

**Framework Contract for the Provision of  
Services for business content development  
related to the data management and  
analytics software used by Frontex**

**Frontex/OP/498/2020/AH**

**Annex II -Terms of Reference**

## Table of Contents

<b>Table of Contents</b>	<b>2</b>
<b>1. Terms and definitions</b>	<b>3</b>
<b>2. Objectives</b>	<b>4</b>
<b>3. Scope of the procurement</b>	<b>4</b>
3.1. Contracting authorities and procurement procedure	4
3.2. Background	4
3.3. Target situation	5
3.4. Duration	6
3.5. Financial Ceiling	6
3.6. Other costs	6
3.7. Payments	6
3.8. Obligation to perform	7
3.9. Exclusivity	7
<b>4. Scope of Work</b>	<b>7</b>
4.1. Definition of scope statement	7
4.2. Work breakdown	7
4.3. Work description	8
4.4. Indicative Implementation plan for the FWC	9
<b>5. General Requirements</b>	<b>10</b>
5.1. Location of work	10
5.2. Security	10
5.3. Working environment and conditions	10
5.4. Transparency and handover	11
5.5. Language	11
5.6. Documentation	11
<b>6. Specific Requirements</b>	<b>12</b>
6.1. Personnel	13
<b>7. Appendices</b>	<b>16</b>
7.1. Security Aspect Letter applicable for the performance of the FWC	16
7.2. Attendance Sheet Form applicable for T&M SCs	25
7.3. Invoice support document on consultant's attendance Form	26
7.4. Model Task / Deliverable Acceptance Form	27
7.5. Declaration of Confidentiality applicable for specific contracts	28
7.6. CV Template	29

## 1. Terms and definitions

The terms in the table below, appearing either in a complete or in an abbreviated form, when used in this document and its appendices, shall be understood to have the following meaning.

Term	Abbreviation	Meaning
24/7/365	24/7	Used for defining services to be provided around the clock every day of a year when the differentiation of Normal and Extended Working Hours is not applied.
Business Intelligence	BI	For the purpose of the document Business Intelligence shall be understood mainly as a software supporting acquisition and transformation of raw data into meaningful and useful for business analysis purposes.
Cascading/Ranking Mechanism	Cascade	The cascade is a mechanism applied for using multiple framework contracts. Frontex ranks the tenderers in descending order, based on the results of the evaluation, with a view to establishing the list of contractors and the sequence in which they will be offered orders. Frontex always contacts the contractor at the top of the list. If that contractor is unavailable or incapable to respond for reasons which do not entail terminating the contract, the second contractor may be contacted, and then, if necessary and under the same conditions, the third.
Commercial Off-The-Shelf Software	COTS	Commercial software products, components, development libraries, templates, scripts, management and development tools which are offered in the commercial marketplace. It can be purchased, leased or licensed to the general public.
Customisation		Alignment of the OOTB, COTS and 3rdP functionalities and features to Frontex requirements by configuration, setting and scripting (including sql queries, power shell, java scripts, SAS code) without Custom development.
Extended Working Hours	EWB	Any working hours other than Normal Working Hours.
Fixed Price	FP	Fixed Price assignments
Framework Contract	FWC	Contract resulting from this call for tenders.
Frontex	FX	The European Border and Coast Guard Agency.
Frontex Headquarters	FX HQ	Frontex premises located in Warsaw, Poland.
ICT	ICT	Frontex ICT Unit
IFC	IFC	Information Fusion Centre
Member State	MS	The European Union member state.
Normal Working Day	NWD	From Mondays to Fridays inclusive, excluding Frontex holidays. Frontex holidays usually cover Easter Break, 1-3 May, 9 May, Corpus Christi in June, Assumption Day in August, 1 and 11 of November, last week of December and 1 day of January. Detailed list will be provided to the Contractor before the start of each calendar year.
Normal Working Hours	NWH	Normal working days from 08:00 to 18:00
Other Locations		Place of performing tasks other than Frontex Headquarters and Contractor's premises.
Out of the Box Software	OOTB	A ready-made software that meets a requirement that works straight after its installation without a special software development effort.
Personal Data		Shall have the same meaning as set out in the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the

		protection of individuals with regard to the processing of personal data and on the free movement of such data, Regulation (EC) 2018/1725 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
SAM		Situation Awareness and Monitoring division
SAS VA		SAS Visual Analytics - online analytical application
SAS EG		SAS Enterprise Guide - desktop SAS client application
SAS Office Add-IN	SAS Office	Microsoft Office plugin - integration with SAS servers from MS Office application
Security Clearance		Security Clearance - shall be understood as a personal security clearance at the level indicated by Frontex (EU Restricted / RESTREINT UE) or its equivalent in accordance with the comparison table in Appendix 2 of Council Decision of 19 March 2001 adopting the Council's security regulations (2001/264/EC, as last amended) and issued by a National Security Authority of an EU Member State.
Technical Platform	Platform	The Technical Platform includes all ICT tangible elements needed for the implementation and usage of the end-user software solutions. Technical Platform covers all the elements of the TOGAF Technical Reference Model TRM 1 except the business applications.

## 2. Objectives

This call for tenders is intended to result in the signature of multiple framework contracts for the provision of on-site (intramuros) and off-site (extramuros) services regarding SAS software (the data management and analytics software used by Frontex), Business Intelligence systems (BI) and other information systems in Frontex using the aforementioned technologies. The intended max. number of FWCs is three (3). The services will cover integration and adaptation, business content development, consultancy and knowledge transfer in the context of Frontex's information systems environment. The services will involve activities such as (not exhaustively listed): project management, pre-analysis, feasibility studies, proof of concept, analysis, advice, design, programming, testing, installation, application administration, customisation, documentation, training, quality check, end-user assistance, transfer of knowledge and information systems consultancy services. Delivery of software licenses is excluded under the contracts resulting from this call for tenders.

## 3. Scope of the procurement

### 3.1. Contracting authorities and procurement procedure

The Framework contract will apply to Frontex.

The procedure chosen is an open procedure for multiple Framework Contracts (services) with ranking mechanism with maximum three (3) contractors. All specific contracts shall be awarded based on the ranking mechanism.

### 3.2. Background

SAS Platform is the analytical solution chosen by Frontex. Situation Awareness and Monitoring division based its entire data integration and reporting processes in the unclassified network on the SAS Software. For more than 10 years of usage, users have gained a lot of knowledge and skills for getting the best from what SAS has to offer. There have been many investments for making the SAS environment

a technically stable environment and for ensuring support services. Due to the proven added value, there is a continuous growing number of satisfied internal and external users. Via the SAS platform we share information and reports based on data collected from Member States, Schengen Associates, Third Countries and several other data sources.

From SAM perspective, some core business activities to be completed on time rely on SAS solutions. Different SAS applications are critical for several procedures regarding data processing, data retrieving and for supporting analytical and situational monitoring functions of the Agency with respect irregular migration and cross-border criminal activity.

SAS Licenses in use (PRD/UAT Unclassified environment):

SAS Analytics Suite:

- SAS Business intelligence Server
- SAS Access to ODBC
- SAS Access to PC File Formats
- SAS/ETS
- SAS/STAT

SAS Visual Analytics:

- SAS Access to ODBC

SAS Data Management Standard

- SAS Data Quality Server
- Data Flux Data Management Server
- SAS Data Remediation
- SAS Access to MS SQL Server
- SAS Access to Oracle
- Platform Computing for SAS

SAS Enterprise Guide

SAS Office

### 3.3. Target situation

This contract is planned to support Frontex in providing the support by max. three (3) ranking framework Contractors in a harmonized and coordinated manner during the next four (4) years.

By concluding these framework contracts, Frontex can order the development of new solutions and services at a relatively short notice, by the experts that specialize in the exact technology and by teams that cooperate with Frontex on a long term and therefore accumulating the required knowledge regarding the business activities of the Agency. This leads to the increased capability to assure service continuity, quick response to business needs, achieving proper level of harmonization and coordination yet sustaining competition. The SAS software is an important tool supporting the daily tasks of Frontex and the system shall be supported and maintained at technical layer as well as in the area of knowledge transfer to the end users of the SAS solutions. Frontex staff should receive regular support from the contractor in all the tasks related to the system in use and its development. There are some needs regarding the improvement of the existing processes as well as some potential new business functionalities for statistical analytical tools identified during the use of SAS solutions by Frontex.

Particularly important areas are the following:

- Centralising statistical information and to provide a single interface for metadata management together with data governance;
- Reinforcing Frontex capacity to verify statistical data and ensure data quality for a vast (and expanding) array of datasets;
- Facilitating the use of common, coherent processes for compiling and presenting statistical information;
- Allowing a more streamlined procedure for the creation of harmonised reports that can be updated efficiently in order to provide an accurate common picture;
- Providing enhanced (statistical) analytical capacity for more complex data analysis and trend modelling in such a framework, These new functionalities should be validated and implemented to the existing Frontex SAS systems / solutions in order to ensure the efficient use of SAS services by Frontex staff members.

### 3.4. Duration

The maximum duration of the Framework contract is two (2) years, starting from the date of its signature by the last contract party, which can be extended, if needed, for up to two (2) additional periods of one year, under the sole discretion of Frontex.

### 3.5. Financial Ceiling

The maximum amount that can be spent under this lot of the FWC cannot exceed 4 000 000 EUR. Nevertheless, Frontex reserves the right to conduct negotiated procedure without prior publication of a contract notice based on point 11.1 (e) of the Annex I to Financial Regulation to increase the ceiling, if such a need occurs and the respective conditions apply.

### 3.6. Other costs

The prices included in the FWC and in the related SCs are fully inclusive. No additional costs are eligible. This includes but is not limited to ordering, processing, logistics, communication, secretariat, customs, training, tooling and equipment used by the Contractor staff.

### 3.7. Payments

Payments for Specific Contracts will be executed based on Contractor's invoice and on the basis of approved Attendance Sheets, after the end of a calendar quarter. At the request of Frontex, an interim payment for the 4th quarter may be divided as follows: a separate interim payment for October and November and a separate interim payment for December, which may also be combined with the next quarterly payment.

Every invoice shall be issued solely in relation to the single Specific Contract.

Invoice may be issued upon completion of the related work and when the Appendix 9.2 Attendance Sheet Form and 9.3 Invoice support document and/or Task Acceptance Form (Appendix 9.4) is duly completed and signed.

The Contractor shall nominate a FWC Contract Officer who shall act as a single contact point vis a vis Frontex for the FWC matters for the duration of the FWC and must be available for Frontex requests. All the contractual correspondence and related coordination will be addressed to him.

The Contractor will nominate a FWC Executive who will be ultimately representing the Contractor's company and subcontractors vis a vis Frontex for the supervision of all the Specific Contracts, overall performance of the Contractor, change management and escalation of issues not solved at the level of the individual specific contracts.

### **3.8. Obligation to perform**

The conclusion of the FWC does not impose on the Contractor the obligation to submit a proposal in reply to each Request for Services; however, Frontex reserves the right to terminate the FWC in the following cases:

- a) in the event the contractor fails to submit the proposal for the third time,
- b) in the event the submitted proposal is evaluated to be below the minimum required levels for the third time.

### **3.9. Exclusivity**

The conclusion of the FWC does not confer on the contractor any exclusive rights in relation to the provision of services or supply of goods specified therein.

## **4. Scope of Work**

### **4.1. Definition of scope statement**

The contracts resulting from this call for tenders shall be considered as a source for generic services related to Frontex analytical platform based on SAS Software and other information systems in Frontex using the aforementioned technologies, under T&M, QT&M or Fixed Price assignments. These contracts will address Frontex needs regarding business content development, existing platform data flow processes enhancements, new analytical trends case study and proof of concept, data management including data integration, quality and governance. It shall be understood in broad meaning with reference to all phases of business processes life cycle and technical aspects of SAS software implementation together with provision of guidance and transfer of knowledge. Therefore it may cover typical business content development as well as evolution of the existing processes and solutions, refactoring, tuning etc.

### **4.2. Work breakdown**

The following categories define the scope of the services covered by prospective Contracts for all Lots:

- A. Consultancy in relation to all the phases of requested services,
- B. Business Content Development
- C. Integration, deployment and maintenance
- D. Prototyping and preparation of feasibility studies
- E. Documentation
- F. Training and Knowledge Transfer
- G. Project Management and advisory services

## H. Cooperation with other Contractors

### I. Workshops and coaching on requested topics, new functionalities, new modules and case studies.

## 4.3. Work description

The following items describe the work planned for this Contract and related competences required. The descriptions cover the majority of works however cannot be considered as exhaustive. These descriptions correspond to the Specific Requirements. The scope items listed below are interdependent. For example - Consultancy provides input to Development and the Development may support Consultancy (e.g. via prototyping). It is a contractual obligation that various works under these Contracts are technically harmonized and organizationally synchronized.

### Consultancy

Consultancy shall be understood in a broad meaning by including: development of an Information Architecture, business and system requirements analysis, concept development, architecting the solutions and producing high level technical designs. The outputs of Consultancy are: documents, presentations and repositories e.g.: for the software solutions, for the design of the user interface, for the organization of technical tasks (e.g. test plans, deployment plans etc.), for content, for assistance to change management related to the implementation of the technical solutions (e.g. development of policies & procedures documents), etc. When combined with development it may deliver Proof of Concepts or prototypes.

### Development

Development shall be considered with a reference to the business content development lifecycle. It covers the development of complete solutions but also extensions, plugins, interfaces, administrative scripts, GUI elements as well as customizations. This work includes prototyping, elicitation of detailed requirements, detail design, production of technical and user documentation, data migration, testing and deploying the solutions. Development services may cover Consultancy services e.g. delivery of Initial Analysis in course of FP assignment for a complete solution.

### Knowledge transfer and trainings

Knowledge transfer covers activities which shall result in an increase of Frontex's staff knowledge and awareness in relation to a specific area. These activities are: performing of dedicated workshops focused on Frontex's use cases, coaching in a daily use of a specific technology and/or software to perform tasks in a more efficient and effective way; coaching in advanced functions facilitating the daily tasks performance. Training should be understood as the delivery of custom designed trainings as requested by Frontex for the software components being in the scope of this Contract as well as its administration and maintenance. Training will be delivered to power users, end users and to administrators in form of training sessions with hands-on workshops as well as delivery of training materials in form of workshop handouts, training environments with training data and scenarios or wiki-like guides. Delivery of standard trainings offered by the producers of the technologies covered by this FWC is not included in the scope.

### Cooperation with other Contractors

Performing tasks under this contract may require a close cooperation with other Frontex's contractors. The cooperation may require both requesting and delivering some specific information enabling the performance of tasks requested by Frontex. Frontex requires that contractors will maintain reasonable transparency and support information sharing when needed. Every contractor must respect the right of others for requesting the information and must offer the necessary support. If not offered in advance



the contractor may in any case request Frontex assistance in such cases. Frontex may require an engagement of the contractor into other projects performed by Frontex or by other contractors in the scope of integration of systems, technologies.

#### 4.4. Indicative Implementation plan for the FWC

The list below presents the indicative plan of the implementation of the Framework Contract, which is not binding on Frontex and will be adapted during the contractual period. The composition of the plan presents the intended flexibility in ordering and delivering various work items. The same work item may be ordered under different types of contracts according to the current needs of Frontex. In addition, one SC may cover more than one work item.

Artificial Intelligence and Data Governance projects are planned subject of most urgent Time & Means Specific Contract. It would require for at least 6 month involvement of the:

- a. Profile of Project Manager: 1
- b. Profile of Subject Matter Expert: 1
- c. Profile of SAS Technical Expert: 2
- d. Profile of SAS Business Content Developer: 6
- e. Profile of Analytical Consultant: 1
- f. Profile of Business Consultant: 2

This indicative plan of this Lot implementation is presented for informational purposes only and may be adapted and/or changed during the Contractual period by Frontex.

- 1. Integration between SAS and ESRI technology for web applications
- 2. Integration between SAS and other technologies used for web reporting
- 3. High-level business use cases and functional requirements identification
- 4. Continuous business content development and maintenance
- 5. Development of data management and quality processes
- 6. Security implementation in accordance with ICT security policy and security audits
- 7. Development of mobile application and services
- 8. Other products and services

## 5. General Requirements

### 5.1. Location of work

The actual venue for each Order and Specific Contract will be defined in the Order Form or the Request for Specific Contract.

The following categorization of place of performance shall be applied:

- Intramural assignments to be performed at Frontex Headquarters (Warsaw, Poland).
- Extramural assignments to be performed at the Contractor's premises.

### 5.2. Security

The Contractor shall respect the Frontex Security Rules and the related policies and procedures. Frontex Security Rules and the relevant policies and procedures will be made available at the beginning of each Specific Contract to the involved employees of the contractor and updates, changes in these documents or publication of new documents will be communicated during the execution of the contracts.

The contractor's staff involved in the execution of the contract will be asked to sign a Declaration of Confidentiality prior to the start date of their direct involvement in the Contract.

If the Contractor or his personnel and, where applicable, subcontractors fail to comply with the Frontex security rules. Frontex may, without prejudice to any indemnity due by the contractor to Frontex, terminate the contract with immediate effect by giving notice in writing to the contractor. In these circumstances, no costs or compensation relating to such termination shall be due by Frontex to the contractor.

Frontex reserves the right to request the contractor to demonstrate the valid excerpt of the criminal record of the contractor staff members planned to participate in the execution of the contract and to refuse participation to any person that has been: convicted of an offence concerning their professional conduct by a judgment, which has the force of res judicata; guilty of grave professional misconduct, the subject of a judgment, which has the force of res judicata for fraud, corruption, involvement in a criminal organisation or any other illegal activity detrimental to the Communities' financial interests. Any classified information shall be handled and protected by the Contractor as described in the European Commission 2015/444 on protection of European Union Classified Information.

In addition, Frontex reserves the right to require the contractor to initiate security screening for his personnel directly involved in the execution of the FWC or SC to obtain the security clearance at RESTREINT UE/EU RESTRICTED level in order to provide specific services planned for the course of this FWC.

### 5.3. Working environment and conditions

Frontex will provide to the Contractor the following resources:

- Access to all necessary premises and elements of infrastructure to conduct the tasks
- Access to all necessary documentation and information in Frontex possession that are necessary to conduct the tasks and for intramural assignments
- Office space for the Contractor's staff performing intramural assignments
- Computers, software licenses and other ICT tools for the duration of the SC Frontex may require exclusive use of it
- All software necessary for the accomplishment of the tasks under this Contract will be installed on Frontex hardware and will remain within Frontex without deletion, change, or deletion of configuration at the end of the Contract.
- Contractor's staff may bring their company or own computers in order to perform some tasks not related to the Contract, e.g. tasks requested by their employer. In line with Frontex security policies,

these devices will not be authorised to connect to any Frontex networks except those foreseen for Frontex guests.

#### 5.4. Transparency and handover

Frontex requires transparency from the Contractor in the provision of services under the Contracts, specifically regarding the organisation and staff engaged, processes and standards used, information and documentation produced in these processes (i.e. bugs repository), and in the methods and tools. At the request of Frontex the Contractor must hand his tasks over to Frontex staff or other indicated third party contractor by the defined date. The handover shall be planned and the plan shall be submitted to Frontex for acceptance. The handover shall enable the taking-over party to continue the tasks of the Contractor at the levels defined in the respective Specific Contract and to provide further maintenance and evolution of the solution with no additional costs for reengineering, redevelopment of documentation or reimplementation of administrative tools. The contractor is required to: train the taking-over party, present his

recommendation for how to continue his tasks, submit all pending reports, return all tools and documents used in the performance of works, archive and handover all information, credentials and documents that are not in the possession of Frontex and might be needed for continuation of the tasks performed by the Contractor. Such a handover takes place by default (without a request from Frontex) at the completion of the FWC.

By the end of the Specific Contract the Contractor is required to: submit all relevant reports, return all tools and documents, handover all on-going tasks to Frontex staff, archive and handover to Frontex all information, credentials and documents that are not already in the possession of Frontex staff and might be needed for the continuation of the tasks performed by the Contractor.

#### 5.5. Language

All the communication and documentation, both in paper and electronic form and any other deliverables, including software, source codes with its naming conventions and comments, shall be in English (U.K.) and shall adhere to a high standard appropriate for technical documentation, with no ambiguities and no mistakes in grammar or spelling. All members of the Contractor's staff allocated to this contract shall speak and write in English at the levels indicated in their profiles, according to the Common European Framework of Reference for Languages.

#### 5.6. Documentation

Frontex requires that all the documents created in the course of the project maintain a high quality. The following criteria shall be adopted when producing the necessary documentation:

- A clear and appropriate document structure, i.e. the document must be organised into chapters, sections, subsections etc. in a clear and logical way.
- Completeness of documents, i.e. the complete presentation of the entire scope of the described issue without any omission.
- Consistency and coherence of documents, i.e. ensuring mutual accordance of all types of information and lack of logical contradictions of information between the submitted documents or between parts of the same document.
- Proper identification of its title, scope, authors, reviewers, related dates, status, versions, history log, audience, quality or acceptance criteria (if the document is subject to acceptance).

The documentation shall be delivered in editable electronic format. Editable source files for all pictures shall be supplied.

## 6. Specific Requirements

The following requirements have to be respected in the FWC (in the management of the FWC, in T&M, QT&M and in FP Specific Contracts, unless the requirement limits the scope to a specific type of assignment) and shall be reflected in the Tenderer proposal. All the requirements shall be taken into account when preparing the Financial Proposal. No alterations, reservations, alternatives, exclusions in any means including assumptions or constraints are acceptable.

## 6.1. Personnel

No	Title	Description
1	Profiles	<i>All Contractor's staff who take part in the performance of this FWC, related Specific Contracts, and the candidates offered for it, shall be assigned to one of the profiles specified in this TOR and fulfil the criteria set out there.</i>
2	Alignment to tasks of SC	<i>For a Specific Contract, Frontex may verify the offered candidate, who is assessed as compliant to the profile, whether the candidate fits to the tasks planned for the SC. In such a case the Request for Specific Contract will define the evaluation criteria.</i>
3	Interviewing candidates	<i>Frontex reserves the right to interview the candidates for the SC before they take up the duties under the FWC or particular SC. Such interview may take place in form of video conference or physical meeting. Frontex may also test candidates in the field of professional and/or technical competences.</i>
4	Replacement of personnel in T&M SC	<p><i>a. When a person, proposed by the Contractor in reply to Request for Specific Contract is no longer available before the start of the contract, the Contractor is obliged to inform Frontex immediately.</i></p> <p><i>b. In case of replacement in the course of the SC, the Contractor shall give one month's notice to Frontex. The prior agreement of Frontex must be obtained in writing about the principle of the replacement and the replacing staff member.</i></p> <p><i>c. In case of replacement, the Contractor will provide Frontex with the CVs of proposed substitutes, CV Compliancy Declaration Form and Statements of Intents. The Contractor must propose a minimum of two replacement persons with the required qualifications and experience for the profile and they must have at least the same level of qualifications/education and experience as the person proposed in the original offer.</i></p> <p><i>d. In case of replacement acceptance by Frontex, the substitute can assume the work at identical financial conditions, if the Contractor ensures the transition of service between the initial consultant and the substitute. The handover period for service transition must be at least 5 working days, free of charge to Frontex. If no handover is possible, and additional training is needed for the replacement person, at least 10 working days (free of charge to Frontex) must be performed by the replacement person.</i></p>
5	Underperformance	<p><i>a. At Frontex' demand, the Contractor must replace personnel who prove to be incapable of carrying out the specified tasks to the required standards.</i></p> <p><i>b. The replacement person will be given sufficient training during an adequate handover period, so that he/she becomes immediately operational when the original expert is withdrawn. Any such replacement and training, if required, will be carried out by the Contractor at no additional cost to Frontex.</i></p>
6	Planned and unplanned absence	<p><i>a. At Frontex' demand, during holidays or other periods of absence of the person involved, the Contractor will be required to provide an adequate replacement.</i></p> <p><i>b. The replacement person will be given sufficient training and provided with all information necessary to guarantee continuity of the service provided to Frontex.</i></p> <p><i>c. All such training and handover work will be carried out at no additional cost to Frontex.</i></p> <p><i>d. Any planned absence shall be agreed by Frontex at least two weeks prior the absence.</i></p> <p><i>e. Frontex shall be informed about any unplanned absence (e.g. sickness) immediately.</i></p>
7	Registering time in T&M	<p><i>a. Each individual performing services under the T&amp;M Specific Contracts is obliged to register the time of work on every entry and leave of the place of work by registering its exact time in a form presented in Appendix 9.2 Attendance Sheet Form.</i></p> <p><i>b. The Attendance Sheets shall be continuously available to Frontex for verification.</i></p>

		<p>c. The Contractor is required to submit monthly attendance sheets duly completed and signed by the performing person for acceptance by Frontex.</p> <p>d. All the time shall be dedicated to the tasks contracted.</p> <p>e. Frontex reserves the right to use Frontex time management system for automatic collection of entry/exit times to replace the attendance sheets.</p>
8	Escalation	<p>a. Frontex requires that any irregularities, vulnerabilities or risks observed by the personnel performing the contract are immediately reported to Frontex in writing.</p> <p>b. Frontex requires that, in relation to the activities performed in direct relation to this FWC, the Contractor implements in his own organisation an effective internal escalation mechanism in order to control and manage risks related to the Specific Contract and the underperformance of its personnel.</p> <p>c. In case of non -acceptance and rejection of the report on tasks in T&amp;M SCs the Contractor shall initiate his internal escalation procedure.</p> <p>d. Frontex may demand the exchange of the person or terminate the Specific Contract.</p>
9	Closure of a Specific Contract	<p>a. By the end of each Specific Contract or the engagement of a specific person in the Specific Contract the Contractor is required to: submit all pending reports, return all tools and documents, handover all on-going tasks to Frontex staff, archive and hand over to Frontex all information, credentials and documents that are not in possession of Frontex staff and might be needed for the continuation of the tasks performed by the Contractor.</p> <p>b. Frontex may task the Contractor, within the scope and duration of the Specific Contract, to hand over his duties and transfer all knowledge acquired in performing the task to Frontex personnel or another third party contractor, irrespective of if the handover tasks was explicitly indicated in the Request for Specific Contract or not.</p>
10	Required minimum number of staff in the profiles	<p>a. Profile of Project Manager: 2</p> <p>b. Profile of Subject Matter Expert: 2</p> <p>c. Profile of SAS Technical Expert: 2</p> <p>d. Profile of SAS Business Content Developer: 6</p> <p>e. Profile of Analytical Consultant: 1</p> <p>f. Profile of Business Consultant: 2</p>
11	Profile of Project Manager	<p>a. Is certified in project management discipline</p> <p>b. Has got at least 1 year hands-on experience in SAS technologies</p> <p>c. Has got at least 5 years hands-on experience as project manager of implementation of IT systems</p> <p>d. Has got at least 10 years overall work experience after graduation</p> <p>e. Presents good command of English, at least at B2 CEFR level</p> <p>f. Present capability for facilitation of team processes and collaboration with the team to create and execute the project plan, liaison between Frontex and the team, to manage projects, guide project teams and consult business stakeholders</p> <p>g. Is capable of assessment and project definition, writing business cases, plans, concept documents, give presentations and chair workshops for business users</p> <p>h. Holds first cycle higher education</p>
12	Profile of Subject Matter Expert	<p>a. Holds at least one highest Certification credentials relevant to the area of required in SC expertise (for SAS FWC evaluation required are Advanced Analytics Professional or Big Data Professional SAS certificate)</p> <p>b. Has got at least 5 years hands on experience in the area of required in SC expertise</p> <p>c. Has got at least 10 years overall work experience after graduation</p> <p>d. Presents good command of English, at least at B2 CEFR level</p> <p>e. Has expertise in a solution, industry or technology required in SC and experience sufficient for providing expert advice for future project steps, transfer of knowledge, providing technical workshops, quality-check of the work performed by the project team, in terms of design, programming efficiency or best practices, implementation of a project</p> <p>f. holds first cycle higher education</p>

13	Profile of SAS Technical Expert	<p>a. Holds SAS Certified credentials relevant to the area of required in SC expertise (for SAS FWC evaluation required are Advanced Programming Professional or Visual Business Analytics 7/8 SAS certificate)</p> <p>b. Has got at least 3 years hands on experience in SAS technologies</p> <p>c. Has got at least 6 years overall work experience after graduation</p> <p>d. Presents good command of English, at least at B2 CEFR level</p> <p>e. Has a capability including expertise and experience for: providing technical advice concerning architecture, performing software installation and configuration tasks, providing technical support during maintenance phase, performing system optimization from performance, security and quality points of view, documenting of technical solutions, etc.</p> <p>f. Holds first cycle higher education</p>
14	Profile of SAS Business Content Developer	<p>a. Holds SAS Certified credentials relevant to the area of listed in SC SAS modules (for SAS FWC evaluation required are Base Programming Professional or Visual Business Analytics 7/8 SAS certificate)</p> <p>b. Has got at least 1 year hands-on experience in SAS technologies</p> <p>c. Has got at least 4 years overall work experience after graduation</p> <p>d. Presents good command of English, at least at B2 CEFR level</p> <p>e. Possesses capability for unassisted development of solutions, solving problems, documentation creation and knowledge transfer</p> <p>f. Is capable for SAS software customizing and for writing, prototyping, testing, implementing, documenting, performing integrations and maintaining applications using SAS software.</p> <p>g. Holds first cycle higher education</p>
15	Profile of Analytical Consultant	<p>a. Holds SAS Certified credentials relevant to the area of listed in SC SAS modules (for SAS FWC evaluation required is Visual Business Analytics 7/8 SAS certificate)</p> <p>b. Has got at least 1 year hands-on experience in SAS technologies</p> <p>c. Has got at least 5 years overall work experience after graduation</p> <p>d. Presents good command of English, at least at B2 CEFR level</p> <p>e. Possesses knowledge or experience in a combination of the following domains: predictive analysis, machine learning, optimization, textual analysis, statistical theory, experiments and / or time series analysis.</p> <p>f. Holds first cycle higher education</p>
16	Profile of Business Consultant	<p>a. Has experience in the review and optimization of processes within a SC specified domain, the strategies and goals of the customer by using e.g. process management techniques (for SAS FWC evaluation required is Data Management certificate i.e. DAMA CDMP Associate or equivalent)</p> <p>b. Has strong communication skills</p> <p>c. Has got at least 5 years overall work experience after graduation</p> <p>d. Presents good command of English, at least at B2 CEFR level</p> <p>e. Possesses capability for follow-up of vision, organization - business strategy and roadmap within the identified business objectives.</p> <p>f. Holds first cycle higher education</p>



## 7. Appendices

### 7.1. Security Aspect Letter applicable for the performance of the FWC

#### **Security Aspects Letter (SAL) for RESTREINT UE/EU RESTRICTED Contracts**

The performance of the Contract will involve national or EUCI up to the level of **RESTREINT UE/EU RESTRICTED** or its national equivalent.

All Contractor's personnel as well as sub-contractors' personnel involved in work under this Contract shall hold the nationality of an EU Member State unless otherwise agreed in advance with Frontex.

For the purpose of this Security Aspects Letter the following definitions shall apply:

- a. **'EU classified information' (EUCI)** means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States;
- b. **'National Classified information'** shall mean information provided in connection with the Contract requiring protection in the interest of the originating EU Member State, and which has been applied a national security classification marking as shown in the table of equivalent security classifications in Annex 1 to this Security Aspect Letter;
- c. **'Document'** means any recorded information regardless of its physical form or characteristics;
- d. **'Material'** means any document or item of machinery or equipment, either manufactured or in the process of manufacture;
- e. **'Facility Security Clearance' (FSC)** means an administrative determination by an NSA or DSA that, from the security viewpoint, a facility can afford an adequate level of protection to EUCI of a specified security classification level and its personnel who require access to EUCI have been appropriately security cleared and briefed on the relevant security requirements necessary to access and protect EUCI.

All industrial or other entities participating in classified contracts which involve access to information classified CONFIDENTIEL UE or SECRET UE must hold a national FSC. The FSC is granted by the NSA/DSA of a Member State to confirm that a facility can afford and guarantee adequate security protection to EU classified information to the appropriate classification level.

Classified Information at RESTREINT UE/EU RESTRICTED level shall be handled and protected as described in Annex 1 to this Security Aspect Letter.

Information generated by the Contractor will require security classification as detailed in Annex 2 to this Security Aspect Letter.

The Agency reserves the right to request the responsible security authorities to monitor at the Contractor's facilities the



implementation of any security requirements as stipulated in this contract.

If the Contractor's responsible national security authority identifies a failure by the Contractor to observe the security provisions described and regulations referred to under this Annex, and this failure is of such a nature as to result in the withdrawal of the Contractor's Facility Security Clearance (where applicable) to handle classified documents as necessary for the execution of the Contract, the Agency shall have the right to terminate the Contract with immediate effect in accordance with the relevant provisions of the General Terms and Conditions for Contracts awarded by Frontex, without prejudice to criminal proceedings against the Contractor.

In case the responsible national security authority has identified such failure to comply with the relevant security regulations by any sub-contractor resulting in the withdrawal of the sub-contractor's Facility Security Clearance (where applicable), the Agency shall be entitled to require the Contractor to terminate the sub-contract with immediate effect, without prejudice to the Agency's right to terminate the contract with immediate effect and/or to initiate criminal proceedings against the sub-contractor.

Visits by personnel of the Agency to the Contractor's facilities or by the Contractor's personnel to other contractor's or sub-contractor's facilities or to government establishments required under the performance of the Contract, shall conform with applicable national or international visit procedures established by the host nation.

For work performed on the Agency's premises, the Contractor and its personnel shall comply with the security requirements as described in Annex 3 to this Security Aspect Letter.

Notwithstanding the general provisions under Annex 3 regarding access to the Agency's premises or works to be carried out there by the Contractor's personnel, for any visits by Contractor's personnel to the Agency requiring access to CONFIDENTIEL UE / SECRET UE information, an assurance of the visitor's security clearance at the appropriate level shall be provided directly to the Agency's Security Officer prior to the visit taking place.

#### **ANNEX 1 Handling and protection of RESTREINT UE/EU RESTRICTED Information**

Documents or material containing **RESTREINT UE/EU RESTRICTED** information, any national classified information of the EU Member States or classified information originated by another international organisation classified at equivalent level, which has been generated or provided in connection with the Contract shall be handled and protected in accordance with the provisions described hereafter unless more stringent handling procedures are prescribed by applicable national security laws and regulations.

The provisions of this document also may be supplemented by specific security provisions applicable to a given multinational project or programme.

#### **Access by Personnel**

RESTREINT UE/EU RESTRICTED information shall only be made accessible to contractor personnel requiring such information for the performance of the Contract ("Need-to-Know-Principle"). All persons having access to RESTREINT UE/EU RESTRICTED information shall be made aware of their

responsibilities for the protection of such information according to these provisions and the consequences of failure to comply.

A Personnel Security Clearance shall not be required.

#### **Restrictions on Use and Release to Third Parties**

**RESTREINT UE/EU RESTRICTED** information furnished to or generated by the Contractor shall not be used for purposes other than those defined by the Contract and shall be released only to EU Government establishments or contractor facilities located in an EU Member State, whose access is necessary in connection with the performance of the Contract.

Release to any other government, international organisation or representatives thereof or to contractors not located in an EU Member State requires prior approval by the Agency or the originator, as appropriate.

#### **Security Classification and Marking of Documents and Material**

**RESTREINT UE/EU RESTRICTED** documents or material provided to the Contractor shall maintain the security classification markings assigned by the Agency or any other originator of the classified information. Accordingly, copies and reproductions of documents or material shall be assigned the security classification and the marking of the original document or material, if appropriate.

However, documents or material and derivatives and reproductions thereof generated by the Contractor in connection with the Contract shall be classified and marked to identify the **RESTREINT UE/EU RESTRICTED** information as provided for in the Security Classification Guide or any other guidance on security classification described by the Agency.

Documents (hard copies and electronic files), copies or reproductions thereof containing **RESTREINT UE/EU RESTRICTED** information will be stamped, typed, printed or written in bold and capital letters at the top and bottom centre of each front cover or cover letter, page, and of all annexes and attachments with the appropriate classification marking as thus:

EXAMPLE:

<b><u>RESTREINT UE/EU</u></b> <b><u>RESTRICTED</u></b>
---

Material or computer storage media and other optical, acoustical or electronic recordings containing **RESTREINT UE/EU RESTRICTED** information shall be marked properly either on the material itself or - if not possible - on the container holding the material in such a manner that any recipient will know **RESTREINT UE/EU RESTRICTED** information is involved (e.g. by affixing a tag or sticker).

#### **Downgrading or Declassification**

Documents containing classified information at **RESTREINT UE/EU RESTRICTED** **must** not be downgraded or declassified without the prior written consent of the Agency or the originator, as appropriate.

#### **Handling and Storage**

Documents or computer storage media as well as interim material containing **RESTREINT UE/EU RESTRICTED** information must not be left unattended or handled in a manner that could result in unauthorised

access. Such **RESTREINT UE/EU RESTRICTED** material must be stored in locked desks, cabinets or similar containers or may be secured in locked rooms/offices provided access to the room is restricted only to persons authorised to have access to the information.

During travel the documents or data storage media must remain under the permanent personal custody of the holder and must not be left unattended in hotel rooms or vehicles and not be displayed in public.

### **Reproduction and Destruction**

Reproductions of documents or material containing **RESTREINT UE/EU RESTRICTED** information shall be produced under conditions that can prevent unauthorised persons from gaining access.

Material, including interim material, such as working drafts, shorthand notes or spoilt copies, containing **RESTREINT UE/EU RESTRICTED** information must be destroyed in a manner to ensure that it cannot be easily reconstructed.

Documents and computer storage media containing **RESTREINT UE/EU RESTRICTED** information should be reviewed on regular intervals to determine whether they can be destroyed.

To prevent unnecessary accumulation of **RESTREINT UE/EU RESTRICTED** information, documents or data storage media containing such information, which is superseded or no longer needed, and provided there is no residual interest, should be destroyed as soon as practicable or returned to the originator.

### **Transfer**

**RESTREINT UE/EU RESTRICTED** information shall normally be transferred in a single envelope either by

- Commercial courier services;
- Personal carriage by staff members without formal courier orders.

However, the envelope must not bear a classification marking.

**RESTREINT UE/EU RESTRICTED** information must not be transmitted by communication systems or via the Internet unless an encryption system is used, which has been properly approved by Council of the EU or the respective EU Member State's security authority.

In exceptional circumstances, telephone conversations, video conferencing or facsimile transmissions containing **RESTREINT UE/EU RESTRICTED** information may be in clear text, if an approved encryption system is not available at that moment and time is of paramount importance.

### **Use of IT-Equipment**

**RESTREINT UE/EU RESTRICTED** information must be stored on stand-alone computers or dedicated networks accredited for the processing and storage of EUCI, which may only be accessed by staff having a need to know the information.

Laptops storing or processing **RESTREINT UE/EU RESTRICTED** information must be password protected, should have a hard disk encryption and must not be directly connected to the Internet.

The following minimum security measures must be in place when processing **RESTREINT UE/EU RESTRICTED** information on IT systems:

- managed access to system and hardware components (up-to-date lists of authorised users, storage in locked rooms);
- proper identification and authentication features (passwords, log-in); positive identification of all users at the start of each processing session;
- Passwords should have a minimum of six (preferably nine) characters and include alphabetical, numeric as well as special characters.
- general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruses and power supply variations);
- software versions (floppy disks, CD ROMs) in use must be checked for presence of malicious software or computer viruses before starting work on **RESTREINT UE/EU RESTRICTED** information;
- removable computer storage media (e.g. floppy discs, compact disks) to be stored as described under Section 5 above;
- proper data backup with secure local or external storage;
- anti-virus software (implementation, with updates, of an acceptable industry standard anti-virus software); such software must be verified at regular intervals to ensure their integrity and correct functioning;
- no use of privately-owned removable computer storage media and software (e.g. floppy disks, compact disks) or other IT hardware like laptops or PCs;
- no direct connection to Internet unless protected by firewall of an acceptable industry standard;
- use of specific software tools designed for proper deletion of data;
- proper instruction on the use of IT systems in place
- proper security monitoring and auditing.

The following events should be recorded:

- all log on attempts whether successful or failed;
- log off, including time out where applicable;
- initial creation, changes or withdrawal of access rights and privileges;
- initial creation or changes of passwords.

Such records must be carried out by dedicated IT specialists only and be accessible to authorised personnel only. Copies of such records should be provided to responsible IT Security Staff, as appropriate.

Each page of hard-copy output or removable computer storage media must be marked with the **RESTREINT UE/EU RESTRICTED** marking.

#### **Destruction and Maintenance of IT systems and Equipment**

At the end of their life-cycle, or for specific operational reasons, removable computer storage media such as diskettes or compact disks shall be erased, degaussed or shredded.

On fixed data media RESTREINT UE/EU RESTRICTED information must be deleted by overwriting after completion of work unless data is not encrypted by means of approved encryption systems.

If deletion is not possible the data media shall be removed and retained.

External facilities involved in the maintenance or repair work must be obliged, where required on a contractual basis, to comply with the applicable provisions for handling of RESTREINT UE/EU RESTRICTED information.

#### Sub-Contracts involving RESTREINT UE/EU RESTRICTED Information

All sub-contractors must be contractually required, under penalty of termination of their contract, to comply with the security requirements for the handling of RESTREINT UE/EU RESTRICTED information as prescribed in this document.

Appropriate statements or supplementary documentation (e.g. "Security Aspects Letter"), identifying the information or those parts of the contract / sub-contract involving RESTREINT UE/EU RESTRICTED must be part of any contractual arrangement.

A Facility Security Clearance shall not be required for contractors/sub-contractors requiring access to RESTREINT UE/EU RESTRICTED information during the performance of contracts/sub-contracts or in pre-contractual stage unless explicitly required under applicable national laws and regulations.

Frontex may - in co-ordination with the responsible NSA/DSA - conduct inspections at contractor facilities to verify the implementation of the security requirements for the handling of RESTREINT UE/EU RESTRICTED information.

#### Loss, Unauthorised Disclosure or Violation of Procedures

Holders of RESTREINT UE/EU RESTRICTED information shall investigate all cases in which it is known or there is reason to suspect that RESTREINT UE/EU RESTRICTED information has been lost or disclosed to unauthorised persons. Any cases of loss, unauthorised disclosure of RESTREINT UE/EU RESTRICTED information or any violation of provision described in this document must be reported to EU Member States' NSA's/DSA's concerned, the Agency and/or the originator of the information, as appropriate. Action may be taken by the competent authorities, as deemed necessary.

#### Termination of Contract

All RESTREINT UE/EU RESTRICTED information provided or generated under this Contract shall continue to be protected in accordance with the provisions of this article in the event of termination of the Contract. Such information shall be destroyed as described in Section 6 and 9 above or shall be returned to the Agency, if requested.

#### Equivalent Security Classification Markings for RESTREINT UE/EU RESTRICTED

The following security classification markings are equivalent:

Frontex / EU

RESTREINT UE/EU RESTRICTED

Country / Organisation	Security Classification	Country / Organisation	Security Classification
<b>Austria</b>	Eingeschränkt	<b>Latvia</b>	Dienesta vajadzībām
<b>Belgium</b>	nota ( 3 ) below <sup>1</sup>	<b>Lithuania</b>	Riboto naudojimo
<b>Bulgaria</b>	За служебно ползване	<b>Luxembourg</b>	RESTREINT Lux
<b>Cyprus</b>	Περιορισμένης Χρήσης Abr: (ΠΧ)	<b>Malta</b>	Ristrett
<b>Czech Republic</b>	Vyhrazené	<b>Netherlands</b>	Dep. VERTROUWELIJK
<b>Denmark</b>	Til tjenestebrug	<b>Poland</b>	Zastrzeżone
<b>Estonia</b>	Piiratud	<b>Portugal</b>	Reservado
<b>Finland</b>	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG	<b>Romania</b>	Secret de serviciu
<b>France</b>	nota ( 4 ) below <sup>2</sup>	<b>Slovakia</b>	Vyhradené
<b>Germany</b>	VS – NUR FÜR DEN DIENSTGEBRAUCH	<b>Slovenia</b>	Interno
<b>Greece</b>	Περιορισμένης Χρήσης Abr: (ΠΧ)	<b>Spain</b>	DIFUSIÓN LIMITADA
<b>Hungary</b>	Korlátozott terjesztésű!	<b>Sweden<sup>3</sup></b>	HEMLIG/RESTRICTED HEMLIG
<b>Ireland</b>	Restricted	<b>United Kingdom</b>	Restricted
<b>Italy</b>	Riservato		

## **ANNEX 2 SECURITY CLASSIFICATION GUIDE**

Hardcopies or electronic versions of documents (e.g. studies, reports, analysis, specifications and descriptions, technical requirements, performances or any other documentation) as well as data storage media (e.g. floppy disks, compact disks, CD ROMS, DVD, MP3, memory sticks, microchips, etc.) containing information generated in connection with the Contract shall be assigned an EU security classification as prescribed in this appendix. This includes copies, reproductions, extracts or any other derivatives of documents or data storage media containing such EUCI.

Unless otherwise specified hereafter each document or data storage media shall bear the overall security classification at maximum **RESTREINT UE/EU RESTRICTED**.

<sup>1</sup> Diffusion RESTREINTe/Bepaalde Verspreiding is not a security classification in Belgium. Belgium handles and protects 'RESTREINT UE/EU RESTRICTED' information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union

<sup>2</sup> France does not use the classification 'RESTREINT' in its national system. France handles and protects 'RESTREINT UE/EU RESTRICTED' information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

<sup>3</sup> Sweden: the security classification markings in the top row are used by the Defence authorities and the markings in the bottom row by other authorities.

In case documents or parts thereof contain information not requiring a security classification or requiring a security classification at a lower level, the different elements shall be identified in a separate check list, stating their respective level of classification. In such a case, each document or data storage media shall bear the highest level of classification of the information contained therein.

A higher classification may be assigned to compilations of documents, which individually require a security classification at a lower level, provided the compilation provides an added factor that warrants a higher classification than that applied to its component parts. However, such classification of compilations shall not exceed the highest classification level provided for under this Contract.

Any uncertainties concerning security classifications to be applied or any proposals for changes or amendments shall be addressed to the Agency.

### **ANNEX 3 ACCESS TO THE AGENCY'S PREMISES**

The contractor or sub-contractor and its personnel shall comply with the Agency's internal security and safety rules and regulations and shall follow any instructions given by the Agency's security personnel.

Any failure to comply with the Agency's security or safety instructions may result in access to the premises being denied or the personnel being expelled from Frontex premises.

Unless otherwise agreed with the Agency, contractor or sub-contractor personnel performing work on the Agency's premises or in Member States Authorities' premises, except attendance of meetings with Frontex representatives, shall hold the nationality of an EU Member State and shall hold a security clearance at CONFIDENTIEL UE level or at SECRET UE level, as required, issued by the Contractor's or sub-contractor's responsible national security authority. The Agency may authorise on a case-by-case basis contractor or sub-contractor personnel to perform work on its premises for whom the security clearance procedure has been initiated or is still in progress.

Any information or material provided to the contractor's or sub-contractor's personnel shall be treated as if supplied officially by the Agency.

The contractor shall notify the Agency's designated department at least 5 working days in advance with the names, date of birth, nationality, and where appropriate the details of vehicles, of all contractor or sub-contractor personnel temporary performing work on the Agency's premises.

The Agency shall be entitled to refuse access to its premises to any contractor or sub-contractor personnel without giving justification, as deemed necessary for security reasons.

Any security-related notices or communication to the Agency shall be addressed to:

Security Officer

Frontex


Plac Europejski 6

Warsaw 00-844

Email: [security@frontex.europa.eu](mailto:security@frontex.europa.eu)



## 7.2. Attendance Sheet Form applicable for T&M SCs



FRONTEX

**Year**  
**Month**  
**Specific Contract**  
**Frontex Project Name**  
**Name of Contractor**  
**Name of Consultant**  
**Frontex Project Manager**


	signature of consultant	1 <sup>st</sup> enter time	1 <sup>st</sup> exit time	2 <sup>nd</sup> enter time	2 <sup>nd</sup> exit time	day total time
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
<b>Total time worked</b>						

### 7.3. Invoice support document on consultant's attendance Form

Report on consultant's attendance within Specific Contract No. NN under the Framework contract ref. aaa.bbb.ccc			
Reporting period from:	DD.MM.YYYY	Reporting period to:	DD.MM.YYYY
Report prepared by (Tenderer Contract Manager):		Data and signature:	DD.MM.YYYY
Report approved by (Frontex Contract Manager):		Date and signature:	DD.MM.YYYY

Summary on man-days usage per consultants profile			
Profile	Man-days used in the reporting period	Man-days still available within specific contract	Man-days requested in the specific contract
<i>Project Manager</i>	nn	nn	nn
<i>Subject Matter Expert</i>	nn	nn	nn
<i>SAS Technical Expert</i>	nn	nn	nn
<i>SAS Business Content Developer</i>	nn	nn	nn
<i>Analytical Consultant</i>	nn	nn	nn
<i>Business Consultant</i>	nn	nn	nn

## 7.4. Model Task / Deliverable Acceptance Form

This document is used to formalize the acceptance of the task/deliverable by Frontex. Acceptance constitutes approval of the task/deliverable and will allow for payment processing.

Contract No		Subject	
Order No		Project/Contract Manager	
Business Unit		Prepared by	
Task/Deliverable name (Please give reference to the Terms of Reference and short description of the task or deliverable)			

Criteria for acceptance (as specified in the contract) <sup>4</sup> and verification against contractual provisions	YES/NO	Comments
Quantity		
Compliance with min. requirements (may be copied from the contract)		
Delivery deadline		
Delivery (other aspects)		
The price in line with contractual provisions and payment schedule		
Thoroughly checked for irregularities (if detected, a report and, if applicable, justification accompanied by Record of Exception must be enclosed)		

I hereby declare that the above criteria have been verified and, consequently, I recommend to:

☐ ACCEPT ☐ REJECT ☐ ACCEPT with RESERVATIONS ☐ PARTIAL ACCEPTANCE

**Reservations:**

**Remarks:**

Signature of the Project/Contract Manager Date:

**Final validation** Signature of the HoU/AO Date

<sup>4</sup> The criteria must be copied from the contract, no additional criteria allowed

## 7.5. Declaration of Confidentiality applicable for specific contracts

FWC no.: Frontex/OP/498/2020/AH  
Framework Contract for .....  
Specific Contract No.: .....

### Declaration of confidentiality Contractor's Personnel

I, \_\_\_\_\_ (Name and Surname)

in my function of \_\_\_\_\_ (full Function name),

representing \_\_\_\_\_ (full Company name),

hereby declare that I will treat the information and/or documents that are made available to me or generated in the context of the execution of the above mentioned contract with the strictest secrecy. No such information and/or documents will be divulged to any third parties.

I am aware that tasks carried out in view of the execution and/or performance of this contract also are governed by this principle of secrecy.

I am also aware of the fact that the principle of secrecy pointed out in the first paragraph will continue to apply after the completion of the above mentioned contract.

All information and documents received will be used solely for the execution and/or performance of this contract.

Name of the person: \_\_\_\_\_

Signature: \_\_\_\_\_

Place, date: \_\_\_\_\_

## 7.6. CV Template

First and Last name :		CV last update date:	DD.MM.YYYY
Type of contract with tenderer:	Full Time Employee/ Part Time Employee / B2B	Permanent / Temporary	Duration of the contract (in total until CV last update date ): nn months
Duration of profile related career:	Nn years	Languages (with CEFR level):	
Summary of experience relevant to the personnel profile within FWC for which candidate is proposed:			

Professional Certification		
Name and level of the certificate:	Certifying Authority and dates of certification:	Comments (justification for equivalency):

Hereby I declare that:

- the Consultant, ....., has given consent to submit his/her CV for the procurement procedure ref. Frontex/OP/498/2021/AH.
- the CV has been checked in relation to the profile requirements and the person listed above fully meets the requirements of the indicated profile;

Date:

Place:

Name and signature of the Legal Representative of the Tenderer: