appropriate action at the time of a security and/or safety incident within the timeframe of 5 minutes.

Intervention Time

In case of incident the maximum intervention time by the guarding service shall be 10 minutes from the time of a security and/or safety incident.

Security and Safety Action

The contractor shall take appropriate action to avoid:

a) any surreptitious or forced entry by an intruder or intrusion attempts to GRC premises,

b) GSA GRC personnel and premises as well as visitors and other personnel permanently employed on GRC premises from being endangered by malicious wilful damage resulting from any violent or other criminal activities,

c) personnel and premises being endangered by fire, explosives or harmful substances.

2.1.2.2.1 WP.02.01: On-Site Guarding

On-Site Guarding and Intervention Service

The Contractor shall provide on-site guarding and intervention services (during normal GRC opening hours) and shall ensure proper access control of GRC premises.

Opening of the GRC Premises

The On-Site Guards shall arrive first to the GRC premises, in time for the normal opening hours, and perform the GRC opening procedure as per the GRC Security Operational Procedures (Annex I.K).

Presence of On-Site Guards

The Contractor shall ensure that there is at least one guard on-site at all times during normal GRC opening hours.

Guarding and Intervention During Extended Opening Hours

If requested by the Contracting Authority, the Contractor shall ensure the presence of an on-site guard for the extended hours (outside the normal GRC opening times). The Contracting Authority may request this service in advance, giving a 24 hours or one week notice. The request may be made on the same day in case of exceptional circumstances.

GRC Site Points of Access

The On-Site Guards shall ensure that access to the site is made exclusively through authorised entrances of the GRC. The main entrance is equipped with electronic access control systems that require activation. The Guards must control the entry and exit of people and objects at all times.

GRC Site Access Control

The Contractor shall control and limit the entry to appropriately authorised personnel and authorised visitors, vehicles and equipment, including parking of vehicles on GRC premises and shall conduct relevant security and, when required, non-contact health checks.

Management of Access Requests

The Guards shall manage the site access requests made by the GRC staff and the associated access logs. All visitors should ideally be planned in advance and information, as per the GRC House rules (see Annex I.K), should be provided 24 hours prior to the arrival of the visitor.

Visitors Identity Check

The Guards shall be able to perform identity checks for visitors and maintain appropriate logbooks or databases and issue visitor badges. The contractor's personnel shall prevent visitors from carrying unauthorised items into or out of the GRC premises and conduct related security checks if necessary.

Visitors Registration and Identity Check

The Guards shall perform visitor registration and provide, where necessary, a visitor's badge to the site for any visitor where it has been indicated to do so.

Visitors Non-Contact Health Check

In times of requirement (e.g. global pandemic, local epidemic), the Guards shall perform a non-contact health check of visitors arriving to the GRC premises and act in line with instructions, as per the GRC Security Operational Procedures (Annex I.K), depending on the result of the check.

Notification to Staff of Visitors

The Guards shall notify relevant staff members of the arrival of a visitor; no visitor is allowed to enter without an escort.

Departure of Visitors

The Guards shall collect the access badge and note the time of departure in the relevant logbook whenever a visitor departs the site at the end of their visit.

Office, Storage and Engineering Areas Access Control

The Contractor shall operate the Access Control System and control the access to offices, storage and operation areas and secured areas that are physically separated from the public area. Access to non-public areas shall be limited to authorised GRC personnel.

Handling of Incoming and Outgoing Goods

The On-Site Guards shall handle incoming and outgoing goods as per the GRC Security Operational Procedures, see Annex I.K.

Patrolling

The Guards shall perform interior and exterior patrols on both regular and irregular intervals.

Tagging During Patrols

During the on-site guard's regular patrols, the electronic tagging system available in the GRC shall be used. Patrols shall pass electronic check points in order to verify that proper performance of patrols is conducted.

Inspection of Operational Cabling

The contractor shall inspect the cables in the operational area as a part of guarding services.

Supervision of Visitors

The Guards shall, where necessary, supervise the works being carried out by maintenance or cleaning contractors.

Alarm System Management

The Guards must manage a set of keys and codes for the GRC alarm system.

Closedown of GRC Premises

The On-Site Guards shall be the last to leave the GRC premises at the end of the working day and shall perform the GRC Closedown procedure as per the GRC Security Operational Procedures, see Annex I.K.

Maintenance of Post

The On-Site Guards shall perform routine maintenance of their post to keep it in perfect condition.

Participation to Drills

The On-Site Guards shall lead, when requested, or participate to evacuation drills while on-duty at the GRC premises.

2.1.2.2.2 WP.02.02: Security and Safety Monitoring

Remote Guarding and Intervention Service

The Contractor shall provide remote guarding and intervention services.

Security and Safety Monitoring of Premises

The Contractor shall provide permanent monitoring of Closed-Circuit Television (CCTV) alarms, Access Control System (ACS), Intrusion Detection System (IDS), Safety Incident Detection (fire, heating, cooling, etc.), on a 24/7/365 basis.

Monitoring System

The Contractor shall be able to manage the security and safety monitoring system and to detect alarms within 5 minutes and react to any intrusion or other security incident within 10 minutes.

Internal Monitoring Service

The GRC premises, with the exception of the Secured Areas – as defined in the Building Information (Annex I.K2), shall be monitored at all times by the security monitoring system.

Outside Monitoring Service

The GRC external security perimeter shall be monitored by the Contractor at all times by the security monitoring system.

Intrusion Detection System

The Contractor's personnel shall be able to operate the security monitoring system (intrusion tools) in order to have an appropriate response to security/safety incidents.

Protection of Operational Elements

All GRC operational elements (Work positions, equipment, etc.) are located in dedicated rooms within the operational area. The Contractor shall permanently monitor via access control system and limit access only to authorised personnel related to GRC operations.

Secured Area Intrusion Protection

All Secured areas of the GRC, where electronic equipment is installed for processing data that is classified at RESTREINT UE / EU RESTRICTED level or higher, shall be protected against physical intrusion in accordance with the National laws and European regulations applicable to the Hosting Site.

2.1.2.3 WP.03: Contract Handover and Handback

2.1.2.3.1 WP.03.01: Contract Handover

Request for Handover

On request from the Contracting Authority, the Contractor shall be ready to perform a service handover of the GRC Guarding, Security, and Safety Monitoring Services from the current economic operator.

Handover Point of Contact

The Contractor shall nominate a Handover Manager who will act as a single point of Contact for the Contracting Authority and the outgoing economic operator for all issues related to the handover phase.

Handover Planning

The Contractor shall provide inputs during the preparation of the Handback plan of the outgoing contractor to ensure that activities can be coordinated successfully.

Handover Execution

During the Handover Phase, the Contractor shall follow the Handback plan, prepared by the current incumbent, to carry out all the activities necessary to ensure the seamless, safe, and secure transition of all activities from the outgoing incumbent to the Contractor.

Security During Handover

During the Handover Phase, the Contractor shall ensure that all handover activities are conducted in a secure manner in accordance with the security requirements.

Impact on Operations During Handover

During the Handover Phase, the Contractor shall ensure that all handover activities are conducted in a manner that has no negative impact on the on-going operations of the GRC.

Handover Manager Activities

The Contractor shall ensure that the Handover Manager undertakes appropriate coordination activities between all the relevant parties involved in the handover, including the outgoing economic operator, the Contracting Authority, and (where necessary) the GRC Hosting Services Manager.

Handling of EUCI During Handover

The Contractor Handover Manager shall be responsible for the handling and management of EUCI between the Contractor, the Contracting Authority, the outgoing economic operator.

Handover Shadowing

The Contractor shall ensure that each team member of the incoming GRC Guarding team is provided sufficient time to shadow their outgoing counterpart to ensure full familiarity with the regular guarding activities.

Handover Lessons Learned

The Contractor shall prepare a report on the Handover phase and describe all lessons learned. These lessons learned shall act as inputs to the Contractor's Handback planning (see 2.1.2.3.2)

2.1.2.3.2 WP.03.02: Contract Handback

Handback Plan

The Contractor shall implement and maintain a Handback Plan that contains an integrated view of the planning of all the Contractor's activities to be carried out during the Handback Phase at the end of the framework contract. This Plan shall contain details on the steps and actions to be undertaken by the Contractor to ensure a successful transition to the incoming economic operator, including ensuring the availability of all information needed by the incoming economic operator for the continuation of the GRC Guarding, Security, and Safety Monitoring Services and associated tasks. The handback activities from the outgoing Contractor to the incoming economic operator shall be planned so as to minimise the impact on the on-going operations of the GRC.

Security During Handback

During the Handback Phase, the Contractor shall ensure that all handback activities are planned so as to be conducted in a secure manner in accordance with the security requirements.

Handback Point of Contact

The Contractor shall identify a Handback Manager who will act as a single point of contact for the Contracting Authority and the incoming economic operator for all issues related to the implementation of the Handback Plan.

Handback Execution

Upon request from the Contracting Authority, the Contractor shall implement the Handback activities in accordance with the approved Handback Plan.

Handback Manager Activities

The Contractor shall ensure that the Handback Manager undertakes appropriate coordination activities between all the relevant parties involved in the handback, including the incoming economic operator, the Contracting Authority, and (where necessary) the GRC Hosting Services Manager.

Handling of EUCI During Handback

The Contractor Handback Manager shall be responsible for the handling and management of EUCI between the Contractor, the Contracting Authority, and the incoming economic operator.

Shadowing During Handback

During the Handback phase, the Contractor shall provide all the necessary support and assistance to ensure a safe, smooth and secure transition of services. This shall include a sufficient period of time for the incoming Contractor to shadow the daily activities.

Handback Lessons Learned

The Contractor shall produce the Handback Lessons Learned Report, to be delivered for the end of contract review, describing in detail:

a) The process followed to achieve the Handback (including all applicable documents);

b) The experiences of the Handback;

c) Suggestions for improving the process in the future.

2.2 Legal and contractual terms of reference

2.2.1 Participation conditions

I. In accordance with Article 18 of the GNSS Regulation, for reasons related to the protection of the essential interest of the security of the European Union or to public security, including the security of the EU Member States, the participation to this tender (including through subcontracting where such subcontracting presents a security aspect) limits the procurement to economic operators established in European Union Members States. This applies at the moment of submission of the tender and for the whole duration of the contract.

Economic operators are considered established in the EU when all of the following conditions are met:

a) they are formed in accordance with the law of an EU Member State, and have their central administration, registered office and principal place of business in an EU Member State (if legal persons) or they are nationals of one of the EU Member States (if natural persons); and

b) their decision-making centres (defined by reference to the criteria set out in Article 22(1) of Directive 2013/34/EU, also including the ultimate controlling entity) comply with the conditions under I.a) above; and

c) The facilities (for goods manufacturing and/or supplying of services) which the candidate would use for the execution of the Contract are located in the EU.

II. In exceptional circumstances related to the nature, cost or availability of specific goods and/or services, the contracting authority may, on the basis of motivated and justified waiver requests submitted in writing by economic operators, authorise participation of:

a. A prime contractor which does not meet the conditions under I b. and/or I.c above;

b. A subcontractor (presenting security aspects as defined in the List of Security Sensitive Procurements) which fails to fulfil one or more of the conditions under I above;

provided that they demonstrate the implementation of sufficient measures in order to guarantee the protection of the essential interest of the security of the European Union or public security, including the security of the EU Member States.

2.2.2 Ceiling volume of the contract

The indicative ceiling estimated for the maximum duration of the FWC is 900,000.00 EUR, including renewals of the initial duration of the FWCs **up to** four (4) years. This budget is only indicative; it will be subject to budget allocations given to the GSA.

The GSA reserves the right to launch an exceptional negotiated procedure for new services with the same contractor in case of need, as foreseen in Article 164(5)(f) in connection with point 11.1(e) of Annex I of FR. The maximum additional value of new services would be 50% of the initial value of the contract.

2.2.3 Place of performance

The services under WP.01 and WP.02.02 shall be provided at the contractor's premises or another location, as agreed with the contracting authority.

The services under WP.02.01 are to be provided on-site at the Galileo Reference Centre (GRC) in Noordwijk, the Netherlands.

The services under WP.03 shall be provided at the contractor's premises or another location, as agreed with the contracting authority, except for the handover and handback execution, which shall be provided on-site at the Galileo Reference Centre (GRC) in Noordwijk, the Netherlands.

2.2.4 Duration

The expected duration of the Framework Service Contract is 1 year from the signature of the Contract, with the possibility of renewal of up to 3 times for 1 year (4 years maximum).

2.2.5 Language of the contract

English shall be the working language of the Contract including all correspondence with the GSA. Therefore, all proposed personnel should have an excellent level of English equivalent, at least B2, proven by a certificate issued by an officially recognized institution.

2.2.6 Compliance with internal rules, professional conflicting interest, security requirements and confidentiality

2.2.6.1 Compliance with GSA internal rules

The contractor shall ensure that its personnel follow any internal rules laid down by the Agency for anyone entering into or staying in the premises of GSA. Such rules include in particular security rules and rules related to health and safety. These rules may evolve in future. Any such rules will be provided to the contractor.

2.2.6.2 Professional Conflicting interest

The contractor shall ensure that its personnel sign a "declaration on confidentiality and absence of professional conflicting interest" with the GSA before commencing any service provision. The current form of such declaration is attached for information to the draft Contract. The form may evolve and cover additional aspects from time to time. This shall not in any way relieve the contractor from any of its obligations. The GSA reserves the right to ask the contractor or its personnel performing the services to sign a declaration regarding confidentiality, non-disclosure and/or declaration regarding precise obligations of processing of personal data.

At the time of submission of the tender and during the term of the FWC, the contractor shall not be in any situation that could compromise the impartial and objective performance of the FWC and the specific contracts. For this purpose, tenderers shall at the time of the tender:

i. either confirm their absence of professional conflicting interest, or
ii. substantiate the potential, perceived or actual professional conflicting interest which may negatively affect the performance of the Contract.

For either (i) or (ii) point above, the Tenderers must provide a comprehensive analysis and justification, with at least the following information:

a) previous and/or current involvement in the Galileo/EGNOS programmes in activities which may have as a result that impartial and objective performance of the present FWC may be compromised;

b) respect of rules on conflict of interest regulating the legal profession, including the professional ethics rules applicable to the tenderer;

c) description of operational structure and mechanisms for monitoring, preventing and resolving conflicting interests during the execution of the FWC which mitigate or eliminate the potential, perceived or actual professional conflicting interests. Under this requirement, the tenderer shall provide an effective and convincing concept to ensure that the respective entity/-ies, including the individuals belonging to it/them, are in a position to work independently in relation to its/their tasks performed in other GNSS projects.

2.2.6.3 Security Requirements

The contractor must be compliant with the security requirements detailed in the Security Aspect Letter (Annex I.H). The tenderer must confirm its compliance to the SAL with the offer. The SAL will be fully signed at the award of the Contract with the successful tenderer and shall comprise Annex VI of the draft Framework Contract.

Last, the tenderer must appoint their Local Security Officer (the "LSO", different from the GSA D/LSO) to be maintained throughout the duration of the FWC. In case of award of the FWC and before start of any service provision under a specific contract, the contractor may be required to declare in writing to the GSA Local Security Officer that its personnel providing the services is

suitable for the performance of his/her duties, free from criminal convictions and enjoy full rights as citizen of EU.

2.2.6.4 Confidentiality Requirements

The tenderer shall pay particular attention to the clauses on confidentiality of the draft FWC. The assignment is to be considered as a highly sensitive issue, considering that the Contractor will not only have direct access and knowledge of the GSA's internal organisation, including personal details of members of staff and external visitors, but will also have to deal with sensitive information.

The Contractor undertakes to treat in the strictest confidence and not make use of or divulge to third parties any information or documents which are linked to performance of the Contract. The Contractor shall continue to be bound by this undertaking after completion of the tasks.

The Contractor shall obtain from each member of its Staff employed at GRC a written statement that they will respect the confidentiality of any information which is linked, directly or indirectly, to execution of the tasks and that they will not divulge to third parties or use for their own benefit or that of any third party any document or information not available publicly, even after completion of the tasks. The signed declaration of confidentiality of each member of staff shall be provided to GSA at the start of employment of the staff member at GRC.

The GSA reserves further rights to ask the Contractor or its Staff performing the services to sign a declaration regarding confidentiality, non-disclosure and/or declaration regarding precise obligations of processing of personal data.

2.2.7 Subcontracting

2.2.7.1 General principles

The contractor may call on subcontractors also to provide specific know-how for the Contract.

However, the contractor will remain the sole entity legally and financially responsible vis-à-vis the GSA. The tenderer must indicate clearly which parts of the work will be sub-contracted and to what extent (proportion in % of turnover and resources). The sub-contractor must not sub-contract further.

Sub-contractors must satisfy the eligibility criteria (i.e. participation conditions, selection criteria, exclusion criteria, minimum requirements) applicable to the award of the contract. The GSA reserves the right to require supporting documents that the subcontractor in question satisfy the exclusion and selection criteria set out in sections 3.1. and 3.2.

If the identity of the intended sub-contractor(s) is already known at the time of submitting the tender, the tenderer must identify the subcontractor in the tender. If the identity of the sub-contractor(s) is not known at the time of submitting the tender, the tenderer who is awarded the contract will have to seek GSA's prior written authorisation before entering into a sub-contract. Where no sub-contracting is indicated in the tender the work will be assumed to be carried out directly by the tenderer.

The Contractor shall not change any sub-contractor without prior authorisation by GSA.

2.2.7.2 Mandatory subcontracting

Tenderers shall clearly indicate in their tenders which part of the services they intend to subcontract as well as their approach for implementing such subcontracting at each specific contract level to demonstrate compliance with the below mentioned requirements.

In accordance with Article 26(1) of the GNSS Regulation the contractor must subcontract an indicative minimum share of 5%. These subcontractors shall be selected outside the tenderer's group[6] (including consortium members).

Competitive tendering outside the tenderer's group is considered to have taken place when more than one offer from an entity outside the tenderer's group has been requested by the tenderer. Each tenderer is responsible for organising its own competitive tender(s) aimed at finding necessary subcontractors respecting the following procurement principles:

- Fair competition & equality of treatment
- Transparency
- Proportionality
- Best value for money

Given the fact that the GSA cannot assume and/or guarantee that the full budget available under the FWC will be consumed, the percentage of subcontracting will be calculated as the percentage from the actually requested services under the FWC and not as a percentage from the maximum nominal volume of the FWC. In order to ensure that the proposed percentage of subcontracting will be achieved, such subcontracting shall be done at the level of each individual specific contract concluded under the respective FWC.

A proof of competitive subcontracting tender(s), including thorough visibility of technical and financial offer of subcontracted entities outside the tenderer's group (envisaged subcontractors) shall be provided together with the tender. If the tenderer does not manage to complete the competitive tender(s) required by the time of tender submission, it shall submit a signed undertaking presenting credible tendering plan it intends to carry out.

If the competitive tenders are completed only during FWC execution, the concluded subcontracts shall not lead to a change of the FWC unless it is in favour of the GSA.

[6] For the purpose of this requirement the expression "group" is meant to encompass i) the entity or the group of entities acting as a tenderer, ii) the entity /entities to which the tenderer or any of the members of the group acting as tenderer is affiliated, iii) the entities affiliated to the tenderer or to any of the members of the group acting as tenderer. An entity shall be deemed affiliated to the tenderer or any of the members of the group acting as tenderer if their links fall within the scope of article 22 of Directive 2013/34/EU, of 26 June 2013.

In case of failure to respect the undertaking of subcontracting or obtaining the said authorisation, the FWC may be terminated for contractor's default with a notice of 3 months after the contractor was given a possibility to remedy the situation.

In case where no competitive tendering is planned to be undertaken, tenderer shall submit a justification providing compelling reasoning for the non-compliance with the above mentioned requirement. Failure to provide such justification may lead to the rejection of the tender.

Tenderers may at any time after tender submission or during the FWC execution be requested to submit supporting evidences of their application of competitive tender for the selection of subcontractors and their compliance with the principles established above. Contractors can be subject to possible auditing according to contractual provisions. Without prejudice to the latter, the GSA may reject the proposed subcontractor(s) and ask for another subcontractor(s) to be proposed as part of the tender. Such rejection shall be justified in writing by the GSA and may be based only on the criteria used for selection of tenderers for the FWC.

2.2.8 Participation of consortia

Consortia may submit a tender on the condition that they comply with the rules of competition. A consortium may be a permanent, legally-established grouping or a grouping which has been constituted informally for a specific tender procedure.

Such consortium must specify the company or person heading the project (the leader). All members of the consortium must sign a power of attorney authorizing this company or person to submit a tender on behalf of the consortium and to represent the consortium for any contract execution issue, including amendments of FWC.

All members of a consortium (i.e. the leader and all other members) are jointly and severally liable to the GSA for performance of FWC.

Each member of the consortium must provide the required evidence for the exclusion and selection criteria (see **section** 3 below). Concerning the selection criteria "economic and financial capacity" as well as "technical and professional capacity", the evidence provided by each member of the consortium will be assessed to ensure that the consortium as a whole fulfils the criteria.

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

3 Assessment of tenders

All admissible Tenders will be assessed. See the admissibility criteria described in Section 3 below. The Tenders will be evaluated in the light of the criteria set out in these Tender specifications.

The evaluation is based solely on the information provided in the submitted tender. It involves the following:

1. Verification of **non-exclusion** of tenderers on the basis of the exclusion criteria;
2. Selection of tenderers on the basis of **selection criteria**;
3. Verification of compliance with the **minimum requirements**;

4. Evaluation of tenders on the basis of the **award criteria**.

The GSA reserves the right to perform the evaluation in a different order.

The Contract will be concluded following the result of the evaluation of admissible tenders.

In order to demonstrate compliance with exclusion criteria, selection criteria and minimum requirements, the tenderers must sign the declaration of honour duly completed, signed and dated (Annex I.B. to this document), and submit any supporting documents as requested in the tables under section 3.2 below. In case of consortia or subcontracting, each member of the consortium and/or each subcontractor must provide a declaration of honour and submit documentary evidence as requested in the tables under section 3.2 below.

3.1 Exclusion criteria

The tenderer shall not be in any exclusion situation described in the declaration of honour included in Annex I.B.

Supporting evidence requested as part of the declaration of honour shall be submitted only by the successful tenderer upon notification of award by the GSA. The tenderers should however start preparing the evidence in original version as soon as possible given the time necessary to gather them. The GSA reserves the right to request the supporting evidence during the tendering procedure.

3.2 Selection criteria

Tenderers must have the capacity below to perform the tasks.

In accordance with point 18.6 of Annex I FR, the candidate may, where appropriate, rely on the capacities of other entities. In such case, the candidate must prove that it has at its disposal the resources necessary for the performance of the contract by producing a commitment by those entities to that effect. The candidate must comply with all the conditions laid down in point 18.6 of Annex I FR.

The tenderer who intends to rely on the capacities of other entities of subcontractors, must indicate the proportion that it intends to subcontract.

The supporting evidences, which must be provided in the tender, are indicated in the column “to be evidenced by” in the tables below.

3.2.1 Legal and regulatory capacity

Ref. #	Legal and regulatory capacity criteria	To be evidenced by:	Applicable to:
L1.	**General requirement** Tenderers (including all	A duly filled in and signed **Legal Entity Form**[7] alongside	Tenderers (including all

[7] For download: https://ec.europa.eu/info/publications/legal-entities_en

	consortium members and any proposed sub-contractors) must prove that they are authorised to perform the contract under the national law.	a copy of the **trade or professional register excerpt** of the entity and the supporting documents required in the form, i.e. copy of the **value added tax (VAT) registration document**.	consortium members and any proposed sub-contractors).
L2.	**Place of establishment** Participation conditions requirement Entity must be established in an EU Member State, i.e. meeting the conditions listed under section 2.2.1(I) a) to c) to be maintained throughout the tender and the implementation of the FWC, in case awarded.	1. Submission of a proof provided for under criterion L1; 2. Filled in dedicated section in the declaration on honour (Annex I.B); **NOTE**: In case of request of a waiver as per section 2.2.1(II), all necessary evidence to demonstrate: - The exceptional circumstances justifying the request for a waiver as described under section 2.2.1; and, - the implementation of sufficient measures to guarantee the protection of the essential interest of the security of the European Union or public security, including the security of the EU Member States.	All economic operators, whereas with respect to subcontractors, the requirement applies only to those whose activities present security aspects.
L3.	**Appointed Local Security Officer** Tenderers handling classified information above CONFIDENTIEL UE/EU CONFIDENTIAL under the FWC must have appointed – **at the time of submission of their**	Submission of a **proof of appointment** of the tenderer's respective LSO. There is no specific format or template for proof of appointment of the LSO. A signed declaration of the duly authorised	Tenderers (including all consortium members and any proposed sub-contractors).

	offer – a Local Security Officer ("**LSO**"), to be maintained throughout the duration of the FWC.	representative of the concerned entity will be sufficient.	
L4.	**Full compliance with the security requirements detailed in the Security Aspect Letter (Annex I.H of the Tender Specifications)**	A filled out and signed Statement of compliance, as provided in the template Annex I.I.	Tenderers (including all consortium members and any proposed sub-contractors that may handle EU Classified Information).

3.2.2 Economic and financial capacity

The tenderer (all legal entities belonging to a consortium) shall demonstrate the financial and economic capacity required for performance of the Contract as follows:

Ref #	Economic and financial capacity criteria	To be evidenced by:	Applicable to:
F1	A stable financial capacity to sustain its business. .	Duly filled in **Financial Statements relating to the Selection Stage** in **Annex I.E.** Submitting a full copy of the **tenderer's annual accounts** (balance sheet, profit and loss account, notes on the accounts and auditors' remarks when applicable) of the last three years approved by external auditors. If, for some exceptional reason which the GSA considers justified, the tenderer is unable to provide the requested documents, the tenderer may prove its capacity by other documents which the GSA considers appropriate. In any case, GSA must, as a minimum, be notified of any exceptional reason and its justification in the tender. The GSA reserves the right to request any other document	Tenderer (all members of consortium cumulatively).

		enabling it to verify the tenderer's economic and financial capacity	
F2.	The tenderer must have a minimum yearly turnover (in EUR) of: 20% of the value of the contract indicated in section 2.2.2 in the last three years preceding the year of launch of the present tender procedure.	Duly filled in Financial Statements relating to the Selection Stage in Annex I.E Submission of a copy of the **tenderer's annual accounts** (profit and loss account, notes on the accounts and auditors' remarks when applicable) of the last three years approved by external auditors.	Tenderer (all members of consortium cumulatively). The tenderer may also include the financial capacity of subcontractors in order to reach the required capacity level.

3.2.3 Technical and professional capacity

The tenderer (all legal entities belonging to a consortium) shall demonstrate the technical and professional capacity required for performance of the Contract as follows:

Ref #	Technical and professional capacity criteria	To be evidenced by:	Applicable to:
T1.	Minimum 3 years of relevant experience with provision of guarding services in high risk environments for public authorities (e.g. embassies, international organisations, military sites, governmental sites, critical national infrastructure).	At least 3 relevant references, each including: - The name and nature of the entity to which the service has been provided, - Associated budget, - Duration and current status of the service, - Number of personnel involved, - An short description of the service (including a description of the tasks and the degree of complexity), - Contact details of the contracting party.	Tenderer (all members of consortium and proposed subcontractors cumulatively)

3.3 Minimum requirements

Tenderers must submit the information below with the tender. Failure to comply with minimum requirements at the submission time of the tender will lead to exclusion of the tenderer from the tender procedure.

The tenderer shall demonstrate compliance with the minimum requirements required for performance of the Contract as follows:

No	Minimum requirements	To be evidenced by	Applicable to
M1.	Compliance with applicable environmental, social and labour law obligations established by European Union law, national legislation, collective agreements or the applicable international social and environmental conventions listed in Directive 2014/24/EU.	Corresponding statements of compliance in the declaration of honour – **Annex I.B**.	Tenderer (all members of consortium and proposed subcontractors cumulatively)
M2.	The tenderer must be able to communicate with the GSA in English (GSA internal working language). The command of English is verified by the fact that the tenderer understands the tender specifications drafted in English.	Corresponding statements of compliance in the declaration of honour – **Annexes I.**A**B**. The GSA reserves the right to request supporting evidence during the tendering procedure or upon notification of award by the GSA.	Tenderer (all members of consortium and proposed subcontractors)
M4.	The selected Contractor shall confirm in writing that the Contractor works in full compliance with all relevant European and national legislation and specifically the European and national legislation related to the organisation and performance of guarding services.	Corresponding statements of compliance in the declaration of honour – **Annexes I.**A**B**. The GSA reserves the right to request supporting evidence during the tendering procedure or upon notification of award by the GSA.	Tenderer (all members of consortium and proposed subcontractors)

3.4 Award stage

For the tender to be evaluated in award stage, the tenderer must have passed the exclusion and selection stages and fulfil the minimum requirements.

The assessment of the tenders in the award stage is carried out against the qualitative and the financial award criteria set out below.

3.4.1 Qualitative award criteria

The technical quality of the Tender will be assessed on the basis of the tenderer's technical proposal. Technical offers will be evaluated on the basis of the following award criteria.
The maximum quality score is 100 points. Tenders who do not obtain at least 50% of the maximum score for each qualitative award criterion and at least 60% of the overall score for all the qualitative award criteria will not be admitted to the next stage of the evaluation procedure.

#	Qualitative Award criteria	Points Maximum: 100 Minimum: 60
Q.1	**Methodology of the planned work organisation, management and allocation of resources** - Quality of the project management organisation ensuring the management and control of the contract activities, organisation of the management team, reporting, review of performance and identifying lessons learned, as well as internal reporting and reporting to the GSA (WP.01) **(15 points)** - Quality of the proposed security operation procedures, including organisation of the work, code of conduct, approach to monitoring and guaranteeing of the daily contract implementation at the required quality standards, and continuity and contingency planning (WP.02) **(20 points)** - Quality of the proposed takeover and handover organisation (WP.03) **(5 points)**	**Max. 40** ***Min. 20***
Q.2	**Quality of proposed personnel and their appropriateness to perform the services** - Overall quality of profiles proposed and their appropriateness to perform the On-site guarding services described under WP.02.01. **(10 points)** - Overall quality of profiles proposed and their appropriateness to perform the Security and Safety Monitoring services described under WP.02.02 **(10 points)**	**Max. 30** ***Min. 15***

	- Overall quality of profiles proposed at management level and their appropriateness to perform the Management of the service and Contract Handover and Handback services described under WP.01 and WP.03 **(10 points)**	
Q.3	**Quality of the company staff management policies** - Selection and recruitment procedure **(4 points)** - Management of Conflict of interest: prevention, identification, handling **(5 points)** - Training program **(4 points)** - System for control of quality **(5 points)** - Companies health and safety policy **(2 points)**	**Max. 20** ***Min. 10***
Q.4	**Quality of staff policy related to turnover of staff** - Measures taken to limit turnover (fluctuation), including the reward structure and staff motivation program **(5 points)**, - Replacement schemes **(5 points)**	**Max. 10** ***Min. 5***

3.4.2 Financial award criteria

3.4.2.1 General

Following the assessment of the qualitative award criteria, the tenders will be evaluated with regard to their financial proposals which shall be submitted in the form provided in Annex I.F.

In order to allow for a comparison of the offers, tenderers are requested to submit their Financial Proposal following the financial table of answers Annex I.F which shall be duly filled in, stamped, initialled, dated and signed by the tenderer, without any omission or addition with regard to the original format. Omissions or additions with regard to the original format may lead to exclusion from the tender procedure.

Prices presented shall be firm and fixed and binding for the tenderer/contractor throughout the duration of the Contract.

In order to assess the financial proposal the Contracting Authority has presented a synthetic evaluation exercise. This is shown in the Financial Template in Annex I.F. This price shall be the one evaluated as per the conditions stated herein.

3.4.2.2 Calculation of financial score of the tender

The financial score will be calculated as follows: the tender offering the least expensive Total Price of the Tender in Annex I.F will receive 100 points. The other tenders will receive points according to the ratio between the least expensive Total Evaluation Price and their one, and then multiplied by 100, as shown in the formula below:

$$\text{Financial Evaluation Score of Tender X} = \left(\frac{\text{cheapest total price received}}{\text{total price of tender X}}\right) \times 100$$

3.4.3 Calculation of final score and ranking of tenders

The Contract will be awarded to the tenderer having passed the selection stage and offering the best value for money, i.e. the highest score in the final evaluation.

The final score of each tender is established by weighting technical quality against price on a **60/40** basis and will be calculated using the following formula:

SCORE FOR TENDER= 60% of Qualitative Evaluation score + 40% of Financial Evaluation score

A ranking list of all tenderers will be established based on the 'score for tender' formula above. The contract will be awarded to the tenderer which will be ranked the highest (the best price-quality ratio).

4 Conditions of submission of tenders

4.1 Disclaimers

Please note disclaimers referred to in the invitation to tender.

4.2 Visits to premises or briefing

Visits to GSA's premises or briefings during the tendering process are not foreseen but they can be organised upon request.

4.3 Variants

Variants are not permitted under this procurement procedure.

4.4 Preparation costs of tenders

Costs incurred in preparing and submitting tenders are borne by the tenderers and will not be reimbursed.

4.5 Presentation of the tender

4.5.1 Language

Tenders shall be drafted in one of the official languages of the European Union, preferably **ENGLISH**.

4.5.2 Outer envelopes

Each Tender must be presented in one (1) outer envelope or parcel, which should be sealed with adhesive tape, signed across the seal.
Each outer envelope shall carry the following information:

- the reference number of the Invitation to Tender GSA/OP/25/20, the project title **"GRC Guarding, Security and Safety Monitoring Services"**
- **the name of the tenderer**
- the indication ***"Tender - Not to be opened by the internal mail service"***
- **the address for submission of tenders** *(as indicated in **section 4.7**)*
- **the date of posting** *(if applicable)* should be legible on the outer envelope.

4.5.3 Inner envelopes

Each outer envelope shall contain **three (3) inner envelopes**, namely, **Envelope 1, 2 and 3 stating the content of each**:

- Envelope 1: "ADMINISTRATIVE DOCUMENTS and DOCUMENTS RELATING TO EXCLUSION and FINANCIAL AND ECONOMIC SELECTION CRITERIA", with the name and stamp of the tenderer and the reference number of the Invitation to Tender "GSA/OP/25/20";
- Envelope 2: "TECHNICAL OFFER", with the name and stamp of the tenderer and the reference number of the Invitation to Tender "GSA/OP/25/20";
- Envelope 3: "FINANCIAL OFFER", with the name and stamp of the tenderer and the reference number of the Invitation to Tender "GSA/OP/25/20".

Each inner envelope shall contain **one (1) ORIGINAL and one (1) COPY in electronic format.** The original tender shall be marked **"ORIGINAL"**.

It is required that tenders be presented in the correct format and include all documents necessary to enable the evaluation committee to assess them. Failure to respect these requirements will constitute a formal error and may result in the rejection of the tender.

The GSA retains ownership of all tenders received under this procedure. Consequently tenderers shall have no right to have their tenders returned to them.

4.6 Content of the tender to be submitted

The tender must be:

- signed by the tenderer or his duly authorised representative;
- perfectly legible so that there can be no doubt as to words and figures;
- drawn up using all model reply forms supplied in the annexes to the Tender Specifications;
- clear and concise, with continuous page numbering, and assembled in a coherent fashion (e.g. bound or stapled or organised in files).

The GSA reserves the right to request additional evidence in relation to the tender submitted for evaluation or verification purposes.

4.6.1 Administrative file (ENVELOPE 1)

Each tender shall include an administrative file, containing:

Ref. #	ENVELOPE 1 – ADMINISTRATIVE DOCUMENTS and DOCUMENTS RELATING TO EXCLUSION and LEGAL AND FINANCIAL/ECONOMIC SELECTION CRITERIA (one (1) ORIGINAL, one (1) ELECTRONIC COPY per envelope)
(1)	A **cover letter**, dated and signed by duly authorized representative of the tender, including: • A declaration of full acceptance of the requirements in this Invitation to Tender; • The tenderer's undertaking to provide the services; • A list of all the documentation included/enclosed in the tender; • A list of the legal entities involved, specifying each entity's role and qualifications; • Tenderer's contact details.
(2)	The duly filled in, signed and dated **identification sheet of the tenderer** using the template in **Annexes I.A**. (**one per tenderer** including all the legal entities involved in the consortium and subcontractors and containing, where appropriate, as many sections as legal entities involved).
(3)	The duly filled in, signed and dated **legal entity form** (**one per economic operator involved** (tender, consortium member or subcontractor) using the template available at: http://ec.europa.eu/budget/contracts_grants/info_contracts/legal_entities/legal-entities_en.cfm and any supporting documents required in this template. Please take into consideration the instructions from this link before filling in the documents: http://ec.europa.eu/budget/library/contracts_grants/info_contracts/instructions_fich_le_en.pdf.
(4)	A duly signed and dated **statement of authorization/power of attorney** containing the name and position of the **representative/signatory** and **official documentary evidence** on the person's legal authority to validly sign the tender and the FWC on behalf of the organization, should it be awarded it.
(5)	The duly filled in, signed and dated **Financial Identification Form** using the template available at: http://ec.europa.eu/budget/contracts_grants/info_contracts/financial_id/financial_id_en.cfm In case of consortia, only one financial identification form for the whole consortium should be submitted, nominating the bank account into which payments are to be made under the SCs (i.e. the account of the consortium leader) in the event that the respective tender is awarded to it. Please pay attention to the supporting documents that should be submitted together with dully filled in financial identification form.
(6)	The duly filled in, signed and dated **Declaration(s) of Honour** relating to **exclusion criteria and selection criteria** using the template in **Annex I.B - one per economic operator** (i.e. tenderer, all consortium members, all subcontractor(s), if any).

(7)	The duly filled in, signed and dated **Financial Statement** relating to the selection stage using the template in **Annex I.E,** complemented by the **full financial statements** for the last three financial years and a **statement of turnover** relating to the relevant services for this tender for the last three financial years as requested in section 3.2.2 of these tender specifications.
(8)	All evidence relating to the selection criteria in section 3.2.
(9)	All evidence relating to : • the minimum requirements in section 3.3.
(10)	In case of consortia, a duly signed and dated **statement/declaration by each of the consortium members specifying the company or person heading the project** and authorised to submit an tender on behalf of the consortium, sign and manage the Contracts, using the template in **Annex I.C**.
(11)	For the proposed subcontractors, duly filled in, signed and dated **subcontractor Letter of Intent** using the template in **Annex I.D**Error! Reference source not found..
(12)	**An electronic copy of each document submitted** in the administrative envelope on CD-ROM or USB stick with the full set of documents in **machine readable format** (MS Office 2003 or later, or Adobe Reader Version 8.0 or later), strictly identical in full to the original tender

4.6.2 Technical proposal (ENVELOPE 2)

Each tender shall include an administrative file, containing:

	ENVELOPE 2 – TECHNICAL OFFER (one (1) ORIGINAL, one (1) ELECTRONIC COPY)
(1)	**Technical Proposal**, in accordance with the requirements of the present Tender Specifications divided into following sections with headings: • Executive Summary (2 pages maximum) • Duly written, signed and dated Statement of Compliance (Annex I.I) in this document and its technical annexes. The tenderer must fill-in Annex I.J and (i) confirm its full compliance and (ii) define its partial or non-compliance to the requirements and tasks described in this document and its technical annexes. Any non-compliance or partial compliance must be explained and the level of compliance committee to be reached shall be indicated. • All evidence relating to the selection criteria in section 3.2 above. • One section per each award criterion, subdivided into subsections per sub-criteria. Each of these sections and subsections shall include the complete approach related to the respective award criteria and sub-criteria. The GSA reserves the right to evaluate the award criterion and sub-criteria only in respect of information provided in the such sections and subsections and not to take into account information provided in other parts of the tender, unless clear references are made to them.
(3)	**An electronic copy of each document submitted** in the technical envelope on CD-ROM or USB stick with the full set of documents in **machine readable format** (MS Office 2003 or later, or Adobe Reader Version 8.0 or later), strictly identical in full to the original tender

4.6.3 Financial proposal (ENVELOPE 3)

4.6.3.1 Content

Each tender shall include a financial offer, containing:

	ENVELOPE 3 – FINANCIAL OFFER (one (1) ORIGINAL and one (1) ELECTRONIC COPY per envelope).
(1)	**Duly signed and dated financial proposal** using the templates in **Annex I.F**
(2)	**An electronic copy of each document submitted** in the financial envelope on CD-ROM or USB stick with the full set of documents in **machine readable format** (MS Office 2003 or later, or Adobe Reader Version 8.0 or later), strictly identical in full to the original tender

The financial offer must respect the following conditions:

4.6.3.2 Unit prices and total price

Unit prices quoted in **Annex I.F**, must be firm and fixed and are not subject to revision. The unit prices in the financial offer will constitute the price list for the duration of the Contract, and shall include all costs and expenses which are necessary for performance of the tasks.

These costs and expenses are indicatively: effort for all the tasks (including drawing up quotations and reports) necessary for their performance, including all costs (e.g. travel expenses, daily subsistence allowance, management of the project, administrative support and any support resource, coordination, quality control or currency conversion fees).

4.6.3.3 VAT exemption

As the GSA is exempt from all taxes and dues, including value added tax (VAT), pursuant to Articles 3 and 4 of the Protocol on the privileges and immunities of the European Union, these must not be included in the price.

4.6.3.4 Currency and exchange rates

The price tendered must be all-inclusive and expressed in Euro without VAT.

4.7 Submission

Without prejudice to the conditions of submission set out below, the Tenderer may submit the Tender only electronically on 3 (three) CD-ROM, DVD or USB sticks with the full set of documents (as requested under section 4.6 of the Tender Specifications). The documents on these media must be identical and they shall be in machine readable format (MS Office 2003 or later, or Adobe Reader Version 8.0 or later). These media must be inserted in the outer envelope as described in section 4.5.2 of the tender specifications. They shall contain the following folders with the corresponding documents requested under section 4.6 of the Tender Specifications:

- Folder 1: ADMINISTRATIVE DOCUMENTS and DOCUMENTS RELATING TO EXCLUSION and FINANCIAL AND ECONOMIC SELECTION CRITERIA
- Folder 2: TECHNICAL DOCUMENTATION
- Folder 3: FINANCIAL OFFER

The electronic versions of the documents are considered as originals.

The Tenderer must ensure that the electronic media and files are readable. In particular, they must take all the necessary measures to protect them during the transport to avoid any damage to them.

Tenderers are advised to:

- use, and include into the outer envelope, different types of media (e.g. DVD and different types of USB sticks) in order to eliminate the risk of non-readable media and files.
- create hashes of submitted files (in the form of algorithm MD-5, SHA-256 or higher) and insert them, preferably as a paper printout, into the outer envelope, together with the media.
- ensure that the data on these media cannot be altered.

If the submitted media and files are not readable, the Tenderer will have the possibility to resubmit the media upon condition that:

- hashes of the original files have been created;
- hashes of the re-submitted files are created and such hashes are strictly identical to the hashes of the original files inserted into the original outer envelope.

If the submitted media and files are not readable and the Tenderer does not resubmit media and files which are strictly identical to the original ones and related hashes, within a reasonable delay upon notification by the Contracting Authority that the files submitted cannot be read, the tender will be rejected.

Tenders may be submitted by post mail, express mail, commercial courier or hand-delivered and are to be submitted not later than the relevant date and time specified in section 1.7 above to the following address:

European GNSS Agency
Procurement and Legal Department
Tender ref: GSA/OP/25/20 "GRC Guarding, Security and Safety Monitoring Services"
Janovskeho 438/2
170 00 Prague 7
Holesovice, Czech Republic

Tenders sent by post mail, express mail and commercial courier shall be addressed to this address not later than 23:59 (local time) of date indicated in section 1.7. In this case, a receipt must be obtained as proof of submission.

In case the tender is hand-delivered, a receipt must be obtained as proof of delivery, signed and dated by the desk officer of the GSA reception. The reception is open from 08.00 to 17.00 Monday to Thursday, and from 8.00 to 16.00 on Fridays. It is closed on Saturdays, Sundays, European Commission holidays and some Czech national holidays. The hand-delivery of tenders outside the indicated business hours cannot be guaranteed and it will be usually not possible due to absence of the desk officer of the GSA reception.

Upon submission of tenders by post mail, express mail, commercial courier or hand-delivery, tenderers shall send an email of notification of submission to tenders@gsa.europa.eu. The subject of the email shall be: "GSA/OP/25/20: submission of tender by *[insert name of legal entity / consortium]*" and it shall contain as attachment the relevant proof of submission.

The documents which must be signed according to the tender specification may be signed electronically with a qualified electronic signature (QES) of the tenderer/applicant. This electronic signature must be provided by a provider which has a qualified status granted by a national competent authority of an EU Member State and which is listed in the national eIDAS Trusted Lists and the EU List of eIDAS Trusted Lists (LOTL) (available at https://webgate.ec.europa.eu/tl-browser/#/).

4.8 Public opening of the tenders

The tenders will be opened on the date and time specified in section 1.7 above, in the offices of the GSA, Janovskeho 438/2, Prague 7, Czech Republic.

This opening session will be public. One representative of each tenderer may attend the opening of the tenders. At the end of the opening session, the Chairman of the opening committee will disclose the name of the tenderers and the decision concerning the admissibility of each offer received. The prices indicated in each tender received will not be communicated.

Tenderers who wish to attend are invited to send a request (at least 5 (five) calendar days before the date of the opening) to the following e-mail address: tenders@gsa.europa.eu, specifying the name of the attending person and the tenderer (s)he represents. The subject of the email shall be: "X*:* request from *[insert name of legal entity / consortium]* to participate to the opening session"

In order to be able to enter the GSA premises for the opening of the tenders, the attending person shall present an ID card or passport at the reception of the GSA. Maximum one representative of a tenderer may attend the opening.

The opening session may be organised via videoconference. Tenderers who expressed interest in participating in the opening session will receive contact details for participation in the videoconference.

The opening session may be recorded. In such a case the participants will be informed about the recording at the beginning of the session.

Maximum one representative of each tenderer may attend the videoconference. At the beginning of the session, the representatives of the tenderers will be asked to point the camera at their ID card or passport and expressly declare their identity.

4.9 Period of validity of the tenders

Period of validity of the tenders, during which tenderers may not modify the terms of their tenders in any respect shall be 9 (nine) months from the closing date for the submission of the tenders.

4.10 Further information

Contacts between the GSA and tenderers are prohibited throughout the procedure save in exceptional circumstances and under the following conditions only:

Before the final date for submission of tenders:

- At the request of the tenderer, the GSA may provide additional information solely for the purpose of clarifying the nature of the contract.
- Any requests for additional information must be made in writing only to tenders@gsa.europa.eu. The subject line of the e-mail has to quote the reference of the procurement procedure: GSA/OP/25/20 GRC Guarding, Security and Safety Monitoring Services.
- Requests for additional information received after deadline specified in section 1.7 above cannot be processed.
- The GSA may, on its own initiative, inform interested parties of any error, inaccuracy, omission or any other clerical error in the text of the Invitation to Tender.

After the opening of tenders:

- If, after the tenders have been opened, some clarification is required in connection with a tender, or if obvious clerical errors in the submitted tender must be corrected, the GSA may contact the tenderer, although such contact may not lead to any substantial alteration of the terms of the submitted tender.

4.11 Information for tenderers

The GSA will inform tenderers of decisions reached concerning the award of the contract in due course, including the grounds for any decision not to award a contract or to recommence the procedure.

If a written request is received, the GSA will inform all rejected tenderers of the reasons for their rejection and all tenderers submitting an admissible tender of the characteristics and relative advantages of the selected tender and the name of the successful tenderer.

However, certain information may be withheld where its release would impede law enforcement or otherwise be contrary to the public interest, or would prejudice the legitimate commercial interests of economic operators, public or private, or might prejudice fair competition between them.

4.12 Data protection

Any personal data that may be included in the tenders received during the present procedure will be processed in accordance with (1) the applicable rules on the protection of natural persons with regard to the processing of personal data by the EU institutions, bodies, offices and agencies (currently Regulation (EU) 2018/1725) and (2) the modalities of the following privacy statement:

Identity of the controller and Data Protection Officer:

- **Controller:** European GNSS Agency (GSA), GSA Head of Galileo Exploitation Department, tenders@gsa.europa.eu.
- **Data Protection Officer:** GSA Data Protection Officer, Janovského 438/2 170 00 Prague 7, Czech Republic, dpo@gsa.europa.eu.

Purpose of the processing:

- the management and administration of the tender procedure
- additionally and only with regard to the personal data of the awarded tenderer(s), the preparation of the contract

Data concerned:

- Contact information of tenderers, e.g. name and last name of authorised representatives, email address, postal address, telephone numbers, company/agency/body and department, country of establishment, position
- Financial information of tenderers, e.g. bank account number, IBAN and BIC codes, address of respective bank branch

- Information that may be included in CVs of experts proposed by tenderers: name and last name of proposed experts, educational background, professional experience including details on current and past employment, technical skills and languages etc.
- Data related to criminal convictions and offences of: (1) members of the administrative, management or supervisory body of tenderers, (2) natural persons who have powers of representation, decision or control of the tenderer, (3) owners of the tenderers as defined in Article 3(6) of Directive (EU) 2015/849, (4) natural persons assuming unlimited liability for the debts of the tenderers, (5) natural persons who are essential for the award or the implementation of the contract; such data are collected through the submission of the declaration of honour

It is specifically noted that:

- the abovementioned processing operations will not entail the processing of any special categories of personal data. If, however, a tenderer submits such data at its own volition and without any specific request, it is implied that the data subject has given its consent to the processing of such data.
- the provision of personal data by the tenderers is a requirement necessary to enter into the FWC

Legal bases: Article 5(1)(a), 5(1)(c), 10(2)(a) and 11 of Regulation (EU) 2018/1725

Lawfulness of the processing:

- Article 5(1)(a): the processing is necessary for the performance of a task carried out in the public interest, specifically the management and functioning of the GSA through the launching of tender procedures.
- Article 5(1)(c): the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; the GSA processes the personal data of the tenderers at their request (through the submission of their tenders) in order to take the necessary steps prior to enter into the contract with the awarded tenderer(s).
- Article 11: the processing of personal data relating to criminal convictions and offences shall be carried out only when authorised by Union law; such processing, in the form of an extract from the judicial record or declaration of honour, is explicitly foreseen in the Financial Regulation[8] (Articles 136-140)
- Article 10(2)(a): as explained above, in case any tenderer submits special categories of data at its own volition and without any specific request, it is implied that the data subject has given its consent to their processing

Recipients of the data processed:

- a limited number of staff of the GSA managing this tender procedure
- data processors:

[8] Regulation (EU, Euratom) 2018/1046

- a limited number of staff of GSA contractors assisting GSA staff in the management of this tender procedure
- a limited number of staff of GSA contractors in charge of the provision of hosting services for the GSA's servers

- bodies charged with a monitoring or inspection task in application of Union law (e.g. internal audits, Financial Irregularities Panel, European Anti-fraud Office – OLAF)
- members of the public: the winning entities will be announced to the public, which may also entail the announcement of the personal data of the representatives of such entities (e.g. name, last name)

Information on the retention period and storage locations of personal data:

- any information pertaining to this tender procedure shall be kept for up to 7 years following the end of the year when the contract(s) has been awarded as a result of the tender procedure; files may also have to be retained until the end of a possible audit if one started before the end of the above period;
- all collected data may be stored:
  - electronically on GSA servers with access control measures (i.e. one or two factor authentication) hosted by GSA contractors which are located in the EU and abiding by the necessary security provisions
  - physically in secure storage cupboards in the GSA HQ in Prague
  - electronically and physically on the servers/cupboards of the processors identified above (all of which are established in an EU Member State)

The data subjects' rights:

- Data subjects have the right of access, rectification and erasure of their personal data or restriction of processing at any time, provided that there are grounds for the exercise of this right, as per the applicable rules
- Data subjects have the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her. Requests shall be addressed to the GSA Legal Department at tenders@gsa.europa.eu by describing the request explicitly. It is noted that pursuant to such a request, the Controller shall no longer process the personal data unless the Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims
- Data subjects may obtain their personal data, submitted to the GSA, in a structured, commonly used and machine-readable format and transmit them to another controller, provided that there are grounds for the exercise of this right, as per the applicable rules
- Data subjects are entitled to lodge a complaint at any time with the European Data Protection Supervisor (http://www.edps.europa.eu; EDPS@edps.europa.eu) if they consider that their rights under the applicable rules 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 have been infringed as a result of the processing of their personal data by the GSA

- Only in cases where the data subjects' consent is used as the legal basis for the processing of personal data (i.e. in case they have submitted special categories of data at their own volition and without any specific request), they can withdraw their consent at any time, without affecting the lawfulness of the processing before the withdrawal

Any request for the exercise of any of the abovementioned rights shall be addressed to the GSA Legal Department at tenders@gsa.europa.eu; data subjects are kindly requested to describe their requests explicitly.

4.13 Tenderer's consent to the use of information supplied in the tender

By submitting a reply to the invitation to tender a tenderer provides its unconditional and irrevocable consent to the Agency to use any information contained in the tender in legal proceedings related to procurement regardless of the parties involved to the extent as necessary or appropriate for due protection of Agency's rights. Should the Agency use the content of the tender for this purpose, the tenderer waives any claim for any compensation of any kind whatsoever or any claim related to confidentiality and/or data protection.

5 Acronyms and Definitions

Acronym	
FWC	Framework Service Contract
NDU	Non-Disclosure Undertaking
LEF	Legal Entity Form
SAL	Security Aspects Letter

6 List of Tender Specifications Annexes

These tender specifications have the following annexes:

Annex	Title
Annexes I.A- I.B-I.C-I.D (Administrative Annexes)	Template Identification Sheet of the Tenderer - Template Declaration of Honour - Power of Attorney - Sub-contractor Letter of Intent
Annex I.E	Financial Statements relating to the Selection Stage
Annex I.F	Template Financial Tables of Answers
Annex I.G	Non-Disclosure Undertaking
Annex I.H	Security Aspect Letter
Annex I.I	Statement of Compliance
Annex I.J	Statement of Applicability of the SAL
Annex I.K	Applicable Documents
Annex I.L	Key Performance Indicators (KPI) Formulae

Annex I.K Applicable Documents

This annex contains the details of the documentation that is outlined as applicable to these Tender Specifications. In the table below, if a document states availability "After NDU" it means that it can only be made available to the tenderer after submission of the signed NDU, as provided under Section 1.8. and Annex I.G.

Document	Reference ID	Issue	Availability
Annex I.K1 GRC Security Operational Procedures	GSA/OP/25/20 GRC Security Operational Procedures	1.0	After NDU
Annex I.K2 GRC House Rules	GSA-GAL-GRC-POL-A09620	1.0	After NDU
Annex I.K3 – Building Information	GSA/OP/25/20 Building Information	1.0	After NDU
EU GNSS Programme Security Classification Guide, latest version (RESTREINT UE/EU RESTRICTED)			After NDU

Annex I.L Key Performance Indicator (KPI) Formulae

The KPIs to be measured under this contract are:

- **KPI-01:** Timely Detection of Alarms,
- **KPI-02:** Timely Response to Security & Safety Incidents,
- **KPI-03:** Availability of On-Site guarding service,
- **KPI-04:** Availability of Remote Monitoring Service,
- **KPI-05**: Timely provision of Security Logs,
- **KPI-06:** Timely provision of Security Report and KPIs.

Timely Detection of Alarms

Each of the KPIs in the table below are determined in the same manner and each measures the effectiveness in timely detection or response of the particular monitoring alarm or incident.

KPI-#	Title	Target Time
KPI-01	Timely Detection of Monitoring Alarms	5 Minutes
KPI-02	Timely Response to Security & Safety Incidents	10 Minutes

The KPI is assessed based on the number of alarms missed or detected out of scope of the requirement, where:

n_i *The number of incidents in which an alarm was missed or detected out of scope.*

The value of the KPI is found using the following lookup table:

n_i	KPI-# Value
0	1
≤ 2	0.6
≤ 4	0.3
> 4	0

Availability of Services

Both of the KPIs in the table below are determined in the same manner and each measures the availability of the service to which they reference in their title.

KPI-#	Title	Target	Minimum
KPI-03	Availability of On-Site Guarding Service	99.99%	99.97%
KPI-04	Availability of Remote Monitoring Service	99.99%	99.97%

The KPI is assessed based on the measured availability of the service when compared to the target and minimum values expected over the duration of the reporting period, where:

T_{target}	*Target availability*
T_{min}	*Minimum availability*
P	*Duration reporting period (calendar days)*
U	*Total Duration of unavailability of the service in the reporting period*
M	*The measured availability in the target period*

$$M = \frac{P - U}{P}$$

$$KPI\ Value = \begin{cases} 1\ if\ M \geq T_{target} \\ 0\ if\ M \leq T_{min} \\ \dfrac{\log_{10}\left((1 - T_{min})/(1 - M)\right)}{\log_{10}\left((1 - T_{min})/(1 - T_{target})\right)} \end{cases} if\ T_{target} > M > T_{min}$$

Provision of Security Logs and Reports

Both of the KPIs in the table below are determined in a similar manner and each evaluates the timely provision of the Security Logs and Security Reports, respectively.

KPI-#	Title	Target Time
KPI-05	Timely provision of Security Logs	1 Day
KPI-06	Timely provision of Security Report and KPIs	7 Days

The KPIs compare the number of days by which the provision of a log or report is late with respect to the target value, where:

d	*Number of working days after the end of the reporting period.*

For KPI-05, where the logs are expected on the first day of the next week, the value is found by using the following lookup table:

d	KPI-05 Value
1	1
2	0.5
≥ 3	0

For KPI-06, where the reports and associated KPI reporting is expected following the end of a quarterly reporting period, the value is found by using the following lookup table:

d	KPI-06 Value
≤ 7	1
≤ 9	0.75

d	KPI-06 Value
≤ 11	0.5
≤ 13	0.25
> 13	0

Application of KPIs and Associated Liquidated Damages

The KPIs, detailed above, are calculated to be used in the following liquidated damage system to provide the Contracting Authority with an economic compensation whenever the Contractor is not able to fulfil the service requirements in relation to the duties of the contract. The liquidated damages related to the KPIs shall be applied without prejudice to Art. I.14 of the FWC.

The liquidated damage shall be calculated for each reporting period (on a quarterly basis), for each of the above KPIs, as follows:

(MLD * (1 - KPI Value for the period) * KPI weight)/
the sum of all KPI weights

Where:

- *KPI is the Key Performance Indicator, which shall be calculated from metrics obtained over a reporting period.*
- *One (1) represents the level of fulfilment when it matches or exceeds that which is required.*
- *MLD is the Maximum Liquidated Damage, calculated as 20% of the service price applicable to the reporting period price.*

This calculation should be done for all KPIs for the period and summed to obtain the value. If all KPIs fulfil the required level (i.e. KPI=1), then no liquidated damages are due.

The maximum liquidated damages that can be applied on any payment is 8% of the reporting period price. In case the contractor reaches this cap in more than three reporting periods, the Contracting Authority has the right to terminate the contract according to Article II.12.1 (k).

KPI-#	Title	KPI Weight
KPI-01	Timely Detection of Alarms	90
KPI-02	Timely Response to Security & Safety Incidents	100
KPI-03	Availability of On-Site Guarding Service	100
KPI-04	Availability of Remote Monitoring Service	100
KPI-05	Timely provision of Security Logs	80
KPI-06	Timely provision of Security Report and KPIs	80

End of Document