1. The European Union (‘the Union’), represented by the European Commission (‘the Commission’), and the following contracting authorities

<table>
<thead>
<tr>
<th>No.</th>
<th>NAME OF THE INSTITUTION, AGENCY OR BODY</th>
<th>ABBREVIATION</th>
<th>LOCATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>European Parliament</td>
<td>EP</td>
<td>Luxembourg (LU)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Brussels (BE)</td>
</tr>
<tr>
<td>2</td>
<td>Council of the European Union / European Council (Secretariat General)</td>
<td>CONSILIUM</td>
<td>Brussels (BE)</td>
</tr>
<tr>
<td>3</td>
<td>Court of Justice of the European Union</td>
<td>CURIA</td>
<td>Luxembourg (LU)</td>
</tr>
<tr>
<td>4</td>
<td>European Economic and Social Committee</td>
<td>EESC</td>
<td>Brussels (BE)</td>
</tr>
<tr>
<td>5</td>
<td>Committee of the Regions</td>
<td>CoR</td>
<td>Brussels (BE)</td>
</tr>
<tr>
<td>6</td>
<td>European External Action Service</td>
<td>EEAS</td>
<td>Brussels (BE)</td>
</tr>
<tr>
<td>7</td>
<td>European Data Protection Supervisor</td>
<td>EDPS</td>
<td>Brussels (BE)</td>
</tr>
<tr>
<td>8</td>
<td>European Public Prosecutors Office</td>
<td>EPPO</td>
<td>Luxembourg (LU)</td>
</tr>
<tr>
<td>9</td>
<td>Single Resolution Board</td>
<td>SRB</td>
<td>Brussels (BE)</td>
</tr>
<tr>
<td>10</td>
<td>Translation Centre for the Bodies of the European Union</td>
<td>CDT</td>
<td>Luxembourg (LU)</td>
</tr>
<tr>
<td>11</td>
<td>Research Executive Agency</td>
<td>REA</td>
<td>Brussels (BE)</td>
</tr>
<tr>
<td></td>
<td>European Schools (Secretariat-General)</td>
<td>EURSC</td>
<td>Brussels (BE)</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------</td>
<td>-------</td>
<td>---------------</td>
</tr>
<tr>
<td>13</td>
<td>Bio-Based Industries</td>
<td>BBI</td>
<td>Brussels (BE)</td>
</tr>
<tr>
<td>14</td>
<td>Clean Sky</td>
<td>CLEANSKY</td>
<td>Brussels (BE)</td>
</tr>
<tr>
<td>15</td>
<td>Electronic Components and Systems for European Leadership</td>
<td>ECSEL</td>
<td>Brussels (BE)</td>
</tr>
<tr>
<td>16</td>
<td>Fuel Cells and Hydrogen</td>
<td>FCH</td>
<td>Brussels (BE)</td>
</tr>
<tr>
<td>17</td>
<td>Innovative Medicines Initiative</td>
<td>IMI</td>
<td>Brussels (BE)</td>
</tr>
<tr>
<td>18</td>
<td>Single European Sky Air Traffic Management Research 2</td>
<td>SESAR2</td>
<td>Brussels (BE)</td>
</tr>
<tr>
<td>19</td>
<td>Shift2Rail</td>
<td>S2R</td>
<td>Brussels (BE)</td>
</tr>
<tr>
<td>20</td>
<td>European Stability Mechanism</td>
<td>ESM</td>
<td>Luxembourg (LU)</td>
</tr>
<tr>
<td>21</td>
<td>Health and Digital Executive Agency</td>
<td>HaDEA</td>
<td>Brussels (BE)</td>
</tr>
</tbody>
</table>

(collectively, ‘the contracting authority’), represented for the purposes of signing this framework contract by [Director, Directorate C “Digital Workplace and Infrastructure”](#1), [Directorate-General for Informatics](#1), of the one part and

2. **PROXIMUS SA**

PLC under Belgian Public Law

Boulevard du Roi Albert II, 27B – 1030 Brussels

VAT registration number: [hereinafter referred to as "the Contractor"], represented for the purposes of the signature of this contract by [Chief Enterprise Market Officer](#1), on the other part

---

1 Or the person deputising for the signee in his/her absence
HAVE AGREED

to the special conditions (Part I), the general conditions (Part II) for framework contracts, the general terms and conditions for information technologies contracts, version 2.1 (Part III) and the following annexes:

| Annex I | • List of services covered by the contract and schedule of prices |
| Annex II | • EMAS Environmental Policy |
| Annex III | • The latest version of the Tender specifications and their annexes for call for tenders DIGIT/2020/OP/0007 – MTS IV of 15/06/2021, including Commission's replies to objections and questions raised by tenderers during the tendering stage of the procedure, published on eTendering at: [https://etendering.ted.europa.eu/cft/cft-display.html?cftId=7354](https://etendering.ted.europa.eu/cft/cft-display.html?cftId=7354) |
| Annex IV | • Contractor's tender, submitted on 28/06/2021, including all replies by the Contractor to clarification requests made by the Commission during the evaluation stage of Call for tenders DIGIT/2020/OP/0007. |
| Annex V | • Order form and specific contract – Draft Templates² |
| Annex VI | • Performance/Retention Money guarantee – Model Not applicable |
| Annex VII | • Service Level Agreement (SLA) |
| Annex VIII | • Model Consent form for On-Site Personnel (with Privacy Statements) |
| Annex IX | • Template for the electronic list of relevant personal data for on-site Personnel |
| Annex X | • Code of conduct and Consultant’s declaration – template |
| Annex XI | • Technical and organisational measures for the security of personal data |
| Annex XII | • List of sub-processors |
| Annex XIII | • Appendices for Security baseline for external connections – remote service delivery³ |

which form an integral part of this framework contract (‘the FWC’).

This FWC sets out:

---

² Provided order forms and specific contracts are only templates. These templates can be updated and actual order forms and specific contracts can differ from them to adjust to concrete situations.

³ The appendices (Appendix I - “Rules for contractors”, Appendix 2 – “Rules for Service providers working from home” and Appendix 3 – “Acceptable use policy”) apply only for service providers who work remotely and have received IT equipment from the Commission.
1. the procedure by which the contracting authority may order supplies and/or services from the contractor;

2. the provisions that apply to any order form or specific contract which the contracting authority and the contractor may conclude under this FWC; and

3. the obligations of the parties during and after the duration of this FWC.

Any reference to specific contract(s) in this FWC applies also to order form(s).

By submitting a tender, the contractor waives its own terms and conditions. All documents of this nature (end-user agreements, contractor's general conditions, etc.) are held inapplicable, unless explicitly mentioned in the special conditions of this FWC. In all circumstances, in the event of contradiction between this FWC and documents issued by the contractor, this FWC prevails, regardless of any provision to the contrary in the contractor's documents.
# TABLE OF CONTENTS

**PREAMBLE** .......................................................................................................................................................... 7

**I. SPECIAL CONDITIONS** .................................................................................................................................. 8

I.1. Order of precedence of provisions .................................................................................................................... 8
I.2. Subject matter ....................................................................................................................................................... 8
I.3. Entry into force and duration of the FWC .......................................................................................................... 8
I.4. Appointment of the contractor and implementation of the FWC ...................................................................... 9
I.5. Prices ................................................................................................................................................................. 9
I.6. Payment arrangements ....................................................................................................................................... 11
I.7. Bank account ...................................................................................................................................................... 12
I.8. Communication details ..................................................................................................................................... 12
I.9. Processing of personal data ............................................................................................................................ 14
I.10. Termination ....................................................................................................................................................... 15
I.11. Applicable law and settlement of disputes .................................................................................................... 16
I.12. Inter-institutional FWC ................................................................................................................................... 16
I.13. Exploitation of the results of the FWC ............................................................................................................ 16
I.14. Specific derogations to General Conditions and to general terms and conditions for information technologies contracts .................................................................................................................. 18
I.15. Specific definitions .......................................................................................................................................... 21
I.16. Specific quality standards ............................................................................................................................... 22
I.17. Specific security rules for services provided on the premises of the contracting authority in Belgium and for services provided remotely by Personnel having received Commission IT equipment .................................................................................................................. 22
I.18. Extension of background checks to other cases .............................................................................................. 24
I.19. Code of Conduct for contractor’s Personnel working on the premises of the contracting authority and contractor’s Personnel working remotely who have received Commission IT equipment .................................................................................................................. 24
I.20. EMAS compliance ............................................................................................................................................. 26
I.21. Equal opportunities .......................................................................................................................................... 26
I.22. Subcontracting ................................................................................................................................................... 26

**II. GENERAL CONDITIONS FOR THE FRAMEWORK CONTRACT** .............................................. 30

II.1. Definitions ......................................................................................................................................................... 30
II.2. Roles and responsibilities in the event of a joint tender .................................................................................. 32
II.3. Severability ......................................................................................................................................................... 32
II.4. Delivery of supplies / Provision of Services .................................................................................................. 33
II.5. Communication between the parties ............................................................................................................... 38
II.6. Liability ................................................................................................................... 40
II.7. Professional conflicting interests ........................................................................... 41
II.8. Confidentiality ........................................................................................................... 42
II.9. Processing of personal data ....................................................................................... 43
II.10. Subcontracting ......................................................................................................... 45
II.11. Amendments ............................................................................................................ 45
II.12. Assignment .............................................................................................................. 46
II.13. Force Majeure .......................................................................................................... 46
II.14. Liquidated damages ................................................................................................. 46
II.15. Reduction in price .................................................................................................... 47
II.16. Suspension of the implementation of the FWC ....................................................... 48
II.17. Termination of the FWC .......................................................................................... 49
II.18. Invoices, value added tax and e-invoicing ............................................................... 51
II.19. Price revision ........................................................................................................... 53
II.20. Payments and guarantees ........................................................................................ 55
II.21. Recovery .................................................................................................................. 57
II.22. Checks and audits .................................................................................................... 58
II.23. Intellectual property rights ....................................................................................... 60
II.24. Reimbursements ...................................................................................................... 64
PREAMBLE

On 17/05/2021, the Commission, acting on its own behalf and on behalf of the abovementioned contracting authorities, launched the call for tenders under the reference n° DIGIT/2020/OP/0007 (MTS IV), for mobile telephony services.

The contractor was selected for Lot No 1 of Call for tenders No DIGIT/2020/OP/0007 at the conclusion of the evaluation process, on the basis of its tender submitted on 28/06/2021 in response to the invitation to tender.

The present FWC is applicable to all the above-mentioned existing contracting authorities.

References to the contracting authority in the FWC shall be understood, as required by the context, as referring to one of the following concepts:

(a) the Commission acting in its capacity as lead contracting authority;
(b) all the institutions, agencies and bodies covered by the FWC (the participating EUIs/the EUIs), in relation to their collective rights and obligations with the contractor, as one of the parties to the FWC;
(c) any of the participating EUIs acting in its own capacity, in particular for matters related to the conclusion, execution or termination of specific contracts with the contractor;

Newly created institutions, agencies, or bodies may join the FWC at any time by way of an amendment. Such amendment shall take the form of a written notification from the contracting authority to the contractor. This written notification shall have full legal effect from the day following the day on which the notification was sent or on the day indicated therein.
I. SPECIAL CONDITIONS

1.1. ORDER OF PRECEDENCE OF PROVISIONS

If there is any conflict between the provisions of the different parts and annexes of this FWC or the specific contracts signed during its implementation, the following order of precedence shall apply:

(a) special conditions (Part I);
(b) Service Level Agreement (Annex VII);
(c) tender specifications (Annex III);
(d) general conditions (Part II);
(e) general terms and conditions for information technologies contracts (Part III);
(f) Contractor's tender (Annex IV);
(g) Specific contracts signed during the FWC execution;
(h) Technical annexes to the specific contracts (if applicable);
(i) Contractor's formal offers for specific contracts (if applicable).

1.2. SUBJECT MATTER

1.2.1 The subject matter of the FWC is the provision to the contracting authority of Mobile Communications services (including helpdesk).

The products and/or services covered by this contract are listed in Annex I.

1.2.2 The FWC does not confer on the contractor any exclusive right to supply the products and to provide the services referred to in the above paragraph.

1.2.3 All specific contracts shall conform to the provisions set out in the FWC, including its annexes.

1.2.4 Upon implementation of the FWC, the contractor shall supply the products and/or provide the services in accordance with the provisions of the contract, including its annexes.

1.3. ENTRY INTO FORCE AND DURATION OF THE FWC

1.3.1 The FWC enters into force on the date on which the last party signs it.

1.3.2 The implementation of the FWC cannot start before its entry into force.

1.3.3 The FWC is concluded for a period of forty-eight (48) months with effect from the date of its entry into force.
I.3.4 The parties must sign any specific contract before the FWC expires or is terminated. Expiry or termination of the FWC does not automatically terminate the related specific contracts.

The FWC continues to apply to ongoing specific contracts after its expiry or termination. The supplies and/ or services relating to such specific contracts must be delivered/performed no later than nine (9) months after the expiry or termination of the FWC.

I.4. APPOINTMENT OF THE CONTRACTOR AND IMPLEMENTATION OF THE FWC

I.4.1. Appointment of the contractor

The contractor was selected for a single FWC.

I.4.2. Period of provision of the supplies and/or services

The period for the provision of the supplies and/or services starts to run from the date on which the specific contract is signed by the last party, except if otherwise agreed by the parties for the purposes of a specific contract.

I.4.3. Implementation of single FWC

Implementation of the FWC (ordering of supplies and/or services) shall be done according to the workflows defined in Annex VII - Service Level Agreement (SLA).

I.4.4. Delivery of supplies / Provision of services

Article II.4.1 (Delivery of supplies) of the General Conditions is not applicable to this FWC.

Article II.4.2 (Provision of services) of the General Conditions is applicable to this FWC. Delivery of supplies / provision of services shall be done according to the workflows defined in the Service Level Agreement.

I.4.4.1 Delivery of supplies

Delivery of supplies is not applicable to this FWC.

I.5. PRICES

I.5.1. Maximum amount of the FWC and maximum prices

The maximum awarded amount covering all purchases under this FWC, is or will be published in the relevant contract award notice. However, this does not bind the contracting authority to purchase for the maximum amount.

The maximum prices of the supplies and/or services are listed in Annex I.
I.5.2. Price revision index

Price revision is not applicable to this FWC.

**Benchmarking procedure:** Benchmarking is an assessment process carried out by a qualified and objective third party which: tests, evaluates and measures the performance of the contractor by comparison with similar services or products provided by other companies; and/or analyses the evolution of the relation between the prices laid down in the FWC and the market prices for similar or equivalent items ("the benchmarking").

The contracting authority may undertake the benchmarking of the levels and the charges of the supplies and/or services provided under this FWC by comparison with similar or equivalent supplies and/or services provided by outsourcing vendors and/or in-house service providers and suppliers. The result of such benchmarking is available in identical form to both the contracting authority and the contractor.

In order to guarantee that a valid comparison is made, the contracting authority will ensure that:

- the scope of the supplies and/or services being provided by the contractor is taken into consideration;
- the comparison group consists of at least four enterprises to ensure statistical significance;
- the relevant comparison data must be guaranteed.

The benchmarking must not exceed four (4) months.

For the first benchmarking exercise, the comparison group is defined in a document entitled "Comparison Group Definition". The contracting authority reserves the right to change the comparison group algorithm to reflect any changes in its business from time to time.

The independent third party carrying out the benchmarking ('the benchmarker') must be a qualified and objective third party selected by the contracting authority through an appropriate market procedure. The contracting authority must pay all of its own costs and the benchmarker’s costs during the benchmarking. The contractor must pay all of its own costs. Interpretation of the results of the benchmarking must be the sole prerogative of the benchmarker.

The contracting authority and the contractor must set aside sufficient time and resources for each stage of the benchmarking, such as:

- identification and location of benchmarking data,
- performing the benchmarking, and
- implementation of the conclusions of the benchmarker.

The contracting authority and the contractor will be free to suggest changes in benchmarking parameters as the supplies and/or services evolve over the term of this FWC.
The benchmarker must treat as confidential, in accordance with Article II.8, all data provided by the contracting authority and the contractor, and must return all material and media once the benchmarking is completed.

If a benchmarking reveals that the level of a supply and/or service does not reach the comparison group’s product quality levels, the contractor must immediately propose a supply and/or service similar or equivalent to the comparison group’s level, as specified by the benchmarker.

If a benchmarking reveals that charges are higher than the comparison group’s charges, the contractor must immediately reduce its charges to the comparison group level specified by the benchmarker, with effect from the date on which the results of the benchmarking were delivered to the parties.

In the event the contractor has not proposed a similar or equivalent supply and/or service or reduced the price in line with the benchmarker’s specification, the contracting authority may decide not to use the FWC and may consider that the contractor is failing to implement the FWC. The contracting authority may take appropriate measures to terminate the FWC in accordance with Article II.17.1, (c). In this case the contracting authority sends a written notification to the contractor and the former is not required to pay compensation.

In derogation to Article II.8, for the purposes of any benchmarking exercise, and to the extent necessary, the contracting authority is entitled to disclose information or documents to the third party benchmarker.

1.5.3. Reimbursement of expenses

Reimbursement of expenses is not applicable to this FWC.

I.6. PAYMENT ARRANGEMENTS

1. Payments under the FWC shall be made in accordance with Article II.20, which is complemented by Article III.1.5 and the provisions of the specific contracts.

2. Payments shall be executed only if the contractor has fulfilled all its contractual obligations by the date on which the invoice is submitted. Payments requests may not be made if payments for previous orders or specific contracts have not been executed as a result of default or negligence on the part of the contractor.

3. In the event of its budget not being adopted, the contracting authority may, after giving prior notice, pay invoices by monthly instalments. In such cases, it shall notify the contractor once it is in a position to resume normal payment arrangements.

I.6.1. Pre-financing

Pre-financing is not applicable to this FWC.

I.6.2. Interim payment

Interim payment(s), if provided for in the specific contract, shall be made in accordance with the provisions of the specific contract.
I.6.3. Payment of the balance

1. The contractor (or leader in case of a joint tender) may claim the payment of the balance in accordance with Article II.20.6.

The contractor (or leader in case of a joint tender) must send an invoice for payment of the balance due under a specific contract, as provided for in the tender specifications and accompanied by the following (if relevant):

- a declaration on the list of all pre-existing rights to the results or parts of the results, or a declaration stating that there are no such pre-existing rights, as provided for in Article II.23.4;

- the progress report in accordance with the instructions laid down in the relevant annexes;

- when payment is linked to acceptance of supporting documents and/or deliverables, the relevant documents indicated in the specific contract;

2. The contracting authority must approve any submitted documents or supplies/deliverables and pay within thirty 30 days from receipt of the invoice.

3. The contracting authority may suspend the time limit for payment specified in point (2.) in accordance with Article II.20.7.

Once the suspension is lifted, the contracting authority shall give its approval and pay within the remainder of the time-limit indicated in point (2.) unless it rejects partially or fully the submitted documents or supplies/deliverables.

I.6.4. Performance guarantee

Performance guarantee is not applicable to this FWC.

I.6.5. Retention money guarantee

Retention money guarantee is not applicable to this FWC.

I.7. Bank account

Payments must be made to the contractor's (or leader's, in case of a joint tender) single bank account denominated in euro, identified as follows:

Name of bank: KBC Bank N.V.
Full address of branch: Avenue du Port 2
Exact denomination of account holder: Proximus s.a.
Full account number including bank codes: [redacted]
IBAN code: [redacted]

I.8. Communication details

I.8.1 Communication via electronic exchange system
After the entry into force of this FWC, at any time during its course the contracting authority may formally notify in writing the contractor that certain communications will be made by electronic means through the EU Funding & Tenders Portal (the Portal), in accordance with the Portal Terms and Conditions and using the forms and templates provided there. The Portal can be accessed via the Europa website4.

The notification shall indicate whether all or only certain communications under the FWC will take place through the Portal. The notification shall have full legal effect from the date specified therein, which shall allow a reasonable period of time for the contractor to complete all necessary steps to have access to the Portal. The activation of the use of the Portal shall be at no additional cost for the contracting authority.

If the use of the Portal is activated, any communication covered by the activation notification related to the implementation of this FWC and any specific contracts shall be made through the Portal (except if explicitly instructed otherwise by the contracting authority or if communication via the Portal is hindered by factors beyond the control of the parties).

Communications by contractors through the Portal must be made by persons authorised according to the Portal Terms and Conditions. For naming the authorised persons to use the Portal, each contractor must designate before the date of effect of the activation notification a ‘legal entity appointed representative (LEAR)’. The role and tasks of the LEAR are stipulated in their appointment letter (see Portal Terms and Conditions).

If the communication via the Portal is hindered, instructions will be provided by the contracting authority by email and may also be published on the Portal.

During the course of the FWC, the contracting authority reserve(s) the right to further extend the coverage of the communications made through the Portal (if its use has been already activated) or to activate the use of other electronic exchange systems, at no additional cost for the contracting authority.

In case of discrepancy between the clauses of the Portal Terms and Conditions or Terms and Conditions of other electronic exchange system and the clauses of this FWC, the clauses of this FWC (including its annexes) shall prevail.

**1.8.2 Mail or email communication**

For the purpose of this FWC, mail or email communications must be sent to the following addresses:

- **Contracting authority:**
  European Commission
  Directorate-General for Informatics
  Directorate “Strategy and Resources”
  Unit “ICT Procurement and Contracts”
  L-107 01/DCS B-1049 Brussels, Belgium
  Email: DIGIT-CONTRACTS-INFO-CENTRE@ec.europa.eu

---

I.9. PROCESSING OF PERSONAL DATA

I.9.1 Processing of personal data by the contracting authority

For the purpose of Article II.9.1,

(a) the data controller for the personal data contained in this FwC or required for its management is the European Commission;

(b) the data controller for the personal data contained in a specific contract or required for its management is the respective signatory - the European Commission or any other organisational entity which determines the purposes and means of the processing of the personal data;

(c) the data protection notice is available at https://ec.europa.eu/info/data-protection-public-procurement-procedures en.

I.9.2 Processing of personal data by the contractor

For the purpose of Article II.9.2,

(a) The subject matter and purpose of the processing of personal data by the contractor are limited to the provision and support of mobile communication services, satellite communications services and services acquired through this FWC, including but not limited to invoicing and reporting to the contracting authority.

The obligations under Article II.9.2 apply only to the extent that the contractor processes personal data on behalf of the contracting authority, i.e. in its capacity as data processor.

The categories of personal data processed by the contractor include the following: identification data, contact details, invoice and billing data, data related to the usage of services, any other personal data that may be provided by the controller to the contractor or collected directly by the contractor.

The categories of data subjects include the following: employees and service providers of the contracting authority.

(b) The localisation of and access to the personal data processed by the contractor shall comply with the following:

i. the personal data shall be processed within the territory of the European Union and the European Economic Area and will not leave that territory;
ii. the data shall only be held in data centres located with the territory of the European Union and the European Economic Area;

iii. access to data may be given on a need to know basis only to authorised persons established in a country which has been recognised by the European Commission as providing adequate protection to personal data;

iv. the contractor may not change the location of data processing without the prior written authorisation of the contracting authority;

v. in case the contracting authority authorises a transfer of personal data to third countries or international organisations under the FWC, such transfer shall fully comply with the requirements laid down in Chapter V of Regulation (EU) 2018/1725.

(c) If for the performance of the services acquired under this FWC, the contractor determines the purposes and means of the processing of personal data, thus acting as controller, the contractor shall comply with the applicable data protection legislation and in particular with Regulation (EU) No 2016/679, Directive 2002/58/EC and the applicable national laws which implement it. In that case, the contractor shall provide to the contracting authority a privacy statement, in accordance with Articles 13 or 14 of Regulation (EU) 2016/679.

I.10. TERMINATION

I.10.1. Termination without cause

Either party may terminate the FWC or the FWC and specific contract(s) without cause by sending formal notification to the other party with at least six (6) months', prior written notice designating the termination date.

If the FWC or the FWC and a specific contract are terminated:

(a) neither party is entitled to compensation unless provided otherwise in the SLA;

(b) the contractor is entitled to payment only for the supplies and/or services delivered before termination of the respective specific contract takes effect, and only subject to their acceptance.

The second, third and fourth paragraphs of Article II.17.4 apply.

---


I.10.2. Termination with cause
For termination with cause, Article II.17 applies.

I.11. APPLICABLE LAW AND SETTLEMENT OF DISPUTES

I.11.1 The FWC is governed by Union law, complemented, where necessary, by the law of Belgium.

I.11.2 The French-speaking courts of Brussels have exclusive jurisdiction over any dispute regarding the interpretation, application or validity of the FWC.

I.12. INTER-INSTITUTIONAL FWC

I.12.1 This FWC is inter-institutional. The Commission acts on its own behalf and on behalf of the bodies listed in the title of the FWC as the contracting authorities, which provided the lead contracting authority with a power of attorney before FWC signature. The Commission signs the FWC and any amendments on behalf of itself and of all other contracting authorities. The Commission may terminate the FWC on behalf of itself and of all other contracting authorities, unless the termination notice provides that the termination will have effect only with respect to one or several contracting authorities.

I.12.2 Each contracting authority is responsible for the particular specific contracts it awards.

I.12.3 If the contractor has a complaint about the conclusion, performance or termination of a specific contract, the contractor remains bound by its obligations under the FWC and other specific contracts.

I.13. EXPLOITATION OF THE RESULTS OF THE FWC

I.13.1. Detailed list of modes of exploitation of the results
In accordance with Article II.23.1 whereby the Union acquires ownership of the results as defined in this FWC, including the tender specifications, these results may be used for any of the following modes of exploitation:

(a) use for its own purposes:

- making available to the staff of the contracting authority;
- making available to the persons and entities working for the contracting authority or cooperating with it, including contractors, subcontractors whether legal or natural persons;
- making it available to the other Union institutions, agencies and bodies, Member States’ institutions;
- installing, uploading, processing;
- arranging, compiling, combining, retrieving;
- copying, reproducing in whole or in part and in unlimited number of copies.
(b) distribution to the public in hard copies, in electronic or digital format, on the internet including social networks as a downloadable or non-downloadable file;

(c) communication through press information services;

(d) inclusion in widely accessible databases or indexes, such as via ‘open access’ or ‘open data’ portals, or similar repositories, whether freely accessible or accessible only upon subscription;

(e) modifications by the contracting authority or by a third party in the name of the contracting authority, including:
   - shortening;
   - summarising;
   - modifying the content, the dimensions;
   - making technical changes to the content (necessary correction of technical errors), adding new parts or functionalities, changing functionalities, providing third parties with additional information concerning the result (e.g. source code) with a view to making modifications;
   - addition of new elements, paragraphs, titles, leads, bolds, legend, table of content, summary, graphics, subtitles, sound;
   - addition of metadata, for text and data-mining purposes; addition of right-management information; addition of technological protection measures;
   - preparation in audio form, preparation as a presentation, animation, pictograms story, slide-show, public presentation;
   - extracting a part or dividing into parts;
   - incorporating, including by cropping and cutting, the results or parts thereof in other works, such as on websites and webpages;
   - translating, inserting subtitles, dubbing in different language versions:
     - English, French, German;
     - all official languages of EU;
     - languages used within EU;
     - languages of candidate countries.

(f) rights to authorise or license the modes of exploitation set out in any of the points (a) to (e) to third parties, provided however that this does not apply to pre-existing rights and pre-existing materials, if they are only licensed to the Union, except as foreseen by Article II.13.2.;

(g) other adaptations which the parties may later agree; in such case, the following rules apply: the contracting authority must consult the contractor. If necessary, the contractor must in turn seek the agreement of any creator or other right holder and must reply to the contracting authority within one month by providing its agreement, including any suggestions of modifications, free of charge. The contractor may refuse the intended modification only if a creator can demonstrate that the intended modification may harm his/her honour or reputation, thereby violating his/her moral rights.

The modes of exploitation may be defined in more details in the specific contract(s).
The list above is in addition to whatever rights already accrue to the Union on the basis of existing exceptions in the applicable legislation, such as the copyright exception to ensure the proper performance or reporting of administrative proceedings, in cases where such exceptions apply.

**I.13.2. Licence or transfer of pre-existing rights**

All pre-existing rights incorporated in the results, if any, are licensed to the Union as set out in Article II.23.2.

**I.13.3. Provision of list of pre-existing rights and documentary evidence**

The contractor must provide the contracting authority with a declaration on pre-existing rights as set out in Article II.23.4 together with the invoice for payment of the balance at the latest.

**I.14. SPECIFIC DEROGATIONS TO GENERAL CONDITIONS AND TO GENERAL TERMS AND CONDITIONS FOR INFORMATION TECHNOLOGIES CONTRACTS**

**I.14.1** By way of derogation from the definition laid down in the general terms and conditions for information technologies contracts, Article III.1.1, the "Person-Day" is defined as follows:

"Person-day":

Eight (8) hours.

**I.14.2** By way of derogation from general terms and conditions for information technology contracts, the following text replaces the last paragraph of Article III.1.5.3:

"The first invoice shall cover the period from the date of signature of the consignment note, or, where applicable, the Certificate of Conformity of the Software, or, as regards maintenance, from expiry of the guarantee, to the end of the whole period, unless otherwise stated in the FWC."

**I.14.3** By way of derogation from general Terms and conditions for information technology contracts, the following text replaces the last sentence of Article III.1.5.4:

"When the total value of a specific contract relates to an amount of less than €25,000 payment shall be made when the supplies and/or service has been fully provided."

**I.14.4** By way of derogation from general terms and conditions for information technology contracts, Article III.2.1.6 shall read as follows:

"The Contractor undertakes to comply with those quality standards. Compliance with the standards shall be monitored by the Commission. Unless otherwise stated in the Framework contract, in the event of non–compliance with certain standards specifically identified in the Service Level Agreement for the purpose of
application of this clause, over a sliding period of three (3) months, the Contractor shall submit an improvement plan. In the event of non-compliance with those standards for three (3) months, consecutive or not, over a sliding period of six (6) months, a Product whose quality has proved substandard may be withdrawn from the Framework contract, or the Contract may be terminated where the overall quality of the Services is substandard."

I.14.5 By way of derogation from general terms and conditions for information technology contracts, Article III.2.2.2 is hereby modified as follows:

"2.2.2 The contractor and its Personnel, when performing tasks for the contracting authority in execution of this FWC, undertake to comply with:

- COMMISSION DECISION (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission, its subsequent versions, its implementing rules (as adapted from time to time) and the corresponding security notices, and
- COMMISSION DECISION (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information, as well as all its subsequent versions;

- Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission, as well as all its subsequent versions, and

- European Commission's security policies and standards that may be relevant and made available for the implementation of specific contracts."

I.14.6 By way of derogation from general terms and conditions for information technology contracts, Article III.2.2.6 is hereby modified as follows:

"2.2.6 The contractor shall take all appropriate steps for each product to ensure that the data and the magnetic media upon which they are stored are safely preserved. The products supplied shall not contain any mechanism (e.g. viruses) which could compromise their availability, integrity or confidentiality or that of other products. The cost of repairing the damage caused by such a mechanism shall be borne by the contractor.

I.14.7 By way of derogation from general terms and conditions for information technology contracts, Article III.2.2.9 is hereby modified as follows:

“2.2.9 Should the Contractor, during the performance of the tasks which are the subject of the Framework contract, need remote access to any communication and information system of the Commission or data sets processed therein, he shall comply with the Commission’s security rules for remote access. This must be achieved by way of signature of a specific convention for remote access provided by the Commission.”

I.14.8 By way of derogation from general terms and conditions for information technology contracts, Article III.2.4.1 is hereby modified as follows:

"2.4.1 The Contractor undertakes to develop and install the Products and provide the Informatics Services in accordance with the agreed service level agreements and where applicable taking into account the constraints imposed by the existing
Commission’s IT architecture. The Contractor agrees to co-operate with other suppliers to make the Products work with those of these other suppliers. It agrees to attend meetings called for that purpose by the Commission."

**I.14.9** By way of derogation from general terms and conditions for information technology contracts, Article **III.8.1** is hereby replaced as follows:

"III.8.1 Compliance with technical specifications

When providing services of development or maintenance of commissioned software to the contracting authority, the contractor undertakes, in addition to the general quality requirements as specified in the FWC, to observe inter alia the constraints imposed by the existing Commission’s IT architecture”

**I.14.10** By way of derogation from general terms and conditions for information technology contracts, Annex **II**: TEMPLATE OF DECLARATION OF CONFIDENTIALITY, is deleted and replaced by Annex X to the Framework Contract.

**I.14.11** By way of derogation from general terms and conditions for information technology contracts Annex **III** is deleted.

**I.14.12** Where in the general terms and conditions for information technology contracts (GTCITC) there are references to articles of the Special conditions, General conditions for the FWC or other documents, these shall be read as follows:

<table>
<thead>
<tr>
<th>Article of the GTCITC where the reference is made</th>
<th>Article to which reference is made in the text of the GTCITC</th>
<th>To be read as (correspondence to the respective article in the text of this FWC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>III.1.2.1</td>
<td>II.12</td>
<td>II.17.1</td>
</tr>
<tr>
<td>III.9.2.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III.1.5.1</td>
<td>II.4</td>
<td>II.14</td>
</tr>
<tr>
<td>III.3.1.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III.4.1.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III.5.1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III.1.7.6</td>
<td>I.7</td>
<td>I.10</td>
</tr>
<tr>
<td>III.2.1.6</td>
<td>II.1</td>
<td>II.4</td>
</tr>
<tr>
<td>III.2.2.2 Reference to Art. 5 of Commission Decision [C(95) 1510 23/11/95]</td>
<td></td>
<td>See derogations in I.14.5 and I.14.10</td>
</tr>
<tr>
<td>III.2.3.2</td>
<td>II.17</td>
<td>II.23</td>
</tr>
</tbody>
</table>
I.15. Specific definitions

I.15.1. Normal Working Days

By way of derogation from general terms and conditions for information technology contracts, the definition of “Normal working days” in Article III.1.1 is hereby replaced as follows:

"From Mondays to Fridays inclusive, except Commission public holidays in the place of delivery of the services."

I.15.2. Normal Working Hours

By way of derogation from general terms and conditions for information technology contracts, the definition of “Normal working hours” in Article III.1.1 is hereby replaced as follows:

“From 8 a.m. to 6 p.m., on Normal Working Days.”
I.15.3. Work outside normal working days and normal working hours

The definition of work outside normal working days and hours is defined herein below:

In exceptional cases and only on request of the contracting authority, it may be necessary to deliver services outside the normal working days and the normal working hours. For these cases, the following surcharges will be applied:

- Service delivery outside normal working hours (on normal working days and on Commission public holidays not corresponding to a national holiday in the place of delivery of the services): Surcharge of 50% [or x% if the tenderer can quote a different % in the financial offer] of the applicable daily rate, applied prorata temporis.

- Service delivery outside normal working days: Surcharge of 100% [or x% if the tenderer can quote a different % in the financial offer] of the applicable daily rate, applied prorata temporis. The surcharge only applies on the condition that service delivery occurs on Commission public holidays which correspond to a national holiday in the place of delivery of the services; thus, if it is a Commission public holiday but it is not a national holiday in the place of delivery of the services, no surcharge applies.

On request and with the agreement of the contracting authority, surcharges may also apply on a pro-rata basis for effective working hours delivered during the travelling time outside normal working hours.

I.16. Specific Quality Standards

Specific quality requirements will be stated in a Service Level Agreement.

I.17. Specific Security Rules for Services Provided on the Premises of the Contracting Authority in Belgium and for Services Provided Remotely by Personnel Having Received Commission IT Equipment

1. For the purpose of this article, the following definitions apply:

‘Personnel’: persons employed directly or indirectly or contracted by the contractor to implement the FWC.

'On-Site Personnel': personnel who is granted access rights to the Contracting Authority premises in Belgium for a short or long term period, when necessary for executing a specific contract.

2. Pursuant to Articles 3, 7 and 8 of Commission Decision (EU, Euratom) 2015/443 of 13.3.2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41), background checks can be carried out on On-Site Personnel in order to prevent and control risks to the security of Commission staff, assets and information. In addition and pursuant to the Belgian Act of 11.12.1998 on classification and security clearances, security certificates and security advices (Belgian Official Gazette of 7.5.1999, p. 15.752), as further amended, access rights for On-Site Personnel to the premises of the Contracting
Authority may be conditional on a positive security advice to be delivered by the Belgian authorities.

3. In order to allow the Belgian authorities to give a security advice, the Contractor will submit to the relevant On-Site Personnel the attached form (Consent form\(^8\)). The duly completed and signed Consent Form and the taking note of the attached privacy statements will be returned to the Commission Department of Security (European Commission, HR.DS (Security screenings) - Rue de la Loi 200, office BERL 3/190, B-1049 Brussels/Belgium). An up-to-date electronic list of relevant personal data as listed in the attached template\(^9\) will be sent to the address "EC-SECURITY-SCREENING@ec.europa.eu" at least 30 days before the start date of a new contract.

4. Failure or refusal to complete the Consent Form may result in refusal of access rights to Commission buildings for the Personnel.

5. The Contracting Authority acknowledges that in exceptional cases it may not be possible for the Contractor to provide at short-term On-Site Personnel having received a positive security advice. Nevertheless, the Contractor undertakes to provide at all times only On-Site Personnel having received a positive security advice for the following Commission buildings: Berlaymont, Breydel, Charlemagne, Centre Albert Borschette, Luxembourg 46, Montoyer 59 and Madou. This list can be subject to modification upon request from the Commission Department of Security. In such case, the Contracting Authority will duly notify the Contractor of such modification. The Contracting Authority may terminate the specific contract if the Contractor is unable to provide at all times only On-Site Personnel having received a positive security advice for the listed Commission buildings.

6. If access rights for On-Site Personnel are granted by means of a Commission access card, this card remains the property of the Commission and must be returned to the Service Card Office (Rue Montoyer 34 — 1049 Brussels – MEZ/120 – Monday to Friday 08:30-16:30) upon request, upon expiry or where the access conditions are no longer met and in particular where the On-Site Personnel does not benefit anymore from a positive security advice.

If the Commission access card is not returned, the Contracting Authority may claim liquidated damages of 100 EUR from the Contractor for each day of delay up to a maximum of EUR 1,000. This represents a reasonable estimate of fair compensation for the damage incurred.

7. In the case where Contractor's personnel uses Commission IT equipment (normally a laptop PC) and connects to the Commission’s internal network via the remote access service for Commission staff, the Contractor is required to put in place minimum security measures in order to mitigate risks to the security of Commission information during the fulfilment of the contracted services. For this purpose, the Contractor undertakes to comply with the requirements outlined in Annex XIII.
I.18. EXTENSION OF BACKGROUND CHECKS TO OTHER CASES

The background checks, as described under Article I.17 for on-site Personnel working in the premises of the contracting authority, may be extended at any time:

- to the Commission’s places of work located outside Belgium; and/or
- to the participating EUIs, in any of their places of work.

The Commission or a participating EUI that decides to extend the procedure as provided for above shall notify to the Contractor the practical modalities for its implementation. This notification shall have full legal effect under the Framework Contract as from the date indicated in the notification.

I.19. CODE OF CONDUCT FOR CONTRACTOR’S PERSONNEL WORKING ON THE PREMISES OF THE CONTRACTING AUTHORITY AND CONTRACTOR’S PERSONNEL WORKING REMOTELY WHO HAVE RECEIVED COMMISSION IT EQUIPMENT

The contractor commits itself, its Personnel, its subcontractors and their respective personnel, that are providing services to the EU Institutions (Contractor’s Personnel), to the following behaviour and rules:

1. Making sure that the tools placed under his/her responsibility are in good working order (i.e. work material, software, networks etc.) and reporting any incidents to this effect. Use of this equipment and infrastructure, including software and access to information systems, must be limited to professional purposes related to the performance of contractual obligations;

2. Using standard computer equipment (including e-mail and Internet access) and fixed telephones for private purposes is tolerated under the same conditions as for EU Institution staff, i.e. (in summary) as long as such use (i) is on a purely occasional basis and does not amount to extensive use; and (ii) is not for illegal or irregular purposes, in any way that might disrupt the functioning of the service itself or in any manner contrary to the interests of the EU Institution;

3. Respecting any safety and security requirements and procedures laid down by the EU Institution;

4. Not letting in nor bringing any unauthorised person inside the buildings of the EU Institutions;

5. Willingly complying with the requirements of the EU Institution’s security services, including the inspection of the personal goods (by scanner or physical inspection);

6. If, at the EU Institution's discretion, Contractor’s Personnel is entitled to use the parking lots available in EU Institution buildings, they must respect strictly the applicable rules and regulations. Failure to do so will result in the removal of the authorisation;

7. Keeping secret the security procedures as well as protection mechanisms which Contractor’s Personnel may come to gain knowledge about in the process of his/her activities;
8. Never jeopardising the good functioning, the security or the confidentiality of the systems or data which Contractor’s Personnel may have access to within the framework of his/her functions;

9. Never copying illegally, carrying, transmitting nor destroying data, documentation, software or application programs, nor any material (even when obsolete);

10. Never accessing, nor even trying to access data, locations or systems to which Contractor’s Personnel has not been granted access or which he/she does not need to access for the implementation of his/her tasks;

11. Not using software other than that which is usually installed on the desktop/laptop without prior formal approval from the person(s) in charge of one of the domains of this Call for Tenders;

12. If granted with access card(s) - returning the access card(s) before Contractor’s Personnel leaves, at first request by the EU Institution;

13. Showing utmost discretion regarding information which such external staff may come to gain knowledge;

14. Never disclosing information concerning matters dealt with by the EU Institution’s services (be it political, judicial, budgetary or financial affairs, or the management of the EU Institution, the personnel or data processing);

15. On EU Institution premises, Contractor’s Personnel may not perform any professional tasks which are not linked to the FWC

16. Not exerting any pressure on EU Institution officials; in particular, not seeking to obtain any information on on-going or forthcoming procurement procedures which is not already in the public domain and refraining from making any gifts or offers of hospitality to EU Institution officials;

17. Abiding by a very high standard of professional deontology, guided by the principle of fair competition. In particular, Contractor’s Personnel should at all times be courteous, show restraint and avoid any form of harassment and competitor-bashing;

18. Not using the EU Institution premises for marketing or recruitment purposes;

19. Not conveying the impression that Contractor’s Personnel are employed by the EU Institution, or that they are authorised to represent the EU Institution; never writing documents with EU Institution's letterhead paper;

20. Showing EMAS awareness in the daily behaviour - for instance, printing on both sides of the paper, switching off the lights and other equipment, using appropriate bins for waste recycling, etc.

In general, Contractor’s Personnel have to respect the Staff notice on acceptable use of the Commission’s ICT services in force, or similar documents adopted by the other EU Institutions.

When Contractor’s Personnel sends e-mails using the EU Institution e-mail system, he/she has to use an e-mail signature indicating the contract name of the contractor, in addition to his/her own name and the EU Institution unit under which responsibility the contract is performed.
Contractor's Personnel must have the necessary competences in order to perform the service in a professional way. An update of the skills should be foreseen in order to cope with the normal evolution of the software products. Those kinds of trainings cannot incur additional costs for the EU Institution.

I.20. EMAS COMPLIANCE

The contractor shall assist the Commission to perform its commitments as set in the EMAS EC Environmental Policy and shall follow EMAS best practices. The Commission’s EMAS Environmental Policy is contained in Annex II.

Environmental considerations are taken into account throughout the complete life cycle of a product or a service.

I.21. EQUAL OPPORTUNITIES

The contractor shall observe a policy on the promotion of equality and diversity in the implementation of the FWC, by applying the principles of non-discrimination and equality set out in the EU Treaties in full and in their entirety.

In the implementation of the FWC, the contractor shall establish, maintain and promote an open and inclusive working environment which respects human dignity and the principles of equal opportunities, especially through the removal of all obstacles to recruitment and all potential discrimination based on sex, race or ethnic origin, religion or convictions, disability, age or sexual orientation.

I.22. SUBCONTRACTING

I.22.1. Definitions

Subcontracting is the situation where a contract has been or is to be established between the contracting authority and the contractor and where the contractor, in order to carry out that contract, enters into legal commitments with other entities for performing part of the contract.

The contracting authority has no direct legal commitment with the subcontractor(s).

Subcontracting by subcontractors (2nd level of subcontracting) is the situation where a subcontractor enters into legal commitments with other entities (2nd level subcontractors) for performing part of the contract.

For this FWC, subcontracting by subcontractors is not authorised.

Further levels of subcontracting are not authorised.

All contractual tasks may be subcontracted unless this FWC expressly reserves the execution of certain critical tasks to the sole tenderer itself, or in case of a joint tender, to a member of the group.

I.22.2. Contractual relations not considered as subcontracting

The following shall not be considered subcontracting:
a) Use of workers posted to the contractor by another company owned by the same group and established in a Member State (“intra-group posting” as defined by Article 1, 3, (b) of Directive 96/71/EC concerning the posting of workers in the framework of the provision of services).

b) Use of workers hired out to the contractor by a temporary employment undertaking or placement agency established in a Member State (“hiring out of workers” as defined by Article 1, 3, (c) of Directive 96/71/EC concerning the posting of workers in the framework of the provision of services).

c) Use of workers temporarily transferred to the contractor from an undertaking established outside the territory of a Member State and that belongs to the same group (“intra-corporate transfer” as defined by Article 3, (b) of Directive 2014/66/EU on the conditions of entry and residence of third-country nationals in the framework of an intra-corporate transfer).

d) Use of staff without employment contract (“self-employed persons working for the contractor”), without the tasks of the self-employed persons being particular well-defined parts of the contract. These can be either individuals (self-employed natural persons who do not employ other IT service providers), or service providers in one of the following situations: i) sole proprietorships in which only one person (employee or not) is active in providing IT services; ii) companies in which only one person (employee or not) is active in providing IT services and iii) companies in which maximum two persons (employees or not) with family ties are active in providing IT services.

e) Use of suppliers of goods and/or transporters by the contractor, in order to perform the contract at the place of performance.

f) Performance of part of the contract by members of an EEIG (European Economic Interest Grouping), when the EEIG is itself a contractor or a group member.

The persons mentioned in points a), b), c) and d) above will be considered as Personnel of the contractor as defined in the contract. In said cases, the contractor must ensure they comply with all obligations and administrative requirements linked to performing their tasks that derive from the legislation in force of the country(ies) in which they will provide their services under the contract. These obligations may include, amongst others, any obligation to be registered for VAT purposes and/or in an enterprise register or database (e.g. Banque-Carrefour des Entreprises in Belgium). At the request of the contracting authority, the contractor must submit any relevant information, including evidence for the compliance of said persons/entities with their aforementioned obligations.

I.22.3. Rules on replacing or adding subcontractors during contract execution

During contract execution, the contractor may wish to replace a subcontractor or to add a new subcontractor.

The contracting authority may also request the contractor to replace a subcontractor found to be in a situation provided for in points (d) and (e) of Article II.17.1.

In case of multiple FWCs, a contractor may not subcontract to another contractor in the same Lot.
The contractor may subcontract without the need to require the prior written authorisation from the contracting authority in the case of subcontractors proposed in the contractor’s Tender (Annex IV) that were not excluded, replaced or removed before the contract signature.

Prior authorisation from the contracting authority is necessary for all cases not covered by the previous paragraph.

The procedures to request authorisation for the use of subcontractors at FWC level and at specific contract level are described below.

**I.22.4. Procedure to request authorization for subcontractors at FWC level**

To replace a subcontractor or to add a new subcontractor at FWC level, the contractor shall submit a formal request for authorization by e-mail to contracting authority’s e-mail address specified in Article I.8. The authorisation request should contain:

- exact name, official address, registration/VAT number of the new subcontractor and its contact details;
- updated descriptive document on subcontracting, requested at tender submission, containing, among others, a list and clear identification of all subcontractors, reasons to subcontract, roles and activities of each subcontractor and the volume / proportion of the subcontracting.
- all the documents requested at tender submission for the replaced subcontractors (in case of replacement) or for subcontractors on whose capacity the tenderer did not rely to fulfil the selection criteria, if any (in case of adding a new subcontractor).

The new subcontractor may not start performing tasks under the contract until the contracting authority provides an explicit written authorisation for subcontracting.

**I.22.5. Procedure to request authorization for subcontractors at specific contracts level**

To add a new subcontractor (i.e. subcontractor not already authorised at FWC level) at the level of a given specific contract, the request for authorization shall be included in the proposal/offer for a specific contract (containing the exact name, official address, registration/VAT number of the new subcontractor and contact details) along with reasons to subcontract and explanation for the involvement and type of services the subcontractor will perform. The request of authorisation shall be accompanied by a declaration of absence of an exclusion situation under Article 137(1) 4th paragraph of the Financial Regulation and a Letter of Intent / Commitment Letter duly signed by an authorised representative of the proposed subcontractor stating that the new entity will put the resources necessary for the performance of the contract at disposal of the contractor.

The authorisation is provided with the acceptance of the offer and signature of the specific contract by the contracting authority.

**I.22.6. Obligations of the contractor in case of subcontracting**

In case of subcontracting the contractor remains bound by its contractual obligations and is solely responsible for the implementation of the FWC.
The contractor must ensure that the subcontracting does not affect the rights of the contracting authority under this FWC, particularly those under Articles II.8, II.9, II.22 and II.23.

For services provided at a facility that is directly under the oversight of the contracting authority (intra-muros services), the contractor must, at the contracting authority's request, indicate the names, contacts and authorised representatives of subcontractors involved in the performance of the contract, including any changes of subcontractors.

SIGNATURES

For the contractor,

Proximus S.A.

Chief Enterprise Market Officer

Signature[s]: ____________________

Done on [date]

For the contracting authority,

Director

Qualified electronic signature by:

Date: 2021-10-12 13:56:14 +02:00

Signature[s]/: ____________________

Done on [date]

Parties explicitly agree that this contract is validly signed in one of the below manners in English:
a) in paper format in duplicate; or
b) in electronic form, with both parties using qualified electronic signature QES; or
c) by one party signing in paper format and the other party signing with QES.

Each party shall receive or have access to an original signed by both parties, and if this is not possible – to the original signed by the other party.

---

10 Or the person deputising for the signee in his/her absence

11 If signed with qualified electronic signature (QES) - signature details can be viewed in the metadata of the pdf document in the Signature Panel of Adobe Acrobat Reader

12 If signed with qualified electronic signature (QES) - signature date can be viewed in the metadata of the pdf document in the Signature Panel of Adobe Acrobat Reader
II. **GENERAL CONDITIONS FOR THE FRAMEWORK CONTRACT**

II.1. **DEFINITIONS**

For the purpose of this FWC, the following definitions apply:

‘**Back office**’: the internal system(s) used by the parties to process electronic documents such as orders and invoices;

‘**Breach of obligations**’: failure by the contractor to fulfil one or more of its contractual obligations.

‘**Confidential information or document**’: any information or document received by either party from the other or accessed by either party in the context of the implementation of the FWC, that any of the parties has identified in writing as confidential. It may not include information that is publicly available;

‘**Creator**’: means any natural person who contributes to the production of the result;

‘**EDI message**’: an electronic document structured by using an agreed standard, prepared in a computer readable format and capable of being automatically and unambiguously processed;

‘**Electronic exchange system**’: is an electronic exchange system meeting the requirements of Article 148 of 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

‘**Force majeure**’: any unforeseeable, exceptional situation or event beyond the control of the parties that prevents either of them from fulfilling any of their obligations under the FWC. The situation or event may not be attributable to error or negligence on the part of the parties or on the part of the subcontractors and must prove to be inevitable despite their exercising due diligence. Defaults, defects in equipment or material or delays in making them available, labour disputes, strikes and financial difficulties may not be invoked as force majeure, unless they stem directly from a relevant case of force majeure;

‘**Formal notification**’ (or ‘formally notify’): form of communication between the parties made in writing, expressly indicated to be formal notification in this FWC.

‘**Fraud**’: an act or omission committed in order to make an unlawful gain for the perpetrator or another by causing a loss to the Union’s financial interests and relating to: i) the use or presentation of false, incorrect or incomplete statements or documents, which has as its effect the misappropriation or wrongful retention of funds or assets from the Union budget, ii) the non-disclosure of information in violation of a specific obligation with the same effect or iii) the misapplication of such funds or assets for purposes other than those for which they were originally granted, which damages the Union’s financial interests;
'Grave professional misconduct': a violation of applicable laws or regulations or ethical standards of the profession to which a contractor or a related person belongs, including any conduct leading to sexual or other exploitation or abuse, or any wrongful conduct of the contractor or a related person which has an impact on its professional credibility where such conduct denotes wrongful intent or gross negligence.

‘Implementation of the FWC’: the purchase of supplies and/or services envisaged in the FWC through the signature and performance of specific contracts;

‘Interoperability network’: independent third party platforms enforcing the European standards and Directives on cross-border interoperability in a certain domain.

‘In writing’ or ‘written’: any worded or numbered expression that can be read, reproduced, and later communicated, and includes, without being limited to information transmitted and stored by electronic means. ‘Irregularity’: any infringement of a provision of Union law resulting from an act or omission by an economic operator, which has, or would have, the effect of prejudicing the Union’s budget;

‘Notification’ (or ‘notify’): form of communication between the parties made in writing including by electronic means;

‘Order form’: a form by which the contracting authority orders supplies and related maintenance under this FWC;

‘Performance of a specific contract’: the performance of tasks and delivery of the purchased supplies/services by the contractor to the contracting authority;

‘Personnel’: persons employed directly or indirectly or contracted by the contractor to implement the FWC;

‘Portal’: EU Funding & Tenders Portal; electronic exchange system managed by the European Commission and used by itself and other EU institutions, bodies, offices or agencies for the management of their funding, prizes and procurement.

‘Pre-existing material’: any material, document, technology or know-how which exists prior to the contractor using it for the production of a result in the implementation of the FWC;

‘Pre-existing right’: any industrial and intellectual property right on pre-existing material; it may consist in a right of ownership, a licence right and/or right of use belonging to the contractor, the creator, the contracting authority as well as to any other third parties;

‘Professional conflicting interest’: a situation in which the contractor’s previous or ongoing professional activities affect its capacity to implement the FWC or to perform a specific contract to an appropriate quality standard;

‘Related person’: any natural or legal person who is a member of the administrative, management or supervisory body of the contractor or who has powers of representation, decision or control with regard to the contractor;

'Result': any intended outcome of the implementation of the FWC, whatever its form or nature. A result may be further defined in this FWC as a deliverable. A result may, in addition to newly created materials produced specifically for the contracting authority by the contractor or at its request, also include pre-existing materials;
‘Request for supplies/services’: a document from the contracting authority requesting that the contractors provide a specific offer for supplies/services whose terms are not entirely defined under the FWC;

‘Specific contract’: a contract implementing the FWC and specifying details of a service to be provided;

II.2. ROLES AND RESPONSIBILITIES IN THE EVENT OF A JOINT TENDER

In the event of a joint tender submitted by a group of economic operators and where the group does not have legal personality or legal capacity, one member of the group is appointed as leader of the group.

II.3. SEVERABILITY

Each provision of this FWC is severable and distinct from the others. If a provision is or becomes illegal, invalid or unenforceable to any extent, it must be severed from the remainder of the FWC. This does not affect the legality, validity or enforceability of any other provisions of the FWC, which continue in full force and effect. The illegal, invalid or unenforceable provision must be replaced by a legal, valid and enforceable substitute provision which corresponds as closely as possible with the actual intent of the parties under the illegal, invalid or unenforceable provision. The replacement of such a provision must be made in accordance with Article II.11. The FWC must be interpreted as if it had contained the substitute provision as from its entry into force.
II.4. Delivery of Supplies / Provision of Services

II.4.1. Delivery of Supplies

II.4.1.1 Signature of the FWC does not guarantee any actual purchase. The contracting authority is bound only by specific contracts implementing the FWC.

II.4.1.2 The contractor must comply with the minimum requirements provided for in the tender specifications. This includes compliance by the contractor and its subcontractors with applicable obligations under environmental, social and labour law established by Union law, national law and collective agreements or by the international environmental, social and labour law provisions listed in Annex X to Directive 2014/24/EU\(^\text{13}\), compliance with data protection obligations resulting from Regulation (EU) 2016/679\(^\text{14}\) and Regulation (EU) 2018/1725\(^\text{15}\).

II.4.1.3 All periods specified in the FWC are calculated in calendar days, unless otherwise specified.

II.4.1.4 The contractor must not present itself as a representative of the contracting authority and must inform third parties that it is not part of the European public service.

II.4.1.5 The contractor is responsible for the Personnel who perform the contract and exercises its authority over its Personnel without interference by the contracting authority. The contractor must inform its Personnel that:

(a) they may not accept any direct instructions from the contracting authority; and

(b) their participation in providing the supplies does not result in any employment or contractual relationship with the contracting authority.

II.4.1.6 The contractor must ensure that the Personnel implementing the FWC and any future replacement Personnel possess the professional qualifications and experience required to provide the supplies, as the case may be on the basis of the selection criteria set out in the tender specifications.

II.4.1.7 At the contracting authority’s reasoned request, the contractor must replace any member of Personnel who:

(a) does not have the expertise required to provide the supplies; or

---

\(^{13}\) OJ L 94 of 28.03.2014, p. 65.


(b) has caused disruption at the premises of the contracting authority.

The contractor bears the cost of replacing its Personnel and is responsible for any delay in providing the supplies resulting from the replacement of Personnel.

II.4.1.8 The contractor must record and report to the contracting authority any problem that affects its ability to deliver the supplies. The report must describe the problem, state when it started and what action the contractor is taking to resolve it.

**II.4.1.9 Delivery**

(a) **Time allowed for delivery**

The time allowed for delivery is calculated in accordance with Article I.4.

(b) **Date, time and place of delivery**

The contracting authority must be notified in writing of the exact date of delivery within the period indicated in Article I.4. All deliveries must be made at the agreed place of delivery during the hours indicated in Article I.4.

The contractor must bear all costs and risks involved in delivering the supplies to the place of delivery.

(c) **Consignment note**

Each delivery must be accompanied by a consignment note in duplicate, duly signed and dated by the contractor or its carrier, giving the specific contract number and particulars of the supplies delivered. One copy of the consignment note must be countersigned by the contracting authority and returned to the contractor or to its carrier.

**II.4.1.10 Certificate of conformity**

Signature of the consignment note by the contracting authority, as provided for in point (c) of Article II.4.1.9 is simply an acknowledgment of the fact that the delivery took place and in no way implies conformity of the supplies with the order form.

Conformity of the supplies delivered must be evidenced by the signature of a certificate to this effect by the contracting authority no later than one month after the date of delivery, unless otherwise specified in the special conditions, in the general terms and conditions for information technologies contracts or in the tender specifications.

Conformity must be declared only where the conditions laid down in the FWC and in the order form are satisfied and the supplies are in conformity with the tender specifications.

If, for reasons attributable to the contractor, the contracting authority is unable to accept the supplies, the contractor must be notified in writing at the latest by the deadline for conformity.

**II.4.1.11 Conformity of the supplies delivered with the FWC**

The supplies delivered by the contractor to the contracting authority must be in conformity in quantity, quality, price and packaging with the FWC and the relevant order form.
The supplies delivered must:

(a) correspond to the description given in the tender specifications and possess the characteristics of the supplies provided by the contractor to the contracting authority as a sample or model;

(b) be fit for any specific purpose required of them by the contracting authority and made known to the contractor at the time of conclusion of this FWC and accepted by the contractor;

(c) be fit for the purposes for which supplies of the same type are normally used;

(d) demonstrate the high quality standards and performance which are normal in supplies of the same type and which the contracting authority can reasonably expect, given the nature of the supplies and taking into account any public statements on the specific characteristics of the supplies made by the contractor, the producer or its representative, particularly in advertising or on labelling; in accordance with the state of the art in the industry and the provisions of this FWC, in particular the tender specifications and the terms of its tender.

(e) be packaged according to the usual method for supplies of the same type or, failing this, in a way designed to preserve and protect them.

II.4.1.12 Remedy

The contractor must be liable to the contracting authority for any lack of conformity which exists at the time the supplies are verified.

In case of lack of conformity, without prejudice to Article II.14 on liquidated damages applicable to the total price of the supplies concerned, the contracting authority is entitled:

(a) either to have the supplies brought into conformity, free of charge, by repair or replacement;

(b) or to have an appropriate reduction made in the price.

Any repair or replacement must be completed within a reasonable time and without any significant inconvenience to the contracting authority, taking account of the nature of the supplies and the purpose for which they are required by the contracting authority.

The term ‘free of charge’ in paragraph (a) refers to the costs incurred to bring the supplies into conformity, particularly the cost of postage, labour and materials.

II.4.1.13 Assembly

If required by tender specifications, the contractor must assemble the supplies delivered within a period of one month unless otherwise specified in the special conditions.

Any lack of conformity resulting from incorrect installation of the supplies must be deemed to be equivalent to lack of conformity of the supplies if installation forms part of the FWC and the supplies were installed by the contractor or under its responsibility. This applies equally if the product was to be installed by the contracting authority and was incorrectly installed due to a shortcoming in the installation instructions.
II.4.1.14 Services provided to supplies

If required by the tender specifications, services to supplies must be provided accordingly.

II.4.1.15 General provisions concerning supplies

(a) Packaging

The supplies must be packaged in strong boxes or crates or in any other way that ensures that the contents remain intact and prevents damage or deterioration. Packaging, pallets, etc., including contents, must not weigh more than 500 kg.

Unless otherwise specified in the special conditions or in the tender specifications (Annex III), pallets must be considered as one-way packaging and must not be returned. Each box must be clearly labelled with the following information:

- Name of contracting authority and address for delivery;
- name of contractor;
- description of contents;
- date of delivery;
- number and date of order form;
- EC code number of article.

(b) Guarantee

The supplies must be guaranteed against all defects in manufacture or materials for two years from the date of delivery, unless provision is made for a longer period in the tender specifications.

The contractor must guarantee that any permits and licences required for manufacturing and selling the supplies have been obtained.

The contractor must replace at its own expense, within a reasonable time limit to be determined by agreement between the parties, any items which become damaged or defective in the course of normal use during the guarantee period.

The contractor is liable for any conformity defect which exists at the time of delivery, even if this defect does not appear until a later date.

The contractor is also liable for any conformity defect which occurs after delivery and is ascribable to non-compliance with its obligations, including failure to provide a guarantee that, for a certain period, supplies used for the purposes for which they are normally used or for a specific purpose will preserve their qualities or characteristics as specified.

If part of an item is replaced, the replacement part must be guaranteed under the same terms and conditions for a further period of the same duration as that specified above.

If a defect is found to originate in a systematic flaw in design, the contractor must replace or modify all identical parts incorporated in the other supplies that are part of the order,
even though they may not have been the cause of any incident. In this case, the guarantee period must be extended as stated above.

**II.4.2. Provision of services**

II.4.2.1 Signature of the FWC does not guarantee any actual purchase. The contracting authority is bound only by specific contracts implementing the FWC.

II.4.2.2 The contractor must provide services of high quality standards, in accordance with the state of the art in the industry and the provisions of this FWC, in particular the tender specifications and the terms of its tender. Where the Union has the right to make modifications to the results, they must be delivered in a format and with the necessary information, which effectively allow such modifications to be made in a convenient manner.

II.4.2.3 The contractor must comply with the minimum requirements provided for in the tender specifications. This includes compliance by the contractor and its subcontractors with applicable obligations under environmental, social and labour law established by Union law, national law and collective agreements or by the international environmental, social and labour law provisions listed in Annex X to Directive 2014/24/EU, compliance with data protection obligations resulting from Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.

II.4.2.4 The contractor must obtain any permit or licence required in the State where the services are to be provided.

II.4.2.5 All periods specified in the FWC are calculated in calendar days, unless otherwise specified.

II.4.2.6 The contractor must not present itself as a representative of the contracting authority and must inform third parties that it is not part of the European public service.

II.4.2.7 The contractor is responsible for the Personnel who carry out the services and exercises its authority over its Personnel without interference by the contracting authority. The contractor must inform its Personnel that:

a) they may not accept any direct instructions from the contracting authority; and

b) their participation in providing the services does not result in any employment or contractual relationship with the contracting authority.
II.4.2.8 The contractor must ensure that the Personnel implementing the FWC and any future replacement Personnel possess the professional qualifications and experience required to provide the services, as the case may be on the basis of the selection criteria set out in the tender specifications.

II.4.2.9 At the contracting authority’s reasoned request, the contractor must replace any member of Personnel who:

a) does not have the expertise required to provide the services; or

b) has caused disruption at the premises of the contracting authority.

The contractor bears the cost of replacing its Personnel and is responsible for any delay in providing the services resulting from the replacement of Personnel.

II.4.2.10 The contractor must record and report to the contracting authority any problem that affects its ability to provide the services. The report must describe the problem, state when it started and what action the contractor is taking to resolve it.

II.4.3. Changes in the exclusion situation

The contractor must immediately inform the contracting authority of any changes in the exclusion situations as declared, according to Article 137 (1) of Regulation (EU) 2018/1046

II.5. COMMUNICATION BETWEEN THE PARTIES

II.5.1. Form and means of communication

Any notifications, communication of information or exchange of documents under the FWC must be made in writing, in the language of the contract and must clearly identify the FWC number and specific contract number, if applicable.

Communication between the parties can take place:

- by electronic means, via electronic exchange system, in accordance with the provisions of Article II.5.2.,
- by electronic means, via email, in accordance with the provisions of Article II.5.3.,
- on paper, via mail - by courier service with proof of delivery or by registered post with proof of delivery, in accordance with the provisions of Article II.5.4.

In the cases where this FWC mandates the use of formal notifications, those formal communications are considered to have been made with their receipt by the receiving party. The specific rules when formal notifications are considered to have been received are provided in Sections II.5.2.2, II.5.3.2 and II.5.4.2 below.

Communication details to be used for all communication between the parties are indicated in Article I.8.
II.5.2. Communication via electronic exchange system (EES)

The contracting authority may use an EES for all exchanges with the contractor during the implementation of the contract.

If communication via the EES is hindered by factors beyond the control of one party, it must notify the other party immediately and the parties must take the necessary measures to restore this communication via the EES. Upon such notification, the parties shall use alternative means of communication until communication via electronic exchange system is restored. The provisions applicable to alternative means of communication are described in Articles II.5.3 and II.5.4 below.

If the EES is temporarily unavailable, the sending party cannot be considered in breach of its obligation to send a communication within a specified deadline. In any event, for reasons linked to business continuity, the contracting authority reserves the right to use alternative means of communication at any moment.

II.5.2.1 Date of communication via electronic exchange system for other than formal notifications

Notifications through the EES are generally considered to have been made when they are sent by the sending party (i.e. on the date and time they are sent through the EES) as indicated by the time logs.

II.5.2.2 Date of communication via electronic exchange system for formal notifications

The receiving date for formal notifications made through the EES will be the date and time the communication is accessed, as indicated by the time logs. Formal notifications that have not been accessed within 10 days after sending, will be considered to have been accessed.

II.5.3. Communication via email

When communicating via e-mail, the parties should send their messages to the email addresses indicated in Article I.8.

II.5.3.1 Date of communications via email for other than formal notifications

Without prejudice to Article II.19.1. below and Point 31.3 of Annex I to the Financial Regulation, notifications via email are generally considered to have been made and the email is deemed to have been received by the receiving party on the date of dispatch of that e-mail, if it is sent to the email address indicated in Article I.8 and does not have characteristics that could reasonably prevent its proper delivery (such as sending extremely voluminous e-mails that can be blocked for their size or emails containing elements that the majority of the spam filers would block). The sending party must be able to prove the date of dispatch. If the sending party sends the email to the email address indicated in Article I.8 and receives a non-delivery report, it must make every reasonable effort to ensure that the other party receives the communication.
II.5.3.2 Date of communications via email for formal notifications

Formal notifications by email are considered to have been received on the date of dispatch of a return email expressly or impliedly acknowledging receipt. In case no email is received by the party who sent the formal notification within a reasonable period, the formal notification should be re-sent via courier service with proof of delivery or registered post (see Article II.5.4.2 below).

II.5.4. Communication via mail

As a rule, mail is used by way of exception for formal notifications and as alternative means of communication when the other means are not available.

When communicating via mail, the parties should send their letters to the postal addresses indicated in Article I.8.

II.5.4.1 Date of communications via mail for other than formal notifications

Without prejudice to Article 116 of the Financial Regulation, notifications via mail are generally considered to have been made at the date of receipt by the receiving party.

Payment requests sent to the contracting authority via mail are deemed to be received on the date when they are registered by the authorised department of the authorizing officer responsible.

II.5.4.2 Date of communications via mail for formal notifications

Formal notifications by courier service with proof of delivery are considered to have been received on the date indicated in the proof of delivery. Formal notifications by registered post with proof of delivery are considered to have been received either on the delivery date registered by the postal service or the deadline for collection at the post office.

II.6. LIABILITY

II.6.1 The contracting authority is not liable for any damage or loss caused by the contractor, including any damage or loss to third parties during or as a consequence of implementation of the FWC.

II.6.2 If required by the relevant applicable legislation, the contractor must take out an insurance policy against risks and damage or loss relating to the implementation of the FWC. It must also take out supplementary insurance as reasonably required by standard practice in the industry. Upon request, the contractor must provide evidence of insurance coverage to the contracting authority.

II.6.3 The contractor is liable for any loss or damage caused to the contracting authority during or as a consequence of implementation of the FWC, including in the event of subcontracting, but only to an amount not exceeding three times the total amount of the relevant specific contract However, if the damage or loss is caused by the gross negligence, wilful misconduct or Grave professional misconduct of
the contractor or of its Personnel or subcontractors, as well as in the case of an action brought against the contracting authority by a third party for breach of its intellectual property rights and/or applicable data protection laws, the contractor is liable for the whole amount of the damage or loss.

II.6.4 If a third party brings any action against the contracting authority in connection with the implementation of the FWC, the contractor must assist the contracting authority in the legal proceedings, including by intervening in support of the contracting authority upon request.

If the contracting authority’s liability towards the third party is established and that such liability is caused by the contractor during or as a consequence of the implementation of the FWC, Article II.6.3 applies.

II.6.5 If the contractor is composed of two or more economic operators (i.e. who submitted a joint tender), they are all jointly and severally liable to the contracting authority for the implementation of the FWC.

II.6.6 The contracting authority is not liable for any loss or damage caused to the contractor during or as a consequence of implementation of the FWC, unless the loss or damage was caused directly by wilful misconduct or gross negligence of the contracting authority.

II.7. PROFESSIONAL CONFLICTING INTERESTS

II.7.1 The contractor must take all the necessary measures to prevent any situation of professional conflicting interest.

II.7.2 The contractor must notify the contracting authority in writing as soon as possible of any situation that could constitute a professional conflicting interest during the implementation of the FWC. The contractor must immediately take action to rectify the situation.

The contracting authority may do any of the following:

(a) verify that the contractor’s action is appropriate;
(b) require the contractor to take further action within a specified deadline;
(c) decide not to award a specific contract to the contractor.

II.7.3 The contractor must pass on all the relevant obligations in writing to:

(a) its Personnel;
(b) any natural person with the power to represent it or take decisions on its behalf;
(c) third parties involved in the implementation of the FWC, including subcontractors.

The contractor must also ensure that the persons referred to above are not placed in a situation which could give rise to professional conflicts of interest.

II.7.4 The contractor declares:
(a) that it has not made, and will not make, any offer of any type whatsoever from which an unlawful advantage can be derived under the FWC;
(b) that it has not granted and will not grant, has not sought and will not seek, has not attempted and will not attempt to obtain, and has not accepted and will not accept, any advantage, financial or in kind, to or from any party whatsoever, where such advantage constitutes an illegal practice or involves corruption, either directly or indirectly, inasmuch as it is an incentive or reward relating to the FWC.

II.8. CONFIDENTIALITY

II.8.1. The contracting authority and the contractor must treat with confidentiality any information or documents, in any format, disclosed in writing or orally relating to the implementation of the FWC and identified in writing as confidential.

II.8.2. Each party must:

(a) not use confidential information or documents for any purpose other than to perform its obligations under the FWC or a specific contract without the prior written agreement of the other party;
(b) ensure the protection of such confidential information or documents with the same level of protection as its own confidential information or documents, and in any case with due diligence;
(c) not disclose directly or indirectly, confidential information or documents to third parties without the prior written agreement of the other party.

II.8.3 The confidentiality obligation set out in this Article is binding upon the contracting authority and the contractor during the implementation of the FWC and for as long as the information or documents remain confidential unless:

(a) the disclosing party agrees to release the receiving party from the confidentiality obligation earlier;
(b) the confidential information or documents become public through other means than a breach of the confidentiality obligation,
(c) the applicable law requires the disclosure of the confidential information or documents.

II.8.4 The contractor must obtain from any natural person with the power to represent it or take decisions on its behalf, as well as from third parties involved in the implementation of the FWC a commitment that they will comply with this Article. At the request of the contracting authority, the contractor must provide a document providing evidence of this commitment.

II.8.5 The contractor may give access to the personal data processed under this FWC to its Personnel, but should strictly limit the access to solely those people who must have access to the personal data to allow the contractor to perform its obligations under the FWC. The contractor shall inform the Personnel concerned in writing of the confidential nature of the personal data, and of the legislative and contractual framework concerning the personal data, and shall contractually impose a confidentiality obligation upon the persons concerned.
II.9. PROCESSING OF PERSONAL DATA

II.9.1 Processing of personal data by the contracting authority

Any personal data included in or relating to the FWC, including its implementation, shall be processed in accordance with Regulation (EU) No 2018/1725. Such data shall be processed solely for the purposes of the implementation, management and monitoring of the FWC by the data controller.

The contractor or any other person whose personal data is processed by the data controller in relation to this FWC has specific rights as a data subject under Chapter III (Articles 14-25) of Regulation (EU) No 2018/1725, in particular the right to access, rectify or erase their personal data and the right to restrict or, where applicable, the right to object to processing or the right to data portability.

Should the contractor or any other person whose personal data is processed in relation to this FWC have any queries concerning the processing of its personal data, it shall address itself to the data controller. They may also address themselves to the Data Protection Officer of the data controller. They have the right to lodge a complaint at any time to the European Data Protection Supervisor.

Details concerning the processing of personal data are available in the data protection notice referred to in Article I.9.

II.9.2 Processing of personal data by the contractor as processor

The processing of personal data by the contractor shall meet the requirements of Regulation (EU) No 2018/1725 and be processed solely for the purposes set out by the controller.

The contractor shall assist the controller for the fulfilment of the controller’s obligation to respond to requests for exercising rights of person whose personal data is processed in relation to this FWC as laid down in Chapter III (Articles 14-25) of Regulation (EU) No 2018/1725. The contractor shall inform without delay the controller about such requests.

The contractor may act only on documented written instructions and under the supervision of the controller, in particular with regard to the purposes of the processing, the categories of data that may be processed, the recipients of the data and the means by which the data subject may exercise its rights.

The contractor shall grant Personnel access to the data to the extent strictly necessary for the implementation, management and monitoring of the FWC. The contractor must ensure that Personnel authorised to process personal data has committed itself to confidentiality or is under appropriate statutory obligation of confidentiality in accordance with the provisions of Article II.8.

The contractor shall adopt appropriate technical and organisational security measures, giving due regard to the risks inherent in the processing and to the nature, scope, context and purposes of processing, in order to ensure, in particular, as appropriate:

(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
(e) measures to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

The contractor shall notify relevant personal data breaches to the controller without undue delay and at the latest within 48 hours after the contractor becomes aware of the breach. In such cases, the contractor shall provide the controller with at least the following information:

(a) nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) likely consequences of the breach;
(c) measures taken or proposed to be taken to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

The contractor shall immediately inform the data controller if, in its opinion, an instruction infringes Regulation (EU) 2018/1725, Regulation (EU) 2016/679, or other Union or Member State data protection provisions as referred to in the tender specifications.

The contractor shall assist the controller for the fulfilment of its obligations pursuant to Article 33 to 41 under Regulation (EU) 2018/1725 to:

(a) ensure compliance with its data protection obligations regarding the security of the processing, and the confidentiality of electronic communications and directories of users;
(b) notify a personal data breach to the European Data Protection Supervisor;
(c) communicate a personal data breach without undue delay to the data subject, where applicable;
(d) carry out data protection impact assessments and prior consultations as necessary.

The processor shall at least implement the technical and organisational measures specified in Annex XI to ensure the security of the personal data.

The contractor shall maintain a record of all data processing operations carried on behalf of the controller, transfers of personal data, security breaches, responses to requests for exercising rights of people whose personal data is processed and requests for access to personal data by third parties.

The contracting authority is subject to Protocol 7 of the Treaty on the Functioning of the European Union on the privileges and immunities of the European Union, particularly as regards the inviolability of archives (including the physical location of data and services as set out in Article I.9.2) and data security, which includes personal data held on behalf of the contracting authority in the premises of the contractor or subcontractor.

The contractor shall notify the contracting authority without delay of any legally binding request for disclosure of the personal data processed on behalf of the contracting authority made by any national public authority, including an authority from a third
country. The contractor may not give such access without the prior written authorisation of the contracting authority.

The duration of processing of personal data by the contractor will not exceed the period referred to in Article II.22.2. Upon expiry of this period, the contractor shall, at the choice of the controller, return, without any undue delay in a commonly agreed format, all personal data processed on behalf of the controller and the copies thereof or shall effectively delete all personal data unless Union or national law requires a longer storage of personal data.

The controller hereby provides its general authorization for the engagement of the sub-processors included in Annex XII (List of sub-processors). The contractor shall inform in writing the controller of any intended changes concerning the addition or replacement of sub-processors at least thirty (30) days prior to such changes, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object. In case the controller objects to the engagement of a sub-processor, the parties shall work together in good faith to find a mutually acceptable solution to address the objection. If the parties do not reach a mutually acceptable solution within a reasonable timeframe, the controller shall have the right to terminate the relevant service, without penalty, by providing written notice before the end of the notice period.

The contractor shall pass on the obligations referred to in Articles I.9.2 and II.9.2 in writing to those parties, including subcontractors by way of a contract. At the request of the contracting authority, the contractor shall provide evidence of this commitment, including the non-confidential parts of the contract with the sub-processor.

The contractor shall remain fully responsible to the controller for the performance of the sub-processor’s obligations in accordance with its contract with the contractor. The contractor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

II.10. SUBCONTRACTING

The rules on subcontracting are detailed in Article I.22 of the Special Conditions.

II.11. AMENDMENTS

II.11.1 Any amendment to the FWC or a specific contract must be made in writing before all contractual obligations have been fulfilled. A specific contract does not constitute an amendment to the FWC.

II.11.2 Any amendment must not make changes to the FWC or a specific contract that might alter the minimum requirements of the initial procurement procedure or result in unequal treatment of tenderers or contractors.
II.12. ASSIGNMENT

II.12.1 The contractor may not assign any of the rights and obligations arising from the FWC, including claims for payments or factoring, without prior written authorisation from the contracting authority. In such cases, the contractor must provide the contracting authority with the identity of the intended assignee.

II.12.2 Any right or obligation assigned by the contractor without authorisation is not enforceable against the contracting authority.

II.13. FORCE MAJEURE

II.13.1 If a party is affected by force majeure, it must immediately notify the other party, stating the nature of the circumstances, their likely duration and foreseeable effects.

II.13.2 A party is not liable for any delay or failure to perform its obligations under the FWC if that delay or failure is a result of force majeure. If the contractor is unable to fulfil its contractual obligations due to force majeure, it has the right to remuneration only for the supplies/services actually delivered and which obtain a certificate of conformity.

II.13.3 The parties must take all necessary measures to limit any damage due to force majeure.

II.14. LIQUIDATED DAMAGES

II.14.1. Liquidated damages for failure of the Contractor to perform obligations within the applicable time limits

For any issues not explicitly regulated by the Service Level Agreement, should the Contractor fail to perform his obligations under the Contract within the time limits set by the Contract or to deliver a result for which a firm and binding time limit is agreed, and without prejudice to the Contractor's actual or potential liability incurred in relation to the Contract or to the Commission's right to terminate the Contract, the contracting authority may decide to impose liquidated damages of 0.5% of the amount of the relevant Specific Contract(s) per calendar day of delay or non-compliance.

The total maximum amount of liquidated damages that can be imposed shall be capped to 50% of the value of the relevant Specific Contract(s) for which the Contractor is in breach.

II.14.2. Precedence of liquidated damages foreseen in the Service Level Agreement

Unless otherwise stipulated in the Service Level Agreement and for the key performance indicators defined therein, the Service Level Agreement liquidated damages prevail over the liquidated damages foreseen above.
II.14.3. Procedure

The contracting authority must formally notify the contractor of its intention to apply liquidated damages and the corresponding calculated amount.

The contractor has 30 days following the date of receipt to submit observations. Failing that, the decision becomes enforceable the day after the time limit for submitting observations has elapsed.

If the contractor submits observations, the contracting authority, taking into account the relevant observations, must notify the contractor:

(a) of the withdrawal of its intention to apply liquidated damages; or

(b) of its final decision to apply liquidated damages and the corresponding amount.

II.14.4. Nature of liquidated damages

The parties expressly acknowledge and agree that any amount payable under this Article is not a penalty and represents a reasonable estimate of fair compensation for the damage incurred due to failure to provide the supplies/services within the applicable time limits or with regard to the required quality and security levels set out in this FWC (including the ones set out in the Service Level Agreement and in the tender specifications).

II.14.5. Claims and liability

Any claim for liquidated damages does not affect the contractor’s actual or potential liability or the contracting authority’s rights under Article II.17.

II.15. REDUCTION IN PRICE

II.15.1. Quality standards

If the contractor fails to deliver the supply and/or provide the services in accordance with the FWC or a specific contract (‘unperformed obligations’) or if it fails to deliver the supply and/or provide the services in accordance with the expected quality and security levels specified in the tender specifications (‘low quality delivery’), the contracting authority may reduce or recover payments proportionally to the seriousness of the unperformed obligations or low quality delivery. This includes in particular cases where the contracting authority cannot approve a document or deliver a certificate of conformity for supply as defined in Article I.6 after the contractor has submitted the required additional information, correction or new supply.

A reduction in price may be imposed together with liquidated damages under the conditions of Article II.14.

II.15.2. Procedure

The contracting authority must formally notify the contractor of its intention to reduce payment and the corresponding calculated amount.

The contractor has 30 days following the date of receipt to submit observations. Failing that, the decision becomes enforceable the day after the time limit for submitting observations has elapsed.
If the contractor submits observations, the contracting authority, taking into account the relevant observations, must notify the contractor:

(a) of the withdrawal of its intention to reduce payment; or

(b) of its final decision to reduce payment and the corresponding amount.

II.15.3. Claims and liability

Any reduction in price does not affect the contractor’s actual or potential liability or the contracting authority’s rights under Article II.17.

II.16. SUSPENSION OF THE IMPLEMENTATION OF THE FWC

II.16.1. Suspension by the contractor

If the contractor is affected by force majeure, it may suspend the performance of a specific contract.

The contractor must immediately notify the contracting authority of the suspension. The notification must include a description of the force majeure and state when the contractor expects to resume the performance of the contract.

The contractor must notify the contracting authority as soon as it is able to resume performance of the specific contract, unless the contracting authority has already terminated the FWC or the specific contract.

II.16.2. Suspension by the contracting authority

The contracting authority may suspend the implementation of the FWC or performance of a specific contract or any part of it:

(a) if the procedure for awarding the FWC or a specific contract or the implementation of the FWC proves to have been subject to irregularities, fraud or breach of obligations;

(b) in order to verify whether the presumed irregularities, fraud or breach of obligations have actually occurred.

The contracting authority must formally notify the contractor of the suspension and the reasons for it. Suspension takes effect on the date of formal notification, or at a later date if the formal notification so provides.

The contracting authority must notify the contractor as soon as the verification is completed whether:

(a) it is lifting the suspension; or

(b) it intends to terminate the FWC or a specific contract under Article II.17.1(f) or (j).

The contractor is not entitled to compensation for suspension of any part of the FWC or a specific contract.
The contracting authority may in addition suspend the time allowed for payments in accordance with Article II.20.7.

II.17. TERMINATION OF THE FWC

II.17.1. Grounds for termination by the contracting authority

The contracting authority may terminate the FWC and/or any ongoing specific contract in the following circumstances:

(a) if provision of the supplies and/or services under an ongoing specific contract has not actually started within 15 days of the scheduled date and the contracting authority considers that the new date proposed, if any, is unacceptable, taking into account Article II.11.2;

(b) if the contractor is unable, through its own fault, to obtain any permit or licence required for implementation of the FWC;

(c) if the contractor does not implement the FWC or perform the specific contract in accordance with the tender specifications or request for supplies/services or is in breach of another substantial contractual obligation or repeatedly refuses to sign specific contracts. Termination of three or more specific contracts in these circumstances also constitutes grounds for termination of the FWC;

(d) if the contractor or any person that assumes unlimited liability for the debts of the contractor is in one of the situations provided for in points (a) and (b) of Article 136(1) of the Financial Regulation16;

(e) if the contractor or any related person is subject to any of the situations provided for in points (c) to (f) of Article 136(1) or to Article 136(2) of the Financial Regulation;

(f) if the procedure for awarding the FWC or the implementation of the FWC prove to have been subject to irregularities, fraud or breach of obligations;

(g) if the contractor or its subcontractors do not comply with applicable obligations under environmental, social and labour law established by Union law, national law, collective agreements or by the international environmental, social and labour law provisions listed in Annex X to Directive 2014/24/EU;

(h) if the contractor is in a situation that constitutes a professional conflicting interest as referred to in Article II.7;

(i) if a change to the contractor’s legal, financial, technical, organisational or ownership situation is likely to substantially affect the implementation of the FWC or substantially modify the conditions under which the FWC was initially awarded or a change regarding the exclusion situations listed in Article 136 of

---

Regulation (EU) 2018/1046 that calls into question the decision to award the contract;

(j) in the event of force majeure, where either resuming implementation is impossible or the necessary ensuing amendments to the FWC or a specific contract would mean that the tender specifications are no longer fulfilled or result in unequal treatment of tenderers or contractors;

(k) if the needs of the contracting authority change and it no longer requires new supplies and/or services under the FWC; in such cases ongoing specific contracts remain unaffected;

(l) if the termination of the FWC with one or more of the contractors means that the multiple FWC with reopening of competition no longer has the minimum required level of competition;

(m) if the contractor is in breach of the data protection obligations resulting from Article II.9.2;

(n) if the contractor does not comply with the applicable data protection obligations resulting from Regulation (EU) 2016/679;

(o) where the contracting authority has evidence that the contractor or any related entity or person has violated any provisions on security and confidentiality included in the FWC and its annexes;

(p) For specific services, where the Commission has evidence or seriously suspects the Contractor of, active or passive, intentional or negligent, disclosure of any data or information issued by the EU institutions and transferred through the network of the contractor during the performance of the current contract, to any authorities, legal or natural persons, with the sole exception of relevant formal requests submitted by EU judicial authorities for the purpose of criminal investigations.

II.17.2. Grounds for termination by the contractor

The contractor may terminate the FWC and/or any ongoing specific contract if the contracting authority fails to comply with its obligations, in particular the obligation to provide the information needed for the contractor to implement the FWC or to perform a specific contract as provided for in the tender specifications.

II.17.3. Procedure for termination

A party must formally notify the other party of its intention to terminate the FWC or a specific contract and the grounds for termination.

The other party has 30 days following the date of receipt to submit observations, including the measures it has taken or will take to continue fulfilling its contractual obligations. Failing that, the decision to terminate becomes enforceable the day after the time limit for submitting observations has elapsed.

If the other party submits observations, the party intending to terminate must formally notify it either of the withdrawal of its intention to terminate or of its final decision to terminate.
In the cases referred to in points (a) to (d), (g) to (i) and (k) to (p) of Article II.17.1 and in Article II.17.2, the date on which the termination takes effect must be specified in the formal notification.

In the cases referred to in points (e), (f) and (j) of Article II.17.1, the termination takes effect on the day following the date on which the contractor receives notification of termination.

In addition, at the request of the contracting authority and regardless of the grounds for termination, the contractor must provide all necessary assistance, including information, documents and files, to allow the contracting authority to complete, continue or transfer the service or delivery of the supplies to a new contractor or internally, without interruption or adverse effect on the quality or continuity of the service or delivery of the supplies. The parties may agree to draw up a transition plan detailing the contractor’s assistance unless such plan is already detailed in other contractual documents or in the tender specifications. The contractor must provide such assistance at no additional cost, except if it can demonstrate that it requires substantial additional resources or means, in which case it must provide an estimate of the costs involved and the parties will negotiate an arrangement in good faith.

**II.17.4. Effects of termination**

The contractor is liable for damage incurred by the contracting authority as a result of the termination of the FWC or a specific contract including the additional cost of appointing and contracting another contractor to provide or complete the supplies/service, except if the damage is a result of a termination in Article II.17.1 (j), (k) or (l) or Article II.17.2. The contracting authority may claim compensation for such damage.

The contractor is not entitled to compensation for any loss resulting from the termination of the FWC or specific contract, including loss of anticipated profits, unless the loss was caused by the situation specified in Article II.17.2.

The contractor must take all appropriate measures to minimise costs, prevent damage and cancel or reduce its commitments.

Within 60 days of the date of termination, the contractor must submit any report and any invoice required for supplies/service that were provided before the date of termination.

In case of joint tenders, the contracting authority may terminate the FWC or a specific contract with each member of the group separately on the basis of points (d), (e), (g), (m) and (n) of Article II.17.1, under the conditions set out in Article II.11.2.

**II.18. INVOICES, VALUE ADDED TAX AND E-INVOICING**

**II.18.1. Invoices and value added tax**

Invoices must contain the contractor’s (or leader’s in case of a joint tender) identification data, the amount, the currency and the date, as well as the FWC reference and reference to the specific contract.

Invoices must indicate the place of taxation of the contractor (or leader in case of a joint tender) for value added tax (VAT) purposes and must specify separately amounts not including VAT and amounts including VAT.
The contracting authority is exempt from all taxes and duties, including VAT, in accordance with Articles 3 and 4 of the Protocol 7 of the Treaty on the Functioning of the European Union on the privileges and immunities of the European Union.

The contractor (or leader in case of a joint tender) must complete the necessary formalities with the relevant authorities to ensure that the supplies and/or services required for implementation of the FWC are exempt from taxes and duties, including VAT.

The contractor shall have sole responsibility for compliance with the tax laws which apply to him. Failure to comply shall make the relevant invoices invalid.

In Belgium, use of this contract constitutes a request for VAT exemption No. 450, Article 42, paragraph 3.3 of the VAT code (circular 2/1978), provided the invoice includes the statement: 'Exonération de la TVA, Article 42, paragraphe 3.3 du code de la TVA (circulaire 2/1978)'.

In Luxembourg, the contractor must include the following statement in the invoices: "Commande destinée à l’usage officiel de l’Union européenne. Exonération de la TVA Article 43 § 1 k 2ème tiret de la loi modifiée du 12.02.79. ‘In the case of intra-Community purchases, the statement to be included in the invoices is: "For the official use of the European Union. VAT Exemption / European Union/ Article 151 of Council Directive 2006/112/EC.’

In other countries, use of this contract constitutes a request for VAT exemption, pursuant to articles 3 and 4 of the Protocol on the privileges and immunities of the European Union. The contractor must receive and keep in his records the form entitled "VAT and Excise Duty Exemption Certificate", duly completed and signed by the contracting authority. The invoice(s) must include the following statement: "VAT Exemption/International Body/Article 151 of Council Directive 2006/112/EC."

For invoices sent to the contracting authority via email, the reception date must be considered as the date on which the invoice arrives in the functional mailbox of the contracting authority. The functional mailbox in which the invoices are to be sent, should be provided in the specific contracts.

II.18.2. E-invoicing

The contractor (or leader in case of a joint tender) submits invoices in electronic format if the conditions regarding electronic signature specified by Directive 2006/112/EC on VAT are fulfilled, i.e. using a qualified electronic signature or through electronic data interchange.

E-invoices must be submitted by electronic means through the Portal, in accordance with the Portal Terms and Conditions and using the forms and templates provided there, or through means of supported interoperability networks compliant with the Directive 2014/55/EU on electronic invoicing in public procurement.
II.19. PRICE REVISION

If Article I.5.2 refers to a formula governing price revision, then the provisions set out in this Article apply.

II.19.1. Yearly price revision

The Parties agree that the prices shall be subject to a yearly price revision according to the provisions set out below.

II.19.2. Date of effect of the yearly price revisions

Price revisions shall always be applicable on 1st January. For a FWC signed during calendar year N, the first price revision shall be calculated as set out below during year N+1 and become applicable on the 1st January of year N+2.

However, when a product or service was not included in a FWC from the beginning, but introduced through an amendment signed in year O, otherwise than as a result of a Change Request, the first price revision for that product or service shall be calculated during year O+1 and become applicable on the 1st January of year O+2.

As regards Hardware, Complex and Other Than Complex Hardware, and unless otherwise agreed by the Parties, when a product is introduced into the FWC through an amendment signed in year P as a result of a Change Request after the procedure set out in section II.19.3 below has been initiated, the new product shall bear the price of the product it replaces, i.e. the non-revised price for the remainder of year P, and the revised price as from the 1st January of year P+1.

II.19.3. Procedure for calculating the yearly price revision

Between 1 July and 30 September every year, the contracting authority shall send to the Contractor an initial written notification informing the latter about the result of the calculation of the yearly price revision.

The contractor has 30 days following the date of receipt to submit observations against the result of the calculation made by the contracting authority. In absence thereof, the initial written notification sent by the contracting authority shall acquire the status of an amendment with full legal effect and enters into force the day after the time limit for submitting observations has elapsed.

Should the Contractor formulate any observations on the correctness of the calculation made pursuant to paragraph 1 above within the deadline set out in paragraph 2 above, the contracting authority shall carefully and expeditiously consider them.

Following this assessment, the contracting authority shall send to the Contractor, within one month from the receipt of Contractor’s letter, a final written notification including the result of the calculation of the yearly price revision. If applicable, this letter should state the reasons having led to the rejection of the observations put forward by the Contractor.

The final written notification sent by the contracting authority shall immediately enter into force and acquire the status of an amendment with full legal effect, but the Contractor shall be free to seek appropriate remedies.

Should, exceptionally, the contracting authority fail to initiate the procedure as set out above, the Contractor may, until 15 October, give formal notice to the contracting
authority requiring the latter to send the initial written notification. The contracting authority shall comply with this requirement within 15 calendar days from receipt of the contractor’s letter. Paragraphs 2, 3, 4 and 5 above shall apply thereafter.

Should the contracting authority not act as provided for in paragraph 1 above, nor the Contractor as provided for in paragraph 6, the yearly price revision shall not apply for the relevant yearly period.

II.19.4. Formula for the yearly price revisions

The yearly price revisions shall be calculated using the following formula:

\[ Pr = Po \times \frac{Ir}{Io} \]

where:

\( Pr \) = Revised price

\( Po \) = Original price in the tender (or, if applicable, in the amendment introducing the price for the service or product for the first time)

\( Ir \) = Index for the month of May of the year in which the yearly price revision is calculated

\( Io \) = Index for the month in which the FWC (or, if applicable, the amendment introducing the price for the service or product for the first time) entered into force

the quotient of \( \frac{Ir}{Io} \) is rounded to the fourth decimal.

II.19.5. Indices to be used for the yearly price revisions

For services: As regards Services, the revision shall be based on the trend in the index “Harmonised Indices of Consumer Prices (HICP all items)”, under “First Published Data (prc_hicp_fp)”, published on Eurostat’s official website.

For supplies: As regards Hardware, Complex and Other Than Complex Hardware, the revision shall be based on the trend in the index “Producer prices in industry, domestic market - monthly data [sts_inppd_m]” (PPI NACE C262), published on Eurostat’s official website.

The precise index to be used is indicated in Article I.5.2.

In case of a change in the base year of an index, the values of \( Io \) and \( Ir \) shall be adapted accordingly on the basis of the official figures published by Eurostat using the latest base year.

Should Eurostat cease to publish any of the indices referred to above, the contracting authority shall —as part of the procedure set out in paragraph II.19.3 above— base the calculation of the revised price on the most similar index which is available, providing reasons for its choice.
II.19.6. Prices applicable for supply and service purchases

The contracting authority shall purchase Hardware, Complex and Other Than Complex Hardware on the basis of the prices applicable on the date of signature of the Specific Contract by the last contracting party.

The contracting authority shall purchase Services on the basis of the prices applicable on the date which is indicated as start date (start of the tasks) of the Specific Contract.

II.20. PAYMENTS AND GUARANTEES

II.20.1. Date of payment

The date of payment is deemed to be the date on which the contracting authority’s account is debited.

II.20.2. Currency

Payments are made in euros, unless another currency is provided for in Article I.7.

II.20.3. Conversion

The contracting authority makes any conversion between the euro and another currency at the daily euro exchange rate published in the Official Journal of the European Union, or failing that, at the monthly accounting exchange rate, as established by the European Commission and published on the website indicated below, applicable on the day when it issues the payment order.

The contractor makes any conversion between the euro and another currency at the monthly accounting exchange rate, established by the Commission and published on the website indicated below, applicable on the date of the invoice.

http://ec.europa.eu/budget/contracts_grants/info_contracts/inf euro/inf_euro_en.cfm

II.20.4. Costs of transfer

The costs of the transfer are borne as follows:

(a) the contracting authority bears the costs of dispatch charged by its bank;
(b) the contractor bears the costs of receipt charged by its bank;
(c) the party causing repetition of the transfer bears the costs for repeated transfer.

II.20.5. Pre-financing, performance and retention money guarantees

If, as provided for in Article I.6, a financial guarantee is required for the payment of pre-financing, as performance guarantee or as retention money guarantee, it must fulfil the following conditions:

(a) the financial guarantee is provided by a bank or a financial institution approved by the contracting authority or, at the request of the contractor and with the agreement of the contracting authority, by a third party; and
(b) the guarantee shall have the effect of making the bank or financial institution or the third party provide irrevocable collateral security, or stand as first-call guarantor of contractor’s obligations without requiring that the contracting authority has recourse against the principal debtor (the contractor).

The contractor bears the cost of providing such guarantee.

Pre-financing guarantees must remain in force until the pre-financing is cleared against interim payments or payment of the balance. Where the payment of the balance takes the form of a debit note, the pre-financing guarantee must remain in force for three months after the debit note is sent to the contractor. The contracting authority must release the guarantee within the following month.

Performance guarantees cover compliance with substantial contractual obligations until the contracting authority has given its final approval for the supply/service. The performance guarantee must not exceed 10% of the total price of the specific contract. The contracting authority must release the guarantee fully after final certificate of conformity of the supply has been delivered and/or the services were approved, as provided for in the specific contract.

Retention money guarantees cover full delivery of the supplies/service in accordance with the specific contract including during the contract liability period and until their final certificate of conformity has been delivered by the contracting authority. The retention money guarantee must not exceed 10% of the total price of the specific contract. The contracting authority must release the guarantee after the expiry of the contract liability period as provided for in the specific contract.

The contracting authority must not request a retention money guarantee for a specific contract where it has requested a performance guarantee.

II.20.6. Interim payments and payment of the balance

The contractor (or leader in case of a joint tender) must send an invoice for interim payment, as provided for in Article I.6 or in the tender specifications or in the specific contract.

The contractor (or leader in case of a joint tender) must send an invoice for payment of the balance within 60 days of the end of the period of provision of the supplies/service, as provided for in Article I.6, in the tender specifications or in the specific contract.

Payment of the invoice and approval of documents does not imply recognition of the regularity, authenticity, completeness and correctness of the declarations and information they contain.

Payment of the balance may take the form of recovery.

II.20.7. Suspension of the time allowed for payment

The contracting authority may suspend the payment periods specified in Article I.6 at any time by notifying the contractor (or leader in case of a joint tender) that its invoice cannot be processed. The reasons the contracting authority may cite for not being able to process an invoice are:

(a) because it does not comply with the FWC;
(b) because the contractor has not produced the appropriate supplies/deliverables or documents; or

(c) because the contracting authority has observations on the supplies/deliverables or documents submitted with the invoice.

The contracting authority must notify the contractor (or leader in case of a joint tender) as soon as possible of any such suspension, giving the reasons for it. In cases b) and c) referred above, the contracting authority shall notify the contractor (or leader in case of a joint tender) the time limits to submit additional information or corrections or a new version of the documents or deliverables if the contracting authority requires it.

Suspension takes effect on the date the contracting authority sends the notification. The remaining payment period resumes from the date on which the requested information or revised documents are received or the necessary further verification, including on-the-spot checks, is carried out. Where the suspension period exceeds two months, the contractor (or leader in case of a joint tender) may request the contracting authority to justify the continued suspension.

Where the payment periods have been suspended following rejection of a document referred to in the first paragraph of this Article and the new document produced is also rejected, the contracting authority reserves the right to terminate the specific contract in accordance with Article II.17.1(c).

II.20.8. Interest on late payment

On expiry of the payment periods specified in Article I.6, the contractor (or leader in case of a joint tender) is entitled to interest on late payment at the rate applied by the European Central Bank for its main refinancing operations in euros (the reference rate) plus eight points. The reference rate is the rate in force, as published in the C series of the Official Journal of the European Union, on the first day of the month in which the payment period ends.

Suspension of the payment period as provided for in Article II.20.7 is not considered as giving rise to late payment.

Interest on late payment covers the period running from the day following the due date for payment up to and including the date of payment as defined in Article II.20.1.

However, when the calculated interest is EUR 200 or less, it must be paid to the contractor (or leader in case of a joint tender) only if it requests it within two months of receiving late payment.

II.21. RECOVERY

II.21.1. Principle

If an amount is to be recovered under the terms of the FWC, the contractor must repay the contracting authority the amount in question.
II.21.2. Recovery procedure

Before recovery, the contracting authority must formally notify the contractor of its intention to recover the amount it claims, specifying the amount due and the reasons for recovery and inviting the contractor to make any observations within 30 days of receipt.

If no observations have been submitted or if, despite the observations submitted, the contracting authority decides to pursue the recovery procedure, it must confirm recovery by formally notifying a debit note to the contractor, specifying the date of payment. The contractor must pay in accordance with the provisions specified in the debit note.

If the contractor does not pay by the due date, the contracting authority may, after informing the contractor in writing, recover the amounts due:

(a) by offsetting them against any amounts owed to the contractor by the Union or by the European Atomic Energy Community or by an executive agency when it implements the Union budget:

(b) by calling in a financial guarantee if the contractor has submitted one to the contracting authority;

(c) by taking legal action.

II.21.3. Interest on late payment

If the contractor does not honour the obligation to pay the amount due by the date set by the contracting authority in the debit note, the amount due bears interest at the rate indicated in Article II.20.8. Interest on late payments will cover the period starting on the day after the due date for payment and ending on the date when the contracting authority receives the full amount owed.

Any partial payment is first entered against charges and interest on late payment and then against the principal amount.

II.21.4. Recovery rules in case of joint tender

If the contract is signed by a group (joint tender), the group is jointly and severally liable under the conditions set out in Article II.6 (liability). The contracting authority shall send the debit note first to the leader of the group.

If the leader does not pay by the due date the whole amount, and if the amount due cannot be offset or can only be offset partially in accordance with Article II.21.2 (a), then the contracting authority may claim the amount still due to any other member or members of the group by respectively notifying them with a debit note in conformity with the provisions laid down in Article II.21.2.

II.22. Checks and audits

II.22.1 The contracting authority and/or the European Anti-Fraud Office (OLAF) may check or require an audit on the implementation of the FWC themselves, or authorise any outside body to do so on their behalf.
Such checks and audits may be initiated at any moment during the provision of the supplies/services and up to five years starting from the payment of the balance of the last specific contract issued under this FWC.

The audit procedure is initiated on the date of receipt of the relevant letter sent by the contracting authority. Audits are carried out on a confidential basis.

II.22.2 The contractor must keep all original documents stored on any appropriate medium, including digitised originals if authorised under national law, for a period of five years starting from the payment of the balance of the last specific contract issued under this FWC.

II.22.3 The contractor must grant the contracting authority’s staff and outside Personnel authorised by the contracting authority the appropriate right of access to sites and premises where the FWC is implemented and to all the information, including information in electronic format, needed to conduct such checks and audits. The contractor must ensure that the information is readily available at the moment of the check or audit and, if so requested, that information is handed over in an appropriate format.

II.22.4 On the basis of the findings made during the audit, a provisional report is drawn up. The contracting authority or its authorised representative must send it to the contractor, who has 30 days following the date of receipt to submit observations. The contractor must receive the final report within 60 days following the expiry of the deadline to submit observations.

On the basis of the final audit findings, the contracting authority may recover all or part of the payments made in accordance with Article II.21 and may take any other measures which it considers necessary.

II.22.5 In accordance with Council Regulation (Euratom, EC) No. 2185/96 of 11 November 1996 concerning on-the-spot checks and inspection carried out by the Commission in order to protect the European Communities’ financial interests against fraud and other irregularities and Regulation (EU, Euratom) No. 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office, the European Anti-Fraud Office may carry out investigations, including on the spot checks and inspections, to establish whether there has been fraud, corruption or any other illegal activity under the contract affecting the financial interests of the Union. Findings arising from an investigation may lead to criminal prosecution under national law.

The investigations may be carried out at any moment during the performance of the contract and up to five years starting from the payment of the balance of the last specific contract issued under this FWC.

II.22.6 The Court of Auditors and the European Public Prosecutor’s Office established by Council Regulation (EU) 2017/1939¹⁷ (‘the EPPO’) and, for the processing of personal data, the European Data Protection Supervisor have the same rights as the contractor to conduct checks and audits.

contracting authority and the controller, particularly right of access, for the purpose of checks, audits and investigations.

II.23. INTELLECTUAL PROPERTY RIGHTS

II.23.1. Ownership of the rights in the results

The Union acquires irrevocably worldwide ownership of the results and of all intellectual property rights on the newly created materials produced specifically for the Union under the FWC and incorporated in the results, without prejudice however to the rules applying to pre-existing rights on pre-existing materials, as per Article II.23.2.

The intellectual property rights so acquired include any rights, such as copyright and other intellectual or industrial property rights, to any of the results and to all technological solutions and information created or produced by the contractor or by its subcontractor in implementation of the FWC. The contracting authority may exploit and use the acquired rights as stipulated in this FWC. The Union acquires all the rights as from the moment the contractor has created the results.

The payment of the price includes any fees payable to the contractor about the acquisition of ownership of rights by the Union including for all modes of exploitation and of use of the results.

II.23.2. Licensing rights on pre-existing materials

Unless provided otherwise in the special conditions, the Union does not acquire ownership of pre-existing rights under this FWC.

The contractor licenses the pre-existing rights on a royalty-free, non-exclusive and irrevocable basis to the Union, which may use the pre-existing materials for all the modes of exploitation set out in this FWC or in specific contracts. Unless otherwise agreed, the licence is non-transferable and cannot be sub-licensed, except as provided hereafter:

(a) the pre-existing rights can be sub-licensed by the contracting authority to persons and entities working for it or cooperating with it, including contractors and subcontractors, whether legal or natural persons, but only for the purpose of their mission for the Union;

(b) if the result is a "document" such as a report or a study, and it is meant to be published, the existence of pre-existing materials in the result may not prevent the publication of the document, its translation or its "reuse", it being understood however that the "reuse" may only be made of the result as a whole and not of the pre-existing materials taken separately from the result; for the sake of this provision, "reuse" and "document" have the meaning given by the Commission Decision of 12 December 2011 on the reuse of Commission documents (2011/833/EU).

All pre-existing rights are licensed to the Union from the moment the results are delivered and approved by the contracting authority.

The licensing of pre-existing rights to the Union under this FWC covers all territories worldwide and is valid for the duration of intellectual property rights protection.
The payment of the price as set out in the specific contracts is deemed to also include any fees payable to the contractor in relation to the licensing of pre-existing rights to the Union, including for all forms of exploitation and of use of the results.

Where implementation of the FWC requires that the contractor uses pre-existing materials belonging to the contracting authority, the contracting authority may request that the contractor signs an adequate licence agreement. Such use by the contractor will not entail any transfer of rights to the contractor and is limited to the needs of this FWC.

II.23.3. Exclusive rights

The Union acquires the following exclusive rights:

(a) reproduction: the right to authorise or prohibit direct or indirect, temporary or permanent reproduction of the results by any means (mechanical, digital or other) and in any form, in whole or in part;

(b) communication to the public: the exclusive right to authorise or prohibit any display, performance or communication to the public, by wire or wireless means, including the making available to the public of the results in such a way that members of the public may access them from a place and at a time individually chosen by them; this right also includes the communication on Internet and broadcasting by cable or by satellite;

(c) distribution: the exclusive right to authorise or prohibit any form of distribution of results or copies of the results to the public, by sale or otherwise;

(d) rental: the exclusive right to authorise or prohibit rental or lending of the results or of copies of the results;

(e) adaptation: the exclusive right to authorise or prohibit any modification of the results;

(f) translation: the exclusive right to authorise or prohibit any translation, adaptation, arrangement, creation of derivative works based on the results, and any other alteration of the results, subject to the respect of moral rights of authors, where applicable;

(g) where the results are or include a database: the exclusive right to authorise or prohibit the extraction of all or a substantial part of the contents of the database to another medium by any means or in any form; and the exclusive right to authorise or prohibit the re-utilization of all or a substantial part of the contents of the database by the distribution of copies, by renting, by on-line or other forms of transmission;

(h) where the results are or include a patentable subject-matter: the right to register them as a patent and to further exploit such patent to the fullest extent;

(i) where the results are or include logos or subject-matter which could be registered as a trademark: the right to register such logo or subject-matter as a trademark and to further exploit and use it;

(j) where the results are or include know-how: the right to use such know-how as is necessary to make use of the results to the full extent provided for by this FWC, and the right to make it available to contractors or subcontractors acting on behalf of the
contracting authority, subject to their signing of adequate confidentiality undertakings where necessary;

(k) where the results are documents:

(i) the right to authorise the reuse of the documents in conformity with the Commission Decision of 12 December 2011 on the reuse of Commission documents (2011/833/EU), to the extent it is applicable and the documents fall within its scope and are not excluded by any of its provisions; for the sake of this provision, "reuse" and "document" have the meaning given to them by this Decision;

(ii) the right to store and archive the results in line with the document management rules applicable to the contracting authority, including digitisation or converting the format for preservation or new use purposes;

(l) where the results are or incorporate software, including source code, object code and, where relevant, documentation, preparatory materials and manuals, in addition to the other rights mentioned in this Article:

(i) end-user rights, for all uses by the Union or by subcontractors which result from this FWC and from the intention of the parties;

(ii) the rights to receive both the source code and the object code;

(m) the right to license to third parties any of the exclusive rights or of the modes of exploitation set out in this FWC; however, for pre-existing materials which are only licensed to the Union, the right to sub-license does not apply, except in the two cases foreseen by Article II.23.2.;

(n) to the extent that the contractor may invoke moral rights, the right for the contracting authority, except where otherwise provided in this FWC, to publish the results with or without mentioning the creator(s)' name(s), and the right to decide when and whether the results may be disclosed and published.

The contractor warrants that the exclusive rights and the modes of exploitation may be exercised by the Union on all parts of the results, be it via a transfer of ownership of the rights, on those parts which were specifically created by the contractor or via a licence of the pre-existing rights, on those parts consisting of pre-existing materials.

Where pre-existing materials are inserted in the results, the contracting authority may accept reasonable restrictions impacting on the above list, provided that the said materials are easily identifiable and separable from the rest, that they do not correspond to substantial elements of the results, and that, should the need arise, satisfactory replacement solutions exist, at no additional costs to the contracting authority. In such case, the contractor will have to clearly inform the contracting authority before making such choice and the contracting authority has the right to refuse it.

II.23.4. Identification of pre-existing rights

When delivering the results, the contractor must warrant that, for any use that the contracting authority may envisage within the limits set in this FWC, the newly created parts and the pre-existing material incorporated in the results are free of claims from creators or from any third parties and all the necessary pre-existing rights have been obtained or licensed.
To that effect, the contractor must establish a list of all pre-existing rights to the results of this FWC or parts thereof, including identification of the rights’ owners. If there are no pre-existing rights to the results, the contractor must provide a declaration to that effect. The contractor must provide this list or declaration to the contracting authority together with the invoice for payment of the balance at the latest.

II.23.5. Evidence of granting of pre-existing rights

Upon request by the contracting authority, the contractor must, in addition to the list mentioned under Article II.23.4., provide evidence that it has the ownership or the right to use all the listed pre-existing rights, except for the rights owned or licensed by the Union. The contracting authority may request this evidence even after the end of this FWC.

This provision also applies to image rights and sound recordings.

This evidence may refer, for example, to rights to: parts of other documents, images, graphs, sounds, music, tables, data, software, technical inventions, know-how, IT development tools, routines, subroutines or other programs (‘background technology’), concepts, designs, installations or pieces of art, data, source or background materials or any other parts of external origin.

This evidence must include, as appropriate:

(a) the name and version number of a software product;

(b) the full identification of the work and its author, developer, creator, translator, data entry person, graphic designer, publisher, editor, photographer, producer;

(c) a copy of the licence to use the product or of the agreement granting the relevant rights to the contractor or a reference to this licence;

(d) a copy of the agreement or extract from the employment contract granting the relevant rights to the contractor where parts of the results were created by its Personnel;

(e) the text of the disclaimer notice if any.

Provision of evidence does not release the contractor from its responsibilities if it is found that it does not hold the necessary rights, regardless of when and by whom this fact is revealed.

The contractor also warrants that it possesses the relevant rights or powers to execute the transfer and that it has paid or has verified payment of all due fees including fees due to collecting societies, related to the final results.

II.23.6. Quotation of works in the result

In the result, the contractor must clearly point out all quotations of existing works. The complete reference should include as appropriate, the following: name of the author, title of the work, date and place of publication, date of creation, address of publication on the internet, number, volume and other information that allows the origin to be easily identified.
II.23.7. Moral rights of creators
By delivering the results, the contractor warrants that the creators will not object to the following on the basis of their moral rights under copyright:

(a) that their names be mentioned or not mentioned when the results are presented to the public;

(b) that the results be divulged or not after they have been delivered in their final version to the contracting authority;

(c) that the results be adapted, provided that this is done in a manner which is not prejudicial to the creator’s honour or reputation.

If moral rights on parts of the results protected by copyright may exist, the contractor must obtain the consent of creators regarding the granting or waiver of the relevant moral rights in accordance with the applicable legal provisions and be ready to provide documentary evidence upon request.

II.23.8. Image rights and sound recordings
If natural persons appear in a result or their voice or any other private element is recorded in a recognisable manner, the contractor must obtain a statement by these persons (or, in case of minors, by the persons exercising parental authority) giving their permission for the described use of their image, voice or private element and, on request, submit a copy of the permission to the contracting authority. The contractor must take the necessary measures to obtain such consent in accordance with the applicable legal provisions.

II.23.9. Copyright notice for pre-existing rights
When the contractor retains pre-existing rights on parts of the results, reference must be inserted to that effect when the result is used as set out in Article I.13.1, with the following disclaimer: ‘© — year — European Union. All rights reserved. Certain parts are licensed under conditions to the EU’, or with any other equivalent disclaimer as the contracting authority may consider best appropriate, or as the parties may agree on a case-by-case basis. This does not apply where inserting such reference would be impossible, notably for practical reasons.

II.23.10. Visibility of Union funding and disclaimer
When making use of the results, the contractor must declare that they have been produced under a contract with the Union and that the opinions expressed are those of the contractor only and do not represent the contracting authority’s official position. The contracting authority may waive this obligation in writing or provide the text of the disclaimer.

II.24. Reimbursements
II.24.1 If provided for in the special conditions or in the tender specifications, the contracting authority must reimburse expenses directly connected with the delivery of supplies or provision of the services either when the contractor provides it with supporting documents or on the basis of flat rates.
II.24.2 The contracting authority reimburses travel and subsistence expenses on the basis of the shortest itinerary and the minimum number of nights necessary for overnight stay at the destination.

II.24.3 The contracting authority reimburses travel expenses as follows:

(a) travel by air: up to the maximum cost of an economy class ticket at the time of the reservation;

(b) travel by boat or rail: up to the maximum cost of a first class ticket;

(c) travel by car: at the rate of one first class rail ticket for the same journey and on the same day;

In addition, the contracting authority reimburses travel outside Union territory if it has given its prior written approval for the expenses.

II.24.4 The contracting authority reimburses subsistence expenses on the basis of a daily subsistence allowance as follows:

(a) for journeys of less than 200 km for a return trip, no subsistence allowance is payable;

(b) the daily subsistence allowance is payable only on receipt of supporting documents proving that the person concerned was present at the destination;

(c) the daily subsistence allowance takes the form of a flat-rate payment to cover all subsistence expenses, including meals, local transport including transport to and from the airport or station, insurance and sundries;

(d) the daily subsistence allowance is reimbursed at the flat rates specified in Article I.5.3;

(e) accommodation is reimbursed on receipt of supporting documents proving the necessary overnight stay at the destination, up to the flat-rate ceilings specified in Article I.5.3.

II.24.5 The contracting authority reimburses the cost of shipment of equipment or unaccompanied luggage if it has given its prior written approval for the expense.
III. GENERAL TERMS AND CONDITIONS
FOR INFORMATION TECHNOLOGIES CONTRACTS
## TABLE OF CONTENTS

1. COMMON ADMINISTRATIVE PROVISIONS .............................................. 5
   1.1. Definitions .......................................................................................... 5
   1.2. Performing Termination of Information Technologies Contracts ....... 10
   1.3. Formulation of Prices for IT Products, Software and Services .......... 11
   1.4. Official price lists ................................................................................ 11
   1.5. Particularities for Invoicing of Information Technologies Contracts ..... 13
   1.6. Insurance of rented or leased equipment ............................................ 14
   1.7. Applicability of the Framework contract to several Institutions, Bodies and Agencies ................................................................. 14
   1.8. Annexes ............................................................................................. 15
2. COMMON TECHNICAL PROVISIONS ................................................ 16
   2.1. Quality and standards ......................................................................... 16
   2.2. Security .............................................................................................. 17
   2.3. Specific Intellectual property rights ...................................................... 18
   2.4. Co-operation ...................................................................................... 20
   2.5. Product developments ....................................................................... 21
   2.6. Product life .......................................................................................... 21
   2.7. Use of Products ................................................................................... 21
   2.8. Documentation ..................................................................................... 22
   2.9. Identifiers ............................................................................................ 22
   2.10. Benchmarking .................................................................................... 23
3. SPECIFIC PROVISIONS RELATING TO THE PURCHASE, RENTAL AND LEASING OF COMPLEX HARDWARE PRODUCTS ........................................................ 25
   3.1. Additional specifications for Hardware Delivery ................................. 25
   3.2. Product installation .............................................................................. 26
   3.3. Acceptance ........................................................................................... 27
   3.4. Guarantee specifications for Complex hardware products .................. 28
   3.5. Leasing and Rental formula ................................................................. 29
   3.6. Termination of the Contract for rental and leasing of Complex Hardware products ................................................................. 30
   3.7. Withdrawal of rented or leased Complex hardware product ............. 30
4. SPECIFIC PROVISIONS RELATING TO THE PURCHASE, RENTAL AND LEASING OF OTHER THAN COMPLEX HARDWARE PRODUCTS. ................................................................. 31

4.1. Configuration and delivery........................................................................31

4.2. Guarantee specifications for other than Complex hardware products .................................................................32

4.3. Leasing and Rental formula ..........................................................................32

4.4. Termination of the Contract for rental and leasing of other than Complex hardware products. .................................................................32

4.5. Withdrawal of rented or leased other than Complex hardware product.............................................................................................32

5. SPECIFIC PROVISIONS RELATING TO LICENSED SOFTWARE ............................................................................................... 33

5.1. Delivery - installation - Documentation ...........................................................33

5.2. Trial - acceptance ..............................................................................................34

5.3. Guarantee specifications for Software ..................................................................34

5.4. Use.......................................................................................................................35

5.5. Compatibility ......................................................................................................35

5.6. Intellectual property rights concerning Software - confidentiality .................................................................35

5.7. Escrow rider .......................................................................................................36

6. SPECIFIC PROVISIONS RELATING TO HARDWARE AND SOFTWARE MAINTENANCE.................................................................38

6.1. Common provisions.........................................................................................38

6.2. One –shot repair of Hardware........................................................................38

6.3. Maintenance ......................................................................................................39

7. SPECIFIC PROVISIONS RELATING TO ALL INFORMATICS SERVICES ................................................................................................. 43

7.1. Types of Services..............................................................................................43

7.2. Time-and-means Contracts............................................................................44

7.3. Quoted times-and-means Contracts...............................................................45

7.4. Fixed-price Contracts.....................................................................................45

7.5. Stability of Services.......................................................................................46

7.6. Timetable..........................................................................................................47

8. SPECIFIC PROVISIONS RELATING TO DEVELOPMENT AND MAINTENANCE OF COMMISSIONED SOFTWARE ...............48
8.1. Compliance with technical specifications .................................................48
8.2. Acceptance ................................................................................................ 48
8.3. Guarantee of proper operation of Commissioned software .........................50
8.4. Intellectual property rights and ownership of source code..........................50
8.5. User manuals and Documentation ................................................................50
8.6. Interfaces and compatibility ......................................................................51
9. SPECIFIC PROVISIONS RELATING TO TRAINING ORGANISED FOR THE COMMISSION ................................................52
9.1. Instructors ..................................................................................................52
9.2. Organisation of courses .............................................................................52
9.3. Instructor's manual ....................................................................................52
9.4. Provision of training Software ...................................................................52
10. SPECIFIC PROVISIONS RELATING TO DOCUMENTATION PRODUCED FOR THE COMMISSION ..........................................................53
ANNEX I : CENTRAL SERVICE DESK ACTION PROCEDURE..........................54
ANNEX II : TEMPLATE OF DECLARATION OF CONFIDENTIALITY ............56
ANNEX III : COMMISSION DECISION ON PROTECTION OF INFORMATION SYSTEMS ..........................................................58
1. COMMON ADMINISTRATIVE PROVISIONS

1.1. Definitions

When used in the Framework contract with a capitalised first letter and in italics, the following terms shall have the following meaning:

“Benchmarking”:

Assessment process carried out by a qualified and objective third party which: tests, evaluates and measures the performance of the Contractor by reference to the specific Quality indicators defined in the Service level agreement, or by comparison with similar Services or Products provided by other companies; and/or analyses the evolution of the relation between the prices laid down in the Framework contract and the market prices for similar Products or Services.

“Benchmarker”:

The independent third party carrying out a Benchmarking.

“Commissioned Software”:

Software developed by the Contractor for the Commission under the Framework contract.

“Commissioning date”:

Date on which the Contractor notifies the Commission that a Product, a System or an Extension thereto has been brought into service.

“Compatibility”:

Ability of a Product to function in accordance with the System specifications or type of equipment into which it will be integrated.

“Complex hardware product”:

Any computer equipment, whether or not it contains Software, which requires installation by skilled staff and acceptance by both Parties. These Products are explicitly described in Annex I to the Framework contract.

“Consignment note”

Note in duplicate duly signed and dated by the Contractor or his carrier, giving the Specific Contract number and particulars of the goods delivered to be countersigned by the Commission and returned to the Contractor or his carrier. This note acknowledges the fact that the goods have been
delivered and in no way implies conformity of the goods with the Specific Contract.

“Certificate of conformity”

Certificate signed by the Commission, evidencing conformity of the goods delivered, no later than one month after the date of delivery, unless provision is made in the Special Conditions or General terms and conditions for Information Technologies contracts for a different period.

“Constant discount”:

Fixed percentage of discount on its Products and Services, awarded by the Contractor to the Commission during the entire duration of the Framework contract, and calculated on the prices as they appear in the Official Price list.

“Delivery date”:

Date, determined in the Framework contract, on which a Product, a System or an Extension thereto is to be delivered to the Commission.

“Documentation”:

Instructions and manuals supplied with the Product(s) and/or Service(s), whether intended for support/technical staff or for end-users, and whether in printed or in electronic form.

“Escrow agent”:

The third party providing the safekeeping facilities specified in the Escrow rider.

“Escrow rider”:

Agreement between the Commission, the Contractor and a third party, by which such third party provides safekeeping facilities for the source code of the Software product(s) covered by the Framework contract and/or for the related Documentation.

“Extension”:

Set of Products to supplement or extend a System.

“Extended working hours”:

Any working hours other than Normal working hours.

“Extra muros”

Outside the Commission’s premises.
“Hardware”:
Any computer equipment purchased, rented, leased or maintained under this Framework contract.

“Informatics Services”:
All Services related to information technology, such as (but not limited to) training, consultancy, removal, logistics, integration work, engineering, development, maintenance and writing of documentation, as further described in the Framework contract.

“Installation date”:
Date notified by the Contractor with a Means of registered communication on which the Contractor will perform the assembly, the installation and the bringing into service of a Hardware Product. This may not be later than fifteen (15) Normal working days after the date of its removal from its place of delivery to its place of installation. This date may be extended upon the Commission’s decision and may be notified by the Commission with a Means of communication.

“Intellectual property rights”:
All industrial and intellectual property rights, such as, but not limited to, copyright, the rights of the producer of a database, rights on semiconductors, patents, patent applications, utility models, trademarks (whether Benelux, Community, international or foreign trademarks), trade names, designs and models.

“Internal use”
Within the Commission’s premises and the use by a European Community official as defined by the Staff Regulations of the Community, elsewhere than in his normal office located in the Commission’s premises, but within the context of his official work.

“Intra muros”
Within the Commission’s premises.

“Means of communication”:
Any communication between the Parties relating to the execution of this Framework contract, whether made by letter, facsimile, telegram, e-mail or by any other Means of communication, the content of which can be printed on paper. These Means of communication also include communication by telephone, SMS, or any other Means of communication whose content cannot be printed on paper, provided such communication
is confirmed within two (2) Normal working days by a communication by one of the means mentioned in the first sentence.

“Means of registered communication”:

Any communication between Parties relating to the execution of this Contract, made by a Means of communication the content of which can be printed on paper whereby an independent third party is able to establish that the communication has reached its destination, whether such destination be a postal, an electronic (e-mail) or any other type of address.

“New release”:

Revision of an existing version of a Software program, usually amending the reference to the Software’s version from for example version 0.1 to version 0.2.

“New version”:

New version of a Software program, usually amending the reference to the Software’s version from for example version 0.1 to version 1.1.

“Normal working days”:

From Mondays to Fridays inclusive, excepting Commission holidays only. Commission holidays are usually — but not necessarily — the same as the national holidays of the place of execution of the Framework contract. When expressly so provided in the Framework contract or in a Specific Contract, Commission on-duty days (such as Holy Thursday, Good Friday, the day following Ascension Day and the period between 27 and 31 December) may be included in the Normal working days. If nothing is provided in this respect, such Commission on-duty days will be regarded as Commission holidays.

“Normal working hours”:

From 8 a.m. to 8 p.m. on Normal working days.

“Official price list”:

Price list, which is

- a constant feature of the Contractor’s sales policy;
- regularly updated by the Contractor;
- addressed to the public, to the Contractor’s customers or to a part of them; and
- accessible to the public, to the Contractor’s customers or to a part of them, e.g. on an Internet site.
“Order Forms”

Document signed by the Commission and the Contractor ordering Products or Services pursuant to the Framework contract. Please note that reference to Specific Contracts may be understood, where relevant, as references to Orders.

“Payment request”

Contractor’s request for a payment, by a Means of communication, for the execution of any of its obligations under the Framework contract.

“Person-day”:

Seven-and-a-half (7½) hours.

“Product”:

Any Software, Hardware or Telecommunications product. Where a distinction between the three types of Products is intended, it shall either be explicit, by the use of one of the three terms, or it may be implicitly deduced from the context of this Framework contract.

“Quality indicators”:

Measurable targets serving as a reference for evaluating the quality of the Services to be provided by the Contractor, and determined in the Service level agreement.

“Services”:

Informatics and/or Telecommunications Services.

“Service level agreement”:

Document annexed to the Framework contract, which lays down:

- the quality of the Services to be provided by the Contractor by reference to the Quality indicators;

- the penalties for total or partial non-performance which will apply to the Framework contract if he fails to meet the Quality indicators.

“Software”:

Any series of instructions constituting a computer-executable program or programs, and being (part of) the object of the Framework contract.

“System”:
Combination of *Products* serving a complete set of functions.

“The Telecommunications products”:

All products and equipment related to the provision of *Telecommunications services*.

“The Telecommunications services”:

All *Services* related to the transmission, emission or receipt of signs, signals, writings, images, sounds or data of whichever nature, whether enabled by wire or wireless means or by any other electromagnetic *System*, such as (but not limited to) training, consultancy, removal, installation, administration, management and maintenance, as further described in the Framework contract.

1.2. Performing Termination of Information Technologies Contracts

1.2.1. If the Commission terminates the Framework contract pursuant to Article II.12 of the General Conditions and the Commission has been assigned the rights on *Commissioned Software* or has paid for maintenance of *Commissioned Software*, the Contractor shall:

- hand over (immediately and without charge) the source code, the *Software* plans, the access keys and the *Documentation* required by the Commission for the proper operation of the *Software*, insofar as the Contractor has a legal right to do so.

- expressly undertake not to use such developments in the future and to purge any copies of the same from his equipments;

- undertake to keep every information in relation to the developed *Software* confidential even after the termination of the Framework contract;

1.2.2. If the Framework contract concerns the provision of *Products* as well as maintenance *Services* relating to these *Products*, the Commission has the right, if the circumstances justifying termination only concern the provision of the *Products*, to terminate only the part of the Framework contract which concerns the provision of *Products*, while keeping the part of the Framework contract relating to the maintenance *Services* in force.

1.2.3. In case of rental and leasing the Contractor shall remove the *Products* or *Systems* at its expense within the time agreed upon between the Parties. The withdrawal of a *Product* shall be recorded in a withdrawal report quoting the Framework contract and Specific Contract concerned.
1.2.4. The Contractor shall not provide any Products or Services if the Framework contract is not in force and if no Specific Contract has been entered into.

1.3. **Formulation of Prices for IT Products, Software and Services**

1.3.1. In general, the Contractor agrees to let the Commission, as a most favoured partner, benefit from its most advantageous prices.

1.3.2. **Products**

Contractual prices for purchase of Products shall be expressed per unit. The prices quoted shall include delivery, installation and assembly where applicable.

Rental of Products shall be distinguished from leasing by the fact that, in the former, the Framework contract shall not include any purchase value at the end of the rental period. In the case of leasing, the Framework contract shall lay down the price for the purchase option at the end of the leasing period.

Maintenance of Products shall be expressed as a percentage of the purchase price or as an absolute figure. It may vary in proportion to the level of service as defined in the Contract, which shall be specified in each Specific Contract.

1.3.3. **Software**

The fees for the maintenance of Software are either expressed as a percentage of the licence fees or are calculated at a fixed price. Duration of the maintenance shall be specified in each price.

1.3.4. **Services**

Service prices shall be defined at a fixed price or by Person-day, and shall include all general expenses and expenses directly connected with the provision of the Services such as company management costs, social security costs, travel and office expenses.

1.4. **Official price lists**

1.4.1. Upon signature of the Framework contract, the Contractor’s Official price list is appended to the Contract as an Annex. The Contractor will use its best endeavours to supply an Official price list which only includes the Products which form the subject of the Framework contract. If the Official Price list also includes items other than such Products, then the Contractor agrees to indicate clearly and accurately, for example by highlighting the relevant items in the electronic version of the document, which subset of items of its Official price list correspond to the Products forming the subject of this Framework contract. If the Contractor fails to
do so, he agrees that he cannot claim payment for, restitution of, nor damages for items delivered to the Commission outside the scope of the object of this Framework contract.

1.4.2. The Contractor agrees to make an updated version of the Official price list available to the Commission at the frequency determined in the Special Conditions of the Framework contract.

1.4.3. The updates of the Official price list will be made available to the Commission either, and by order of preference, for download by remote access to a website, to an FTP site, to an intranet site, in electronic format (e.g. by e-mail) or in hard copy (or e.g. on CD-ROM), as specified in the Special Conditions of the Framework contract. When it is therein agreed that such updates may be downloaded, then the Contractor shall precisely indicate the location of the download area (such as from an area on the Contractor’s website, from an FTP site, etc.) and provide the Commission, by a Means of communication, with full and accurate instructions, including access codes, enabling it to perform such downloads. Should the Official price list be made available to the Commission by remote access, the Contractor must inform the Commission in advance by a Means of communication of the moment on which it will be made available on line.

1.4.4. When the Official price list is treated as confidential information by the Contractor, the Contractor agrees to make the updates of the Official price list available to the Commission not later than on the day it is for the first time made available to any other customer of the Contractor. If not, the Commission may claim damages for total or partial non-performance.

1.4.5. Once the update of the Official price list is made available to the Commission, the Commission must accept or refuse it within the time limit set forth in the Framework contract. Such acceptance or refusal will be communicated to the Contractor by a Means of communication. The Contractor agrees to provide the updates in a manner allowing an easy way of comparing the different versions of the Official price list.

1.4.6. The Contractor agrees to make updates of the Official price list available to the Commission only when, considering the volumes of each Product already ordered by the Commission, the global average price for all the Products is lower than the preceding versions of the Official price list. Individual products prices already included in the list shall not be increased, unless otherwise agreed in the Framework contract. If this is not the case, the Commission may refuse to apply the proposed update. The Commission will then continue to benefit from the prices of the last accepted version of the Official price list.

1.4.7. When the Commission’s acceptance of the update of the Official price list has been communicated to the Contractor by a Means of communication, the new prices will be immediately applicable to all orders placed by the Commission on and from the day following such a communication.
1.4.8. The Constant discount rate(s) must be applied to clearly defined groups of Products and/or Services.

1.4.9. The Constant discount(s) fixed in the Framework contract are applicable to all the accepted updates of the Official price list.

1.4.10. The present Article does not prevent the Parties agreeing on a higher percentage for the Constant discount(s) by Amendment.

1.5. Particularities for Invoicing of Information Technologies Contracts

1.5.1. The invoices are to be sent to the address stated in the Specific Contracts. The payment period shall not be binding on the Commission if any invoice is sent to a different address. An invoice should be submitted not later than six (6) months after delivery of the Consignment note, or, where applicable, the Certificate of Conformity. In accordance with Article II.4 of the General Conditions, the Contractor will be liable to liquidated damages in the case of invoices submitted out of time.

1.5.2. Products

Purchases shall be invoiced when the relevant Consignment note, or, where applicable, the Certificate of Conformity has been signed.

Invoices in respect of rental, leasing and maintenance shall be submitted quarterly unless otherwise provided for in the Framework contract. The first invoice in respect of rented or leased Products shall cover the period from the date of signature of the Consignment note, or, where applicable, the Certificate of Conformity of the Products, or, as regards maintenance, from expiry of the guarantee, to the last day of the current calendar quarter.

1.5.3. Software

One-off licence fees shall be invoiced when the relevant Consignment note, or, where applicable, the Certificate of Conformity has been signed.

Yearly licence fees and maintenance fees may be invoiced per calendar year and in advance for the whole year. The first invoice shall cover the period from the date of signature of the Consignment note, or, where applicable, the Certificate of Conformity of the Software, or, as regards maintenance, from expiry of the guarantee, to the end of the current calendar year.

1.5.4. Services

Invoices in respect of Services consisting in a single performance, for example the provision of a report, a project or a training measure, shall be submitted in accordance with the terms of the Specific Contracts.
Invoices with respect of continuous Services shall be submitted at the end of the calendar quarter. The first invoice shall cover the period from the start date indicated in the Specific Contract until the end of the current calendar quarter. When the invoice relates to an amount of less than €25,000 payment shall be made when the service has been fully provided.

1.6. **Insurance of rented or leased equipment**

1.6.1. The Contractor shall insure the Products rented or leased under this Framework contract from the Delivery date until the date the rental or lease have expired. The Commission shall in no case be considered responsible for any deterioration, destruction, theft or loss of any Products rented or leased by the Contractor under this Framework contract, unless the damage or loss is caused by a serious fault or serious negligence on the part of the Commission.

1.7. **Applicability of the Framework contract to several European Union Institutions, Bodies and Agencies**

1.7.1. Unless otherwise stated in the Preamble of the Framework contract, the Framework contract covers the provision of Products and Services to the Commission alone.

1.7.2. If the Framework contract stipulates that it is applicable to the Commission and to one or more of the other European Union Institutions, Bodies and Agencies, the Commission shall sign the Framework contract acting as agent for the Institutions, Bodies and Agencies to which it is applicable.

1.7.3. In so doing, should one or more of the other Institutions, Bodies and Agencies have their own legal personality separate from that of the European Community, the Commission guarantees the Contractor that it has received any mandates required to that effect.

1.7.4. Once the Framework contract is signed by the Commission acting as an agent for the Institutions, Bodies and Agencies to which it is applicable, each of them shall sign with the Contractor their own Specific Contracts governing the provision of Products and Services to it.

1.7.5. References to the Commission in the Framework contract shall be understood, as required by the context, as referring to one of the following concepts:

- all the Institutions, Bodies and Agencies covered by the Framework contract, in relation to their collective rights and obligations with the Contractor, as one of the Parties to the Framework contract;

- any one of the Institutions, Bodies and Agencies acting in its own capacity, in particular for matters related to the conclusion, execution or termination of Specific Contracts between itself and the Contractor;
the Commission acting in its capacity as agent for the Institutions, Bodies and Agencies to which the Framework contract is applicable.

The Commission shall as far as possible make clear to the Contractor whether it is acting in its own capacity or as agent for the Institutions, Bodies and Agencies to which the Framework contract is applicable.

1.7.6. In the event of the Contractor having a complaint against an Institution, Body or Agency in relation to the conclusion, execution or termination of Specific Contracts, the Contractor remains bound to his obligations under the Framework contract and Specific Contracts concluded with the other Institutions, Bodies or Agencies. Without prejudice to Article I.7 of the Special Conditions, the Contractor expressively renounces hereby to compensate or suspend the execution of Specific Contracts related to the other Institutions, Bodies or Agencies.

1.8. Annexes

The following documents are annexed to the General terms and conditions for Information Technologies Contracts and shall form an integral part of it:

Annex I : Central service desk action procedure.

Annex II : Confidentiality Agreement

Annex III : Commission decision on protection of information Systems [C(95) 1510 23/11/95]
2. COMMON TECHNICAL PROVISIONS

2.1. Quality and standards

2.1.1. The Contractor shall perform the Services and provide the Products in full knowledge and consideration of the Commission's computing environment. It shall perform it in accordance with technical norms, standards and procedures based on best professional practice in the informatics and/or telecommunications field, for instance the ISO 9000 standards.

2.1.2. The Commission shall supply, without delay, all the assistance, data and information that the Contractor considers necessary or useful for providing its Products and Services.

2.1.3. The Commission and the Contractor shall notify each other by a Means of communication of any factor likely to impair or delay the proper execution of the Framework contract.

2.1.4. The Contractor guarantees that Software delivered under this Framework contract, whether or not developed in execution of this Framework contract, will not fail to execute its programming instructions due to defects and workmanship when properly installed and used on the device designated by the Contractor. It shall be devoid of any deliberate mechanism which leaves it under the Contractor's control after supply to the Commission. It shall meet the operating requirements, specifications and characteristics specified in the Contractor's documents or laid down in the Framework contract.

2.1.5. The quality of the Contractor's Products and Services shall be measured by reference to the definitions, quality standards and procedures defined in the present General terms and conditions for Information Technologies Contracts, Framework contract or the Specific Contract, and by reference to the Quality indicators defined in the Service level agreement. Quality standards may be revised in line with developments on the market.

2.1.6. The Contractor undertakes to comply with those quality standards. Compliance with the standards shall be monitored by the Commission. Unless otherwise stated in the Framework contract, in accordance with article II.1 of the General Conditions, in the event of non–compliance with one or more of the standards over a sliding period of three (3) months, the Contractor shall submit an improvement plan. In the event of non–compliance with one or more of the standards for three (3) months, consecutive or not, over a sliding period of six (6) months, a Product whose quality has proved substandard may be withdrawn from the Framework contract, or the Contract may be terminated where the overall quality of the Services is substandard.

2.1.7. Stand–by System (outside the guarantee period)
Unless otherwise stated in the Framework contract, in the event of a complete System failure lasting more than twenty-four (24) hours from the time it is notified by a Means of communication to the Contractor, or in the event of intermittent failures lasting more than forty-eight (48) hours for any reason whatsoever, the Contractor shall, upon a duly substantiated request, make available to the Commission within twenty-four (24) hours at the most, an equivalent System or the necessary hardware and software enabling the Commission to run its applications in the interim. The cost of such equivalent material shall be charged to the Contractor.

If the Contractor can demonstrate that the failure is not attributable to it, it may charge the cost to the Commission at the rates shown in the Annexes.

2.2. Security

2.2.1. Contractors working in the Commission premises must conform to any internal Commission security rules, including the Commission’s Information Systems Security Policy. If the Contractor's staff are working in Commission buildings, the Contractor is required, at the Commission's request, to replace immediately and without compensation any person considered undesirable by the Commission.

2.2.2. The Contractor undertakes to comply with Article 5 of the Commission decision on protection of information Systems [C(95) 1510 23/11/95] and any subsequent versions. (See Annex III)

2.2.3. The security requirements for each individual project shall be described in the Specific Contracts.

2.2.4. The Contractor agrees to impose the security obligations of this Article upon any of its subcontractors and their staff who perform tasks for the Commission in execution of this Framework contract.

2.2.5. The Contractor recognises that no Products, equipment or material whatsoever owned by the Commission or present at the Commission's premises, may be moved or removed without the Commission's express written approval and the signature of a Specific Contract relating thereto. Each move or removal of a Product, equipment or material whatsoever, shall be recorded in a note, as specified in the Specific Contract in execution of which these Products, equipments or materials are moved or removed.

2.2.6. The Contractor shall take all appropriate steps for each Product to ensure that the data and the magnetic media upon which they are stored are safely preserved. The Products supplied shall not contain any mechanism (e.g. viruses) which could compromise their proper operation or that of other Products. The cost of repairing the damage caused by such a mechanism shall be borne by the Contractor.
2.2.7. The Contractor undertakes to inform the Commission by a Means of registered communication as soon as it has any knowledge of defaults in its Products that endanger the security of the configurations of which they form a part. It shall immediately take any measures necessary to restore the security of the configurations and correct the defaults.

2.2.8. The Contractor shall ensure that all security precautions for each Product are clearly spelled out in the relevant Documentation supplied to the Commission.

2.2.9. Should the Contractor, during the performance of the tasks which are the subject of the Framework contract, need remote access to internal informatics resources from the external domain, he shall be requested to comply with the Commission’s internal rules on practical and technical security for remote intervention. This must be achieved by way of signature of a specific agreement for remote intervention provided by the Commission.

2.3. Specific Intellectual property rights

2.3.1. As regards all Software or other protected material for which the Intellectual property rights are the property of the Commission or which have been licensed to the Commission by third Parties, and which the Contractor is likely to use in the execution of its obligations under this Framework contract, the Commission expressly authorises the Contractor to use such Software or other protected material, within the limits strictly necessary for the execution of this Framework contract.

In view of the preceding, the Contractor undertakes:

- not to copy any such Software or other protected material without prior written authorisation from the Commission;

- to use such Software or other protected material exclusively in the context of this Framework contract;

- to protect and indemnify the Commission against all third-party claims or actions alleging a breach of their Intellectual property rights, or a use of such Software or other protected material in contravention with the present Article.

2.3.2. Pursuant to Article II.17 of the General Conditions and as regards the results or rights obtained in performance of the Framework contract, the Contractor undertakes to obtain written consent from the Commission prior to:

- filing a trademark, patent or design application in relation with any of the results or rights obtained in performance of the Framework contract in his own name or that of a third party.
- claiming a copyright over the results or rights obtained in performance of the Framework contract in his own name or of that of a third party.

- allowing a third party to do such filings or claims.

Failure to obtain permission from the Commission will entitle the Commission to seek damages against the Contractor and will not prevent the Commission from protecting the rights assigned under the Framework contract.

2.3.3. The Contractor declares that it is the rightful owner of the **Intellectual property rights** to all **Products** and/or their components delivered under this Framework contract, and that it is entitled to assign or licence those rights in accordance with the terms of this Framework contract. If those **Intellectual property rights** are the property of third Parties, the Contractor guarantees that it has requested and obtained those third Parties’ written authorisation to grant to the Commission the assignment or licence of their **Intellectual property rights** to the extent as provided under this Framework contract. The Contractor shall be solely responsible for taking the necessary steps, under the laws and regulations in force at the place where the tasks assigned to the Contractor are to be performed, to ensure the opposability to third Parties of the assignments or licences granted to the Commission by the Contractor or by such third Parties.

2.3.4. The Contractor guarantees that none of the **Products**, **Documentation** or other protected material delivered, whether or not developed in execution of this Framework contract, infringes any third party’s **Intellectual property rights**.

2.3.5. Each party shall inform the other party of the existence or threat of any third party’s action or claim alleging an infringement of its **Intellectual property rights** by the Commission’s use of any **Products**, **Documentation** or other protected material delivered under this Framework contract, provided such use is made in conformity with the terms of this Framework contract.

2.3.6. In the event of such a dispute or threat thereof, the Contractor undertakes to conduct all litigation, arbitration or negotiations for settlement, in its own name as well as in the Commission’s name, at its own and sole expense.

The Commission agrees to provide the Contractor with all information and assistance that may reasonably be required, at the Contractor’s own and sole expense.

However, the Commission reserves the right to decide to conduct its own defence or to negotiate its own settlement, at its own discretion. The Contractor will be responsible for any payment arising out of any settlement or judgement following such a dispute or threat, except for the payment of a settlement made by the Commission without the
Contractor’s written consent. Such consent may not be withheld without reasonable grounds.

If the infringement of a third party’s *Intellectual property right* on a *Product* and its *Documentation* is declared in a judgement, arbitration sentence or party settlement, or if such is likely to happen, the Contractor agrees to (1) either procure for the Commission the right to continue using the *Product* and its *Documentation*, (2) either replace them with substantially equivalent non-infringing *Products*, or, if none of the foregoing is available, (3) grant to the Commission a credit in the amount corresponding to the purchase price of the proportion of the *Product* which can no longer be used.

The Contractor will not be responsible under the present guarantee for any third party claiming an infringement of its *Intellectual property rights* based on (1) the Commission’s use of *Products* in combination with equipment not delivered by the Contractor, if such combined use is the cause of the claimed infringement, or (2) the Commission’s use of any *Product* and *Documentation* delivered hereunder in a form other than the one delivered by the Contractor, if such change in form is the cause of the claimed infringement.

2.3.7. The guarantee against third party claims is due by the Contractor until five (5) years following the end of the Framework contract, or until five (5) years following the last use by the Commission of the Product and its Documentation delivered by the Contractor, whichever period ends last.

2.4. Co-operation

2.4.1. The Contractor undertakes to develop and install the *Products* and provide the *Informatics Services* in accordance with the document “Informatics Architecture”, as updated from time to time. On the day of completion of this version of the General terms and conditions, the latest version of that document is available at the URL [http://europa.eu.int/comm/dgs/informatics/publications/index_en.htm](http://europa.eu.int/comm/dgs/informatics/publications/index_en.htm) which the Contractor agrees to visit regularly for updating purposes. The Contractor agrees to co-operate with other suppliers to make the *Products* work with those of these other suppliers. It agrees to attend meetings called for that purpose by the Commission.

2.4.2. The Contractor shall assist and advise the Commission on the use of its *Products* and *Services*. It shall be responsible for *Product* integration as regards its inclusion in the Framework contract, its operation in the Commission’s environment and the introduction of *New versions*. 
2.5. **Product developments**

2.5.1. Any *Product* delivered under this Framework contract shall have been demonstrated by the Contractor, at its expense, to conform to the technical specifications sent to the Contractor as part of the invitation to tender or the negotiation pursuant to which the present Framework contract has been drawn up.

2.5.2. Any *Product* capable of replacing a previously approved *Product* in the same operational environment, with no loss of performance and at no extra cost to the Commission, may be added to the relevant Annexes of the Framework contract.

2.5.3. Proposals to include new *Products* involving new features or functions not previously available amongst the *Product* listed in the Framework contract’s Annexes, shall only be considered in the context of the principal *Product* classifications and specifications covered by the call for tenders referred to in the preamble of the Framework contract.

2.5.4. Even if a *Product* is approved by the Commission, any incompatibility with previous *Products* that becomes apparent in the course of its use shall be resolved by the Contractor as swiftly as possible and at no cost to the Commission.

2.5.5. Evaluation procedures and trials of new products before inclusion in the price list may be specifically defined in the Framework contract.

2.6. **Product life**

2.6.1. The Contractor shall ensure that the *Product*, or replacing *Product*, are marketed or available during the lifetime of the Framework contract from the date of their inclusion in the relevant Annex of the Framework contract.

The Contractor shall ensure that maintenance of the *Product* delivered under this Framework contract may be requested and provided for a period of at least five (5) years from the date of signature of their *Consignme note*, or, where applicable, of their *Certificate of Conformity*, whichever is the latest.

2.7. **Use of Products**

2.7.1. From the date of signature of the *Consignme note*, or, if applicable, of the *Certificate of Conformity*, whichever is the latest, the Commission may make unrestricted use of the *Products* under normal operating conditions. The Commission may use the *Products* for *Services* it is carrying out for other Institutions, Agencies or Bodies. If the *Products* are rented or leased, the right of use applies for the duration specified in the
Specific Contract. If a guarantee applies, maintenance may not start until the guarantee has expired.

2.7.2. The Contractor must ensure that the Commission may add to a System or connect to it, either directly or via telecommunications networks, compatible Products of any origin.

2.7.3. In view of the Commission's supranational nature, the Contractor shall not exert any right of inspection over the Commission's use of the Products.

2.8. Documentation

The Contractor shall provide the Commission with its Documentation and updates, as soon as they become available to its customers, in as many copies, whether in machine-readable form or on paper, as are stated in the Framework contract or a Specific Contract.

The Commission may reproduce this Documentation in full or in part for any Internal use by its staff. The Commission shall reproduce all references to Intellectual property rights appearing on the originals.

2.9. Identifiers

The Commission may decide to assign an identifier to a unit of a delivered Product. In such case, the Contractor commits itself to using an identifier for every unit of a Hardware or Telecommunications Product delivered to the Commission. This identifier is communicated to the Contractor by the Commission when the Consignment note, or, if applicable, the Certificate of Conformity for such unit has been signed. The identifier(s) shall be given in electronic file(s) in such manner as shall have been agreed by both Parties. The Contractor’s original identifier mentioned in its delivery documents is associated with the Commission's identifier. After that, only the Commission's identifier is to be used in all instances when the Contractor refers to the unit in question (for example in all operations relating to the service desk, invoicing of maintenance, technical intervention, etc.).

The identifier is an alphanumeric code of 15 characters. The format of the identifier may be changed by the Commission at any moment. In that case, the Contractor will be notified by a Means of communication.

Examples of correctly formulated identifiers are:

02DI20030764930
02BX19954381081
02LX19926036740
02XXXXXXX0572190
02YYYYYY0032078
04DI99996134114
2.10. **Benchmarking**

The Commission may undertake a *Benchmarking* of the levels and the charges of the *Services* and supplies provided under this Framework contract by comparison with similar *Services* and supplies provided by outsourcing vendors and/or in-house IT service providers and suppliers. The results of such *Benchmarking* shall be available in identical form to both the Commission and the Contractor.

In order to guarantee that a valid comparison is made, the Commission will ensure that:

- the scope of the *Services* and supplies being provided by the Contractor is taken into consideration;
- the comparison group consists of at least four enterprises to ensure statistical significance;
- the relevant comparison data must be guarantee

The *Benchmarking* shall not exceed four (4) months

For the first *Benchmarking* exercise, the comparison group shall be defined in a document entitled “Comparison Group Definition”. The Commission reserves the right to change the comparison group algorithm to reflect any changes in its business from time to time.

The *Benchmarker* shall be a qualified and objective third party selected by the Commission through an appropriate market procedure. The Commission will pay all of its own costs and the *Benchmarker’s* costs during the *Benchmarking*. The Contractor will pay all of its own costs. Interpretation of the results of the *Benchmarking* shall be the sole prerogative of the *Benchmarker*.

The Commission and the Contractor shall set aside sufficient time and resources for each stage of the *Benchmarking*, such as:

- identification and location of *Benchmarking* data,
- performing the *Benchmarking*, and
- implementation of the conclusions of the *Benchmarker*.

The Commission and the Contractor will be free to suggest changes in *Benchmarking* parameters as the *Services* and supplies evolve over the term of this Framework contract.

The *Benchmarker* shall treat as confidential, in accordance with Article II. 16 of the General Conditions, all data provided by the Commission and the Contractor, and will return all material and media once the *Benchmarking* is completed.
If a Benchmarking reveals that the level of a Service does not reach the comparison group’s service levels, the Contractor shall immediately prepare an action plan, which will specify all actions necessary to rectify the deviations. The full and measurable implementation of the action plan shall in no circumstances exceed one (1) year. If the Contractor fails to fully implement the action plan, the Commission may claim damages.

If a Benchmarking reveals that charges are higher than the comparison group’s charges, the Contractor shall immediately reduce its charges to the comparison group level, with effect from the date on which the results of the Benchmarking were delivered to the Parties.
3. SPECIFIC PROVISIONS RELATING TO THE PURCHASE, RENTAL AND LEASING OF COMPLEX HARDWARE PRODUCTS

3.1. Additional specifications for Hardware Delivery

3.1.1. Terms

All Complex hardware products shall be tested by the Contractor before their delivery. The Contractor shall be able to demonstrate that the pre-delivery test was satisfactory if the Commission so requests.

The number of copies of Documentation to be supplied shall be specified in the Specific Contract, but must be at least equal to one (1) copy per unit of Complex hardware product.

The Contractor shall notify the Commission by a Means of communication of its packaging terms at least two (2) weeks prior to the Delivery date. The Contractor shall remove all packaging material used during delivery.

The height of the Contractor's delivery vans may not exceed 4.5 m and only "EURO"–type pallets shall be used.

3.1.2. Dates

The Delivery date shall be indicated in each Specific Contract.

Failure regarding the Delivery date is considered as damage to the Commission as defined in Article II.4 of the General Conditions.

Should the Contractor be unable to deliver on the specified Delivery date, it must then supply an equivalent Complex hardware product or System with the Commission's prior consent.

Where the Commission has incurred costs vis-a-vis a third party by reason of a delay in delivery or commissioning attributable to the Contractor, then the Contractor shall reimburse those costs upon production of supporting documents, provided that the Commission has notified the Contractor by a Means of communication of the risk of incurring damages due to the late delivery soon after having been informed of the Contractor’s inability to deliver on time.

If a Delivery date is overrun by more than forty-five (45) calendar days, the Commission is entitled to immediately terminate the Specific Contract in question.
3.1.3. Procedure

The Contractor shall confirm the exact Delivery date of each Complex hardware product at least eight (8) calendar days in advance to the Commission by a Means of communication.

The Commission shall, during Normal working days and hours, provide access to its premises for delivery on the notified Delivery date. Delivery and installation costs shall be borne by the Contractor. Deliveries shall be complete.

Receipt of each delivery of Products shall be recorded in a Consignment note signed by the Commission as stated in article II.1.1 of the General Conditions (including the balance to be delivered for each Product)

3.2. Product installation

3.2.1. Installation requirements

For each Product listed in the Annexes of the Framework contract, the Contractor shall specify by a Means of communication the technical installation requirements and any refurbishment necessary for the premises intended to house the Products.

The Commission shall ensure that from then onwards the premises where the Products are installed satisfy the conditions set out by the Contractor regarding access, air–conditioning and electric power supplies and are equipped with the necessary data transmission lines.

The Commission shall grant the Contractor access to its premises for the assembly of Complex hardware products on the Installation date, which must be duly notified by the Contractor with a Means of registered communication within five (5) Normal working days upon the Commission’s notification referred to in the last paragraph of Article III.3.2.2.

3.2.2. Procedure

– Pre-installation meeting

A pre-installation meeting may be organised. A technical representative of the Contractor will be available for each Specific Contract for a pre-installation meeting organised on the Commission’s premises. The purpose of this meeting is to review practical issues related to installation of the Products covered in the relevant Specific Contract. The minutes of each pre-installation meeting should be drafted after the pre-installation meeting by the Contractor, unless otherwise agreed in this meeting.

– Installation
Installation will be done in conformity with the relative Specific Contract and/or Service Level agreement and with the minutes of the pre-installation meeting and in accordance the methodology agreed in the pre-installation meeting if appropriate.

If the place of delivery is not the place of installation, the Commission shall arrange for Products to be moved at its own risk from the place of delivery to the place of installation within fifteen (15) Normal working days from the day of signature of the Consignment note and undertakes to notify the Contractor of the place of the move by a Means of communication within five (5) Normal working days upon successful move of the Products to the installation site.

3.3. Acceptance

3.3.1. The Commissioning date

The assembly of Complex hardware products and the bringing into service of a System shall be executed by the Contractor at its own expense, unless otherwise agreed in the Framework contract.

A Complex hardware product or System shall be assembled, installed, and brought into service no later than fifteen (15) Normal working days after the date of notification by the Commission of its removal to the installation site unless another time limit is laid down in the Specific Contract.

Upon successful installation, the Contractor shall notify the Commission by a Means of communication of the date on which the Complex hardware product or System has been brought into service, which date will be the Commissioning date for this particular Product or System.

3.3.2. The acceptance period

The acceptance period will run up to seventy-five (75) Normal working days from the Commissioning date.

During this acceptance period, the Commission shall notify any defaults in the Complex hardware product or System to the Contractor by a Means of communication. As from the date of such notification, the running of the acceptance period will be suspended up to the date on which the Contractor notifies by a Means of communication that it has remedied the notified default, this date will reinitiate the acceptance period for the rest of the seventy-five (75) Normal working days period, with a guaranteed minimum period of twenty-five (25) Normal working days after the last notification by the Contractor that it has remedied a default.

Upon the expiry of the acceptance period, acceptance of a Product will be recorded in a Certificate of Conformity, as stated in article II.1.1 of the
General Conditions that shall indicate inter alia the detailed nature of the accepted *Complex hardware products* and the reference number of this Framework contract and of the Specific Contract concerned.

If no *Certificate of Conformity* has been issued at the end of the acceptance period and if no notification of faulty operation is pending, the Commission is considered as having accepted the *Complex hardware product*.

3.3.3. Termination

If, due to faulty operation by the Contractor, acceptance cannot be completed within a maximal time limit of hundred and fifty (150) calendar days from the *Commissioning date*, unless a different time limit has been specified by Specific Contract, the Commission shall be entitled to terminate the Specific Contract after giving the Contractor a thirty (30) calendar days' notice by a *Means of communication* to meet its obligations. This provision is without prejudice to the Commission’s other rights under Article II.12.4 of the General Conditions.

3.4. Guarantee specifications for *Complex hardware products*

The Contractor shall guarantee all goods delivered in conformity with article II.1.2 of the General Conditions. During the two years guarantee period stated in article II.1.2 of the General Conditions the Contractor shall provide maintenance at its own and sole expenses.

The guarantee period shall be automatically extended by the total duration of stoppages attributable to the Contractor during that period, as recorded under the maintenance procedures. For this purpose only stoppages lasting eight (8) consecutive *Normal working hours* or more shall be counted. One day's extension therefore corresponds to a stoppage of eight (8) consecutive *Normal working hours*, which may be interrupted by a period of hours not defined as *Normal working hours*.

If failures during the guarantee period are such as to make a *Product* unusable for an uninterrupted period of more than one (1) calendar week, the Commission shall be entitled to have the *Complex hardware product* immediately replaced free of charge by the Contractor.

If the aggregate unavailability of a *Product* during *Normal working hours* exceeds forty-eight (48) hours, the Commission is entitled to terminate the part of the Specific Contract relating to that *Product*. 
3.5. **Leasing and Rental formula**

3.5.1. Determination of the periodic rental/leasing to be paid \( n \) times at the beginning of each period for an investment of \( PV \) with no residual value \( FV \) at the end of the \( n \) periods.

\[
PMT = PV \frac{i}{1 + i} \frac{1}{(1 + i)^n} \]

3.5.2. Determination of the periodic rental/leasing to be paid \( n \) times at the beginning of each period for an investment of \( PV \) with a residual value \( FV \) at the end of the \( n \) periods.

\[
PMT = (PV - FV) \frac{i}{1 + i} \frac{1}{(1 + i)^n} + FV \frac{i}{1 + i} \]

3.5.3. Determination of the periodic rental to be paid \( n \) times at the end of each period for an investment of \( PV \) with no residual value \( FV \) at the end of the \( n \) periods.

\[
PMT = PV \frac{i}{1 + i} \frac{1}{(1 + i)^n} \]

3.5.4. Determination of the periodic rental to be paid \( n \) times at the end of each period for an investment of \( PV \) with a residual value \( FV \) at the end of the \( n \) periods.

\[
PMT = (PV - FV) \frac{i}{1 + i} \frac{1}{(1 + i)^n} + FV \cdot i \]

**Abbreviation**  
**Description**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMT</td>
<td>Periodic payment</td>
</tr>
<tr>
<td>Ni</td>
<td>Nominal annual interest rate at order time</td>
</tr>
<tr>
<td>Mi</td>
<td>Margin on annual basis as defined in the Framework contract</td>
</tr>
<tr>
<td>i</td>
<td>Interest rate per period as defined in the Framework contract</td>
</tr>
<tr>
<td>NY</td>
<td>Number of payments per year</td>
</tr>
<tr>
<td>N</td>
<td>Total number of payments</td>
</tr>
<tr>
<td>PV</td>
<td>Investment amount = Present Value</td>
</tr>
<tr>
<td>FV</td>
<td>Residual Value = Future Value as defined in the Framework contract</td>
</tr>
<tr>
<td>P-P³</td>
<td>Percentages as defined in the Framework contract</td>
</tr>
</tbody>
</table>
3.5.5. Determination of the interest rate applicable for a term smaller than one year. For the calculation of the periodic interest rate applicable for a term smaller than one year, the formula is as follows:

\[ 1 + Ni = (1 + i)^{NY} \text{ or } i = (1 + Ni)^{NY} - 1 \]

3.5.6. Determination of the residual value. The residual value to be used for the sole purpose of computing a rental is given for the different horizons:

<table>
<thead>
<tr>
<th>Rental horizons</th>
<th>Residual value</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 years</td>
<td>P % of PV</td>
</tr>
<tr>
<td>3 years</td>
<td>P¹ % of PV</td>
</tr>
<tr>
<td>2 years</td>
<td>P² % of PV</td>
</tr>
<tr>
<td>1 year</td>
<td>P³ % of PV</td>
</tr>
</tbody>
</table>

3.6. Termination of the Contract for rental and leasing of Complex Hardware products

If one of the Parties terminate the Framework contract or Specific Contract on its own volition, the other party shall be compensated in accordance with the relative formula stated in 3.5 above.

3.7. Withdrawal of rented or leased Complex hardware product

Upon termination of a rental or leasing Specific Contract or Framework contract, the Product will be withdrawn by the Contractor at its own expense.
4. SPECIFIC PROVISIONS RELATING TO THE PURCHASE, RENTAL AND LEASING OF OTHER THAN COMPLEX HARDWARE PRODUCTS

4.1. Configuration and delivery

4.1.1. Configuration

In respect of each order:

(1) the other than Complex hardware products shall be specified in the Specific Contract and its Annexes;

(2) installation of other than Complex hardware products, including Software, shall be carried out in accordance with the specifications annexed to the Specific Contract or the relevant Service level agreement.

4.1.2. Delivery

The Delivery date shall be set at maximum thirty (30) calendar days from the date of signature of the Specific Contract, unless a different term has been specified in the Special Conditions of the Framework contract or in the Specific Contract.

If the Delivery date is overrun by more than twenty-one (21) calendar days, the Commission shall be entitled to terminate the Specific Contract in question.

A failure regarding the Delivery date is considered as damage to the Commission as defined in Article II.4 of the General Conditions.

The place of delivery shall be specified in each Specific Contract. There may be more than one place of delivery in a Specific Contract.

At the time of delivery, the incoming Products may be subject to quantitative and qualitative checks by the Commission within five (5) working days. The receipt of each delivery of Products shall be then recorded in a Consignment note signed by the Commission. Such Consignment note will be established as stated in article II.1.1. of the general Conditions.

If no Certificate of Conformity has been issued at the end of the one month acceptance period stated in Article II.1.1 and if no notification of faulty operation is pending, the Commission is considered as having accepted the other than Complex hardware product.
Unless expressly requested by the Commission, partial delivery of an item of a Specific Contract is not allowed.

4.2. **Guarantee specifications for other than Complex hardware products**

The Contractor shall guarantee all goods delivered in accordance with Article II.1.2 of the General Conditions.

When, under the terms of a Specific Contract, other than Complex hardware products are delivered on several dates, the guarantee period shall for all the components of the other than Complex hardware products expire with the end of the guarantee period of the final component of the other than Complex hardware product delivered in accordance with the Specific Contract.

During the two year guarantee period stated in Article II.1.2 of the General Conditions, the Contractor shall provide maintenance at its own and sole expense.

4.3. **Leasing and Rental formula**

See 3.5 above

4.4. **Termination of the Contract for rental and leasing of other than Complex hardware products.**

If one of the Parties terminates the Framework contract or Specific Contract on its own volition, the other Party will be compensated in accordance with the formula stated in the Framework contract.

4.5. **Withdrawal of rented or leased other than Complex hardware product**

Upon termination of a rental or leasing Specific Contract or Framework contract, the Products will be withdrawn by the Contractor at its own expenses.
5. SPECIFIC PROVISIONS RELATING TO LICENSED SOFTWARE

5.1. Delivery - installation - Documentation

5.1.1. The Delivery date of the Software shall be set at maximum ten (10) working days from the date of signature of the Specific Contract, unless a different term has been specified in the Framework contract or Specific Contract.

A failure concerning the Delivery date is considered as a damage to the Commission, as defined in Article II.4 of the Framework contract. The Commission may decide to claim the payment of damages, under the provision stated in the Framework contract.

5.1.2. The Commission shall be permitted to request additional assistance from the Contractor to install the Software on the adequate hardware equipment and for training of its personnel at the time of production start-up. Those additional expenses shall be charged to the Commission at the prices mentioned in the Framework contract.

5.1.3. The Commission and the Contractor shall each designate in due time one person each in charge of decisions regarding the delivery and installation of the Software.

5.1.4. The manner in which the Software shall be delivered shall be agreed upon in the Framework contract or Specific Contract.

When it is agreed that the Software shall be delivered as material support, the Software shall be delivered on a machine-readable medium (diskette or other) reproducing the original Software kept in the Contractor's or the Commission's archives. It shall be sent with one copy of the Documentation per licensed copy unless agreed otherwise between the Parties. Any additional copy of the Documentation shall be invoiced to the Commission at the price shown in the Framework contract.

When it is agreed that the Software may be downloaded by the Commission, then the Specific Contract shall precisely indicate the location of the download area (such as from an area on the Contractor’s website, from an FTP site, etc.) and provide the Commission, by a Means of communication, with the accurate and complete instructions, including access codes, enabling it to perform such downloads.

5.1.5. Delivery of the Software shall be recorded in a Consignment note, presented by the Contractor for signature by the Commission. In the event that the Software is downloaded, the Commission will issue the Consignment note based on the communication of the Contractor with the downloading instructions.
5.1.6. If no Certificate of Conformity has been issued at the end of the one month acceptance period stated in Article II.1.1 and, if no notification of faulty operation is pending, the Commission is considered as having accepted the Software.

5.1.7. The Contractor authorises the Commission to reproduce the Documentation for any Internal use provided that any copyright indication in the Documentation is also reproduced.

5.2. Trial - acceptance

5.2.1. Upon request of the Commission the Contractor shall grant for each new licensed Software or each New version of the Software a one (1)-month trial period during which the Software shall be available for non-productive use. Longer test periods and their conditions may be convened in the Framework contract or by Specific Contract.

5.2.2. The trial period shall begin on the day of the installation of the Software by the Contractor on the appropriate hardware equipment, or if the Commission does not require installation of the Software by the Contractor, fifteen (15) calendar days after signature of the Consignment note.

5.2.3. At the end of the trial period, acceptance of the Software shall only result from the signature, by both Parties, of the Certificate of Conformity as stated in Article II.1.1 of the General Conditions. If no Certificate of Conformity has been issued at the end of the trial period and, if no notification of faulty operation is pending, the Commission is considered as having accepted the Software.

5.2.4. At any moment during the trial period, the Commission may terminate the testing licence upon notification by a Means of communication with immediate effect if the Software does not perform and conform to its description, its specifications or its Documentation. Additional acquisitions of Software already tested by the Commission shall be accepted by signature of the Consignment note.

5.3. Guarantee specifications for Software

5.3.1. The Contractor shall guarantee all goods delivered in conformity with Article II.1.2 of the General Conditions.

5.3.2. The Contractor warrants that:

(1) the Software is in conformity with the Documentation supplied;

(2) the Software is capable of performing the functions described in the aforementioned Documentation and conform to the specifications described in the Framework contract or Specific Contract under consideration.
5.3.3. The Contractor does not warrant that the Software will enable the Commission to achieve its target aims, productivity levels or time savings.

5.3.4. Guarantee period

During the two-year guarantee period stated in Article II.1.2 of the General Conditions, the Contractor shall provide maintenance at its own and sole expense.

5.4. Use

5.4.1. The Contractor hereby grants, and the Commission accepts, a non-exclusive licence to use the Software, under the conditions set hereunder.

5.4.2. The Commission may use the Software for its Internal use.

5.4.3. The Commission may acquire "floating licences" for use by external, service-providing companies working under contract on projects for the Commission. At the end of the project, the Commission shall reclaim these licences and may either add them to the existing licence scheme or reallocate them to another company.

5.4.4. The Commission undertakes not to reproduce the Software in part or in whole, except for the purposes of back-ups and archives, and after taking all the necessary precautions. Such copies shall remain the Contractor's property.

5.4.5. The Parties may by Framework contract agree that the licence be an exclusive licence for the Commission to use the Software.

5.4.6. For the purpose of this Article III. 5.4., the Software shall be read as including its Documentation.

5.5. Compatibility

The Contractor guarantees to the Commission that at the date of signature of each Specific Contract the Software is compatible with all hardware or software described in the Specific Contract under consideration.

5.6. Intellectual property rights concerning Software — confidentiality

5.6.1. The Intellectual property rights attached to the Software and its Documentation shall remain the Contractor's exclusive property.

5.6.2. The Commission undertakes:

(1) to take all measures necessary vis-à-vis its end user personnel and persons having access to the Software and its Documentation, to ensure that the confidentiality of the Software is observed;
(2) not to pledge, assign, sub-license, transfer or lend, for payment or otherwise, the Software and its Documentation except in the manner set out under Article III.5.4;

(3) to inform the Contractor immediately in the event of seizure, to protest against it and to take all necessary steps in order to safeguard the integrity of the Contractor’s Intellectual property rights.

5.6.3. In the event of unauthorised disclosure of confidential information by either party, the other party shall address it a warning by a Means of Registered communication, requesting the first party to confirm that it will no longer disclose the said information. If no satisfactory response is obtained within the requested time limit, the other party is entitled to terminate this Framework contract. The parties recognise that damages may not constitute sufficient compensation for the other party, who may require reparation by injunction or other relief judged appropriate or necessary by the appropriate court of law.

5.7. Escrow rider

5.7.1. Except as set forth in Article III.5.7.4., the Commission and the Contractor shall appoint by mutual agreement an Escrow agent who will provide appropriate safekeeping facilities for the Product and its Documentation. The Escrow rider shall be concluded between the Contractor, the Escrow agent and the Commission. The Escrow rider shall provide that the Contractor must deposit with the Escrow agent a copy of all necessary Software and Documentation, source code and that the Commission shall have access to this copy as provided under Article III.5.7.2.

5.7.2. The Escrow rider shall provide that if the Contractor discontinues the maintenance of the Product, the Commission may instruct the Escrow agent to deliver a copy of the actual source code for the Products involved, including associated control statements required for operation, maintenance and use of the source code, each in programmer-readable form (collectively: "the Source code"), along with any associated Documentation including updates, to the relevant installation site. If the Commission receives the Source code in the manner provided hereunder, no additional fees shall be charged. Title to the Source code shall remain with the Contractor.

5.7.3. The Commission shall have the right at any time to contact the Escrow agent for the purpose of confirming the existence of the Source code and associated Documentation including updates thereto and for verification of the instructions to the Escrow agent to release the Source code under the circumstances specified under this Article.

5.7.4. The Contractor may propose to apply or to enter into a two-party escrow agreement with a third party escrow. In this case, the Contractor shall
provide, prior to applying or entering into such agreement, a copy of the proposed agreement to the Commission without charge and all fees in relation to it will be afforded by the Contractor. Should the Contractor fail to provide this copy, the Commission shall be entitled to claim execution of Article III.5.7.1.

5.7.5. When the Commission considers that the terms of the proposed escrow agreement offer sufficient guarantees to it, it will authorise the Contractor to apply or enter into such agreement with this third party escrow. If the Commission is not entirely satisfied, it may request additional guarantees before authorising the Contractor to enter into the agreement.

5.7.6. After having applied or entered into the authorised agreement, the Contractor shall notify the Commission in advance by a Means of registered communication and request its consent for the following:

- the implementation of any change in the terms of this agreement,
- its termination by the third party escrow,
- its replacement by a new Contract,
- a change in third party escrow, or any other change materially affecting the contractual guarantee offered to the Commission,

The Commission may offer its comments and may withhold its consent should it find that the change may result in the absence of the necessary guarantees of access to the Source code within the duration of the Framework contract.

5.7.7. In the event of the escrow agreement being terminated by the third party escrow, or its terms being changed such that the contractual guarantee is materially affected, the Contractor shall immediately notify the Commission of such fact by a Means of registered communication. The Contractor shall then seek a new escrow agreement meeting the requirements of this Article, subject to the Commission’s consent prior to the signature of such agreement.

5.7.8. Should the Contractor fail to notify the Commission of any change in accordance with the present Article, the Commission shall be entitled to terminate the Framework contract at the Contractor's expense. The Commission shall also be entitled to seek damages and interest from the Contractor resulting from the Contractor’s failure to fulfil its obligations under this Article.
6. SPECIFIC PROVISIONS RELATING TO HARDWARE AND SOFTWARE MAINTENANCE

6.1. Common provisions

6.1.1. Contractual maintenance shall commence on the day after expiry of the guarantee period applying to the Products delivered, unless another date is specified in the Framework contract or Specific Contract.

6.1.2. The Contractor shall at all times comply with the quality standards and the maintenance security rules contained in the Framework contract.

6.1.3. The maintenance shall be provided during Normal working hours on Normal working days. The Commission may require the Contractor to offer maintenance outside these times (Extended working hours), provided that there is an explicit provision in the Framework contract or Specific Contract stating the applicable rates in this case.

6.1.4. Maintenance is deemed to comprise all operations necessary to maintain a Product in perfect working order, or to restore a defective Product or one of its components to perfect working order, inclusive of the costs of travelling, parts and labour.

6.1.5. The provisions on Informatics Services consisting of maintenance apply to maintenance of both Software and Hardware, except where it is apparent from the provision that only one type of Product is concerned.

6.2. One-shot repair of Hardware

Where the Framework contract does not explicitly cover maintenance of Hardware, the Contractor agrees to perform one-shot repairs to Hardware at the Commission’s request. In response to such a request, the Contractor shall prepare without delay an estimate of the price of the repair and a timetable for its execution. The estimate and the timetable shall be provided free of charge to the Commission, regardless of whether or not the repair is executed. If the Commission accepts the estimate and timetable, an order shall be signed between the Parties. The Contractor shall not start to repair until it has received the relevant order signed by the Commission. It is explicitly agreed that all other conditions of the Framework contract shall also apply to a one-shot repair.
6.3. Maintenance

6.3.1. Terms

The Contractor undertakes to maintain the *Products* covered by this Framework contract in perfect working order.

In order to do this, the Contractor shall at all times have a stock of spare parts or shall obtain the necessary parts at its own and sole expense.

The Contractor shall provide maintenance service on site within four (4) hours at the Commission's request. This time limit is reduced to two (2) hours in the case of a blocked server. These time limits may be within either *Normal* or *Extended working hours*, depending on the choice made in accordance with Article III.6.1.3.

If the Contractor is of the opinion that a repair will not be possible within the maximum repair time from its arrival, it shall make a substitute *Product* available to the Commission for the duration of the repair.

Repairs, *Extensions* and modifications to the *System* shall be carried out only by the Contractor or the firms authorised by it.

Preventive maintenance operations shall be scheduled periodically, by agreement between the Commission and the Contractor.

The Contractor shall carry out corrective maintenance involving debugging, repair or replacement of faulty *Products* at the Commission's request. The Contractor undertakes, during these operations, to comply with the Commission's current central service desk action procedure when the failure occurs, as is described in Annex I.

The Contractor will formally close each maintenance operation. At the same time it will supply the information needed to measure the quality of the service and the *Products* against the standards laid down in the Framework contract. Where computer security has been affected it will submit a report.

The Contractor shall compile a monthly management report giving the following particulars of corrective maintenance carried out, without prejudice to the relative *Service Level Agreement*:

(1) a list of outstanding problems, with the cause and the expected date of resolution;

(2) an analysis of problems encountered by type of failure and *Product*;

(3) various statistics as requested by the Commission to enable it to produce an internal audit report.
6.3.2. **Hardware**

On the part of the Commission, hardware maintenance shall involve the obligation to use the *Products* as specified in the *Documentation* and the installation requirements, and not to alter or repair them itself.

On the part of the Contractor, without prejudice to the relative *Service level agreement*, corrective hardware maintenance shall involve:

1. diagnosing the cause of failures affecting *Products* or *Systems*, whether they are due to its *Products* or not;
2. correcting faults as rapidly as possible;
3. replacing components, printed circuits and electronic units that prove defective in the course of normal use, and effecting any alterations deemed necessary by it to improve operation of the *Systems*;
4. acting as the link with its own central maintenance departments;
5. reprogramming or replacing *Software* in the event of error;
6. providing "hot-line" support to resolve urgent problems and *System* failures;
7. providing drivers for correct function of *Hardware products*.

Maintenance shall not include the complete repair of all or part of any *Hardware products* that are no longer functional as a result of everyday wear and tear. If the Commission decides not to carry out the restoration proposed by the Contractor, the *Hardware products* in question will be withdrawn from the Framework contract.

6.3.3. **Software**

On the part of the Commission, without prejudice to the relative *Service level agreement*, *Software* maintenance shall involve:

1. preparing and sending the Contractor all documents and additional information at its disposal which the Contractor might reasonably request in order to detect and correct errors;
2. testing and accepting, when it is reasonable to do so, *New versions* or *New releases of Software*, as proposed by the Contractor. One year after the date of such an acceptance, the Contractor is no longer required to provide maintenance for previous versions or releases of *Software* and any dependent *Products*;
(3) installing any preventive corrections provided by the Contractor as long as it is agreed that such corrections are necessary.

On the part of the Contractor, without prejudice to the relative Service level agreement Software maintenance shall involve:

(1) diagnosing errors or faults encountered by the Contractor or the Commission in the content of the Software and making any necessary corrections; the Contractor shall effect corrections only if the error can be reproduced or if the Commission provides the Contractor with sufficient information from which the error can be diagnosed;

(2) providing the Commission with successive Software versions and releases and the relevant reference Documentation; installing New releases and New versions free of charge on the existing hardware at the Commission’s request; where necessary, adapting Products and/or information Systems that were using the previous version of the Software, free of charge;

(3) effecting all the Software corrections (including patches) needed to ensure that the Systems operate as specified in the Documentation within thirty (30) Normal working days of receipt of a notification by a Means of communication from the Commission giving details of a problem;

(4) rewriting the Software where necessary so as to correct all known problems or faults diagnosed by the Contractor;

(5) providing telephone support for the Commission during Normal working hours to advise it on the use of Software;

(6) providing "hot–line" support to resolve urgent problems and System failures.

6.3.4. The Contractor undertakes to provide the Commission, upon request, with any remote maintenance service, which it operates or intends to set up. The remote maintenance service must comply with the rules set out in the Framework contract. All terminal connection, utilisation and communication charges shall be borne by the Contractor.

6.3.5. Responsibility for diagnosis

The Contractor has sole responsibility for diagnosing and determining the origin of failures affecting all or part of the System or Products. As part of this obligation, the Contractor shall, in the event of a diagnosis error, reimburse any costs incurred by the Commission as a result of needless corrective action carried out by another supplier.
6.3.6. The expenses due to an intervention of the Contractor necessitated by a serious error of the Commission, recognised as such by the Commission, shall be borne by the Commission, according to the conditions and prices in the Framework contract.

6.3.7. Technical modifications by the Contractor

The Contractor may propose modifications on its own initiative. It will implement them, with the Commission's consent, at times agreed by both Parties. These modifications may not entail any additional cost to the Commission or cause any deterioration in performance or loss of function.

6.3.8. Equipment

Test equipment, tools, documents, programs and files kept on the Commission's premises for maintenance purposes shall remain the property of the Contractor and shall be insured by the Contractor.
7. SPECIFIC PROVISIONS RELATING TO ALL INFORMATICS SERVICES

7.1. Types of Services

7.1.1. Unless the Framework contract specifies to the contrary, Informatics services shall be provided, both Intra muros and Extra muros, during the Commission's Normal working hours on Normal working days.

7.1.2. Training relating to the use of the Products

Training shall be provided at the sites of the Commission in Brussels or Luxembourg. Training shall be addressed to users of the Product and to the technicians responsible for support within the Commission. The number of participants for each course shall be determined by mutual agreement between the Parties at the time of signature of the Specific Contract. Training and course materials must be available in at least English and French.

When training is provided on Commission premises, the infrastructure necessary to the courses (buildings, data-processing equipment, video equipment etc.), the administrative organisation of the courses (planning, notifications, and evaluation) and the reproduction of course documentation shall be provided by the Commission.

7.1.3. Consultancy relating to the use of the Products

Consultancy Informatics Services consist of transmitting know-how for the use of the Products covered by the Framework contract. They may be provided in Brussels and Luxembourg.

7.1.4. Technical Documentation of the Products

These Informatics Services shall relate to the drafting of any technical Documentation in relation to the Products covered by the Framework contract. They may be provided in Brussels and Luxembourg.

Technical Documentation shall be available in, at least, English and French. It shall be intended for users, both experienced and inexperienced, and for the Commission's technicians responsible for support or maintenance. The Contractor shall produce the Documentation on the basis of the content and structure specifications notified to it by the Commission. Reproduction of Documentation shall not form part of the service.
7.1.5. Integration work

This type of service not being covered by a maintenance Specific Contract aims at ensuring the correct operation of the Contractor's Products in an evolving multi-manufacturer environment. Informatics Services are performed on the basis of integration specifications communicated by the Commission. They may be provided on site in Brussels, Luxembourg, Dublin and Strasbourg.

7.1.6. Informatics engineering and maintenance

Informatics engineering consists of building and implementing projects of data-processing infrastructure (system software, telecommunications networks etc.) and maintenance on the basis of specifications provided by the Commission. Work may be provided on site in Brussels, Luxembourg, Dublin and Strasbourg.

7.1.7. Software development, maintenance and related activities

This consists of Software development, maintenance and related activities (e.g. studies, consultancy, documentation, quality assurance etc.) using the standard Commission Informatics Architecture, on the basis of specifications provided by the Commission. Details of work to be carried out will form part of the Specific Contract. Work may be provided on site in Brussels and Luxembourg.

7.1.8. Removals

Removals consist of transferring any Products from one specified place to the other, whether or not within the same building or city; they can take place during Normal or Extended working hours.

7.1.9. Logistics

Logistics includes but is not limited to, inventory, counting, equipment tagging, security labelling, just-in-time delivery, unpacking and installation in end-user’s office.

7.2. Time-and-means Contracts

7.2.1. Informatics Services shall be provided on a time-and-means basis when the Parties agree in the Specific Contract that a specified daily sum is to be paid for a given number of days in return for the provision of the means to perform the Informatics Services. In all cases, the Specific Contract shall state the purpose of the provision of the Services; this may involve an obligation for the Contractor to achieve a specific result.

7.2.2. At the request of the Commission, the Contractor shall supply all the necessary personal information regarding the staff providing the service
7.2.3. Every day during which Services are provided, the Contractor or its staff shall record the time worked. The records shall be set up in the manner defined by the Commission's technical representative named in the Specific Contract. At the end of each month, the Contractor or its staff shall complete and sign the attendance sheet proposed by the Commission and forward it to the Commission's technical representative who shall be in charge of checking the consistency between the daily records and the monthly attendance sheet.

7.3. **Quoted time-and-means Contracts.**

7.3.1. The “Quoted Time & Means” method may be used for service providers outside the Commission premises.

7.3.2. For Quoted Time & Means projects, the work will be ordered for a total number of days and will be divided into various sub-tasks (or "quoted time & means").

7.3.3. The Commission will provide the Contractor with a detailed description of each sub-task. The Contractor will then send the Commission an estimate of the number of days needed to carry out the sub-task and the expected Delivery date.

7.3.4. Once the estimate has been accepted by the Commission, only the number of days indicated in the estimate will be chargeable.

7.3.5. The invoicing, approved by the Commission, will be carried out on the basis of each sub-task accepted and signed for by the Commission using a specific form.

7.4. **Fixed-price Contracts**

7.4.1. *Informatics Services* shall be provided at a fixed price when the Parties agree in the Specific Contract that an overall sum, which must be justified using the agreed daily rates in the Framework contract, is to be paid following express acceptance of the work by the Commission.

7.4.2. The work shall be undertaken by the Contractor in accordance with the specifications set out in the Specific Contract. The specifications shall comprise in particular a description of the work, the timetable, reports, standards, reference manuals and details of the results and deliverables required.

7.4.3. Each result and deliverable shall be subject to acceptance by the Commission, in order to ensure conformity with the specifications. The acceptance period will run up to a maximum of seventy-five (75) Normal working days from the day of signature of a Consignment note. During this acceptance period, the Commission may notify any defaults in the result or deliverable to the Contractor by a Means of communication. As from the date of such notification, the running of the acceptance period
will be suspended up to the date on which the Contractor notifies by a *Means of communication* that it has remedied the notified default, which date will reinitiate the acceptance period for the rest of the seventy-five (75) *Normal working days* period, with a guaranteed minimum period of twenty-five (25) *Normal working days* after the last notification by the Contractor that it has remedied a default. Upon successful expiration of the acceptance period, the Commission will sign a *Certificate of Conformity* as stated in Article II.1.1 for each delivered result or deliverable. If no *Certificate of Conformity* has been issued at the end of the acceptance period and no default is pending, the Commission is considered as having accepted.

### 7.5. Stability of Services

#### 7.5.1. Prior to any Specific Contract, the Commission and the Contractor shall exchange the information needed for the Informatics Services to be provided. Throughout the term of the Framework contract they shall maintain the required level of information and make it available to the other party for the purpose of providing the Informatics Services. The updating of information shall not give rise to any payment.

#### 7.5.2. In accordance with Article II.1.3 of the General Conditions, throughout the term of the Framework contract the Contractor shall ensure that a stable service is maintained as required for the proper implementation of the Specific Contracts.

#### 7.5.3. When a change of staff or Informatics Services is unavoidable there should be a ten-day period of adjustment when both the replacement and original personnel should work side by side for training and transfer of relevant information. The costs of this period of adjustment shall be borne by the Contractor.

In no event shall the Contractor be able to plead a change of staff as a reason for not meeting any of its obligations, in particular with regard to deadlines and quality.

For all tasks with a low degree of substitutability, for example project co-ordination, studies and development, the Contractor shall ensure that staff are changed only in the event of "force majeure". The Commission must be notified in advance of any staff changes and reserves the right to refuse them.

#### 7.5.4. In the case of a time-and-means Framework contract, the Commission must be notified in advance of staff changes and reserves the right to refuse them. The Contractor agrees to organise these changes at no extra cost for the Commission and to provide for a transition period necessary for the outgoing staff to duly instruct and train the incoming staff.
7.6. **Timetable**

7.6.1. The timetable for the performance of the *Informatics Services* shall be laid down in each Specific Contract.

7.6.2. The Contractor shall propose a full and detailed timetable for *Software* development or related tasks. If such a timetable cannot be prepared for projects of longer duration, the Parties shall first fix a provisional timetable. The final timetable shall be fixed at a date stated in the Specific Contract.

7.6.3. The time needed by the Contractor to install and prepare *Software* or a *System* for operation shall be stated in the Specific Contract. If no time is specified, the period shall be fifteen (15) calendar days.
8. SPECIFIC PROVISIONS RELATING TO DEVELOPMENT AND MAINTENANCE OF COMMISSIONED SOFTWARE

8.1. Compliance with technical specifications

When providing Services of development or maintenance of Commissioned software to the Commission, the Contractor undertakes, in addition to the general quality requirements as specified in the Framework contract, to observe inter alia the latest version of the Commission’s document “Informatics Architecture”.

Except where expressly stated, the present Article III.8 shall also apply to the development and maintenance of a System commissioned by the Commission.

8.2. Acceptance

8.2.1. The Commissioned software shall be developed in accordance with its specifications as agreed upon under the Specific Contract, and the maintenance Services shall be provided in accordance with the conditions specified in the Specific Contract.

8.2.2. Delivery of the Commissioned software, or as the case may be, its different versions, shall be recorded in a Consignment note in accordance with Article II.1.1, presented by the Contractor for signature by the Commission.

8.2.3. Acceptance period

The acceptance period will run up to a maximum of seventy-five (75) Normal working days from the day of signature of the Consignment note. During this acceptance period, the Commission shall notify any defaults in the Commissioned software to the Contractor by a Means of registered communication. As from the date of such notification, the running of the acceptance period will be suspended up to the date on which the Contractor notifies by a Means of registered communication that it has remedied the notified default, which date will reinitiate the acceptance period for the rest of the seventy-five (75) Normal working days period, with a guaranteed minimum period of twenty-five (25) Normal working days after the last notification by the Contractor that it has remedied a default.

8.2.4. The Certificate of Conformity

Upon the expiry of the acceptance period, acceptance of the Commissioned software will be recorded in a Certificate of Conformity, as stated in Article II.1.1 of the General Conditions, which shall indicate inter alia any reservations the Commission may have regarding the Commissioned software. If no Certificate of Conformity has been issued at
the end of the acceptance period and, if no notification of faulty operation is pending, the Commission is considered as having accepted the Software.

8.2.5. If, after three (3) attempts at acceptance, the Commissioned software still fails to meet the terms of the Framework contract, the Commission shall have the following options:

(1) to require the Contractor to supply, without charge, a replacement or additional set of Software;

(2) to accept and retain part of the Commissioned software, at a reduced price agreed between the Commission and the Contractor;

(3) to refuse the Commissioned software and cancel the Framework contract or Specific Contract on reimbursement of any sums unduly paid.
8.2.6. The *Certificates of conformity* shall be annexed to the corresponding Specific Contract.

8.3. **Guarantee of proper operation of Commissioned software**

8.3.1. Except in the case of hidden defects, for which its liability shall be of unlimited duration, the Contractor shall guarantee the proper operation of *Commissioned software* in conformity with Article II.1.2 of the General Conditions. It shall be held responsible for the immediate repair, at its own expense, of any breakdowns that occur during the guarantee period, unless it can prove that such breakdowns have occurred for reasons other than mistakes made in performance of the service, or other than manufacturing or design errors in that portion of the work for which it was responsible.

8.3.2. The Commission shall notify by a *Means of communication* the Contractor of the type and scale of any failure as soon as it occurs. If the Contractor does not repair the *Commissioned software* without delay, the Commission may have it repaired by a third party, on the responsibility and at the own and sole expense of the Contractor.

8.3.3. The Parties shall jointly define and duly record in minutes the major problems that might affect the *Commissioned software*.

8.3.4. The duration of the guarantee shall be extended by the period which elapses between the notification of a major problem to the Contractor duly sent by the Commission during the stated guarantee period and the date at which the Commission accepts the corrected work.

8.4. **Intellectual property rights and ownership of source code**

8.4.1. Pursuant to the relevant article of the General Conditions, the Contractor hereby assigns to the Commission, which accepts, all *Intellectual property rights* on the *Commissioned software*, for the entire world, for the entire duration of the *Intellectual property rights* involved, and on an exclusive and definite manner.

8.4.2. The Commission shall become the owner of source code, results, *Documentation* and sets of tests that correspond to payments already made, except when the same relate to pre-existing *Software*. Further to Article III.2.3.4 of the General Terms and Conditions, the use of pre-existing *Software* shall be subject to the Commission's prior written consent.

8.4.3. The Commission shall have the right to disseminate and distribute a *Commissioned software* to third Parties, even if it contains pre-existing *Software*, subject to observance of any licence terms in respect of third party *Software*.

8.5. **User manuals and Documentation**
8.5.1. The Contractor shall prepare the manuals and Documentation needed for the appropriate and proper operation of the Commissioned software and shall make them available to the Commission. It shall comply with the provisions under Article III.10 in preparing such manuals and Documentation.

8.5.2. The material shall as a rule comprise:

(1) an installation manual;
(2) a “Getting Started” manual;
(3) an administration manual;
(4) a user manual;
(5) implementation Documentation.

8.5.3. The manuals and the Documentation shall be in the file format of a word processing Software used by the Commission and prepared so that they may be published on the Commission's intranet.

8.5.4. The user manuals and the Documentation shall be supplied in at least English and French, unless otherwise agreed.

8.5.5. The Contractor shall update and, if necessary, replace at a reasonable cost the user manuals and Documentation files for the maximum length of the Framework contract.

8.6. Interfaces and Compatibility

8.6.1. Where the Specific Contract mentions interfaces that need to be observed, the Contractor shall not modify such interfaces without the Commission's written agreement. Such agreement shall not be unreasonably withheld.

8.6.2. Where the Commissioned software supplied utilises Software from a third party and where that Software is updated, the Contractor shall adapt the Commissioned software in accordance with terms jointly agreed.

8.6.3. The Contractor shall ensure that all the Commissioned software supplied under the Framework contract is compatible and operates by means of interfaces with all other Software specified in the Framework contract.
9. SPECIFIC PROVISIONS RELATING TO TRAINING ORGANISED FOR THE COMMISSION

9.1. Instructors

Instructors shall be proposed to the Commission on the basis of their professional experience and their ability to provide the Services. Instructors accepted shall appear on the Commission's authorised list. The Commission must be notified in advance of staff changes and reserves the right to refuse them.

9.2. Organisation of courses

9.2.1. The Parties shall draw up a schedule of courses and preparatory measures for a period of several months, normally six (6) months. The schedule shall outline the content of the courses and measures their duration, the dates on which they are to take place, the intended instructors, the number of participants, and the cost.

9.2.2. The Parties shall make a final decision on all the data no later than four (4) weeks prior to the date on which training is to take place. The Contractor shall then specify, at the latest, the timetables for the courses and undertakes to adhere to it. If the schedule is disrupted by one or other party, that party shall endeavour to find an equivalent solution.

9.2.3. When an instructor is not available, a course may be cancelled or postponed no later than ten working days prior to its commencement. If three courses have been cancelled or postponed without meeting these conditions, the Commission shall be entitled to terminate the Framework contract pursuant to the provisions under Article II.12.

9.3. Instructor's manual

The Contractor shall comply with the Commission's standard practice as regards:

(1) the preparation and holding of courses;

(2) administrative regulations;

(3) health and safety regulations.

9.4. Provision of training Software

9.4.1. Training Software that has been developed specifically for the Commission shall be owned in full by the Commission.

9.4.2. The provision of training software shall be covered by a site licence, whose terms shall be consistent with the nature and subject of the training.
10. SPECIFIC PROVISIONS RELATING TO DOCUMENTATION PRODUCED FOR THE COMMISSION

10.1.1. The Intellectual property rights in the Documentation that has been developed specifically for the Commission shall rest exclusively with the Commission.

10.1.2. The provision of reference Documentation shall be covered by a site licence, the terms of which shall be consistent with the nature and subject of the Documentation.
ANNEX I:

CENTRAL SERVICE DESK ACTION PROCEDURE

The Commission’s Central Service Desk (SDC) also known as Central Call Dispatch, is responsible for handling and dispatching all service requests relating to office equipment and computers and telecommunications services. The SDC does not itself resolve problems: it is a central point for their receipt, registration and onward transmission to the appropriate internal or external support unit. It is also responsible for monitoring and follow-up of the service supplied.

The term Service requests covers both request for assistance and requests for corrective action: requests of the latter kind are denominated incidents. An incident may later be re-classified as a problem, indicating that resolution requires some long-term action (e.g. a Software bug or hardware design problem) or as a known error, meaning that a solution is available and awaiting implementation by agreement.

(1) Requests shall be notified by the SDC to the Contractor’s Service Desk (CSD) by telephone or any other agreed means immediately after assignment of the request.

(2) The SDC always confirms in writing each request addressed to the CSD, giving all relevant details.

(3) The CSD shall confirm receipt of a request to the SDC by returning its own reference number.

(4) Each telephone communication between the SDC and the CSD shall be confirmed immediately by fax, email or, where the CSD has access, by direct entry into the Commission’s SDC database.

(5) The CSD shall deal only with requests that have been sent by the SDC. The Contractor shall immediately provide to the SDC full details of any request received from any other source within the Commission.

(6) Each action on a request shall be notified to the SDC. A report shall be sent immediately by the CSD indicating the action’s nature, starting date and time and probable duration. If the request has not been resolved, the reasons shall be given, along with an estimated date and time for resolution.

(7) Should an action require contact within a DG and the responsible person at the DG be unavailable, the Contractor shall report this to the SDC as soon as possible.

(8) Completion of a request that has been satisfied shall be notified as soon as possible by the CSD to the SDC. Mention shall be made of the cause, the date and time the action started, its duration in minutes, and any other relevant details. The
Contractor shall be responsible for the accuracy of the information he supplies. The reporting user shall be notified immediately by the person carrying out the action.

(9) The resolution time given by the Contractor shall be accepted by the SDC if it is no more than 24 hours prior to receipt of the complete closure by fax or email. Otherwise its arrival time at the SDC will be taken as resolution time.

(10) A request shall be closed by the SDC if the DG concerned explicitly accepts the results of the action. If it does not, the request shall remain open for one week. If the DG does not indicate its rejection during this period, the request shall automatically be closed definitively.

(11) Where a Framework contract defines service quality requirements for incident handling and/or service requests performance, the Contractor’s performance with respect to these requirements shall be calculated on the basis of the information recorded in the Commission’s SDC database.

Unless otherwise specified in the Framework contract, quality requirements shall in general be based on two elements: ‘response time’ and ‘resolution time’

Response time shall be defined as the period between:

- the time of assignment of a service request by the SDC to the CSD, and
- the commencement of the diagnostic or repair work by the Contractor's qualified representative at the location indicated in the report or, if attendance at the incident location is not required, the commencement of by telephone or other agreed means.

Resolution time shall be defined as the time between:

- the time of assignment of a service request by the SDC to the CSD, and the notification of completion of the action to the SDC (see paragraphs 8 and 9 above), or the re-classification or re-assignment of the incident.
- repeated incidents of the same type applying to the same item over a short period may be cumulated for purposes of calculating the resolution time.

The clock stops running:

- outside the defined hours of cover
- if access to the contact person or equipment cannot be effected. In this case the SDC shall be notified immediately and the grounds for the delay explained
- if by agreement with the reporting user, an appointment is made for the beginning of the action. The clock shall restart at the time of the appointment.

(12) On request, the Contractor shall be sent a daily or weekly summary of all open requests by the SDC.
ANNEX II: TEMPLATE OF DECLARATION OF CONFIDENTIALITY

EUROPEAN COMMISSION

DECLARATION OF CONFIDENTIALITY

The Commission and the Contractor

having signed a Framework contract, number on …

and a Specific Contract, number on …

For carrying out work governed by these agreements I, the undersigned, declare that I have read and shall comply with the security and confidentiality rules laid down in:

– Articles I.8 of the Special Conditions, II.16 of the General Conditions and III.2.2 of the General terms and conditions for Information Technologies contracts

– Article 5 of the Commission decision on protection of information systems [C(95) 1510 23/11/95].


Date and place:

[signature]

NAME
ANNEX III:

COMMISSION DECISION ON PROTECTION OF INFORMATION SYSTEMS
[C(95) 1510 23/11/95]
Annex I

List of services covered by the contract and schedule of prices
MTS IV Lot 1
List of services covered by the contract and schedule of prices
Annex I to Framework Contract DI/07910

**CONTRACTOR:** PROXIMUS SA

<table>
<thead>
<tr>
<th>Table of content:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A - Mobile voice &amp; data</td>
<td>This worksheet contains the prices proposed by the contractor regarding the mobile voice &amp; data communications services (see §5.2, §5.3, §5.4 and §5.5 of the service specifications)</td>
</tr>
<tr>
<td>B - Satellite</td>
<td>This worksheet contains prices proposed by the contractor regarding the satellite communications services (see §5.16 of the service specifications)</td>
</tr>
<tr>
<td>C - Indoor coverage</td>
<td>This worksheet contains prices proposed by the contractor regarding the indoor coverage infrastructure projects, to cover future new EU buildings (see §5.10 of the service specifications)</td>
</tr>
<tr>
<td>D - Service Desk</td>
<td>This worksheet contains prices proposed by the contractor regarding the off site service desk (see §5.11 of the service specifications)</td>
</tr>
<tr>
<td>Countries</td>
<td>This worksheet indicates the repartition of each country within each geographical zone (EU, ROW1, ROW2, ROW3) proposed by the contractor (see §5.1 of the Service requirements). Such choice will serve as a basis for the invoicing of the services consumed within the FWC</td>
</tr>
</tbody>
</table>
### MOBILE VOICE & DATA COMMUNICATIONS PRICES

#### Value added tax (price is EUR per unit, with 6% included)

<table>
<thead>
<tr>
<th>EU</th>
<th>MNO1</th>
<th>MNO2</th>
<th>MNO3</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Value added tax (price is EUR per unit, with 4% included)

<table>
<thead>
<tr>
<th>EU</th>
<th>MNO1</th>
<th>MNO2</th>
<th>MNO3</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Value added tax (price is EUR per unit, with 2% included)

<table>
<thead>
<tr>
<th>EU</th>
<th>MNO1</th>
<th>MNO2</th>
<th>MNO3</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Value added tax (price is EUR per unit, with 0% included)

<table>
<thead>
<tr>
<th>EU</th>
<th>MNO1</th>
<th>MNO2</th>
<th>MNO3</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

#### Data charges (price is EUR per unit, with 6% included)

<table>
<thead>
<tr>
<th>EU</th>
<th>MNO1</th>
<th>MNO2</th>
<th>MNO3</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

#### Data charges (price is EUR per unit, with 4% included)

<table>
<thead>
<tr>
<th>EU</th>
<th>MNO1</th>
<th>MNO2</th>
<th>MNO3</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

#### Data charges (price is EUR per unit, with 2% included)

<table>
<thead>
<tr>
<th>EU</th>
<th>MNO1</th>
<th>MNO2</th>
<th>MNO3</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

#### Data charges (price is EUR per unit, with 0% included)

<table>
<thead>
<tr>
<th>EU</th>
<th>MNO1</th>
<th>MNO2</th>
<th>MNO3</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SATELLITE COMMUNICATIONS PRICES</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monthly subscription, per SIM card, for satellite service</td>
<td>Unit price (in EUR)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection fee per satellite communication</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Price per 20 seconds of satellite communication</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Price per minute (60 seconds) of satellite data transmission</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monthly fee for the leasing of a compatible satellite phone (for the duration of the PWC)</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IRIDIUM GO! Text and Call - 6-months voucher</td>
<td>5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## INDOOR COVERAGE PRICES (for future new EUI building)

<table>
<thead>
<tr>
<th>PRELIMINARY IMPLEMENTATION PROJECT (unit price in EUR)</th>
<th>Unit price (in EUR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site survey, walk test, documentation and price proposal (for small building, i.e. &lt;1,000 m²)</td>
<td></td>
</tr>
<tr>
<td>Site survey, walk test, documentation and price proposal (for medium building, i.e. &lt;10,000 m²)</td>
<td></td>
</tr>
<tr>
<td>Site survey, walk test, documentation and price proposal (for large building, i.e. &gt;10,000 m²)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BUILDING BLOCKS for MULTI-PROVIDER DISTRIBUTED ANTENNAS SYSTEM - DAS - (unit price in EUR)</th>
<th>Unit price (in EUR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Renting of base station (BTS) 2-4G for the duration of the FWC</td>
<td></td>
</tr>
<tr>
<td>Provisioning of antenna 2-4G, including all connectivity (coaxial cabling, splitters, etc.)</td>
<td></td>
</tr>
<tr>
<td>Provisioning of access point 5G (connectivity via fiber and structural cabling will be provided by EUI)</td>
<td></td>
</tr>
<tr>
<td>SERVICE DESK PRICES</td>
<td>Unit price (in EUR) per month</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Price for initiating Service Desk (below 1,000 active SIM/e-SIM cards)</td>
<td></td>
</tr>
<tr>
<td>Price for service desk per each 1,000 additional active SIM and/or e-SIM cards</td>
<td></td>
</tr>
<tr>
<td>[OPTION]: Price for using contractor’s ticketing tool, in case EUI do not own its own ticketing system</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>Geographical Zone</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Afghanistan</td>
<td></td>
</tr>
<tr>
<td>Albania</td>
<td></td>
</tr>
<tr>
<td>Algeria</td>
<td></td>
</tr>
<tr>
<td>American Samoa</td>
<td></td>
</tr>
<tr>
<td>Andorra</td>
<td></td>
</tr>
<tr>
<td>Anguilla</td>
<td></td>
</tr>
<tr>
<td>Antigua and Barbuda</td>
<td></td>
</tr>
<tr>
<td>Argentina</td>
<td></td>
</tr>
<tr>
<td>Armenia</td>
<td></td>
</tr>
<tr>
<td>Aruba</td>
<td></td>
</tr>
<tr>
<td>Australia</td>
<td></td>
</tr>
<tr>
<td>Australian External Territories</td>
<td></td>
</tr>
<tr>
<td>Austria</td>
<td></td>
</tr>
<tr>
<td>Azerbaijan</td>
<td></td>
</tr>
<tr>
<td>Bahamas</td>
<td></td>
</tr>
<tr>
<td>Bahrain</td>
<td></td>
</tr>
<tr>
<td>Bangladesh</td>
<td></td>
</tr>
<tr>
<td>Barbados</td>
<td></td>
</tr>
<tr>
<td>Belarus</td>
<td></td>
</tr>
<tr>
<td>Belgium</td>
<td></td>
</tr>
<tr>
<td>Belize</td>
<td></td>
</tr>
<tr>
<td>Benin</td>
<td></td>
</tr>
<tr>
<td>Bermuda</td>
<td></td>
</tr>
<tr>
<td>Bhutan</td>
<td></td>
</tr>
<tr>
<td>Bolivia</td>
<td></td>
</tr>
<tr>
<td>Bonaire, Saint Eustatius and Saba</td>
<td></td>
</tr>
<tr>
<td>Bosnia and Herzegovina</td>
<td></td>
</tr>
<tr>
<td>Botswana</td>
<td></td>
</tr>
<tr>
<td>Brazil</td>
<td></td>
</tr>
<tr>
<td>British Virgin Islands</td>
<td></td>
</tr>
<tr>
<td>Brunei</td>
<td></td>
</tr>
<tr>
<td>Bulgaria</td>
<td></td>
</tr>
<tr>
<td>Burkina Faso</td>
<td></td>
</tr>
<tr>
<td>Burundi</td>
<td></td>
</tr>
<tr>
<td>Cambodia</td>
<td></td>
</tr>
<tr>
<td>Cameroon</td>
<td></td>
</tr>
<tr>
<td>Canada</td>
<td></td>
</tr>
<tr>
<td>Cape Verde</td>
<td></td>
</tr>
<tr>
<td>Cayman Islands</td>
<td></td>
</tr>
<tr>
<td>Central African Republic</td>
<td></td>
</tr>
<tr>
<td>Chad</td>
<td></td>
</tr>
<tr>
<td>Chile</td>
<td></td>
</tr>
<tr>
<td>China</td>
<td></td>
</tr>
<tr>
<td>Colombia</td>
<td></td>
</tr>
<tr>
<td>Comoros</td>
<td></td>
</tr>
<tr>
<td>Congo</td>
<td></td>
</tr>
<tr>
<td>Congo Democratic Republic</td>
<td></td>
</tr>
<tr>
<td>Cook Islands</td>
<td></td>
</tr>
<tr>
<td>Costa Rica</td>
<td></td>
</tr>
<tr>
<td>Croatia</td>
<td></td>
</tr>
<tr>
<td>Cuba</td>
<td></td>
</tr>
<tr>
<td>Curacao</td>
<td></td>
</tr>
<tr>
<td>Cyprus</td>
<td></td>
</tr>
<tr>
<td>Czech Republic</td>
<td></td>
</tr>
<tr>
<td>Denmark</td>
<td></td>
</tr>
<tr>
<td>Diego Garcia</td>
<td></td>
</tr>
<tr>
<td>Djibouti</td>
<td></td>
</tr>
<tr>
<td>Dominica</td>
<td></td>
</tr>
<tr>
<td>Dominican Republic</td>
<td></td>
</tr>
<tr>
<td>East Timor</td>
<td></td>
</tr>
<tr>
<td>Ecuador</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Egypt</td>
<td></td>
</tr>
<tr>
<td>El Salvador</td>
<td></td>
</tr>
<tr>
<td>Equatorial Guinea</td>
<td></td>
</tr>
<tr>
<td>Eritrea</td>
<td></td>
</tr>
<tr>
<td>Estonia</td>
<td></td>
</tr>
<tr>
<td>Ethiopia</td>
<td></td>
</tr>
<tr>
<td>Falkland Islands</td>
<td></td>
</tr>
<tr>
<td>Faroe Islands</td>
<td></td>
</tr>
<tr>
<td>Fiji</td>
<td></td>
</tr>
<tr>
<td>Finland</td>
<td></td>
</tr>
<tr>
<td>France</td>
<td></td>
</tr>
<tr>
<td>French Departments and Territories in the Indian Ocean</td>
<td></td>
</tr>
<tr>
<td>French Guiana</td>
<td></td>
</tr>
<tr>
<td>French Polynesia</td>
<td></td>
</tr>
<tr>
<td>Gabon</td>
<td></td>
</tr>
<tr>
<td>Gambia</td>
<td></td>
</tr>
<tr>
<td>Georgia</td>
<td></td>
</tr>
<tr>
<td>Germany</td>
<td></td>
</tr>
<tr>
<td>Ghana</td>
<td></td>
</tr>
<tr>
<td>Gibraltar</td>
<td></td>
</tr>
<tr>
<td>Greece</td>
<td></td>
</tr>
<tr>
<td>Greenland</td>
<td></td>
</tr>
<tr>
<td>Grenada</td>
<td></td>
</tr>
<tr>
<td>Guadeloupe</td>
<td></td>
</tr>
<tr>
<td>Guam</td>
<td></td>
</tr>
<tr>
<td>Guatemala</td>
<td></td>
</tr>
<tr>
<td>Guinea</td>
<td></td>
</tr>
<tr>
<td>Guinea-Bissau</td>
<td></td>
</tr>
<tr>
<td>Guyana</td>
<td></td>
</tr>
<tr>
<td>Haiti</td>
<td></td>
</tr>
<tr>
<td>Honduras</td>
<td></td>
</tr>
<tr>
<td>Hong Kong</td>
<td></td>
</tr>
<tr>
<td>Hungary</td>
<td></td>
</tr>
<tr>
<td>Iceland</td>
<td></td>
</tr>
<tr>
<td>India</td>
<td></td>
</tr>
<tr>
<td>Indonesia</td>
<td></td>
</tr>
<tr>
<td>Iran</td>
<td></td>
</tr>
<tr>
<td>Iraq</td>
<td></td>
</tr>
<tr>
<td>Ireland</td>
<td></td>
</tr>
<tr>
<td>Israel</td>
<td></td>
</tr>
<tr>
<td>Italy</td>
<td></td>
</tr>
<tr>
<td>Ivory Coast</td>
<td></td>
</tr>
<tr>
<td>Jamaica</td>
<td></td>
</tr>
<tr>
<td>Japan</td>
<td></td>
</tr>
<tr>
<td>Jordan</td>
<td></td>
</tr>
<tr>
<td>Kazakhstan</td>
<td></td>
</tr>
<tr>
<td>Kenya</td>
<td></td>
</tr>
<tr>
<td>Kiribati</td>
<td></td>
</tr>
<tr>
<td>Kosovo</td>
<td></td>
</tr>
<tr>
<td>Kuwait</td>
<td></td>
</tr>
<tr>
<td>Kyrgyzstan</td>
<td></td>
</tr>
<tr>
<td>Laos</td>
<td></td>
</tr>
<tr>
<td>Latvia</td>
<td></td>
</tr>
<tr>
<td>Lebanon</td>
<td></td>
</tr>
<tr>
<td>Lesotho</td>
<td></td>
</tr>
<tr>
<td>Liberia</td>
<td></td>
</tr>
<tr>
<td>Libya</td>
<td></td>
</tr>
<tr>
<td>Liechtenstein</td>
<td></td>
</tr>
<tr>
<td>Lithuania</td>
<td></td>
</tr>
<tr>
<td>Luxembourg</td>
<td></td>
</tr>
<tr>
<td>Macao</td>
<td></td>
</tr>
<tr>
<td>Macedonia</td>
<td></td>
</tr>
<tr>
<td>Madagascar</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td></td>
</tr>
<tr>
<td>Malawi</td>
<td></td>
</tr>
<tr>
<td>Maldives</td>
<td></td>
</tr>
<tr>
<td>Mali</td>
<td></td>
</tr>
<tr>
<td>Malta</td>
<td></td>
</tr>
<tr>
<td>Marshall Islands</td>
<td></td>
</tr>
<tr>
<td>Martinique</td>
<td></td>
</tr>
<tr>
<td>Mauritania</td>
<td></td>
</tr>
<tr>
<td>Mauritius</td>
<td></td>
</tr>
<tr>
<td>Mexico</td>
<td></td>
</tr>
<tr>
<td>Micronesia</td>
<td></td>
</tr>
<tr>
<td>Moldova</td>
<td></td>
</tr>
<tr>
<td>Monaco</td>
<td></td>
</tr>
<tr>
<td>Mongolia</td>
<td></td>
</tr>
<tr>
<td>Montenegro</td>
<td></td>
</tr>
<tr>
<td>Montserrat</td>
<td></td>
</tr>
<tr>
<td>Morocco</td>
<td></td>
</tr>
<tr>
<td>Mozambique</td>
<td></td>
</tr>
<tr>
<td>Myanmar</td>
<td></td>
</tr>
<tr>
<td>Namibia</td>
<td></td>
</tr>
<tr>
<td>Nauru</td>
<td></td>
</tr>
<tr>
<td>Nepal</td>
<td></td>
</tr>
<tr>
<td>Netherlands</td>
<td></td>
</tr>
<tr>
<td>New Caledonia</td>
<td></td>
</tr>
<tr>
<td>New Zealand</td>
<td></td>
</tr>
<tr>
<td>Nicaragua</td>
<td></td>
</tr>
<tr>
<td>Niger</td>
<td></td>
</tr>
<tr>
<td>Nigeria</td>
<td></td>
</tr>
<tr>
<td>Niue</td>
<td></td>
</tr>
<tr>
<td>North Korea</td>
<td></td>
</tr>
<tr>
<td>Northern Mariana Islands</td>
<td></td>
</tr>
<tr>
<td>Norway</td>
<td></td>
</tr>
<tr>
<td>Oman</td>
<td></td>
</tr>
<tr>
<td>Pakistan</td>
<td></td>
</tr>
<tr>
<td>Palau</td>
<td></td>
</tr>
<tr>
<td>Palestinian Authority</td>
<td></td>
</tr>
<tr>
<td>Panama</td>
<td></td>
</tr>
<tr>
<td>Papua New Guinea</td>
<td></td>
</tr>
<tr>
<td>Paraguay</td>
<td></td>
</tr>
<tr>
<td>Peru</td>
<td></td>
</tr>
<tr>
<td>Philippines</td>
<td></td>
</tr>
<tr>
<td>Poland</td>
<td></td>
</tr>
<tr>
<td>Portugal</td>
<td></td>
</tr>
<tr>
<td>Puerto Rico</td>
<td></td>
</tr>
<tr>
<td>Qatar</td>
<td></td>
</tr>
<tr>
<td>Romania</td>
<td></td>
</tr>
<tr>
<td>Russia</td>
<td></td>
</tr>
<tr>
<td>Rwanda</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Saint Helena, Ascension and Tristan da Cunha</td>
<td></td>
</tr>
<tr>
<td>Saint Kitts and Nevis</td>
<td></td>
</tr>
<tr>
<td>Saint Lucia</td>
<td></td>
</tr>
<tr>
<td>Saint Pierre and Miquelon</td>
<td></td>
</tr>
<tr>
<td>Saint Vincent and the Grenadines</td>
<td></td>
</tr>
<tr>
<td>Samoa</td>
<td></td>
</tr>
<tr>
<td>San Marino</td>
<td></td>
</tr>
<tr>
<td>Sao Tome and Principe</td>
<td></td>
</tr>
<tr>
<td>Satellite</td>
<td></td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td></td>
</tr>
<tr>
<td>Senegal</td>
<td></td>
</tr>
<tr>
<td>Serbia</td>
<td></td>
</tr>
<tr>
<td>Seychelles</td>
<td></td>
</tr>
<tr>
<td>Sierra Leone</td>
<td></td>
</tr>
<tr>
<td>Singapore</td>
<td></td>
</tr>
<tr>
<td>Sint Maarten (Dutch part)</td>
<td></td>
</tr>
<tr>
<td>Slovak a</td>
<td></td>
</tr>
<tr>
<td>Slovenia</td>
<td></td>
</tr>
<tr>
<td>Solomon Islands</td>
<td></td>
</tr>
<tr>
<td>Somal a</td>
<td></td>
</tr>
<tr>
<td>South Africa</td>
<td></td>
</tr>
<tr>
<td>South Korea</td>
<td></td>
</tr>
<tr>
<td>South Sudan</td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td></td>
</tr>
<tr>
<td>Sri Lanka</td>
<td></td>
</tr>
<tr>
<td>Sudan</td>
<td></td>
</tr>
<tr>
<td>Suriname</td>
<td></td>
</tr>
<tr>
<td>Swaziland</td>
<td></td>
</tr>
<tr>
<td>Sweden</td>
<td></td>
</tr>
<tr>
<td>Switzerland</td>
<td></td>
</tr>
<tr>
<td>Syria</td>
<td></td>
</tr>
<tr>
<td>Taiwan</td>
<td></td>
</tr>
<tr>
<td>Tajikistan</td>
<td></td>
</tr>
<tr>
<td>Tanzania</td>
<td></td>
</tr>
<tr>
<td>Thailand</td>
<td></td>
</tr>
<tr>
<td>Togo</td>
<td></td>
</tr>
<tr>
<td>Tokelau</td>
<td></td>
</tr>
<tr>
<td>Tonga</td>
<td></td>
</tr>
<tr>
<td>Trinidad and Tobago</td>
<td></td>
</tr>
<tr>
<td>Tunisia</td>
<td></td>
</tr>
<tr>
<td>Turkey</td>
<td></td>
</tr>
<tr>
<td>Turkmenistan</td>
<td></td>
</tr>
<tr>
<td>Turks and Caicos Islands</td>
<td></td>
</tr>
<tr>
<td>Tuvalu</td>
<td></td>
</tr>
<tr>
<td>Uganda</td>
<td></td>
</tr>
<tr>
<td>Ukraine</td>
<td></td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td></td>
</tr>
<tr>
<td>United Kingdom</td>
<td></td>
</tr>
<tr>
<td>Universal Personal Telecommunications (UPT) - I.e. Countries without a proper international prefix</td>
<td></td>
</tr>
<tr>
<td>Uruguay</td>
<td></td>
</tr>
<tr>
<td>US Virgin Islands</td>
<td></td>
</tr>
<tr>
<td>USA</td>
<td></td>
</tr>
<tr>
<td>Uzbekistan</td>
<td></td>
</tr>
<tr>
<td>Vanuatu</td>
<td></td>
</tr>
<tr>
<td>Vatican City</td>
<td></td>
</tr>
<tr>
<td>Venezuela</td>
<td></td>
</tr>
<tr>
<td>Vietnam</td>
<td></td>
</tr>
<tr>
<td>Wallis and Futuna</td>
<td></td>
</tr>
<tr>
<td>Yemen</td>
<td></td>
</tr>
<tr>
<td>Zambia</td>
<td></td>
</tr>
<tr>
<td>Zimbabwe</td>
<td></td>
</tr>
</tbody>
</table>
Annex II

EMAS ENVIRONMENTAL POLICY
EMAS Environmental Policy

In 1997, the European Commission started a process of green housekeeping activities and subsequently in 2001, decided to pilot an environmental management system as laid down in Regulation (EC) 761/2001 allowing voluntary participation by organisations in a Community eco-management and audit scheme (EMAS).

In 2009, the Commission decided to extend this environmental management system to all its activities and buildings in Brussels and Luxembourg as described in Decision C (2009) 6873). In making this commitment, the European Commission recognises the positive contribution it can make to sustainable development as a long-term goal, through its policy and legislative processes as well as in its day-to-day operations and decisions.

Concretely, the Commission commits to minimise the environmental impact of its everyday work and continuously improve its environmental performance by:

1. Taking measures to prevent pollution and to achieve more efficient use of natural resources (mainly energy, water and paper);
2. Taking measures to reduce overall CO₂ emissions (mainly from buildings and transport);
3. Encouraging waste prevention, maximising waste recycling and reusing and optimising waste disposal;
4. Integrating environmental criteria into public procurement procedures and into the rules regarding the organisation of events;
5. Complying with relevant environmental legislation and regulations;
6. Stimulating the sustainable behaviour of all staff and subcontractors through training, information and awareness-raising actions;
7. Progressively extending all the above to all its activities and buildings;

and in relation to the Commission's core business by:

8. Systematically assessing the potential economic, social and environmental impacts of major new policy and legislative initiatives and promoting the systematic integration of environmental objectives into Community policies;
9. Ensuring the effectiveness of environmental legislation and funding in creating environmental benefits;
10. Promoting transparent communication and dialogue with all interested parties, both internally and externally.
By virtue of the powers conferred on the Appointing Authorities, the European Commission's EMAS Steering Committee, hereby approves the Policy Statement and commits to adopt the EMAS objectives, targets and action plan of the Commission, supervise the functioning of the system and monitor the use of the human and financial resources allocated to EMAS for an efficient deployment of the environmental management system.

This document shall take effect on the date of its signature, Brussels

On Behalf of the EMAS Steering Committee,

Chairman
Annex V

SPECIFIC CONTRACT (TEMPLATE)
SPECIFIC CONTRACT N° [as specified under Specific Contract Number in the Data Appendix]

implementing Framework Contract n° DI/0xxxx (SLG.AVT.DI0xxxx)

-------

FIXED PRICE

The European Union referred to below as the Commission of the one part and the Contractor of the other part – [as specified under The Parties in the Data Appendix]

HAVE AGREED

the following as regards the implementation of Framework Contract n° DI/0xxxx (SLG.AVT.DI0xxxx) signed by the Commission and the Contractor on [as specified under Framework Contract Signature Date in the Data Appendix].

Article 1. PREAMBLE

1.1 This Specific Contract is based on the Contractor's formal offer under Request n° [as specified under Request Number in the Data Appendix] – Annex II to this Specific Contract. Once signed by the parties, the Specific Contract shall be governed by the Framework Contract. This Specific Contract does not amend the provisions of the afore mentioned Framework Contract. The terms of this Contract Body, the Data Appendix and the Technical Annex (Annex I) shall take precedence over the terms of the formal offer (Annex II).

Article 2. SUBJECT MATTER

2.1 The subject matter of this Specific Contract is [as specified under Subject in the Data Appendix].

2.2 The Contractor undertakes, subject to the terms set out in the Framework Contract and in this Specific Contract and its Annexes, which form an integral part of it, to perform the tasks specified in Annexes I and II.

Article 3. DURATION AND LOCATION

3.1. This Specific Contract shall enter into force [as specified under Start Date in the Data Appendix].

The execution of the tasks shall [as specified under End Date in the Data Appendix].

3.2. The tasks shall be performed as specified under the Request referenced under article 1.1. The period of execution of the tasks may be extended only with the express written agreement of the parties by means of an amendment to this specific contract.
before such period elapses. In no case shall the tasks be executed later than six (6) months after expiry of the Framework Contract.

3.3. The tasks shall be performed [as specified under Place of Delivery in the Data Appendix].

Article 4. PERFORMANCE

4.1. The tasks performed by the Contractor under this Specific Contract shall result in "deliverables", defined according to the provisions specified in Annexes I and II.

Article 5. PRICES AND PAYMENTS

5.1. The Commission undertakes to pay the Contractor, in consideration for the services rendered under the Specific Contract, a total maximum price of [as specified under Total Amount in the Data Appendix].

It is understood that this amount shall cover all expenditure incurred by the Contractor in carrying out the Specific Contract.

5.2. In conformity with Article III.1.5.4 of the General Terms and Conditions for Information Technologies Contracts, the invoicing procedures for the services, once accepted by the Commission, are as follows [as specified under Invoicing Procedure in the Data Appendix].

5.3. Payments shall be made to account n° [as specified under Bank Account in the Data Appendix] on production of the invoice showing separately the amount of the fees and the VAT applied and within no more than 30 calendar days from the date the invoice is received by the Unit indicated in Article 5.4 below. Invoices presented by the Contractor shall indicate his place of taxation for VAT purposes and shall specify separately the amounts not including VAT and those including VAT. The payment shall be deemed to have been effected on the day the Commission's financial account is debited.

For Contractors established in Belgium, the provisions of this contract constitute a request for VAT exemption No 450, provided the Contractor includes the following statement in their invoice(s): “Exonération de la TVA, article 42, paragraphe 3.3 du code de la TVA (circulaire 2/1978)” or an equivalent statement in the Dutch or German language.

For other countries

Pursuant to articles 3 and 4 of the Protocol on the Privileges and Immunities of the European Communities, the Commission is exempt from all taxes, duties and charges, in particular value added tax, on payments made under this order. The contractor receives and keeps in his records the form entitled "VAT and Excise Duty Exemption Certificate" duly completed and signed by the Commission. The invoice must contain the following statement: "VAT Exemption / International Body / Article 151 of Council Directive 2006/112/EC".

5.4. The address for invoices is:

[as specified under Invoicing information in the Data Appendix].
Article 6. **SUBCONTRACTING**  
[as specified under Subcontracting in the Data Appendix].

Article 7. **PERFORMANCE GUARANTEES**  
[as specified under Performance Guarantees in the Data Appendix].

Article 8. **ADMINISTRATIVE PROVISIONS**

8.1. The persons responsible for implementing this Contract are:

*For the Commission*: [as specified under Persons Responsible for the Customer in the Data Appendix].

*For the Contractor*: [as specified under Persons Responsible for the Contractor in the Data Appendix].

8.2. All communications relating to the implementation of the Specific Contract must be in the form of written correspondence and be sent to the appropriate responsible persons.

Article 9. **EXPLOITATION OF THE RESULTS**

9.1. In accordance with Art.I.13 of the Framework Contract.

Article 10. **ADDITIONAL PROVISIONS**  
[as specified under Additional Provisions in the Data Appendix].

Article 11. **ANNEXES**

The following documents are annexed to the Specific Contract and form an integral part of it:

- **Annex I**: Technical Annex. In case e-Request is used, Technical Annex is available in the e-Request application under Request n° [as specified under Request Number in the Data Appendix].

- **Annex II**: Contractor’s formal offer. In case e-Request is used, Contractor's formal offer is available in the e-Request application under Request n° [as specified under Request Number in the Data Appendix].

- **Annex III**: Task Acceptance Form / Dispatch advice (Service Receipt)

- **Annex IV**: Declaration on the list of pre-existing rights
**ANNEX III**

**TASK ACCEPTANCE FORM / DISPATCH ADVICE (SERVICE RECEIPT)**

**RECEIPT ADVICE SLIP FOR "DELIVERABLES" FOR SPECIFIC CONTRACT N° xxxxx**  
**UNDER FRAMEWORK CONTRACT N° DI/xxxx**

**Original document - duly signed - to be attached to the invoice**

**Invoicing period: from ____/____/____ till ____/____/____**

**RECEIPT OF WORK**

*To be filled in by the Contractor and by the Commission*

<table>
<thead>
<tr>
<th>Contractor</th>
<th>Commission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of <strong>last delivery of invoicing period</strong></td>
<td></td>
</tr>
<tr>
<td>Person responsible for checking (in block capitals)</td>
<td></td>
</tr>
<tr>
<td>Comments</td>
<td></td>
</tr>
<tr>
<td>Date and signature</td>
<td></td>
</tr>
</tbody>
</table>
Data Appendix

In case of paper flow (non e-Ordering), this Data Appendix is valid when accompanied with the Contract Body duly initialed by the parties and referring to the same Specific Contract Number and Framework Contract Number

-------------------------------------------------

Specific Contract n°

Framework Contract n°

FP version 13 12 2016

Contract Type: Fixed Price

Specific Contract Number:

Framework Contract Number:

The Parties

European Union

The European Union (hereinafter referred to as "the Union"), represented by the European Commission (hereinafter referred to as "the Commission"), which is represented for the purposes of the signature of this contract by Mr/Mrs XXXXXXXXXXXXX , Job Title, Directorate General – Directorate X

The Contractor

[NAME

ADDRESS

VAT N°]

which together form XXX CONSORTIUM, represented by Mr/Ms XXXXXXXXXXXXX - Job Title XXX -&- Mr/Ms XXXXXXXXXXXXX - Job Title XXX

the contractor identified above shall be jointly and severally liable vis-à-vis the Commission for the performance of this contract

Framework Contract Signature Date: DD/MM/YYYY

Request Number: TEST II-XXXXXXXXXXXXXXXX dated DD/MM/YYYY

Subject: XXXXXXXXXXXXX

Start Date:

[OPTION 1]
on the date it is signed by the last contracting party.

[OPTION 2]
on the later between the following two dates: the date it is signed by the last contracting party and the date following the end of Specific Contract n° yyyyyyy.

[OPTION 3]
on the later between the following two dates: the date it is signed by the last contracting party and dd/mm/yyyy.

[OPTION 4]
on the latest among the following three dates: the date it is signed by the last contracting party, dd/mm/yyyy and the date following the end of Specific Contract n° yyyyyyy.

End Date:

[OPTION 1]
be completed at the latest on dd/mm/yyyy.

[OPTION 2]
end on dd/mm/yyyy.

[OPTION 3]
last for a duration of XX months.

Place of Delivery:

[OPTION 1]
on the premises of the Contractor in

[OPTION 2]
on the premises of the Commission in

[OPTION 3]
on the premises of both of the Contractor and the Commission in

Total Amount: XXXXX EUR

Invoicing Procedure

[OPTION 1a - WHEN THE SPECIFIC CONTRACT RELATES TO AN AMOUNT LESS THAN €25,000, NO LIST OF PRE-EXISTING RIGHTS REQUIRED]

- 100 % of the total price of the specific contract shall be invoiced when the service has been fully provided, based on receipt advice slips accepted and signed by the Commission in accordance with the form in Annex III (to be attached to the invoice).

[OPTION 2a - FOR SERVICES CONSISTING IN A SINGLE PERFORMANCE WHEN THE SPECIFIC CONTRACT RELATES TO AN AMOUNT OF €25,000 OR MORE, NO LIST OF PRE-EXISTING RIGHTS REQUIRED]
Data Appendix

Maximum of 30 % of the total price of the specific contract shall be invoiced on receipt of first deliverable, based on receipt advice slips accepted and signed by the Commission in accordance with the form in Annex III (to be attached to the invoice).

The remaining amount shall be invoiced on completion of the work, based on receipt advice slips accepted and signed by the Commission in accordance with the form in Annex III (to be attached to the invoice).

[OPTION 3a - FOR CONTINUOUS SERVICES (INCLUDING SERVICES PERFORMED IN PERIODIC INSTALLMENTS) WHEN THE SPECIFIC CONTRACT RELATES TO AN AMOUNT OF €25,000 OR MORE, NO LIST OF PRE-EXISTING RIGHTS REQUIRED]
- For the deliverables specified in the Annex I, invoices shall be submitted periodically - at the end of the calendar [quarter][month] based on receipt advice slips accepted and signed by the Commission in accordance with the form in Annex III (to be attached to the invoice).

[OPTION 1b - WHEN THE SPECIFIC CONTRACT RELATES TO AN AMOUNT LESS THAN €25,000, LIST OF PRE-EXISTING RIGHTS IS REQUIRED]
- 100 % of the total price of the specific contract shall be invoiced when the service has been fully provided, based on receipt advice slips accepted and signed by the Commission in accordance with the form in Annex III (to be attached to the invoice).

With the invoice, the Contractor shall provide the Commission with a list of the pre-existing rights and third parties' rights including its personnel, creators or other right holders as provided for in Article II.23.4 of the Framework Contract.

[OPTION 2b - FOR SERVICES CONSISTING IN A SINGLE PERFORMANCE WHEN THE SPECIFIC CONTRACT RELATES TO AN AMOUNT OF €25,000 OR MORE, LIST OF PRE-EXISTING RIGHTS IS REQUIRED]
- Maximum of 30 % of the total price of the specific contract shall be invoiced on receipt of first deliverable, based on receipt advice slips accepted and signed by the Commission in accordance with the form in Annex III (to be attached to the invoice).

The remaining amount shall be invoiced on completion of the work, based on receipt advice slips accepted and signed by the Commission in accordance with the form in Annex III (to be attached to the invoice).

With the last invoice, the Contractor shall provide the Commission with a list of the pre-existing rights and third parties' rights including its personnel, creators or other right holders as provided for in Article II.23.4 of the Framework Contract.

[OPTION 3b - FOR CONTINUOUS SERVICES (INCLUDING SERVICES PERFORMED IN PERIODIC INSTALLMENTS) WHEN THE SPECIFIC CONTRACT RELATES TO AN AMOUNT OF €25,000 OR MORE, LIST OF PRE-EXISTING RIGHTS IS REQUIRED]
- For the deliverables specified in the Annex I, invoices shall be submitted periodically - at the end of the calendar [quarter][month] based on receipt advice slips accepted and signed by the Commission in accordance with the form in Annex III (to be attached to the invoice).

With the last invoice, the Contractor shall provide the Commission with a list of the pre-existing rights and third parties' rights including its personnel, creators or other right holders as provided for in Article II.23.4 of the Framework Contract.

Bank Account: XXXXXXXXXXXXXXXXXXXX held with XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Subcontracting
[OPTION 1] Not applicable

[OPTION 2]

6.1. In accordance with Article II.10 of the General Conditions, the Contractor has been authorised to subcontract under the present specific contract by way of acceptance of its offer submitted under the Request referenced in Art.1.1. and signature of the present specific contract concerning the subcontractor(s) mentioned in the offer.

6.2. Tasks stated under the Request referenced under article 1.1. may be performed by the subcontractor, entirely at the risk of the Contractor

6.3. Without prejudice to the Commission's other rights under Article II.17 of the General Conditions, if the Contractor fails to meet his obligations, the Specific Contract with the Commission may be terminated in accordance with Article II.17 (k) of the General Conditions. This clause applies throughout the term of the Specific Contract.

Performance Guarantees
Not applicable

Invoicing information
Department code:
Address:

Persons Responsible for the Customer
Administrative matters:
[NAME]
[OFFICE] [TEL]

Technical matters:
[NAME]
[OFFICE] [TEL]

Persons Responsible for the Contractor
[NAME]
[TEL] [EMAIL]

Additional Provisions
Not applicable

In case of paper flow (non e-Ordering), done in duplicate at Brussels on

For the Contractor For the Commission
Framework contract DI-07910

Mobile Telephony Services
(MTS IV)
Lot 1

ANNEX VII

Service Level Agreement (SLA)
1. INTRODUCTION ........................................................................................................................................................................... 4

1.1. DOCUMENT OVERVIEW.................................................................................................................................................. 4
1.2. SCOPE AND OBJECTIVES ........................................................................................................................................... 4
1.3. DEFINITIONS AND ACRONYMS .................................................................................................................................................. 4
  1.3.1 Acronyms ................................................................................................................................................................................. 4
  1.3.2 ITIL Best Practices ................................................................................................................................................................. 4
  1.3.3 Service Hours ...................................................................................................................................................................... 4
  1.3.4 Planned Maintenance ......................................................................................................................................................... 5
1.4. VALIDITY AND REVIEW PROCESS ........................................................................................................................................... 5

2. INTERFACES ................................................................................................................................................................................... 5

2.1 CONTRACTOR INTERFACES ................................................................................................................................................... 6
  2.1.1 Account Manager ......................................................................................................................................................... 6
  2.1.2 Service Manager ............................................................................................................................................................ 6
  2.1.3 IT Security/GDPR Coordinator .................................................................................................................................... 6
2.2 EUI INTERFACES ..................................................................................................................................................................... 6
  2.2.1 Administrative contact .................................................................................................................................................. 6
  2.2.2 Technical contact .......................................................................................................................................................... 6

3. LIQUIDATED DAMAGES AND CLOCK MANAGEMENT ........................................................................................................... 6

6.7 GENERAL .................................................................................................................................................................................. 6
6.8 PRINCIPLES OF CALCULATION OF LIQUIDATED DAMAGES .................................................................................................. 7
6.9 MAXIMUM AMOUNT FOR A LIQUIDATED DAMAGE ............................................................................................................... 7
6.10 PAYMENT OF LIQUIDATED DAMAGES .................................................................................................................................. 7
6.11 BOUNDARY CONDITIONS AND “FORCE MAJEURE” ........................................................................................................ 7
6.12 ROUNING OFF OF VALUES .................................................................................................................................................. 8
6.13 CLOCK MANAGEMENT IN RELATION WITH THE MEASUREMENT OF SERVICE QUALITY ......................................................... 8

4. SERVICE LEVEL OF ORDERING AND INVOICING ................................................................................................................... 8

4.1 ORDERING PROCESS ........................................................................................................................................................... 8
  4.1.1 Process workflow .......................................................................................................................................................... 8
  4.1.2 Process indicator, Minimum Service Level Requirements ........................................................................................... 9
  4.1.3 Liquidated damages ........................................................................................................................................................ 9
4.2 INVOICING QUALITY PARAMETERS ....................................................................................................................................... 9
  4.2.1 Process indicators, Minimum Service Level Requirements .......................................................................................... 9
  4.2.2 Liquidated damages ...................................................................................................................................................... 10

5. SERVICE LEVEL OF GENERAL ADMINISTRATIVE SERVICES ................................................................................................ 10

5.1 SERVICE REVIEW REPORT AND SERVICE REVIEW/AD-HOC MEETINGS .............................................................................. 10
  5.1.1 Process indicators, Minimum Service Level Requirements .......................................................................................... 11
  5.1.2 Liquidated damages ........................................................................................................................................................ 11
5.2 STEERING COMMITTEE MEETINGS (SCM) ............................................................................................................................. 12
  5.2.1 Process indicators, Minimum Service Level Requirements .......................................................................................... 12
  5.2.2 Liquidated damages ...................................................................................................................................................... 13
5.3 CODE OF CONDUCT AND OFFICIAL-COMPLAINTS ........................................................................................................... 13
  5.3.1 Process indicators, Minimum Service Level Requirements .......................................................................................... 13
  5.3.2 Liquidated damages ...................................................................................................................................................... 14
5.4 SERIOUS FAULTS ................................................................................................................................................................... 14
  5.4.1 Process indicators, Minimum Service Level Requirements .......................................................................................... 14
  5.4.2 Liquidated damages ...................................................................................................................................................... 15

6. SERVICE LEVEL FOR SERVICE MANAGEMENT PROCESSES ............................................................................................ 15

6.1 INCIDENT MANAGEMENT .................................................................................................................................................... 15
  6.1.1 Process indicators, Minimum Service Level Requirements .......................................................................................... 19
  6.1.2 Liquidated damages ...................................................................................................................................................... 19
6.2 AVAILABILITY MANAGEMENT .................................................................................................................................................. 20
6.2.1. Process indicators, Minimum Service Level Requirements .......................................................... 21
6.2.2. Liquidated damages ...................................................................................................................... 22
6.3 REQUEST FULFILLMENT (APPLICABLE ONLY TO LOT 1) .......................................................... 22
6.3.1. Process indicators, Minimum Service Level Requirements .......................................................... 22
6.3.2. Process indicators, Minimum Service Level Requirements .......................................................... 22
6.3.3. Liquidated damages ...................................................................................................................... 22
6.4 CHANGE MANAGEMENT .................................................................................................................. 23
6.4.1. Process indicators, Minimum Service Level Requirements .......................................................... 23
6.4.2. Process indicators, Minimum Service Level Requirements .......................................................... 24
6.4.3. Liquidated damages ...................................................................................................................... 24
6.5 PROBLEM MANAGEMENT ................................................................................................................. 25
6.5.1. Process indicators, Minimum Service Level Requirements .......................................................... 25
6.5.2. Process indicators, Minimum Service Level Requirements .......................................................... 25
6.5.3. Liquidated damages ...................................................................................................................... 25
6.6 SERVICE ESCALATION PROCEDURE .................................................................................................. 25
6.6.1. Process indicators, Minimum Service Level Requirements .......................................................... 25
6.6.2. Process indicators, Minimum Service Level Requirements .......................................................... 26
6.6.3. Liquidated damages ...................................................................................................................... 26
6.7 COMMUNICATION QUALITY ............................................................................................................... 26
6.7.1. Definition ........................................................................................................................................... 26
6.7.2. Process indicators, Minimum Service Level Requirements .......................................................... 27
6.7.3. Liquidated damages ...................................................................................................................... 27
6.7.4. Benchmarking of communication quality ....................................................................................... 27
6.8 REPORTING SERVICES .......................................................................................................................... 28
6.8.1. Process indicators, Minimum Service Level Requirements .......................................................... 28
6.8.2. Liquidated damages ...................................................................................................................... 28
6.9 PHASE-IN SERVICES ............................................................................................................................ 29
6.9.1. Process indicators, Minimum Service Level Requirements .......................................................... 29
6.9.2. Liquidated damages ...................................................................................................................... 30
6.10 PHASE-OUT SERVICES ...................................................................................................................... 30
6.10.1. Process indicators, Minimum Service Level Requirements .......................................................... 30
6.10.2. Liquidated damages ...................................................................................................................... 30
7. SERVICE/BUSINESS CONTINUITY MANAGEMENT .............................................................................. 31
7.1. Process indicators, Minimum Service Level Requirements .............................................................. 32
7.2. Liquidated damages ............................................................................................................................ 32
8. DATA PROTECTION COMPLIANCE ...................................................................................................... 32
8.1. Process indicators, Minimum Service Level Requirements .............................................................. 32
8.2. Liquidated damages ............................................................................................................................ 33
9. INFORMATION SECURITY MANAGEMENT ........................................................................................... 33
9.1. Process indicators, Minimum Service Level Requirements .............................................................. 33
9.2. Liquidated damages ............................................................................................................................ 33
10. ANNEX 1 – SUMMARY OF COMMITTED SERVICE LEVELS (SL) AND KEY PERFORMANCE INDICATORS (KPI) .................................................................................................................. 35
11. ANNEX 2: GLOSSARY .......................................................................................................................... 47
1. **INTRODUCTION**

1.1. **Document overview**

This document sets out the Service Level Agreement (SLA), whose acceptance by the contractor is mandatory. It details the minimum services to be provided, the minimum service levels, the procedures and the applicable liquidated damages in case of non-fulfilment of the required service levels.

The SLA described hereafter defines technical terms, targets and conditions of the Framework contract with the Contractor and forms an integral part of the Framework contract.

1.2. **Scope and objectives**

The Service Level Agreement is a part of the Framework Contract between the Contractor and the participating EU Institutions, Bodies and Agencies (called "EUI"), and supplements its clauses and conditions.

It documents the Contractor’s committed service level performance quality indicators (hereafter mentioned as "Key Performance Indicators", or just "KPI") for the services provided under the Framework Contract, to the EUI.

This Service Level Agreement provides services quality indicators (or metrics). A single SLA will be used for the Framework Contract which concerns all EUIs. This Service Level Agreement applies for the management of quality in the delivery of the Service by the Contractor to each EUI. The way in which the quality parameters, defined in this Service Level Agreement, are measured and the way they are reported upon is done individually by EUI, directly by the Contractor with each of the EUIs.

Other aspects that are particular to a single EUI may be added in the specific contract of the concerned EUI. Such provisions can only change details in the execution of the Framework Contract, but they can neither change the provisions of the Framework Contract nor change this SLA.

1.3. **Definitions and acronyms**

1.3.1 **Acronyms**

Acronyms are explained in the tendering specifications and in Annex 8 *Service requirements* of the Tender specifications.

1.3.2 **ITIL Best Practices**

The EUI adopts ITIL-based best practices for ICT Services Management. ITIL V3 terminology is therefore also used hereafter, in the context of this SLA document.

The Contractor acknowledges this fact and accepts to adopt similar best practice in its interfaces with the EUI concerning the delivery of the Service, assuring a smooth interface with the internal ITIL-based terminology, tools, processes and procedures of the EUI.

1.3.3 **Service Hours**

The service hours are the periods of time during which the Service shall be available. The following service hours are applicable:
### 1.3.4 Planned Maintenance

Maintenance that may affect the service quality shall be subject to prior approval, at least two weeks before the intervention, mentioning a detailed description of the planned activities, their impact and risks.

All planned maintenance interventions shall be undertaken outside of the normal working time for the EUI, in a maintenance window on **normal working days from 7 p.m. to 7 a.m., or at any time on days that are not normal working days.**

All maintenance that are not being communicated beforehand will be considered as incidents and liquidated damages will be applied consequently.

### 1.4. Validity and review process

The SLA will be part of the Framework Contract. It will be applicable from the signature of the framework contract to its termination and the termination of all specific contracts and order forms signed under the framework contract.

During the lifetime of the Framework Contract, the Contracting Authority may propose changes in the Service Level Agreement. These changes cannot be in contradiction with the contract itself. Their purpose is to clarify or help the execution of the contract. They will need the agreement of the contractor. After approval, a new version will be signed by both parties and incorporated into the Framework Contract by way of an amendment.

Any new services component introduced during the course of the contract execution will be subject to the same SLA, unless dictated otherwise by business needs.

### 2. Interfaces

Contact persons are defined by both parties, and clearly identified with their names, e-mail addresses and telephone numbers, either in the Framework Contract or in the relevant Specific Contracts and order forms covering the Service.
2.1 Contractor interfaces

The Contractor commits to provide at least two contact persons:

2.1.1 Account Manager

The Account Manager is responsible for all commercial aspects of the Service and all matters that may affect the commercial relationship between the EUI and the Contractor. The Account Manager must be reachable by the EUI during normal working hours. In case of absence, a pre-designated back-up person must be reachable.

2.1.2 Service Manager

The Service Manager is the interface for all the technical and operational matters. He/She will have to perform and receive notifications and escalations related to any Incident or Crisis situations related to the Service delivered to the EUI. He/She will also have to follow up all the SLA matters, thereby being responsible on the Contractor side for meeting the Service Delivery and Service Management KPI defined in this SLA.

The Service Manager will also act as the main responsible interface for the service desk for any specific issues, whereas the Contractor’s service-desk operators will be in contact with the EUI for the daily service operations.

2.1.3 IT Security/GDPR Coordinator

The contractor will designate a dedicated IT security risk coordinator, who will work in close collaboration with DIGIT’s security compliance team. The roles and responsibilities of this position are described in Annex 8 – Service Requirements of the Tender specifications.

2.2 EUI interfaces

The EUI commits to provide at least two contact persons:

2.2.1 Administrative contact

The Administrative contact is in charge of managing all administrative and contractual issues related to the Service with the Contractor.

2.2.2 Technical contact

The Technical contact is in charge of managing all technical and operational issues related to the Service with the Contractor. He/She will have to perform and receive notifications and escalations related to any Incident or Crisis situations related to the Service delivered by the Contractor. He/She will be in charge of the follow-up of all the SLA matters, thereby being responsible on the EUI side for assuring that the Service Delivery and Service Management KPI defined in this SLA are met by the Contractor.

3. LIQUIDATED DAMAGES AND CLOCK MANAGEMENT

6.7 General

All calculations are done on a per EUI basis.
6.8 Principles of calculation of liquidated damages

Liquidated damages may be applied when the parameters covered by the SLA do not reach the required service levels.

The EUI use Incident Management, Change Management, Request management, Problem Management and other processes inspired by ITIL best practices. For European Commission, these processes are supported by a Service Management Tool (SMT) used for reference for Service Management, where the required information is entered into tickets. Other participating EUIs may use their own ticketing systems for service management.

Liquidated damage calculations are based on a “Liquidated Damages Unit”, called LDU, and the EUI’s consumption calculated in Euro.

A LDU for both lot 1 and lot 2 is defined as follows:

$$LDU = \frac{AVG_3}{200},$$

where consumption is represented by the value $AVG_3$ as defined below:

$$AVG_3 = \frac{\sum_{m=3}^{1} (Monthly\_Invoice_m)}{3}$$

In other words, $AVG_3$ is the average amount of the monthly invoices of the last three previous months for all Services provided by the Contractor to the concerned EUI in the context of the Framework Contract.

6.9 Maximum amount for a liquidated damage

All liquidated damages are cumulative during a given month, but the total of all liquidated damages paid by the Contractor to the EUI on monthly basis is capped by the following amount:

$$\sum \text{Liquidated damages per month} \leq 15\% \text{ of } AVG_3$$

Liquidated damages linked to serious faults in relation to a security incident are not capped.

6.10 Payment of liquidated damages

Liquidated damages are applied as a rebate on the next invoice received after their occurrence. They are calculated using liquidated damages in case the service objectives are not met as described in this document. The table provided in Annex 1 of this document gives a summary of all the service objectives.

6.11 Boundary conditions and “Force Majeure”

“Force Majeure” is formally defined in the Framework Contract.

No liquidated damages are applied in the case of a situation of “Force Majeure”, or if the situation results from some wrong doing on the part of the EUI or one of its representatives.

Specifically excluded from the calculations of availability and Incident Management are outages caused by:
• Situations of *Force Majeure*;
• Actual maintenance duration (in minutes) during scheduled maintenance windows;
• Wrong operation of the equipment or service, or delay introduced by the EUI.

Such occurrences will be logged by the Contractor and communicated to the EUI as part of the Service management activities.

Power failures of Contractor's equipment installed at the EUI site will not be excluded from the calculations of the availability. The Contractor must foresee uninterruptible power supply systems for his equipment.

6.12 **Rounding off of values**

Whenever mathematical functions are used for the measurement of metrics or for the calculation of liquidated damages, two significant digits after the decimal point must be kept.

6.13 **Clock management in relation with the measurement of service quality**

The resolution time for P1 and P2 incidents is measured 24/7. Exceptionally a stop-clock may be applied if the Contractor justifies that the incident is outside its scope of control/action.

The resolution time for P3 and P4 incidents is measured during SDH (service desk hours) on NWD (normal working days):

Service desk hours SDH are provided in section 1.3.3 of this document.

The defined priority levels are P1, P2, P3 and P4 (P1 being the most critical level). A non-exhaustive list of typical incidents and their associated priority levels is provided in section 6.1 of this document.

4. **SERVICE LEVEL OF ORDERING AND INVOICING**

4.1. **Ordering process**

4.1.1. *Process workflow*

The EUI initiates the order process by issuing a request to the contractor. An attached technical annex will provide the high-level parameters or values to be used to prepare a proposal.

The contractor shall send the proposal (or, in case a revision is requested by the EUI, a revised proposal) that meets the requirements set by the technical annex within 3 normal working days.

After acceptance, the EUI proposes a specific contract and requests the contractor to have it signed.

The contractor sends back the signed specific contract within 2 normal working days.

After acceptance, the EUI signs the specific contract and sends a copy to the contractor.
### 4.1.2. Process indicator, Minimum Service Level Requirements

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order Execution Quality (OEQ)</td>
<td>This quality parameter measures the overall quality of the execution of the ordering process for basic services.</td>
</tr>
<tr>
<td></td>
<td>The proposal must be in line with the EUI’s requirements.</td>
</tr>
<tr>
<td>Respect of deadlines (ORD)</td>
<td>The proposal (or, in case a revision is requested by the EUI, a revised proposal) is sent by the Contractor within 3 normal working days after receipt of EUI’s request. The specific contract is sent back signed by the Contractor within 2 normal working days after the receipt of the EUI’s proposal.</td>
</tr>
</tbody>
</table>

### 4.1.3. Liquidated damages

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order Execution Quality (OEQ)</td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of 0,08 LDU in case the number of revisions necessary to attain the expected level of quality is greater or equal to 3.</td>
</tr>
<tr>
<td>Respect of deadlines (ORD)</td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of 0,08 LDU per day of delay.</td>
</tr>
</tbody>
</table>

### 4.2. Invoicing Quality Parameters

#### 4.2.1. Process indicators, Minimum Service Level Requirements

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invoice accuracy</td>
<td>This quality parameter measures the ability of the contractor to produce accurate invoices.</td>
</tr>
<tr>
<td></td>
<td>The invoices shall give accurate information and cover the elements as described in the corresponding Specific Contract. This parameter will be measured against the number of invoice rejections before the invoice can be accepted:</td>
</tr>
<tr>
<td></td>
<td>This parameter is measured based on the following KPI’s:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Invoicing Accuracy (INVA)</strong> KPI: 100% of invoices must be accurate</td>
</tr>
<tr>
<td></td>
<td>- <strong>Correction of invoice (INVCOR)</strong> KPI: Delivery of corrected invoice within 5 normal working days after error notification.</td>
</tr>
<tr>
<td>Invoice timeliness &amp; follow-up</td>
<td>This quality parameter measures the ability of the contractor to produce invoices in due time and to follow-up the consumption of ad-hoc services.</td>
</tr>
<tr>
<td></td>
<td>The invoices shall be produced in due time. This parameter will be measured against the number of invoices received outside the deadlines indicated in the Contract:</td>
</tr>
</tbody>
</table>
- **Invoicing Punctuality (INVP) KPI**: 20th calendar day on month N+1, or next normal working day.

100% of invoices must be received according to the expected deadline.

---

### 4.2.2. Liquidated damages

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Invoicing Quality (INVA)</strong></td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of <strong>0.08 LDU per incorrect invoice</strong>.</td>
</tr>
<tr>
<td><strong>Respect of deadlines (INVP)</strong></td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of <strong>0.08 LDU per day of delay</strong>.</td>
</tr>
<tr>
<td><strong>Inaccuracy of invoicing follow-up (INVCOR)</strong></td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of <strong>0.08 LDU per day of delay</strong>.</td>
</tr>
</tbody>
</table>

---

### 5. SERVICE LEVEL OF GENERAL ADMINISTRATIVE SERVICES

#### 5.1. Service Review report and Service review/ad-hoc meetings

Each EUI may decide to request monthly Service Review Meetings.

Service review meetings (SRM) are held on a monthly basis. The Contractor’s Account Manager, the Service Manager and the EUTs Technical contact – and/or their nominated representatives - attend these meetings.

A Service Review Report must be provided by the Contractor to the EUI at the latest on the 20th calendar day of the month after the service period. In addition, the documents must be made available at the latest **2 normal working days before each service review meeting**. If the meeting is cancelled on a given month, the report is still due, and must be sent to the EUI via email.

The Contractor's Service Manager produces the meeting report at the latest **5 normal working days after the meeting** and submits it for approval by the EUI.

The main objectives of the Service review meetings are as follows (this list is not exhaustive):

- Review of the last meeting minutes;
- Review of SLA indicators and the main reports;
- Review the status of the outstanding actions;
- Review the list of Incident and Problem tickets, as well as service requests;
- Review of complaints;
- Review of on-going specific contracts and orders and of outstanding invoices;
- Agree the plan for any outstanding Requests For Change (RFC);
- Setup/Update the actions list.
- For the service review report held by the Contracting Authority, contract management and outstanding issues of the other EUI’s
Either party can also organise on demand other periodic or ad-hoc meetings to discuss specific subjects or projects.

Other members of the Contractor's team, (e.g. Service Desk, Project Team) can be involved and attend the meeting to present more detail on aspects related to their area of responsibility. Other representatives of the EUI may attend the meetings according to the issues and points on the agenda.

Upon agreement between the EUIs and the Provider, these meetings may be conducted by conference/video call.

5.1.1. *Process indicators, Minimum Service Level Requirements*

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Review meeting timeliness</td>
<td>Service Review meetings will take place at the latest the 20th calendar day of the month.</td>
</tr>
<tr>
<td>Communication of the meeting's agenda and documents</td>
<td>The contractor sends the agenda and the documents for the meeting including a report of the service level indicators relating to the period discussed during the meeting. The agenda as well as the documents are provided by the Contractor to the EUI, at the latest 2 normal working days before the meeting.</td>
</tr>
<tr>
<td>Meeting minutes deadlines</td>
<td>The Contractor's Service Manager produces the meeting report at the latest 5 normal working days after the meeting and submits it for approval by the EUI. Should the EUI propose changes to the minutes of the meetings, the contractor will provide an updated version of the minutes (with the proposed changes accepted or rejected) within 3 normal working days.</td>
</tr>
</tbody>
</table>

5.1.2. *Liquidated damages*

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeliness (SRM)</td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of 0.08 LDU per day of delay if the contractor fails to organize a meeting (unless the contractor receives from the EUI a request to delay the organization of such a meeting).</td>
</tr>
<tr>
<td>Respect of deadlines (SRM)</td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of 0.08 LDU per day of delay in the delivery of the documents requested for the meeting (agenda, reports, meeting minutes, etc.).</td>
</tr>
</tbody>
</table>
5.2. **Steering Committee meetings (SCM)**

The EUI may take the initiative to hold a Steering Committee meeting (SCM) once or twice a year or when a crisis situation arises. When such a meeting is called, the Contractor assures a minimal list of participants from its side:

- The Account Manager;
- The Service Manager;
- The hierarchical managers above both the Account Manager and the Service Manager.

Other participants may be required depending on the specific points in the agenda of the particular Steering Committee meeting.

On the EUI side, at least the Technical contact and his/her hierarchical manager will attend the Steering Committee meetings.

The main objectives of the Steering Committee meetings are as follows (this list is not exhaustive):

- Crisis situation review, when relevant;
- Review of technical and contractual achievements (including compliance with SLA) since the last Steering Committee meeting;
- Definition of the strategic action plan for the coming months or years;
- State of the different report and document required (e.g., security plan, risk assessments, etc.)
- Other points may be added as needed.

The Contractor provides to the EUI, at the latest two normal working days before the meeting, the required documents, including a report of Incident and Problem tickets and the RFC and SLA indicators relating to the previous period.

The Contractor's Service Manager produces the meeting report at the latest 10 normal working days after the meeting and submits it for approval by the EUI.

### 5.2.1. Process indicators, Minimum Service Level Requirements

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Steering Committee timeliness</strong></td>
<td>Steering Committee meeting will take place once or twice per year or when a crisis situation arises.</td>
</tr>
<tr>
<td><strong>Communication of the meeting’s agenda and documents</strong></td>
<td>The contractor sends the agenda and the supporting documents for the meeting to the EUI, at the latest 2 normal working days before the meeting.</td>
</tr>
<tr>
<td><strong>Meeting minutes deadlines</strong></td>
<td>The Contractor’s Service Manager produces the meeting report at the latest 10 normal working days after the meeting and submits it for approval by the EUI. Should the EUI propose changes to the minutes of the meetings, the contractor will provide an updated version of the minutes (with the proposed changes accepted or rejected) within 3 normal working days.</td>
</tr>
</tbody>
</table>
5.2.2. **Liquidated damages**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respect of deadlines (SCM)</td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of 0,15 LDU per day of delay in the delivery of the documents requested for the meeting (agenda, reports, meeting minutes, etc.).</td>
</tr>
</tbody>
</table>

5.3. **Code of Conduct and Official-complaints**

End-users’ complaints will be addressed to the EUI service manager. The complaints can be of two types: complaint about the mobile telephony services provided and complaints about the behaviour of a MTS IV contractor’s team member.

Each complaint will be formalised. The Contractor will be considered as responsible if the complaint is related to a fault of the Contractor in the execution of tasks falling under its full responsibility.

Within 10 normal working days, the Contractor will send to the EUI a report mentioning:

- the acceptance or non-acceptance of the complaint.
- in case of acceptance, a detailed report mentioning the corrective measures that will be taken during the rectification period of 3 months, to avoid such complaints in the future.
- In case of non-acceptance, the report will contain a justification explaining the reasons of non-acceptance of the complaint.

The objective mentioned herewith is valid for complaints about the operational service or situations that could have been avoided if operations had been executed as foreseen in the service specifications.

There cannot be a recurrence of the same complaint (regarding the same non-conformity) within one year after the rectification period.

5.3.1. **Process indicators, Minimum Service Level Requirements**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service : Number of formal complaints (COMPL)</td>
<td>Official and motivated relevant complaints from customers regarding inappropriate service level are not acceptable.</td>
</tr>
<tr>
<td>Code of Conduct : Number of official complaints (CCDT)</td>
<td>Official and motivated relevant complaints from customers or suppliers regarding inappropriate behaviour, negative attitudes or lack of professional approach from the contractor are not acceptable.</td>
</tr>
<tr>
<td>Signature of a code of conduct (SCCDT)</td>
<td>Each MTS IV contractor’s team member working off-site, but having received EUI’s corporate IT accesses and/or equipment, will sign a code of conduct - Consultant’s declaration document, which</td>
</tr>
</tbody>
</table>
is an annex to the FWC (Annex 10). The signed declarations are provided by the Contractor at the start of the first specific contract signed after the start of the framework contract or at the moment a new team member joins the MTS IV contractor’s team.

5.3.2. **Liquidated damages**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service: Official complaints (COMPL)</strong></td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of <strong>1 LDU</strong> if such a complaint is registered.</td>
</tr>
<tr>
<td></td>
<td>If, within a one-year period after the decision to impose liquidated damages for a service official complaint, a new case of the same type of fault is established, the EUI shall register a serious fault and the contractor shall, upon claim by the EUI, pay the associated liquidated damages.</td>
</tr>
<tr>
<td><strong>Code of Conduct: Official complaints (CCDT)</strong></td>
<td>The contractor shall, upon claim by the EUI pay liquidated damages of <strong>2 LDU</strong> in case such complaint is submitted.</td>
</tr>
<tr>
<td></td>
<td>If, within a one-year period after the decision to impose liquidated damages for a service official complaint, a new case of the same type of fault is established, the EUI shall register a serious fault and the contractor shall, upon claim by the EUI, pay the associated liquidated damages.</td>
</tr>
<tr>
<td><strong>Code of conduct (SCCDT)</strong></td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of <strong>0.08 LDU</strong> per day of delay in the delivery of a signed Consultant’s declaration document.</td>
</tr>
</tbody>
</table>

5.4. **Serious faults**

The occurrence of certain faults indicates the overall ability and trustworthiness of the Contractor. The following actions could give rise to the registration by the EUI of a serious fault:

- Interventions or incidents created by the Contractor being a main cause for major service delivery problems
- Interventions or incidents created by the Contractor being a root cause for a security incident
- Interventions or incidents created by the Contractor being a root cause for a data leakage
- Serious fault registered after several official complaints.

5.4.1. **Process indicators, Minimum Service Level Requirements**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serious faults</td>
<td>Serious faults are not acceptable.</td>
</tr>
</tbody>
</table>
The associated KPI are specified here below:

- **SFLT (Serious Fault)** KPI measures the number of serious faults of the MTS IV contractor registered by the EUI.

- **RSFLT (Recurrent Serious Fault)** KPI measures the number of repeated serious faults of the same type within a one-year period after its first occurrence (confirmed by a decision to impose liquidated damages).

- **SSFLT (Security Serious Fault)** KPI measures the number of serious faults being the root cause of a security incident or a data leakage.

- **RSSFLT (Recurrent Security Serious Fault)** KPI measures the number of repeated serious faults related to a security incident or a data leakage of the same type.

### 5.4.2. Liquidated damages

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Serious faults (SFLT)</strong></td>
<td>For each case of serious fault being established by the EUI, the contractor shall, upon claim by the EUI, pay liquidated damages of 3 LDU.</td>
</tr>
<tr>
<td><strong>Recurrent Serious Fault (RSFLT)</strong></td>
<td>If, within a one-year period after the decision to impose liquidated damages for a serious repeated fault, a new case of the same type of fault is established, the contractor shall, upon claim by the EUI, pay liquidated damages of 4 LDU. The rule of the previous sentence could be applied repeatedly and as many times as serious faults happen.</td>
</tr>
<tr>
<td><strong>Serious fault being the root cause of a security incident or a data leakage (SSFLT)</strong></td>
<td>For each case of serious fault being established by the EUI, the contractor shall, upon claim by the EUI, pay liquidated damages of 10 LDU.</td>
</tr>
<tr>
<td><strong>Recurrent Serious fault being the root cause of a security incident or a data leakage (RSSFLT)</strong></td>
<td>If, after the decision to impose liquidated damages for a serious fault being the root cause of a security incident, a new case of the same type of fault is established, the contractor shall, upon claim by the EUI, pay liquidated damages of 20 LDU. The rule of the previous sentence could be applied repeatedly and as many times as serious faults happen.</td>
</tr>
</tbody>
</table>

### 6. SERVICE LEVEL FOR SERVICE MANAGEMENT PROCESSES

#### 6.1. Incident management

An Incident (also referred to as service outage) is defined as an event or action or omission that directly or indirectly causes a contractual service or service element to degrade partially or totally.
In case of ongoing incident or crisis, the Contractor makes all possible efforts to reduce the pain factor to a bare minimum for the EUI. The EUI has to be informed of any action foreseen and provide an agreement for any work-around that may be proposed by the Contractor. The Contractor regularly updates the EUI on the evolution of the troubleshooting.

Incidents are classified according to their level of severity or priority level defined by the general criteria of number of users impacted, the urgency to restore the service and the business impact.

The defined priority levels are P1, P2, P3 and P4 (P1 being the most critical level).

The following rules will apply:

- For P1 and P2 incidents, the time is expressed in hours (H)
  - if such an incident ticket arrives before 6 p.m., the Contractor must work on the incident without interruption until its resolution (or dispatching to another team).

- For P3 and P4 incidents, the time is expressed in normal working hours (WH)
  - if such an incident ticket arrives before 6 p.m., the time will be recorded from the moment it arrives until 6 p.m. (stop of the clock) and then the time recording will be resumed from 8 a.m. the following normal working day until resolution;
  - if such a ticket arrives after 6 p.m., the time will be recorded from 8 a.m. the following normal working day until resolution.

The table below summarizes a non-exhaustive list of typical incidents and their associated priority levels:

- P1: General outage affecting a large number of subscribers
- P2: General outage affecting several subscribers or partial outage affecting a large number of subscribers
- P3: General outage affecting one subscriber or partial outage affecting several subscribers
- P4: Non service impacting incident

<table>
<thead>
<tr>
<th>Lot 1 - Incident category</th>
<th>Priority Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete outage of voice, data or SMS communications</td>
<td>P1</td>
</tr>
<tr>
<td>• in one or more building of the EUI (indoor and/or outdoor coverage if available), or</td>
<td></td>
</tr>
<tr>
<td>• one zone of more than 300 m long in Brussels, or Luxembourg (city), or</td>
<td></td>
</tr>
<tr>
<td>• for at least 25% of the EUI mobile users in Belgium, or</td>
<td></td>
</tr>
<tr>
<td>• for at least 50% of the EUI mobile users in Luxembourg (country).</td>
<td></td>
</tr>
<tr>
<td>No Hotline operator is reachable by phone for more than 5 minutes</td>
<td>P1</td>
</tr>
<tr>
<td>Security breach (see below)</td>
<td>P1</td>
</tr>
</tbody>
</table>
No outgoing or incoming voice call is possible, or no data connection is possible or no SMS can be sent or received or other form of service degradation on the contractor’s network, for at least 10 mobile users of the EUI caused by the same issue.  

<table>
<thead>
<tr>
<th>Incident Description</th>
<th>Priority Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>P3 incident affecting one VIP mobile user (VIPs are listed by each EUI with a maximum of 5% of its users)</td>
<td>P2</td>
</tr>
<tr>
<td>P3 incident affecting several VIP mobile users</td>
<td>P1</td>
</tr>
<tr>
<td>Complete outage for one mobile subscriber</td>
<td>P3</td>
</tr>
<tr>
<td>Incorrect alerts, blocking/throttling or volume reports</td>
<td>P3</td>
</tr>
<tr>
<td>Service degraded for one mobile subscriber</td>
<td>P4</td>
</tr>
</tbody>
</table>

**Lot 2 - Incident category**

<table>
<thead>
<tr>
<th>Incident Description</th>
<th>Priority Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>No SMS can be sent through any of the interfaces</td>
<td>P1</td>
</tr>
<tr>
<td>The API interface (SOAP/HTTP) is unavailable, unstable, not responding or not sending SMS</td>
<td>P1</td>
</tr>
<tr>
<td>No Hotline operator is reachable by phone for more than 5 minutes</td>
<td>P1</td>
</tr>
<tr>
<td>The SMS sending/receiving or the API throughput is less or equal than 50% of the contracted/required throughput</td>
<td>P1</td>
</tr>
<tr>
<td>SMS to EU operators (excluding MVNOs) are not delivered or received within 10 minutes and this delay is not seen from other sending operators (*)</td>
<td>P1</td>
</tr>
<tr>
<td>The API interface takes more than 3 seconds to respond</td>
<td>P1</td>
</tr>
<tr>
<td>SMS to non-EU operators (excluding MVNOs) are not delivered or received within 10 minutes and this delay is not seen from other sending operators (*)</td>
<td>P2</td>
</tr>
<tr>
<td>The SMS sending/receiving or API throughput is between 50% and 75% of the contracted/required throughput</td>
<td>P2</td>
</tr>
<tr>
<td>Incorrect reporting or update of message delivery status on the SMS sending platform (impacting &gt;100 users)</td>
<td>P2</td>
</tr>
<tr>
<td>SMS to 5 or more users of a main mobile network (excluding Belgium or Luxembourg) are not delivered or received exceeding 15 minutes when this delay is not present from other sending operators (*)</td>
<td>P3</td>
</tr>
<tr>
<td>The administration or report tool interface is not available</td>
<td>P3</td>
</tr>
</tbody>
</table>

*Note: Not applicable if the provider can prove that the incident is fully generated by a remote operator.

**Specific case of Incidents related to security breaches**

Examples of potential security breaches which may happen are (the list is not exhaustive):

- Unauthorised access to data held in systems.
- Tapping into data transfer flows.
- Tapping into voice communications.
- Lack of service vulnerability patching potentially causing data or information leakage.
- Other unauthorised access to data or information.

The contractor pays particular attention to avoiding any Incidents related to security, by putting in place the required policies, processes and tools to avoid them.

Security-related Incidents are registered and documented in Incident tickets of severity P1. A Security-related incident will also lead to the registration of a serious fault.

For P1, P2, and P3, the liquidated damages are calculated every month, by taking the sum of all resolution time indexes for all Incident tickets, grouped by each level of priority.

**For P1 (IMP1),** liquidated damages occur after a cumulative resolution time of 2 hours, and are increased by steps of 4 hours, according to the following table:

\[
\sum P1 = \text{cumulative resolution time index for all P1 tickets during the considered period}
\]

\[
p \text{ is a positive integer } 0, 1, 2, 3, 4, 5, \text{ etc...}
\]

<table>
<thead>
<tr>
<th>( \sum P1 )</th>
<th>( p = 0 )</th>
<th>( p = 1 )</th>
<th>( p = 2 )</th>
<th>( p = 3 )</th>
<th>.....</th>
<th>( p = 4\times p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penalties</td>
<td>0</td>
<td>10*LDU</td>
<td>20*LDU</td>
<td>30*LDU</td>
<td></td>
<td>10*LDU</td>
</tr>
</tbody>
</table>

**For P2 (IMP2),** liquidated damages occur after a cumulative resolution time of 4 hours, and are increased by steps of 4 hours, according to the following table:

\[
\sum P2 = \text{cumulative resolution time index for all P2 tickets during the considered period}
\]

\[
p \text{ is a positive integer } 0, 1, 2, 3, 4, 5, \text{ etc...}
\]

<table>
<thead>
<tr>
<th>( \sum P2 )</th>
<th>( p = 0 )</th>
<th>( p = 1 )</th>
<th>( p = 2 )</th>
<th>( p = 3 )</th>
<th>.....</th>
<th>( p = 4\times p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penalties</td>
<td>0</td>
<td>4*LDU</td>
<td>8*LDU</td>
<td>12*LDU</td>
<td></td>
<td>4*LDU</td>
</tr>
</tbody>
</table>

**For P3 (IMP3),** liquidated damages occur after a resolution time of 1 NWD (normal working day), and are increased by steps of 1 NWD, according to the following table:

\[
P3 = \text{resolution time index for P3 tickets during the considered period}
\]

\[
p \text{ is a resolution time index for P3 tickets during the considered period}
\]

<table>
<thead>
<tr>
<th>( P3 )</th>
<th>( p = 0 )</th>
<th>( p = 1 )</th>
<th>( p = 2 )</th>
<th>( p = 3 )</th>
<th>.....</th>
<th>( p = \times NWD )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penalties</td>
<td>0</td>
<td>1*LDU</td>
<td>2*LDU</td>
<td>3*LDU</td>
<td></td>
<td>p*LDU</td>
</tr>
</tbody>
</table>

**Example:** No voice communication is possible on the contractor's network in one zone of more than 300 m long in Brussels, so the situation is that of a P1 Incident. The Average amount of the last 3 monthly invoices for that EUI was 200K€ (value of AVG₃). Using the formula above, LDU
equals 1,300€. The solution to the Incident was not found under the 2 hours of maximum time period for a P1, but in 8 hours – this means that "p" is equal to 2 units. The liquidated damage to apply concerning deviation from the Incident Management service level would then be of 10\*2\*1.300€ = 26,000€.

**For P4 (IMP4)**, liquidated damages occur when the resolution time of an incident exceeds two normal working days.

### 6.1.1. Process indicators, Minimum Service Level Requirements

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incident resolution time (per service)</strong></td>
<td>Measurement: The resolution time is defined by default as the period of time between opening and closing of an incident in the Service Management Tool of the EUI. The closing of a trouble ticket is done in common agreement after restoring the service to normal operation. The restore can be a temporary workaround in anticipation of the final repair.</td>
</tr>
<tr>
<td></td>
<td>If the incident arises outside the normal working hours of the service desk, or in the case of an EUI without service desk, incident opening can be performed by phone call to the hotline, which registers the opening time and closing time, and informs the EUI, and the service desk where applicable.</td>
</tr>
<tr>
<td></td>
<td>In case the Contractor experiences hindrance(s) caused by the EUI for resolution of an Incident (e.g. no access to the location for reconfiguration and/or testing, unable to contact the EUI after several attempts), the resolution time will be frozen until complete solving of the hindrance(s).</td>
</tr>
<tr>
<td></td>
<td>If one issue is the root cause of the creation of several Incident tickets, only the resolution time linked to this initial ticket is taken into account in the liquidated damages calculation.</td>
</tr>
<tr>
<td></td>
<td>The contractor remains the incident owner until the incident is closed but is not considered as responsible of delays caused by a third party not under his responsibility. However, the contractor will take all necessary measures to ensure a timely resolution of the incident by the involved third parties.</td>
</tr>
</tbody>
</table>

### 6.1.2. Liquidated damages

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incident resolution time</strong></td>
<td>The contractor shall, upon claim by the EUI, pay the following liquidated damages in case the service level <strong>per service</strong> is not the one expected.</td>
</tr>
<tr>
<td>Priority</td>
<td>Liquidated damages</td>
</tr>
<tr>
<td>P1 (IMP1)</td>
<td>10*p*LDU</td>
</tr>
<tr>
<td>P2 (IMP2)</td>
<td>4*p*LDU</td>
</tr>
<tr>
<td>P3 (IMP3)</td>
<td>p*LDU</td>
</tr>
<tr>
<td>P4 (IMP4)</td>
<td>0.05 LDU per additional day of delay in the closure of the incident</td>
</tr>
</tbody>
</table>

"p" represents the number of additional hours the resolution time exceeded the agreed upon period.
6.2. Availability Management

Due to the criticality of some services under the responsibility of the EUI, it is of utmost importance that the Contractor proposes and operates a stable and robust infrastructure that the services can rely on.

Measurement of service availability will be based on the target availability metrics as specified in the table here below. If the target availability for a service is not reached due to reasons linked to the Contractor’s performance, then liquidated damages may be applied by the EUI. The formulas used to calculate liquidated damages in this case are detailed below.

Service availability refers here to a global outage affecting the totality of the service (voice data outage in the whole country for example), partial outage like group of users or specific building outage is not taken in account in this chapter.

Service availability is measured as the average percentage of the time that the service was functioning in accordance with the specifications over a given reference period. Planned maintenances and unavailability outside the responsibility of the Contractor are not to be included in this calculation.

If the Contractor fails in measuring the availability of a service, a default loss of availability of 2% (target availability - 2%) will be taken into account for the calculation of the liquidated damages.

Service availability for a reference period (1 month) is calculated using the following formula:

\[ AV_s = 100 \times \frac{t_{tot} - \Sigma (t_i \times c_i)}{t_{tot}} \]

Where:

\( AV_s \) = service availability during the period, expressed as a percentage value.

\( t_i \) = index of the occurred downtime or incidents.

\( t_{tot} \) = Total time in seconds during which a Service was not functioning as specified for a specific incident or downtime, not counting specifically excluded duration of actual maintenance and scheduled upgrades during scheduled maintenance windows subject to a prior notice to the EUI.

\( c_i \) = Impact correction factor. This value is determined as follows:

- Minor incidents/downtime (incidents and downtime affecting less than 10% of service), the value of the correction factor is 0.1.
- For any other incidents and downtimes, the value is set to 1.

EUI can decide to lower the impact correction factor for an unavailability if the real impact was lower.

\( t_{tot} \) = the total number of seconds for the period of measurement (so given the month: 30 days = 2592000 s, 31 days = 2678400 s...).
For services where availability is measured, failure to achieve the defined availability target may result in application of liquidated damages. These will be calculated using the following formula:

\[ LD_s = 5 + (100 - AV_{SC}) \times W_s \text{ when } AV_{SC} < AV_T \]

Where:

\( LD_s \) = Liquidated damages for the service, expressed in LDU

\( AV_{SC} \) = Corrected service availability measured during the period, expressed as a percentage value. Corrected in this context means that downtime due to factors outside of the responsibility and control of the Contractor are excluded.

\( AV_T \) = Target service availability, expressed as a percentage value.

\( W_s \) = Weight of the service, as defined in table given hereunder.

Example: For a service with a \( W_s \) of 20 and an \( AV_{SC} \) of 99%, the \( LD_s \) will be 25 LDU.

Note: In principle, incidents and downtime that have a main cause outside of the control and responsibility of the Contractor or services which by design cannot be proposed in a redundant mode are excluded for the purposes of calculating liquidated damages. This does not absolve the contractor from all responsibility however. If the contractor fails to put in place reasonable mitigating measures for repeated incidents with the same main cause, these incidents will start to be taken into account starting from the next reporting period for calculating the liquidated damages.

Service availability will only be measured for the services listed in the table. Typical exceptions are supporting services that are not directly provided to clients of the EUI. In these cases, downtime may indirectly impact service availability of other services that rely on the supporting service.

For each service, a minimum acceptable availability is also defined. Failure to reach at least this level of availability for a service can lead to the notification of a serious fault. **The registration of the serious fault will lead to the activation of liquidated damages.**

### Table 1: Service Availability Characteristics

<table>
<thead>
<tr>
<th>Service</th>
<th>Availability Target (%)</th>
<th>Minimum Acceptable Availability (%)</th>
<th>Weight (# LDU)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Voice service availability</td>
<td>99,99</td>
<td>99,00</td>
<td>20</td>
</tr>
<tr>
<td>Mobile Data service availability</td>
<td>99,95</td>
<td>99,00</td>
<td>20</td>
</tr>
<tr>
<td>SMS Lot 1 service availability</td>
<td>99,95</td>
<td>98,00</td>
<td>10</td>
</tr>
<tr>
<td>SMS Gateway Lot 2 service availability</td>
<td>99,99</td>
<td>99,00</td>
<td>20</td>
</tr>
</tbody>
</table>

6.2.1. **Process indicators, Minimum Service Level Requirements**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability of services</td>
<td>The different services availability must be measured. For each service, the expected availability service level is indicated in table</td>
</tr>
</tbody>
</table>
above.

The availability is calculated on a **monthly basis**. Where possible, measurements will be based on the duration of an unavailability of an equipment a service depends on.

For services for which there are discrepancies between expected availability and measured availability, an improvement plan must be defined and executed.

### 6.2.2. **Liquidated damages**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability of services (AVSV)</td>
<td>The contractor shall, upon claim by the EUI, pay the liquidated damages as detailed above in case the availability objectives per service are not met</td>
</tr>
</tbody>
</table>

### 6.3. **Request Fulfillment** *(applicable only to Lot 1)*

#### 6.3.1. **Process indicators, Minimum Service Level Requirements**

EUI’s Request Fulfilment procedure, which is often inspired by ITIL V3 best practices.

The Request implementation Time is measured as the time period between the receipt of a validated request for a modification and the time the modification is taken into account by the network, including the time taken by the Contractor to update the EUI operational databases and documentation.

Request fulfilment includes all modifications or service activation on an existing SIM/e-SIM card (in case of physical SIM cards: maximum 100 SIM cards per day per EUI), delivery of a SIM/e-SIM card, user account creation or change on the SMS gateway platform, request for information etc.

#### 6.3.1. **Process indicators, Minimum Service Level Requirements**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request resolution time</td>
<td>The requests must be implemented within 4 normal working hours.</td>
</tr>
</tbody>
</table>

### 6.3.2. **Liquidated damages**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Resolution Time (RQFF)</td>
<td>For Lot 1 all changes will be registered in the Service Management Tool.</td>
</tr>
<tr>
<td></td>
<td>The contractor shall, upon claim by the EUI, pay <strong>0,15 LDU per late change</strong> and per additional normal working day late.</td>
</tr>
</tbody>
</table>
6.4. **Change management**

6.4.1. *Process indicators, Minimum Service Level Requirements*

We define here the service level quality parameters to be applied when the EUI requests for new services or major changes to existing services. Major changes are not changes to be performed on individual SIM cards or user profiles: those are standard changes and are treated using the request fulfilment procedure applicable.

For major changes to happen to the Service, the Contractor receives from the EUI a written Request For Change (or RFC). Alternatively, if for some reason the Contractor must propose a change to the EUI on the Service it delivers, it must also issue a RFC.

Such RFC could be the request to implement an indoor infrastructure in a building.

In some cases, the RFC is issued to ask for new Services or for work in the form of a Project, for which the Contractor must then make an offer, which includes its implementation details and corresponding price quote.

An RFC includes any required specifications and details and can take several forms: request issued during a meeting, letter, electronic mail message, RFC ticket, or any other form of written communication. In each case, the EUI and the Contractor agree whether the request should be considered a Project.

In those cases when the Contractor has to make an offer, a maximum time period is respected between the moment when the RFC was first issued, including all the required specifications and details, and the moment when the offer has been officially provided to the EUI by the Contractor. This deadline is called the **Offer Production Deadline (OPD)** and is fixed at **five normal working days maximum**. For exceptional and more complex RFCs, the EUI may decide to allow a longer time period, in writing at the moment of the request. The deadline then specified becomes the OPD for that specific RFC.

The Service Manager proposes an implementation plan for the RFC. The EUI can propose an alternative date for the completion of the RFC. A **Ready for Service Date (RFSD)** is defined as the target value for the completion of the RFC. Both parties agree the RFSD for each RFC. In the case of new Services, as there is a need for a new offer and a resulting new Specific Contract, the RFSD is discussed and agreed and then it is formalised in the offer by the Contractor. In the case of an RFC for existing Services, as there is no need for a new Specific Contract and therefore there is no request for an offer, the RFSD is discussed and agreed and then it is formalised in the RFC details.

In the case of an indoor antennas infrastructure to be deployed in a building, the Contractor has to provide a technical study with all details of the proposed installations, including the information about health and security. This study, called **Indoor Technical Study Date (ITSD)**, has to be provided after a maximum time limit of **2 months for small or medium buildings (<10,000m²) and 3 months for large buildings (>10,000m²)**. An **Indoor Infrastructure Service Data (IISD)** is defined as the target value for the completion of the installations (ready to use). The implementation time will not exceed **3 months for a small or medium building, and 6 months for a large building**.

RFC activities include but are not limited to following activities:
<table>
<thead>
<tr>
<th>Change (RFC)</th>
<th>Lot</th>
</tr>
</thead>
<tbody>
<tr>
<td>New/change/deletion of a user profile</td>
<td>Lot 1</td>
</tr>
<tr>
<td>New/review Indoor coverage</td>
<td>Lot 1</td>
</tr>
<tr>
<td>New API and associated users</td>
<td>Lot 2</td>
</tr>
<tr>
<td>Modification of SMS sending throughput</td>
<td>Lot 2</td>
</tr>
</tbody>
</table>

### 6.4.1. Process indicators, Minimum Service Level Requirements

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change timeliness</td>
<td>The OPD, RFSD, ITSD, IISD deadlines are respected</td>
</tr>
<tr>
<td>Maintenance operations – Timeliness of the communication (PLUN)</td>
<td>EUI is informed about any maintenance impacting one of the services in scope of this call for tender:</td>
</tr>
<tr>
<td></td>
<td>For normal changes: at least 10 days in advance and the intervention time is agreed by EUI.</td>
</tr>
<tr>
<td></td>
<td>For emergency changes: at least 5 hours in advance.</td>
</tr>
</tbody>
</table>

### 6.4.2. Liquidated damages

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Timeliness</td>
<td>The contractor shall, upon claim by the EUI, pay the following liquidated damages:</td>
</tr>
<tr>
<td></td>
<td>- OPD (Change Management Offers production deadline): 0,15 LDU per offer per day of delay.</td>
</tr>
<tr>
<td></td>
<td>- RFSD (Change Management Ready for Service Date): 0,15 LDU per RFC per day of delay.</td>
</tr>
<tr>
<td></td>
<td>- ITSD (Indoor technical study) – Delivery of technical study: 0,15 LDU per day of delay in the delivery of a technical study.</td>
</tr>
<tr>
<td></td>
<td>- IISD (Indoor infrastructure service date): 0,15 LDU per day of delay.</td>
</tr>
<tr>
<td></td>
<td>All changes will be registered in the Service Management Tool.</td>
</tr>
<tr>
<td>Maintenance operations – Timeliness of the communication (PLUN)</td>
<td>The contractor shall, upon claim by the EUI, pay 1 LDU in case he failed to communicate about maintenance operations at least one week before the intervention. In addition, in the case of non-communication, the maintenance will not be excluded from the</td>
</tr>
</tbody>
</table>
6.5. **Problem Management**

6.5.1. **Process indicators, Minimum Service Level Requirements**

An EUI uses a Problem Management (PM) procedure, which is inspired by ITIL V3 best practices. When a problem ticket is created, an estimated time for solution must be proposed by the Contractor for discussion with the EUI. Once the details have been verified and an agreement has been reached by both parties, the agreed time limit is documented in writing (in a meeting report and in the ticketing system) and becomes the contractual time limit to solve the specific Problem.

### Process indicators, Minimum Service Level Requirements

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem Management resolution time (PM)</td>
<td>The defined deadlines for the resolution of the problem are respected</td>
</tr>
</tbody>
</table>

6.5.2. **Liquidated damages**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem Management Resolution Time (PM)</td>
<td>The contractor shall, upon claim by the EUI, pay 0.15 LDU per day of delay after the mutually agreed time limit is exceeded.</td>
</tr>
</tbody>
</table>

6.6. **Service escalation Procedure**

6.6.1. **Process indicators, Minimum Service Level Requirements**

The Contractor must provide a clear escalation procedure.

This procedure shall describe how an incident or a problem is escalated within the contractor’s organisation and define the different escalations both at operational and strategic levels, in addition to the contact persons defined in the “Contractor Interfaces” section here above.

Should there be important deviations from either the Incident or the Problem Management service levels, repeated deviations, or critical situations, the Contractor or the EUI may decide to escalate these situations to other levels of responsibilities. This means that escalation may be done immediately and directly to the hierarchical managers above the Service Manager of the Contractor.

The Contractor ensures the follow-up of all the incidents and problems and must use Service Desk tickets to provide regular updates to the EUI (minimum hourly updates, or another frequency agreed between the two parties at the moment of triggering the crisis management procedure).

The hierarchical and functional escalation measures the ability of the Contractor to escalate in case a service is unavailable and when the resulting incident is qualified as Priority Level 1 or 2.
6.6.1. Process indicators, Minimum Service Level Requirements

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Escalation procedure</td>
<td>The contractor shall deliver an escalation procedure at the end of the phase-in period</td>
</tr>
<tr>
<td>Escalation timeliness (ESM)</td>
<td>The hierarchical and functional escalation measures the ability of the Contractor to escalate in case a service is unavailable and when the resulting incident is qualified as Priority Level 1 or 2. The escalation must be proposed one hour at the latest after a crisis situation has started; a P1 or P2 incident is opened.</td>
</tr>
</tbody>
</table>

6.6.2. Liquidated damages

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Escalation timeliness (ESM)</td>
<td>The contractor shall, upon claim by the EUI,</td>
</tr>
<tr>
<td></td>
<td>• Pay 0.5 LDU in case a P1 or P2 incident hasn’t been escalated within one hour after the start of the incident.</td>
</tr>
<tr>
<td></td>
<td>• Pay 0.1 LDU per hour of delay (during NWH).</td>
</tr>
</tbody>
</table>

6.7. Communication quality

6.7.1. Definition

Communication quality (CALLQ) is defined with respect to the average user perception of how good is his/her experience during a telephone call or a data communication, using the Services provided by the Contractor to the EUI. A non-exhaustive list of the elements of communication quality, together with their definition, is provided below:

• Connection drops – abrupt interruption of a connection.
• Connection cuts - perceptible signal cuts during a conversation.
• Echo - perceptible signal reflection during a conversation, which affects the understanding of the message.
• Noise - perceptible noise (including mixed conversations, crosstalk) during a conversation which affects the understanding of the message.
• Latency - perceptible delay in the transmission of the voice during a conversation, which affects the understanding of the message.
• Connection Completion Ratio (CCR) - the ratio of successful connections to the total number of connection attempts in a specified time period for a specific location.
• Post-Dialling time period - the period starting when the dial number required for setting up the call is received by the network and finishing when the called party busy tone or ringing tone or answer signal is received by the calling party.
• **Throughput of data traffic**: the data transfer rate is significantly lower than the usually supported throughput at that location.

• **SMS sending success rate**: the ratio of successful SMS correctly transmitted to the total number of SMS sending attempts in a specified time period.

### 6.13.1 Process indicators, Minimum Service Level Requirements

A communication is of good quality if it doesn’t motivate from the average user a justified complaint. Should there be, during a certain period of time (defined as one month), a number of justified complaints by a significant number of users, then Contracting authority can conclude that there is a problem of communication quality. This can be for a certain period of time, from a certain location, to a certain destination, for inbound or for outbound connections, or a combination of several situations.

When one or more communication quality Incidents are reported, investigation is triggered involving the EUI and the Contractor, so as to confirm that there is a justified problem of communication quality, to define what the problem is, to launch the troubleshooting and to measure the extent of the impact for the users and the EUI.

When users complain about communication quality, the complaint is reported by the EUI to the Contractor and is logged as an Incident of priority 4. The Contractor investigates the cause and takes all necessary actions to diagnose the problem, and, should the cause fall under the Contractor’s responsibility, to correct the problem. Depending on the level of impact the priority of the incident might be escalated.

### 6.7.1. Process indicators, Minimum Service Level Requirements

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication Quality (COMMQ)</td>
<td>The Contractor commits to limit the occurrences of communication quality complaints to the bare minimum. Communication quality complaints are based on the perception of the quality by a user. The number of complaints about the quality of communication must not exceed <strong>10</strong> on a monthly basis.</td>
</tr>
</tbody>
</table>

### 6.7.2. Liquidated damages

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication Management (COMMQ)</td>
<td>The contractor shall, upon claim by the EUI, pay <strong>2 LDU</strong> per group of 10 complaints in case the number of monthly acceptable complaints is exceeded.</td>
</tr>
</tbody>
</table>

### 6.7.3. Benchmarking of communication quality

The EUI may decide to perform measurement tests at any time and, when that happens, the results must conform to the values specified in the relevant international standards, ITU-T, and market standards for Connection Quality. Non-conformity with these values may be treated as an Incident.
A written report will be created describing the results of the tests, which is then considered as valid input for the decision to apply any liquidated damage related to this KPI.

6.8. **Reporting services**

The required reporting services are described in Annex 8 *Service requirements* of the Tender Specifications.

6.8.1. Process indicators, Minimum Service Level Requirements

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reporting accuracy</strong></td>
<td>This quality parameter measures the ability of the contractor to produce accurate reports.</td>
</tr>
<tr>
<td></td>
<td>The invoices shall give accurate information and cover the elements as described in the corresponding Specific Contract. This parameter will be measured against the number of reports rejections before the report can be accepted:</td>
</tr>
<tr>
<td></td>
<td>This parameter is measured based on the following KPI’s :</td>
</tr>
<tr>
<td></td>
<td>- <strong>Reporting Accuracy (REPA) KPI:</strong> 100% of reports must be accurate.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Correction of report (RCOR) KPI:</strong> Delivery of corrected report within 5 normal working days after error notification.</td>
</tr>
<tr>
<td><strong>Reporting timeliness &amp; follow-up</strong></td>
<td>This quality parameter measures the ability of the Contractor to produce reporting in due time.</td>
</tr>
<tr>
<td></td>
<td>The reports shall be produced in due time. This parameter will be measured against the number of reports received outside the deadlines indicated in the Contract:</td>
</tr>
<tr>
<td></td>
<td>This parameter is measured based on the following KPI’s :</td>
</tr>
<tr>
<td></td>
<td>- <strong>Monthly Service Punctuality (RPM) KPI:</strong> 20(^{th}) calendar day on month N+1, or next normal working day.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Yearly Service Punctuality (RPy) KPI:</strong> 1(^{st}) of February or next normal working day of year+1.</td>
</tr>
<tr>
<td></td>
<td>100% of reports must be received according to the expected deadline.</td>
</tr>
</tbody>
</table>

6.8.2. Liquidated damages

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reporting Quality (REPA)</strong></td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of <strong>0,15 LDU per incorrect report.</strong></td>
</tr>
<tr>
<td><strong>Inaccuracy of reporting follow-up</strong></td>
<td>The contractor shall, upon claim by the EUI, pay</td>
</tr>
<tr>
<td>Parameters</td>
<td>Required Service Levels</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td><strong>(RCOR)</strong></td>
<td>Liquidated damages of (0.08) LDU for each normal working day the report is late.</td>
</tr>
<tr>
<td><strong>Respect of deadlines (RPM, RPY)</strong></td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of (0.15) LDU per day of delay in the delivery of a report.</td>
</tr>
</tbody>
</table>

6.9. **Phase-in services**

A transition period is foreseen to ensure a smooth running-in of the Contractor, without impact on the services or service level degradation.

The required services are described in Annex 8 Service Requirements of the *Tender specifications*.

6.9.1. **Process indicators, Minimum Service Level Requirements**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase-in plan (PHI-PL)</td>
<td>A plan to transition from MTS III to MTS IV services is made available by the Contractor at the start of the Phase-in services.</td>
</tr>
<tr>
<td>Service Desk (PHI-HD)</td>
<td>Hotline and service desk must be operational at the end of the Phase-in period.</td>
</tr>
<tr>
<td>Portability (Applicable to Lot 1) (PHI-NP)</td>
<td>All GSM numbers and SIM and/or e-SIM cards (with a basic alerting or blocking functionality) must be migrated during the phase-in period. The migration must be finished at the end of the phase-in period.</td>
</tr>
<tr>
<td>SMS Platform (Applicable to Lot 2) (PHI-SMS)</td>
<td>At the end of the phase-in period, SMS sending platform, interfaces and API’s are fully operational.</td>
</tr>
<tr>
<td>Technical infrastructure documentation (PHI-AR)</td>
<td>The contractor must deliver a draft of the architecture and API documentation at the end of the phase-in period. A final version of the document must be delivered no later than 6 months after the end of the phase-in period.</td>
</tr>
<tr>
<td>Indoor coverage (Applicable to Lot 1) (PHI-IND-E and PHI-IND-NE)</td>
<td>Indoor coverage must be operational for existing buildings with passive equipment already available within 6 months after the signature of the framework contract (PHI-IND-E). Indoor equipment for buildings needing full installation (not equipped with passive equipment if the signal is not sufficient and the EUI confirms the request) must be provided at a pace of 1 building every 2 months starting the 7th month after the signature of the framework contract (PHI-IND-NE).</td>
</tr>
<tr>
<td>Custom functionality (Applicable to Lot 1) (PHI-CUS)</td>
<td>Daily CDR’s, user profiles, usage monitoring and alerting must be ready within 6 months after the signature of the framework contract.</td>
</tr>
<tr>
<td>Procedure Handbook (PHI-PH)</td>
<td>A draft version of the procedure handbook must be available at the end of the phase-in period. A final version of the document must be delivered not later than 6 months after the end of the phase-in period. The procedure handbook must be updated when a change occurs.</td>
</tr>
</tbody>
</table>
A yearly review of the procedure handbook must be performed.

### 6.9.2. Liquidated damages

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase-in plan (PHI-PL)</td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of 0.15 LDU per day of the delay in the availability of phase-in plan.</td>
</tr>
<tr>
<td>Service Desk availability (PHI-HD)</td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of 2 LDU per day of the delay in the availability of the service desk.</td>
</tr>
<tr>
<td>Portability migration (PHI-NP)</td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of 1 LDU per day of delay in the migration.</td>
</tr>
<tr>
<td>SMS platform (PHI-SMS)</td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of 2 LDU per day of delay in the availability of the SMS platform.</td>
</tr>
<tr>
<td>Technical infrastructure documentation delivery (PHI-AR)</td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of 0.15 LDU per day of delay in the delivery of the architecture documentation (draft or final).</td>
</tr>
<tr>
<td>Indoor coverage (PHI-IND-E)</td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of 0.08 LDU per day of delay in case the indoor coverage for buildings equipped with passive equipment is not available.</td>
</tr>
<tr>
<td>Indoor coverage (PHI-IND-NE)</td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of 0.08 LDU per day of delay in case the indoor coverage for buildings equipped without passive equipment is not available.</td>
</tr>
<tr>
<td>Custom functionality (PHI-CUS)</td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of 0.08 LDU per day of delay in the delivery of the custom functionality.</td>
</tr>
<tr>
<td>Procedure handbook (PHI-PH)</td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of 0.15 LDU per day of delay in the availability of the draft/final/updated version of the procedure handbook. The contractor shall, upon claim by the EUI, pay liquidated damages of 5 LDU in case the procedure handbook isn’t reviewed on a yearly basis or not updated after a change occurred</td>
</tr>
</tbody>
</table>

### 6.10. Phase-out services

The required services are described in Annex 8 Service Requirements of the Tender specifications.
6.10.1. Process indicators, Minimum Service Level Requirements

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase-out plan</td>
<td>The phase-out plan is ready at the latest one month before the start of the phase-out.</td>
</tr>
<tr>
<td>Information transfer</td>
<td>The new Contractor will commit to hand over any relevant information to a potential future Contractor <strong>within 3 months</strong> at the end of the Framework Contract derived from this Call for Tenders, in order to ensure a smooth transition and the business continuity, and with respect to the following aspects:</td>
</tr>
<tr>
<td>(PHO-INF)</td>
<td>- Hotline and Service Desk activities,</td>
</tr>
<tr>
<td></td>
<td>- migration of all GSM numbers,</td>
</tr>
<tr>
<td></td>
<td>- indoor signal coverage and infrastructure</td>
</tr>
</tbody>
</table>

6.10.2. Liquidated damages

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase-out plan</td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of 0.15 LDU <strong>per day of delay in the availability of phase-out plan</strong>.</td>
</tr>
<tr>
<td>Information transfer</td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of 0.5 LDU <strong>per day of delay in the start of the phase-out activities</strong>.</td>
</tr>
<tr>
<td>(PHO-INF)</td>
<td></td>
</tr>
</tbody>
</table>

7. SERVICE/BUSINESS CONTINUITY MANAGEMENT

The Service delivered by the Contractor to the EUI is a critical service. Consequently, the EUI expects from the Contractor that a proper Business Continuity Management (BCM) policy exists for the provision and operation of the Service and requires that the Contractor establishes an operational Business Continuity Plan (BCP) for this Service.

The Contractor accepts to deliver a complete BCP according to its own BCM situation. This work must be finished **by the end of the 6th month** after the signature of the Specific Contract with the specific EUI. After the publication of the first version of that BCP, both parties commit to keep the BCP up-to-date during all the period of validity of this SLA.

The Contractor must provide a Business Continuity Plan, including Disaster Recovery Plan (DRP) details for all Service elements.

The Contractor must also provide an escalation plan in case a business continuity situation is declared at the contractor’s side or in case the EUI needs to activate a business continuity situation with the contractor.

A complete Business Continuity Plan (BCP) covering all service elements must be provided during the phase-in period, kept up-to-date and regularly tested.
7.1.1. Process indicators, Minimum Service Level Requirements

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Timeliness (PHI-BCP)</strong></td>
<td>The contractor must deliver a Business continuity plan covering the services in scope of the contract within 6 months from the signature of the framework contract.</td>
</tr>
<tr>
<td><strong>Adequacy</strong></td>
<td>The different plans are up-to-date and reflect the current situation of a service.</td>
</tr>
<tr>
<td><strong>Communication and escalation plan</strong></td>
<td>Crisis management teams have been identified and are in place to manage incidents. At the end of the phase-in period, crisis communication plans are available, including steps to communicate the information about an incident from its detection to analysis, to recovery, to resumption of normal operations.</td>
</tr>
<tr>
<td><strong>Updates</strong></td>
<td>A plan or a document must be corrected 10 normal working days after an error has been logged and a table-top exercise on this BCP scenario must be arranged. The different documents must be reviewed at least once a year.</td>
</tr>
<tr>
<td><strong>Usage</strong></td>
<td>The different plans are used in case of an incident. The execution of the effective resumption plan must be checked against the set of activities described in a plan.</td>
</tr>
</tbody>
</table>

7.1.2. Liquidated damages

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Timeliness</strong></td>
<td>The contractor shall, upon claim by the EUI, pay liquidated damages of <strong>0,15 LDU per day of delay in the delivery of the services BCP or crisis management procedure</strong></td>
</tr>
<tr>
<td><strong>Usage</strong></td>
<td>The contractor shall, upon claim by the EUI pay liquidated damages of <strong>5 LDU</strong> each time an incident type described in a plan is resolved without respecting the different activities of the plan.</td>
</tr>
</tbody>
</table>

8. DATA PROTECTION COMPLIANCE

The required services are described in Annex 8 Service Requirements of the Tender specifications.

8.1.1. Process indicators, Minimum Service Level Requirements

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access to personal data on a need-to-know basis (DP-APD)</strong></td>
<td>Only the Contractor’s team members who need to have access to personal data of the EUI for the provision of their services under this framework contract can access to such data on a strict need-to-know basis.</td>
</tr>
</tbody>
</table>
| **Personal data breach**                               | Personal data breaches must be immediately notified to EUI and at
8.1.2. **Liquidated damages**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access to personal data on a need-to-know basis (DP-APD)</strong></td>
<td>In case a discrepancy is detected, the EUI may notify the contractor of a serious fault. The registration of the serious fault will lead to the activation of liquidated damages.</td>
</tr>
<tr>
<td><strong>Personal data breach (DP-PDB)</strong></td>
<td>In case a personal data breach is the main cause of a data leakage, EUI may notify the contractor of a serious fault. The registration of the serious fault will lead to the activation of liquidated damages.</td>
</tr>
</tbody>
</table>

9. **INFORMATION SECURITY MANAGEMENT**

The required services are described in Annex 8 Service Requirements of the Tender specifications.

The contractor shall deliver:

- **At the end of the Phase-In of the framework contract:**
  - the timetable for the development of the risk assessment for the services in scope of MTS IV.
  - the timetable for the development of the security plan for the services in scope of MTS IV.

- **For every year of Basic services starting from year1:**
  A yearly review of the risk assessment and security plan for the services in scope of MTS IV.

9.1.1. **Process indicators, Minimum Service Level Requirements**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Required Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Adequacy (ISA)</strong></td>
<td>The different risk assessments and security plans are up-to-date and reflect the current situation of a service .</td>
</tr>
<tr>
<td><strong>Updates (ISU)</strong></td>
<td>A plan or a document has to be corrected 10 normal working days after an error has been detected. The different documents must be reviewed at least once a year.</td>
</tr>
</tbody>
</table>

9.1.2. **Liquidated damages**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Liquidated damages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Adequacy (ISA)</strong></td>
<td>In case it is detected a risk assessment or security plan is not up to date, a serious fault will be registered.</td>
</tr>
<tr>
<td>Updates (ISU)</td>
<td>The contractor shall, upon claim by the <strong>Contracting Authority</strong>, pay liquidated damages of <strong>0.15 LDU</strong> per day of delay in the delivery of the updated risk assessment or security plan.</td>
</tr>
</tbody>
</table>
### Annex 1 – Summary of Committed Service Levels (SL) and Key Performance Indicators (KPI)

<table>
<thead>
<tr>
<th>SL #</th>
<th>Scope</th>
<th>Measured value</th>
<th>Service level (minimum required)</th>
<th>Measurement period</th>
<th>Liquidated damage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>GENERAL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SH</td>
<td>Service Hours</td>
<td>Availability of service (except planned maintenance)</td>
<td>24h/24h 365d/365d</td>
<td>Month</td>
<td>Via other KPIs</td>
</tr>
<tr>
<td>SHPM</td>
<td>Service Hours</td>
<td>Planned maintenance window (by mutual agreement)</td>
<td>7 p.m. to 7 a.m. local time</td>
<td>Month</td>
<td>Via other KPIs</td>
</tr>
<tr>
<td>MON</td>
<td>Monitoring</td>
<td>Records kept for a certain period of time, for inspection on demand</td>
<td>Current year plus full previous calendar year, taking into account the legal obligations.</td>
<td>Month</td>
<td>Via other KPIs</td>
</tr>
<tr>
<td>SDH</td>
<td>Service Hours</td>
<td>Service desk hours</td>
<td>8 a.m. – 6 p.m.</td>
<td>Month</td>
<td>Via other KPIs</td>
</tr>
<tr>
<td>HL</td>
<td>Hot line</td>
<td>Hotline Service Hours</td>
<td>24h/24h 365d/365d</td>
<td>Month</td>
<td>Via other KPIs</td>
</tr>
</tbody>
</table>
## Annex 1 – Committed Service Levels (SL) and Key Performance Indicators (KPI)

<table>
<thead>
<tr>
<th>KPI #</th>
<th>Scope</th>
<th>Measured value</th>
<th>KPI (minimum required)</th>
<th>Applies to</th>
<th>Measurement period</th>
<th>Liquidated damage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>PHASE-IN MANAGEMENT QUALITY</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PHI-PL</td>
<td>Phase-in Plan</td>
<td>A plan to transition from MTS III to MTS IV services is available</td>
<td>At the start of the Phase-in services</td>
<td>Lot 1 &amp; 2</td>
<td>Phase-in period’s start</td>
<td>0,15 LDU per normal working day of delay</td>
</tr>
<tr>
<td>PHI-HD</td>
<td>Service Desk</td>
<td>Hotline and service desk are operational</td>
<td>At the end of the phase-in period</td>
<td>Lot 1 &amp; 2</td>
<td>3 Phase-in period’s start</td>
<td>2 LDU per normal working day late</td>
</tr>
<tr>
<td>PHI-NP</td>
<td>Portability</td>
<td>Mobile numbers and SIM cards are migrated</td>
<td>At the end of the phase-in period</td>
<td>Lot 1</td>
<td>Phase-in period’s start</td>
<td>1 LDU per normal working day late</td>
</tr>
<tr>
<td>PHI-SMS</td>
<td>SMS platform</td>
<td>SMS sending platform, interfaces and APIs are fully operational</td>
<td>At the end of the phase-in period</td>
<td>Lot 2</td>
<td>Phase-in period’s start</td>
<td>2 LDU per normal working day late</td>
</tr>
<tr>
<td>PHI-BCP</td>
<td>BCP</td>
<td>Delivery of BCP</td>
<td>Within 6 months from the signature of the FWC</td>
<td>Lot 1 &amp; 2</td>
<td>6 Months</td>
<td>1 LDU per normal working day late</td>
</tr>
<tr>
<td>PHI-AR</td>
<td>Architecture documentation</td>
<td>Delivery of architecture and API documentation</td>
<td>At the end of the phase-in period</td>
<td>Lot 2</td>
<td>Phase-in period’s start</td>
<td>0,15 LDU per normal working day late</td>
</tr>
<tr>
<td>PHI-IND-E</td>
<td>Indoor coverage</td>
<td>Indoor coverage must be operational for existing buildings with passive equipment already present</td>
<td>Within 6 months from c.s.</td>
<td>Lot 1</td>
<td>6 Months</td>
<td>0,08 LDU per normal working day late</td>
</tr>
<tr>
<td>KPI #</td>
<td>Scope</td>
<td>Measured value</td>
<td>KPI (minimum required)</td>
<td>Applies to</td>
<td>Measurement period</td>
<td>Liquidated damage</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>-------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>PHI-IND-NE</td>
<td>Indoor coverage</td>
<td>Indoor equipment operational for buildings needing full installation</td>
<td>1 building every 2 months starting the 7th month from the signature of the FWC</td>
<td>Lot 1</td>
<td>2 Months</td>
<td>0.08 LDU per normal working day late</td>
</tr>
<tr>
<td>PHI-CUS</td>
<td>Custom functionality</td>
<td>Daily CDRs, user profiles, usage monitoring and alerting</td>
<td>Within 6 months from the signature of the FWC</td>
<td>Lot 1</td>
<td>6 Months</td>
<td>0.08 LDU per normal working day late</td>
</tr>
<tr>
<td>PHI-PH</td>
<td>Procedure Handbook</td>
<td>A draft version of the procedure handbook and final version of the document</td>
<td>Draft version at the end of phase-in period. Final version no later than 6 months after phase-in period</td>
<td>Lot 1 &amp; 2</td>
<td>6 months</td>
<td>0.15 LDU per normal working day of delay and 5 LDU if not delivered</td>
</tr>
<tr>
<td>KPI #</td>
<td>Scope</td>
<td>Measured value</td>
<td>KPI (minimum required)</td>
<td>Applies to</td>
<td>Measurement period</td>
<td>Liquidated damage</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>------------</td>
<td>--------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>PHASE-OUT MANAGEMENT QUALITY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PHO-INF</td>
<td>Information transfer</td>
<td>The relevant information transfer is successfully done</td>
<td>Within 1 month from next contract signature</td>
<td>Lot 1 &amp; 2</td>
<td>3 Months</td>
<td>0.5 LDU per normal working day late</td>
</tr>
<tr>
<td></td>
<td>SERVICE MANAGEMENT QUALITY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRM</td>
<td>Service Review meetings</td>
<td>Number of meeting support documents (agenda 2 working days before and minutes 5 working days after) sent late</td>
<td>≤ 1</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>0.08 LDU per normal working day late, per document</td>
</tr>
<tr>
<td>SCM</td>
<td>Steering Committee meetings</td>
<td>Number of meeting support documents (agenda 2 working days before and minutes 10 working days after) sent late</td>
<td>&lt; 1</td>
<td>Lot 1 &amp; 2</td>
<td>Per meeting</td>
<td>0.15 LDU per normal working day late, per document</td>
</tr>
<tr>
<td>PM</td>
<td>Problem Management</td>
<td>Number of Problems unsolved after the mutually agreed time limit, at the end of each calendar month</td>
<td>≤ 1</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>0.15 LDU per normal working day late, per Problem</td>
</tr>
<tr>
<td>ESM</td>
<td>Escalation Management</td>
<td>Number of incidents of priority 1 or 2, or crisis situation, not escalated within 1H</td>
<td>≤ 1</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>0.5 LDU in case an incident hasn’t been escalated within one hour after the start of the incident 0.1 LDU per hour of delay</td>
</tr>
<tr>
<td>KPI #</td>
<td>Scope</td>
<td>Measured value</td>
<td>KPI (minimum required)</td>
<td>Applies to</td>
<td>Measurement period</td>
<td>Liquidated damage</td>
</tr>
<tr>
<td>------</td>
<td>-------</td>
<td>----------------</td>
<td>-----------------------</td>
<td>------------</td>
<td>--------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>COMM Q</td>
<td>Communication Quality</td>
<td>Perception of communication quality by the users, measured by the number of related justified Incident tickets</td>
<td>≤ 10 complaints</td>
<td>Lot 1</td>
<td>Month</td>
<td>2 LDU per group of 10 complaints</td>
</tr>
<tr>
<td>COMPL</td>
<td>Formal complaints</td>
<td>Number of recurrences of the same complaint within 1 year</td>
<td>&lt; 1 recurrence</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>1 LDU per complaint</td>
</tr>
<tr>
<td>CCDT</td>
<td>Code of Conduct complaints</td>
<td>Number of relevant complaints from customer regarding inappropriate behaviour from MTS IV contractor</td>
<td>&lt; 1 recurrence</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>2 LDU per complaint submitted, and serious fault applies in case of recurrence of the same type of fault.</td>
</tr>
<tr>
<td>SCCDT</td>
<td>Signature of Code of Conduct</td>
<td>Each contractor’s team member having received EUI’s corporate IT accesses and/or equipment will sign a Consultant declaration document</td>
<td>&lt; 1 recurrence</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>0,08 LDU per day of delay in the delivery of a signed Consultant’s declaration document</td>
</tr>
<tr>
<td>SFLT</td>
<td>Serious Fault</td>
<td>Number of serious faults of the MTS IV contractor registered by the EUI contractor</td>
<td>&lt; 1 recurrence</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>3 LDU per serious fault</td>
</tr>
<tr>
<td>RSFLT</td>
<td>Recurrent Serious Fault</td>
<td>Number of repeated serious fault of the same type, within a one-year period after the decision to impose liquidated damages for a serious repeated fault</td>
<td>&lt; 1 recurrence</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>4 LDU per recurrent serious fault</td>
</tr>
<tr>
<td>KPI #</td>
<td>Scope</td>
<td>Measured value</td>
<td>KPI (minimum required)</td>
<td>Applies to</td>
<td>Measurement period</td>
<td>Liquidated damage</td>
</tr>
<tr>
<td>-------</td>
<td>------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>------------</td>
<td>--------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>SSFLT</td>
<td>Security Serious Fault</td>
<td>Number of serious faults being the root cause of a security incident or a data leakage</td>
<td>&lt; 1 recurrence</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>10 LDU per security serious fault</td>
</tr>
<tr>
<td>RSSFLT</td>
<td>Recurrent Security Serious Fault</td>
<td>Number of repeated serious faults related to a security incident or a data leakage of the same type</td>
<td>&lt; 1 recurrence</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>20 LDU per recurrent security serious fault</td>
</tr>
</tbody>
</table>
# Annex 1 – Committed Service Levels (SL) and Key Performance Indicators (KPI)

<table>
<thead>
<tr>
<th>KPI #</th>
<th>Scope</th>
<th>Measured value</th>
<th>KPI (minimum required)</th>
<th>Applies to</th>
<th>Measurement period</th>
<th>Liquidated damage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>CHANGE MANAGEMENT QUALITY</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OPD</td>
<td>Change Management - Offers production deadline (OPD)</td>
<td>Number of offers sent after the agreed deadline (OPD)</td>
<td>≤ 1</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>0,15 LDU per normal working day late, per offer</td>
</tr>
<tr>
<td>RFSD</td>
<td>Change Management – Ready For Service Date (RFSD)</td>
<td>Number of RFC implemented after the agreed deadline (RFSD)</td>
<td>≤ 1</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>0,15 LDU per normal working day late, per RFC</td>
</tr>
<tr>
<td>ITSD</td>
<td>Indoor technical study</td>
<td>Delivery of technical study</td>
<td>Delivery within 2 months after request for implementation</td>
<td>Lot 1</td>
<td>Month</td>
<td>0,15 LDU per normal working day late</td>
</tr>
<tr>
<td>IISD</td>
<td>Indoor infrastructure service date</td>
<td>Implementation of indoor infrastructure</td>
<td>Implementation within agreed deadline</td>
<td>Lot 1</td>
<td>Month</td>
<td>0,15 LDU per normal working day late</td>
</tr>
<tr>
<td>RQFF</td>
<td>Request Fulfillment</td>
<td>Number of standard changes not implemented within 4 working hours</td>
<td>≤ 1</td>
<td>Lot 1</td>
<td>Month</td>
<td>0,15 LDU per late change and per additional day late</td>
</tr>
<tr>
<td>PCFC</td>
<td>Pipe configuration change</td>
<td>Additional bandwidth request or change of the Readlocation of inbound or outbound throughput (pipes) not implemented within 10 working days</td>
<td>≤ 1</td>
<td>Lot 2</td>
<td>Month</td>
<td>0,15 LDU per normal working day late</td>
</tr>
<tr>
<td>KPI #</td>
<td>Scope</td>
<td>Measured value</td>
<td>KPI (minimum required)</td>
<td>Applies to</td>
<td>Measurement period</td>
<td>Liquidated damage</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>------------</td>
<td>--------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>PLUN</td>
<td>Planned intervention</td>
<td>Number of planned intervention not communicated at least 1 week before</td>
<td>≤ 1</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>1 LDU per late communication</td>
</tr>
</tbody>
</table>
### Annex 1 – Committed Service Levels (SL) and Key Performance Indicators (KPI)

<table>
<thead>
<tr>
<th>KPI #</th>
<th>Scope</th>
<th>Measured value</th>
<th>KPI (minimum required)</th>
<th>Applies to</th>
<th>Measurement period</th>
<th>Liquidated damage</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMP1</td>
<td>Incident Management</td>
<td>Ticket of priority P1 (highest, cumulative resolution time ≤ 2h)</td>
<td>≤ 2+(4*p) hours</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>10<em>p</em>LDU</td>
</tr>
<tr>
<td>IMP2</td>
<td>Incident Management</td>
<td>Ticket of priority P2 (cumulative resolution time ≤ 4h)</td>
<td>≤ 4+(4*p) hours</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>4<em>p</em>LDU</td>
</tr>
<tr>
<td>IMP3</td>
<td>Incident Management</td>
<td>Ticket of priority P3 (resolution time)</td>
<td>≤ 1 normal working day</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>p*LDU</td>
</tr>
<tr>
<td>IMP4</td>
<td>Incident Management</td>
<td>Ticket of priority P4 (resolution time)</td>
<td>≤ 2 normal working days</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>0,05 LDU per late resolution and per additional day late</td>
</tr>
<tr>
<td>AVSV</td>
<td>Availability of Services</td>
<td>Average percentage of the time that the service was functioning in accordance with the specifications over a given reference period.</td>
<td>$AV_S = 100 \times \frac{t_{tot} - \sum(t_i \times c_i)}{t_{tot}}$</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>$LD_s = 5 + (100 - AV_{SC}) \times W_S$ when $AV_{SC} &lt; AV_T$</td>
</tr>
</tbody>
</table>
## Annex 1 – Committed Service Levels (SL) and Key Performance Indicators (KPI)

<table>
<thead>
<tr>
<th>KPI #</th>
<th>Scope</th>
<th>Measured value</th>
<th>KPI (minimum required)</th>
<th>Applies to</th>
<th>Measurement period</th>
<th>Liquidated damage</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPM</td>
<td>Monthly Service Reporting</td>
<td>Punctuality</td>
<td>20th calendar day on month N+1, or next working day</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>0,15 LDU for each normal working day the reports are late</td>
</tr>
<tr>
<td>RPY</td>
<td>Yearly Service Report</td>
<td>Punctuality</td>
<td>1st of February or next working day of year+1</td>
<td>Lot 1 &amp; 2</td>
<td>Year</td>
<td>0,15 LDU for each normal working day the reports are late</td>
</tr>
<tr>
<td>REPA</td>
<td>Reporting</td>
<td>Reporting Accuracy</td>
<td>Number of incorrect reports ≤ 1</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>0,15 LDU per incorrect reports</td>
</tr>
<tr>
<td>RCOR</td>
<td>Reporting</td>
<td>Reporting correction</td>
<td>Delivery of corrected reports within 5 working days after error notification</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>0,08 LDU per normal working day late</td>
</tr>
<tr>
<td>OEQ</td>
<td>Order Execution Quality</td>
<td>Proposal quality</td>
<td>The proposal must be in line with the EUI’s requirements</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>0,08 LDU in case the number of revisions necessary to attain the expected level of quality is greater or equal to 3</td>
</tr>
<tr>
<td>ORD</td>
<td>Invoicing</td>
<td>Description</td>
<td>Lot</td>
<td>Payment Frequency</td>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------</td>
<td>-------------------</td>
<td>-------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>ORD</td>
<td>Order respect of deadlines</td>
<td>The proposal and the contract is sent by the contractor before defined deadlines. The revised proposal is sent within 3 normal working days after receipt of EUI’s request. The contract is sent within 2 normal working days after the receipt of the EUI’s proposal.</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>0,08 LDU per normal working day of delay</td>
<td></td>
</tr>
<tr>
<td>INVP</td>
<td>Invoicing</td>
<td>Invoice Punctuality</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>0,08 LDU for each working day the invoice is late</td>
<td></td>
</tr>
<tr>
<td>INVCOR</td>
<td>Invoicing</td>
<td>Correction of invoice</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>0,08 LDU per normal working day late</td>
<td></td>
</tr>
<tr>
<td>INVA</td>
<td>Invoicing</td>
<td>Invoicing accuracy</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>0,08 LDU per incorrect invoice</td>
<td></td>
</tr>
<tr>
<td>KPI #</td>
<td>Scope</td>
<td>Measured value</td>
<td>KPI (minimum required)</td>
<td>Applies to</td>
<td>Measurement period</td>
<td>Liquidated damage</td>
</tr>
<tr>
<td>-------</td>
<td>-------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>------------</td>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DATA PROTECTION AND INFORMATION SECURITY MANAGEMENT</td>
<td></td>
<td></td>
<td></td>
<td>Serious fault associated LD</td>
</tr>
<tr>
<td>DP-APD</td>
<td>Access to personal data on a need to know basis</td>
<td>Only the MTS IV organisation team members who need to have access to personal data of the EUI for the provision of their services can access to such data on a strict need-to-know basis.</td>
<td>In case a discrepancy is detected</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Serious fault associated LD</td>
</tr>
<tr>
<td>DP_PDB</td>
<td>Personal data breach</td>
<td>Personal data breaches must be immediately notified to EUI</td>
<td>At the latest within 48 hours.</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td></td>
</tr>
<tr>
<td>ISA</td>
<td>Information Security Adequacy</td>
<td>The different risk assessments and security plans are up-to-date and reflect the current situation of a service.</td>
<td>Up to date</td>
<td>Lot 1 &amp; 2</td>
<td>Month</td>
<td>Serious fault associated LD</td>
</tr>
<tr>
<td></td>
<td>Information Security Updates</td>
<td>Document Updates</td>
<td>A plan or a document has to be corrected 10 normal working days after an error has been detected The different documents must be reviewed at least once a year.</td>
<td>Lot 1 &amp; 2</td>
<td>Year</td>
<td>The contractor shall pay liquidated damages of 0,15 LDU per day of delay in the delivery of the updated risk assessment or security plan.</td>
</tr>
</tbody>
</table>
11. **ANNEX 2: GLOSSARY**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AM</td>
<td>Account Manager</td>
</tr>
<tr>
<td>AVG&lt;sub&gt;3&lt;/sub&gt;</td>
<td>Average amount of the monthly invoices of the last three previous months for all Services</td>
</tr>
<tr>
<td>EUI</td>
<td>Any participating EU Institution, Agency or Body</td>
</tr>
<tr>
<td>LDU</td>
<td>Liquidated Damage Unit</td>
</tr>
<tr>
<td>NWH / NWD</td>
<td>Normal Working Hours / Normal Working Days – The timeframe / schedule during which offices are opened (generally Mon-Fri 8 a.m. – 6 p.m. or otherwise specified timeframe, outside specific holidays).</td>
</tr>
<tr>
<td>ROW</td>
<td>Rest Of the World zone</td>
</tr>
<tr>
<td>SMT</td>
<td>Service Management Tool</td>
</tr>
<tr>
<td>ITIL</td>
<td>Information Technology Infrastructure Library</td>
</tr>
</tbody>
</table>
Annex VIII

MODEL CONSENT FORM FOR ON-SITE PERSONNEL (FR, NL)

PRIVACY STATEMENT – BELGIAN AUTHORITIES (FR, NL)

PRIVACY STATEMENT - EUROPEAN COMMISSION (EN)
Annexe avis de sécurité : Formulaire de consentement
Exécution des articles 22quinquies à 22septies compris de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité

AVERTISSEMENT
À remplir en double exemplaire : un exemplaire destiné à la personne concernée à titre d'accusé de réception, et un exemplaire que l'officier de sécurité compétent transmet à l'autorité compétente pour délivrer l'avis de sécurité.

La présente demande de vérification de sécurité est adressée à : Autorité Nationale de Sécurité (ANS)
Rue des Petits Carmes, 15
1000 BRUXELLES

La personne reprise à la rubrique 1 est avertie par l'officier de sécurité que, pour le motif exposé à la rubrique 3, elle doit être soumise à une vérification de sécurité.

1. IDENTIFICATION DE LA PERSONNE CONCERNÉE
Une erreur ou omission dans les données ci-dessous peut entraîner la suspension de la procédure de vérification

Uniquement des caractères latins

Nom : .................................................................
Prénom(s) : ...........................................................
Fonction ou profession : ..............................................
Nationalité : ..........................................................
Numéro national belge : .............................................
N° d'identité ou passeport : ........................................... valable du / / au / / Pays de délivrance : ..............
Lieu de naissance* : ..................................................
Date de naissance* : ..................................................
Adresse complète de résidence* : ..................................
Entreprise : ............................................................
Numéro d'entreprise : ..............................................

(*) Doit être complété par les personnes qui n'ont pas de numéro national belge

2. AUTEUR DE LA DEMANDE DE VERIFICATION
Autorité administrative qui sollicite l'avis de sécurité : SPF Affaires Etrangères de Belgique
Secteur pour lequel l'avis de sécurité est demandé : Institutions et organes européens

3. JUSTIFICATION DE LA DEMANDE DE VERIFICATION
Avis de sécurité préalable à l'autorisation d'exercer une profession, une fonction, une mission, un mandat ou d'accéder à des locaux, bâtiments ou sites, à la délivrance d'un permis, à une nomination ou à une désignation - Date de la demande d'avis, nature, base légale ou réglementaire et durée de validité de l'acte administratif à préciser ci-dessous.

Date de la demande : .........................
Nature (raison pour laquelle cette demande est introduite) : La mise en œuvre de vérifications de sécurité pour les employés des contractants externes devant accéder aux Institutions européennes, agences et organismes.
Base légale : Les articles 22quinquies à 22septies compris de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité


Durée demandée (maximum 5 ans) : 5 ans

4. REFUS/CONSENTEMENT DE LA VERIFICATION DE SECURITE

4.a Refus de la vérification de sécurité

La personne qui ne souhaite pas faire l’objet d’une vérification de sécurité peut le faire savoir à tout moment en cochant la case ci-dessous conformément à l’article 30bis de l’arrêté royal du 24 mars 2000 et en le renvoyant par pli recommandé à l’auteur de la demande de vérification (SPF Affaires Etrangères de Belgique).

Si l’avis de sécurité est requis pour un accès, une autorisation, un permis, une nomination ou une désignation, le refus explicite de la vérification entraîne la privation de cet accès, cette autorisation, ce permis, cette nomination ou désignation.

☐ Je ne souhaite pas/plus faire l’objet d’une vérification de sécurité

4.b. Consentement de la vérification de sécurité

☐ Je prends connaissance de la vérification de sécurité à laquelle je serai soumis.e et l’accepte

5. Déclaration sur la protection des données à caractère personnel

☐ Je prends connaissance des déclarations sur la protection des données des autorités belges et des Institutions et organes européens

Lu et approuvé Date : ........................................

Nom, prénom : .......................................................... Signature : ..................................................

Coordonnées de l’Officier de Sécurité de l’autorité administrative compétente :

(Champs à remplir uniquement par le SPF Affaires Etrangères belge)

Nom:................................................................. Grade ou fonction:..................................................

Pris connaissance le (jj/mm/aaaa): ........................................ Signature: ..................................................

NOTICE EXPLICATIVE A LA PRESENTE ANNEXE

1. BASE LEGALE

La loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, les articles 22quinquies, à 22septies compris ;


2. LA VERIFICATION DE SECURITE

a. Objectif

Dans les cas où la protection de l’information classifiée n’est pas en jeu mais bien l’ordre public et la sécurité de l’État, l’autorité administrative compétente peut juger nécessaire de subordonner l’accès à une profession, une fonction, directement ou indirectement, ou l’octroi d’une licence à des mesures spéciales, l’« avis de sécurité ».

b. Sources de renseignements

Les données et informations qui peuvent être consultées dans le cadre d’une vérification de sécurité sont décrites dans l’article 22sexies, §1, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

c. Délais

L’avis de sécurité est délivré ou refusé dans un délai fixé à l’article 30sexies de l’AR du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité qui s’élève à maximum un mois.

3. L’ORGANE DE RECURS EN MATIÈRE DE VERIFICATIONS DE SECURITE

Lorsque suite de la demande de vérification de sécurité l’avis de sécurité est négatif, lorsque la décision n’est pas intervenue ou n’a pas été notifiée dans le délai prévu, la personne pour laquelle l’avis de sécurité a été demandé peut, conformément à l’article 4, §3, de la loi du 11 décembre 1998 portant création d’un organe de recours en matière d’habilitations, d’attestations et d’avis de sécurité, dans les huit jours suivant respectivement la notification de la décision ou de l’avis ou l’expiration du délai, introduire un recours en deux exemplaires par lettre recommandée auprès de l’organe de recours au siège du Comité permanent de contrôle des services de renseignements et de sécurité, Rue de Louvain 48/5, 1000 Bruxelles, T (0)2 286 29 11, www.comitari.be.
Bitlage veiligheidsadvies : Verklaring van toestemming

In uitvoering van de artikelen 22quinquies tot en met 22septies van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen

KENNISGEVING

In te vullen in twee exemplaren: één exemplaar is bestemd voor de betrokken persoon, als ontvangstbewijs, en één exemplaar wordt door de bevoegde veiligheidsofficier doorgestuurd naar de overheid die bevoegd is voor het verstrekken van het veiligheidsadvies.

Dit verzoek tot veiligheidsverificatie wordt gericht aan de Nationale Veiligheidsoverheid (NVO)
Kamelletensstraat 15
1000 BRUSSEL

De in rubriek 1 vermelde persoon wordt er door de veiligheidsofficier van in kennis gesteld dat hij om de in rubriek 3 genoemde reden aan een veiligheidsverificatie moet worden onderworpen.

1. PERSOONSGEGEVEN VAN DE BETROKKEN PERSOON

Een fout of weglating in de onderbouwde gegevens kan leiden tot de opschorting van de verificatieprocedure.

Enkel Latijnse lettertekens gebruiken

<table>
<thead>
<tr>
<th>Naam</th>
<th>.................................</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voornaam(a)m(en)</td>
<td>.................................</td>
</tr>
<tr>
<td>Functie of beroep</td>
<td>.................................</td>
</tr>
<tr>
<td>Nationaliteit</td>
<td>.................................</td>
</tr>
<tr>
<td>Belgisch rijksregisternummer:</td>
<td>.................................</td>
</tr>
<tr>
<td>Nr. identiteitskaart of paspoort:</td>
<td>geldig van / / tot / / Land van afgifte: .................................</td>
</tr>
<tr>
<td>Geboorteplaats*</td>
<td>.................................</td>
</tr>
<tr>
<td>Geboortedatum*</td>
<td>.................................</td>
</tr>
<tr>
<td>Volledig verblijfssadres*</td>
<td>.................................</td>
</tr>
<tr>
<td>Onderneming</td>
<td>.................................</td>
</tr>
<tr>
<td>Ondernemingsnummer</td>
<td>.................................</td>
</tr>
</tbody>
</table>

(*) Verplicht in te vullen door personen die geen Belgisch rijksregisternummer hebben

2. STELDER VAN HET VERZOEK OM EEN VERIFICATIE

Administratie overheid die om het veiligheidsadvies verzoekt: FOD Buitenlandse Zaken van België
Sector waarvoor het veiligheidsadvies wordt aangevraagd: Europese instellingen en organen

3. VERANTWOORDING VOOR HET VERZOEK OM VERIFICATIE

Veiligheidsadvies voorafgaand aan de machtiging om een beroep, een functie, een opdracht of een mandaat uit te oefenen of toegang te hebben tot lokalen, gebouwen of terreinen, aan de afgifte van een vergunning, aan een benoeming of een aanstelling: Datum en aard van het verzoek om een advies, wettelijke of regelgevende basis en geldigheidsduur van de administratieve beslissing hieronder vermelden.

Datum van het verzoek: .................................

Aard (reden waarom dit verzoek wordt ingediend): Uitvoering van veiligheidsverificaties voor de werknemers van externe dienstverleners die toegang moeten krijgen tot de Europese instellingen, agentschappen en organisaties.

Wettelijke basis: De artikelen 22quinquies tot en met 22septies van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen


Gevraagde geldigheidsduur (maximum 5 jaar): 5 jaar

4. WEIGERING VAN/TOESTEMMING TOT DE VEILIGHEIDSVERIFICATIE

2 Europese Parlement, Europese Raad / Raad van de Europese Unie, Europese Commissie, Europese dienst voor extern optreden, Europees economisch en sociaal comité, Europees comité van de regio's, Europees defensieagentschap
4.a Weigering van de veiligheidsverificatie

De persoon die niet wil onderworpen worden aan een veiligheidsverificatie kan dit te allen tijde laten weten door onderstaand vakje aan te vinken zoals bepaald in artikel 30bis van het koninklijk besluit van 24 maart 2000 en door het document bij aangetekende brief terug te sturen naar de steller van het verzoek om een verificatie (FOD Buitenlandse Zaken van België).

Indien het veiligheidsattest of het veiligheidsadvies vereist is voor een toegang, een toelating, een vergunning, een benoeming of een aanstelling, betekent de expliciete weigering om aan een verificatie te worden onderworpen dat de toegang, toelating, vergunning, benoeming of aanstelling niet kunnen worden toegekend.

☐ Ik wens niet/niet meer onderworpen te worden aan een veiligheidsverificatie

4.b. Toestemming tot de veiligheidsverificatie

☐ Ik neem kennis van de veiligheidsverificatie waaraan ik zal worden onderworpen en ik aanvaard deze

5. Verklaring betreffende de bescherming van persoonsgegevens

☐ Ik neem kennis van de verklaringen betreffende gegevensbescherming van de Belgische autoriteiten en van de Europese instellingen en organen

Gelezen en goedgekeurd Datum : …………………………………
Naam, voornaam : ……………………………………………………………… Handtekening : …………………………………………………

Gegevens van de Veiligheidsofficier van de bevoegde administratie :
(velden uitsluitend in te vullen door de FOD Buitenlandse Zaken van België)

Naam:………………………………………………………………………. Rang of functie:………………………………………………………
Kennisneming op (dd/mm/jjjj): ……………………………………… Handtekening: ………………………………………………………

TOELICHTING BIJ DEZE BIJLAGE

1. WETTELIJKE BASIS

De wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, de artikelen 22 en 23 tot en met 27sexies;
Het koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, de artikelen 30 en 30sexies.

2. VEILIGHEIDSVERIFICATIE

a. Doelstelling

In gevallen waarin de bescherming van geclassificeerde informatie niet in het geding is, maar wel de openbare orde en de veiligheid van de staat, kan de bevoegde administratieve autoriteit het nodig achten de toegang tot een beroep of functie, direct of indirect, of het verlenen van een vergunning te onderwerpen aan speciale maatregelen, het "veiligheidsadvies".

b. Inlichtingenbronnen

De gegevens en informatie die in het kader van een veiligheidsverificatie kunnen worden geraadpleegd staan beschreven in artikel 22sexies, §1, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

c. Termijnen

Het veiligheidsadvies moet worden verstrekt of geweigerd binnen een termijn van ten hoogste een maand, zoals vastgelegd in artikel 30sexies van het KB van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

3. BEROEPSORGAALEN INZAKE VEILIGHEIDSVERIFICATIES

Wanneer ingevolge het verzoek om een veiligheidsverificatie, het veiligheidsadvies negatief is of de beslissing niet is genomen of niet ter kennis is gebracht binnen de gestelde termijn, kan de persoon voor wie het veiligheidsadvies is gevraagd, zoals vastgelegd in artikel 4 §3, van de wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, binnen de acht dagen na de respectieve kennisgeving van de beslissing of van het advies of het verstrijken van de termijn, in twee exemplaren bij aangetekende brief beroep instellen bij het beroepsorgaan op de zetel van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, Leuvenseweg 48/5, 1000 Brussel, tel. 02-286 28 11, www.comiteri.be
Déclaration sur la protection des données à caractère personnel fournies dans le cadre de vérifications de sécurité pour les employés des contractants externes devant accéder aux institutions et organes européens

1. Introduction

Le Service Public Fédéral des Affaires Étrangères (ci-après « SPF Affaires Étrangères ») s'engage à protéger vos données à caractère personnel et à respecter votre vie privée. Le SPF Affaires Étrangères procède à la collecte et au traitement ultérieur des données à caractère personnel conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) et conformément à la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

La présente déclaration explique la raison du traitement de vos données à caractère personnel, la façon dont nous collectons, traitons et assurons la protection de toutes les données à caractère personnel fournies, la manière dont les informations sont utilisées ainsi que les droits que vous pouvez exercer à l'égard de vos données. Cette déclaration comprend également les coordonnées du Responsable du traitement compétent auprès duquel vous pouvez exercer vos droits, ainsi que du Délégué à la protection des données.

2. Pourquoi et comment traitons-nous vos données à caractère personnel ?

En mai 2019, les autorités belges et les institutions et organes européens ont conclu un protocole d'accord pour la mise en œuvre de la vérification de sécurité des employés des contractants externes ayant besoin d'un accès aux institutions et organismes de l'UE en Belgique.

L'Autorité administrative belge en charge est le SPF Affaires étrangères ou son délégué. Il agit en tant qu'intermédiaire entre les institutions et organes européens et l'Autorité Nationale de Sécurité (ci-après ANS).

La vérification de sécurité est à la demande des institutions et des organes européens et elle est effectuée par l’ANS. Celle-ci est compétente pour émettre un avis de sécurité positif ou négatif pour chaque employé de prestataires externes. Cet avis vise à garantir la sécurité du personnel et des biens des institutions et organes européens, la confidentialité de leurs informations ainsi que, la protection de leur réputation en tant qu'organisations internationales. Les vérifications de sécurité permettent aux institutions de décider en connaissance de cause si elles octroient l'accès à leurs locaux au personnel de prestataires externes.

Les données à caractère personnel des employés des contractants travaillant pour les institutions et organes européens seront traitées dans le cadre d'une vérification de sécurité.
Ces données ne seront pas utilisées pour la prise de décision automatisée, y compris le profilage.

3. Sur quelle base juridique traitons-nous vos données à caractère personnel ?

Nous traitons vos données à caractère personnel conformément à l'article 6, paragraphe 1, point c) et e) du règlement (UE) 2016/679, c'est-à-dire, que le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

Spécifiquement pour le traitement des données à caractère personnel par l'ANS dans le cadre des habilitations, attestations et avis de sécurité visés par la loi du 11 décembre 1998, les données sont traitées conformément à l'article 108, 3° de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Cet article dispose que le traitement de données à caractère personnel ne peut être effectué dans ce contexte que s'il est nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis en vertu d'une loi.

Base juridique :

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
- Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.
- Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.
- Arrêté royal du 8 mai 2018 déterminant la liste des données et informations qui peuvent être consultées dans le cadre de l'exécution d'une vérification de sécurité.
- Arrêté royal du 8 mai 2018 fixant les secteurs d'activités et les autorités administratives compétentes visées à l'article 22quinquies, § 7, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

4. Quelles sont les données à caractère personnel que nous recueillons et traitons ?

Aux fins de réaliser cette opération de traitement, le SPF des Affaires Étrangères recueille les catégories suivantes de données à caractère personnel :

- Nom
- Prénom(s)
- Fonction ou profession
- Nationalité
5. Combien de temps vos données à caractère personnel sont-elles conservées ?

Le SPF des Affaires Étrangères ne conserve vos données à caractère personnel que pendant le temps nécessaire pour atteindre la finalité de leur collecte ou de leur traitement ultérieur, à savoir au maximum cinq ans à compter de la réception de l’avis de sécurité ou, en cas de plainte, pendant toute la durée de la procédure en justice.

6. Comment protégeons-nous et sauvegardons-nous vos données à caractère personnel ?

Toutes les données à caractère personnel sous format électronique (e-mails, documents, lots de données téléchargés, etc.) sont enregistrées sur les serveurs du SPF des Affaires Étrangères.

Les sous-traitants des institutions et organes européens sont liés par une clause contractuelle spécifique pour toute opération de traitement de vos données pour le compte de ces institutions et de ces organes européens, et par les obligations de confidentialité dérivées de l’application du règlement (UE) 2016/679 dans les États membres de l’UE.

En vue de protéger les données à caractère personnel, le SPF des Affaires Étrangères a mis en place plusieurs mesures techniques et organisationnelles. Les mesures techniques incluent notamment des actions appropriées concernant la sécurité en ligne, le risque de perte de données, l’altération des données ou l’accès non autorisé, en prenant en compte le risque présenté par le traitement et la nature des données à caractère personnel qui sont traitées. Les mesures organisationnelles visent notamment à restreindre l’accès aux données à caractère personnel aux seules personnes autorisées, ayant un besoin légitime de les connaître pour les finalités de cette opération de traitement.

7. Qui a accès à vos données à caractère personnel et à qui sont-elles communiquées ?


Outre l’Autorité Nationale de Sécurité, les institutions et organes européens concernés et votre employeur auront accès aux données personnelles fournis dans le formulaire de consentement.
8. Quels sont vos droits et comment pouvez-vous les exercer ?

Vous avez des droits spécifiques en qualité de personne concernée aux articles 112-115 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Ce chapitre inclut le droit de demander au responsable du traitement l'accès aux données à caractère personnel limité à l'information que vous avez vous-même fournie, la rectification ou la suppression des données à caractère personnel inexactes, la vérification auprès de l'autorité de contrôle compétente du respect des dispositions applicables de la loi du 30 juillet 2018.

9. Coordonnées de contact

- Responsable du traitement des données : SPF des Affaires Étrangères, 15 rue des Petits Carmes à 1000 BRUXELLES

Si vous souhaitez exercer vos droits au titre du règlement (UE) 2016/679, ou si vous avez des commentaires, des questions ou des préoccupations à exprimer, ou si vous souhaitez soumettre une plainte relative à la collecte et à l’utilisation de vos données à caractère personnel, n’hésitez pas à contacter le Responsable du traitement de données.

- Délégué à la protection des données (DPD-DPO) :
  
  • Du SPF des Affaires Étrangères : dpo@diplobel.fed.be

10. Où trouver de plus amples informations ?

Contactez le délégué à la protection des données (DPD-DPO) du SPF des Affaires Étrangères. Celui-ci publie un registre de toutes les opérations de traitement de données à caractère personnel effectuées par le SPF des Affaires Étrangères, qui ont été documentées et qui lui ont été notifiées.
1. Inleiding

De Federale Overheidsdienst Buitenlandse Zaken (hierna "FOD Buitenlandse Zaken") verbindt zich ertoe uw persoonsgegevens en uw persoonlijke levenssfeer te beschermen. De FOD Buitenlandse Zaken verzamelt en verwerkt de persoonsgegevens overeenkomstig verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) en overeenkomstig de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van de persoonsgegevens.

In deze toelichting leggen we uit waarom we uw persoonsgegevens verwerken, hoe we ze verzamelen en verwerken en hoe we zorgen voor de bescherming van de verstrekte persoonsgegevens, hoe we de informatie gebruiken en welke rechten u met betrekking tot uw persoonsgegevens kunt uitoefenen. U vindt er ook de contactgegevens van de bevoegde Verwerkingsverantwoordelijke ten aanzien van wie u uw rechten kunt uitoefenen en van de Functionaris voor gegevensbescherming.

2. Waarom en hoe worden uw persoonsgegevens verwerkt?

In mei 2019 sloten de Belgische overheid en de Europese instellingen en organen een protocoleakkoord over de uitvoering van veiligheidsverificaties voor de werknemers van externe dienstverleners, die toegang dienen te hebben tot de instellingen en organen van de EU in België.

De bevoegde administratieve overheid in België is de FOD Buitenlandse Zaken of haar afgevaardigde. Hij treedt op als tussenpersoon tussen de Europese instellingen en de Nationale Veiligheidsoverheid (hierna NVO).

Op vraag van de Europese instellingen en organen voert de NVO een veiligheidsverificatie uit. Ze is bevoegd om positieve of negatieve veiligheidsadviezen af te leveren met betrekking tot werknemers van externe dienstverleners. Dit advies heeft tot doel de veiligheid van het personeel en van de goederen van de Europese instellingen en organen te waarborgen, de vertrouwelijkheid van hun informatie te vrijwaren en hun reputatie als internationale organisaties te beschermen. Aan de hand van de veiligheidsverificaties kunnen de instellingen met kennis van zaken beslissen of ze het personeel van externe dienstverleners toegang tot hun gebouwen verlenen.

De persoonsgegevens van de medewerkers van de dienstverleners, die voor de Europese Instellingen en organen werken, worden in het kader van een veiligheidsverificatie verwerkt.
Deze gegevens worden niet gebruikt voor een geautomatiseerde besluitvorming, waaronder profilering.

3. Op welke rechtsgrond worden uw persoonsgegevens verwerkt?

We verwerken uw persoonsgegevens overeenkomstig artikel 6, paragraaf 1, punt c) en e) van verordening (EU) 2016/679, die bepaalt dat de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting waaraan de verwerkingsverantwoordelijke is onderworpen en voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend.

Wat meer in het bijzonder, de verwerking van persoonsgegevens door de NVO in het kader van de in de wet van 11 december 1998 bedoelde veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen betreft, worden de gegevens verwerkt overeenkomstig artikel 108, 3° van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van de persoonsgegevens. Dit artikel bepaalt dat persoonsgegevens in deze context slechts mogen worden verwerkt wanneer de verwerking noodzakelijk is om een verplichting na te komen waaraan de verwerkingsverantwoordelijke is onderworpen krachtens een wet.

Rechtsgrond:

- Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).
- Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van de persoonsgegevens.
- Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.
- Koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.
- Koninklijk besluit van 8 mei 2018 tot bepaling van de lijst van de gegevens en informatie die geraadpleegd kunnen worden in het kader van de uitvoering van een veiligheidsverificatie.
- Koninklijk besluit van 8 mei 2018 tot vaststelling van de activiteitensectoren en de bevoegde administratieve overheden bedoeld in artikel 22quinquies, § 7, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

4. Welke persoonsgegevens worden verzameld en verwerkt?

Om de verwerking te kunnen uitvoeren, verzamelt de FOD Buitenlandse Zaken de volgende categorieën van persoonsgegevens:
Toelichting inzake de bescherming van persoonsgegevens

5. Hoelang worden uw persoonsgegevens bewaard?

De FOD Buitenlandse Zaken bewaart uw persoonsgegevens enkel voor de periode die nodig is om het doel waarvoor ze werden verzameld, of het doel van hun verdere verwerking te bereiken, met name maximaal vijf jaar te rekenen vanaf de ontvangst van het veiligheidsadvies of, in geval van een klacht, gedurende de hele gerechtelijke procedure.

6. Hoe worden uw persoonsgegevens beschermd en opgeslagen?

Alle in elektronische vorm verstrekte persoonsgegevens (e-mails, documenten, gedownload datasets, enz.) worden op de servers van de FOD Buitenlandse Zaken opgeslagen.

De onderaannemers van Europese Instellingen en organen zijn voor elke verwerking van uw persoonsgegevens voor rekening van deze Europese Instellingen en organen gebonden door een specifieke clausule en door de geheimhoudingsverplichtingen die voortvloeien uit de toepassing van verordening (EU) 2016/679 in de lidstaten van de EU.

Met het oog op de bescherming van de persoonsgegevens heeft de FOD Buitenlandse Zaken een reeks technische en organisatorische maatregelen getroffen. Technische maatregelen zijn bijvoorbeeld passende maatregelen inzake online veiligheid, het risico op verlies of wijziging van of de ongeoorloofde toegang tot de gegevens, rekening houdend met het risico dat de verwerking en de aard van de persoonsgegevens die worden verwerkt, met zich meebrengen. De organisatorische maatregelen zijn bedoeld om de toegang tot persoonsgegevens te beperken tot die personen die hiertoe bevoegd zijn en die een gerechtvaardigde behoefte hebben om er kennis van te nemen met het oog op de doelen van de verwerkingsactiviteit.

7. Wie heeft toegang tot uw persoonsgegevens en aan wie worden ze meegedeeld?

Het team van de FOD Buitenlandse Zaken dat verantwoordelijk is voor de uitvoering van de verwerking en het gemachtigd personeel op een “need-to-know”-basis hebben toegang tot uw persoonsgegevens. Deze medewerkers moeten de verplichtingen inzake statutaire geheimhoudingsplicht in acht nemen (artikel 10, §2 van het Koninklijk besluit van 2 oktober 1937 en de artikelen 23 en 24 van de wet van 11 december 1998).
Bovendien hebben de Nationale Veiligheidsoverheid, de betrokken Europese instellingen en organen en uw werkgever toegang tot de persoonsgegevens die in het toestemmingsformulier worden verstrekt.

8. Welke rechten hebt u en hoe kunt u deze uitoefenen?

Als betrokken persoon hebt u specifieke rechten die vermeld zijn in de artikelen 112-115 van hoofdstuk VI van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

Dit hoofdstuk omvat het recht om de verwerkingsverantwoordelijke te vragen om inzage te krijgen in de persoonsgegevens die u zelf heeft verstrekt, om onjuiste persoonsgegevens te laten verbeteren of verwijderen en om de naleving van de toepasselijke bepalingen van de wet van 30 juli bij de bevoegde toezichthoudende autoriteit te verifiëren.

9. Contactgegevens

- Verwerkingsverantwoordelijke: FOD Buitenlandse Zaken, Karmelietenstraat 15, 1000 BRUSSEL

Als u uw rechten overeenkomstig verordening (EU) 2016/679 wilt uitoefenen of als u opmerkingen of vragen heeft of uw bezorgdheid wilt uiten of een klacht wilt indienen over het verzamelen en het gebruik van uw persoonsgegevens, neem dan contact op met de verwerkingsverantwoordelijke.

- Functionaris voor gegevensbescherming (DPD-DPO) :
  
  • van de FOD Buitenlandse Zaken : dpo@diplobel.fed.be

10. Waar vindt u meer informatie ?

Hiervoor kunt u contact opnemen met de functionaris voor gegevensbescherming (DPD-DPO) van de FOD Buitenlandse Zaken. Hij publiceert een register van alle door de FOD Buitenlandse Zaken gedocumenteerde en aangemelde verwerkingsactiviteiten met betrekking tot persoonsgegevens.
PROTECTION OF YOUR PERSONAL DATA

This privacy statement provides information about the processing and the protection of your personal data.

Processing operation: HR – Background checks for contractor staff

Data Controller: DG HR.DS

Record reference: DPR-EC-00675

Table of Contents

1. Introduction
2. Why and how do we process your personal data?
3. On what legal ground(s) do we process your personal data?
4. Which personal data do we collect and further process?
5. How long do we keep your personal data?
6. How do we protect and safeguard your personal data?
7. Who has access to your personal data and to whom is it disclosed?
8. What are your rights and how can you exercise them?
9. Contact information
10. Where to find more detailed information?
1. **Introduction**

The European Commission (hereafter ‘the Commission’) is committed to protect your personal data and to respect your privacy. The Commission collects and further processes personal data pursuant to 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 (repealing Regulation (EC) No 45/2001).

This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.

The information in relation to processing operation HR – Background checks for contractor staff undertaken by the Security Directorate (DG HR.DS) is presented below.

2. **Why and how do we process your personal data?**

**Purpose of the processing operation:** The Security Directorate collects and uses your personal information to make an informed decision on whether to grant access to the Commission’s premises.

Belgian authorities and EU Institutions and Bodies (European Commission, European Parliament, European Council, Council of the European Union, European External Action Service, European Economic and Social Committee, Committee of the Regions, European Defence Agency) (‘EUI’) have signed in May 2019 a Memorandum of Understanding for the implementation of Security Verification’s of external contractors.

The verification is at the request of European Institutions and Bodies and will result in either a positive or negative security advice for each individual assessed, granted by the Belgian National Security Authority.

Any employee of an external contractor who will be subject to a security verification will give his permission to initiate the security verification necessary to obtain a security advice. If the employee of the external contractor refuses to be subjected to a security verification, s/he may express her/his refusal by indicating it on the consent form and sending it, by registered mail.

The firm will electronically transmit in an Excel sheet the following data of the person(s) involved: last name, first name, function or profession, nationality, Belgian national number, ID or passport number, date and place of birth, address, company and company ID number.

Your personal data will **not** be used for an automated decision-making including profiling.

3. **On what legal ground(s) do we process your personal data?**

The legal basis for processing data is provided by Article 5 (1) a) and b) of Regulation (EU) 2018/1725.

Therefore, we process your personal data, because:

(a) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body;
(b) processing is necessary for compliance with a legal obligation to which the controller is subject

Processing according to lit (a) above refers to the Commission’s task of ensuring security in the Commission as provided for by Article 22 (2) of European Commission Decision (EU, Euratom) 2015/443.

Processing by the Belgian national authorities is then carried out within the following Belgian legal and regulatory framework on security verifications:

- Act of 11 December 1998 on classification and security clearances, security certificates and security advice, its accompanying Royal Decree of 24 March 2000 and the Royal Decree of 8 May 2018 modifying the aforementioned Decree;

- Royal Decree of 8 May 2018 establishing the activity sectors and the competent administrative authorities as referred to in Article 22 quinquies, § 7,

- Royal Decree of 8 May 2018 establishing the list of data and information that can be consulted in the context of the execution of a security verification.

4. **Which personal data do we collect and further process?**

In order to carry out this processing operation the Security Directorate (DG HR.DS) collects the following categories of personal data:

- Last name and first name;
- Address;
- Function or profession;
- Nationality;
- Date and place of birth;
- Nationality;
- Belgian national number,
- ID or passport number,
- Date and place of birth,
- Company and company ID number;

The provision of personal data is mandatory to meet the contractual requirement on services provided on the premises of the Commission. If you do not provide your personal data, possible consequences are refusal of access rights to Commission buildings.

5. **How long do we keep your personal data?**

The Security Directorate (DG HR.DS) only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing, namely for five years from obtaining the security advice, which constitutes the latter’s maximum validity period.

6. **How do we protect and safeguard your personal data?**

All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored either on the servers of the European Commission. All processing operations are carried out pursuant to the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.
In order to protect your personal data, the Commission has put in place a number of technical and organisational measures in place. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

7. **Who has access to your personal data and to whom is it disclosed?**

Access to your personal data is provided by the consent form you filled in to the Commission staff responsible for carrying out this processing operation and to authorised staff according to the “need to know” principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

The consent form is sent to the Belgian Ministry of Foreign Affairs, who will then have access to your personal data.

The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law.

However, when a negative security advice is received, the European Commission will inform about it to the other institutions and bodies participating in the MoU.

8. **What are your rights and how can you exercise them?**

You have specific rights as a ‘data subject’ under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access, rectify or erase your personal data and the right to restrict the processing of your personal data. Where applicable, you also have the right to object to the processing or the right to data portability.

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given under Heading 9 below.

Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description (i.e. their Record reference(s) as specified under Heading 10 below) in your request.

9. **Contact information**

- **The Data Controller**

If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the Data Controller, the Security Directorate (DG HR.DS) and EC-SECURITY-SCREENING@ec.europa.eu

- **The Data Protection Officer (DPO) of the Commission**

You may contact the Data Protection Officer (DATA-PROTECTION-OFFICER@ec.europa.eu) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

- **The European Data Protection Supervisor (EDPS)**
You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor [edps@edps.europa.eu] if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.

10. Where to find more detailed information?

The Commission Data Protection Officer (DPO) publishes the register of all processing operations on personal data by the Commission, which have been documented and notified to him. You may access the register via the following link: http://ec.europa.eu/dpo-register.

This specific processing operation has been included in the DPO’s public register with the following Record reference: DPR-EC-00675
Annex IX

TEMPLATE FOR THE ELECTRONIC LIST OF RELEVANT PERSONAL DATA FOR ON-SITE PERSONNEL (LIST OF DATA)
<table>
<thead>
<tr>
<th>Pers ID</th>
<th>Name</th>
<th>First name</th>
<th>Address</th>
<th>Nr N°</th>
<th>Zip code</th>
<th>Code Postal</th>
<th>City</th>
<th>Commune</th>
<th>Country</th>
<th>Pays</th>
<th>National Number</th>
<th>N° de registre national</th>
<th>Nationality</th>
<th>Nationalité</th>
<th>Date of birth</th>
<th>Date de Naissance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Legend:**
- to be completed by the employer
- to be completed by European Institutions and Bodies
<table>
<thead>
<tr>
<th>Place of birth</th>
<th>Function - Fonction</th>
<th>Consent Date - Date Consentement</th>
<th>Employer - Employeur</th>
<th>Company number - Numéro d'entreprise</th>
<th>Company e-mail adresse-adresse e-mail entreprise</th>
<th>IR - Initial request or renewal Demande Initiale ou renouvellement</th>
<th>Date of request - Date de demande</th>
<th>Result - Résultat (POSITIF, POSITIF -5, RADIE, NO RNN ou NEGATIF)</th>
<th>Security advice valid until... - Avis de sécurité valable jusqu'à...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Annex X to FwC DI/07910

**CODE OF CONDUCT FOR CONTRACTORS AND CONSULTANT’S DECLARATION**
I. CODE OF CONDUCT FOR CONTRACTORS

1. PURPOSE AND SCOPE OF THIS DOCUMENT

This Code of Conduct lays down general guidelines about the high standards of ethical behaviour that the EU Institution expects from its contractors. These guidelines do not replace the contractors’ strict obligations under the terms of the Framework Contract and the applicable law, but, rather, they supplement and clarify those obligations as appropriate.

Contractors are also expected to ensure that their subcontractors, if any, are aware of, and abide by, these guidelines.

It should be borne in mind that the guidelines laid down below do not necessarily have the same begin and end dates as the Framework Contract itself. In particular, some guidelines are appropriate for the phase-in and/or phase-out stages of a Framework Contract, irrespective of whether the latter has already been signed and/or has already expired.

2. DEFINITIONS

In the context of this document:

- “Contractor” refers to a sole contractor, to a consortium or to each member of a consortium (as well as, by extension and when appropriate, to subcontractors).
- “Personnel” refers to individuals who are employed by (or work as freelancers for) a contractor.
- “Consultant” refers to external service providers providing a service to the EU Institution.\(^1\)

3. GUIDELINES FOR THE CONDUCT OF THE CONTRACTOR IN RELATION TO ITS PERSONNEL

3.1. Personnel in general

- The contractor shall not act in such a way that the continuity of the hierarchical link between itself and its Personnel may be called into question.
- The contractor shall ensure that members of its Personnel do not convey the impression that they are employed by the EU Institution, or that they are authorised to represent the EU Institution.
- The contractor shall refrain from asking those members of its Personnel allocated to full-time assignments under the Framework Contract to perform other tasks.
- The contractor shall make sure that all members of its Personnel provided to the EU Institution have the necessary competences in order to perform the service in a professional manner.

\(^1\) This definition applies as well to Contractor’s Personnel hosted outside Commission premises with a “replicated” environment: i.e. using Commission IT equipment and having received a Commission IT account.
way; an update of the skills should be foreseen in order to cope with the normal evolution of
the software products. This kind of trainings may not incur additional costs for the EU
Institution.

3.2. Additional guidelines for Personnel working on the EU Institution’s premises or having
received Commission IT equipment

– The contractor shall ensure that all members of its Personnel working as consultants for the
EU Institutions read, understand and are aware of the ethical principles and obligations laid
down in the “Consultant’s declaration” found in Section II of this document. It shall take
all measures deemed appropriate to ensure that its Personnel does in fact follow those
guidelines. The contractor shall require those members of its Personnel working as
consultants for the EU Institutions to sign a copy of the above-mentioned “Consultant’s
declaration” and provide the EU Institution with a signed copy.

– The contractor shall pay special attention to the respect by its Personnel of any safety and
security requirements and procedures laid down by the EU Institution.

4. GUIDELINES FOR THE CONDUCT OF THE CONTRACTOR IN RELATION TO THE EU INSTITUTION
AND THE EU INSTITUTION’S PERSONNEL

– The contractor shall not seek to obtain financial, contractual, commercial or other sensitive
information that is not necessary for performing the Framework Contract. If — for whatever
reason — such information is in fact obtained, the contractor shall refrain from using or
disclosing it, unless the EU Institution explicitly authorises it to do so. The above does not
apply to information that is already publicly available.

– The contractor shall not exert any pressure on the EU Institution’s officials. In particular, it
shall not seek to obtain any information on on-going or forthcoming procurement procedures
that is not already in the public domain.

– The contractor shall refrain from making any gifts or offers of hospitality to the EU
Institution’s officials.

5. GUIDELINES FOR THE CONTRACTOR IN RELATION TO ITS COMPETITORS

The contractor’s competitors are likely to include other contractors of the EU Institution as
well as (prospective) tenderers in procurement procedures run, or to be run, by the EU
Institution. The EU Institution will not interfere with the contractor’s dealings with these, or
indeed any other, competitors.

The EU Institution does, however, expect the contractor to abide by a very high standard of
professional deontology, guided by the principle of fair competition. In particular, the
contractor should at all times be courteous, show restraint and avoid any form of competitor-
bashing and harassment. In all cases, the EU Institution premises may not be used for
marketing or recruitment purposes.

6. GUIDELINES IN RELATION TO PERSONAL DATA

Under Regulation (EU) No 2018/1725, the EU Institution is responsible for the protection of
personal data, which it holds pertaining to third parties (“data subjects”). These include the
contractor’s Personnel — but likewise the staff employed by other contractors of the EU Institution.

It is possible that, while performing a Framework Contract, the contractor or its Personnel becomes aware of contact details about staff employed by other contractors, such as their telephone, e-mail address and/or office provided to them by the EU Institution. Such contact details coincide with “personal data” related to “data subjects” in the sense of Regulation (EU) No 2018/1725, which the EU Institution is obliged to protect.

The EU Institution will not interfere with the contractor’s relations with such third parties, in particular for marketing or recruitment purposes. Hence, it is permissible for the contractor to contact them for such purposes, provided that this does not cause the EU Institution to be in breach, or to appear to be in breach, of its obligations under Regulation (EU) No 1725/2018.

To this end, the following principles should be respected:

– The contractor must have become aware of the information in question as a result of normal professional contact and/or market knowledge — but not through access to internal information systems of the EU Institution.

– In any case, the contractor must be able to show that it has obtained the addressee’s unambiguous consent for this type of contacts, and give him/her the opportunity to revoke that consent.

– Under no circumstances can the EU Institution’s premises or infrastructure be used for marketing or recruitment purposes.

7. GUIDELINES ON USE OF IT EQUIPMENT, INFRASTRUCTURE AND RISK MANAGEMENT

When delivering or using any equipment, infrastructure and/or software, during implementation of IT projects of the EU Institutions, the contractor shall always make sure that it is aligned with the established technology risk management framework. Those should be compliant with the IT Security guidelines applicable to the contract.

The contractor should make his Personnel aware of the applicable guidelines linked to the usage, deployment and/or access to IT infrastructure and IT-related resources. IT assets should be adequately used (e.g. preventing unauthorised access, misuse, deletion, disclosure).
II. CONSULTANT’S DECLARATION

Under initial / extension request No …
Specific contract No …
Framework contract No DI/07910

[To be filled in and signed by the consultant, and submitted to the Commission]

– In case of initial requests, this document has to be filled in by each consultant providing services under the present FwC.

– In case of extension requests, this declaration has to be filled in the following cases:
  a) in case of replacement of the consultant;
  b) in case of change of the consultant’s status (e.g. from permanent employee of the contractor or its subcontractors to a self-employed/one-person company);
  c) in case of change of the consultant’s employer.

– In case of replacement of a consultant during the period of implementation of a specific contract, this declaration has to be filled in in all cases (including in the case of replacement of replacements).
Definitions

In the context of this document:

- “Contractor” refers to a sole contractor, to a consortium or to each member of a consortium (as well as, by extension and when appropriate, to subcontractors).

- “Personnel” refers to individuals who are employed by (or work as freelancers for) a contractor.

- “Consultant” refers to external service providers (contractor’s employees or freelancers) providing a service to the EU Institution.2

I, the undersigned, ……………………………………………………………,…

[Employee of / freelancer]3 of the company: ………………………………………………………………,

Declare that I have read and understood the following ethical principles and obligations that apply to me as a service provider to the European Commission, agree with them and undertake to respect them.

Employer / Hierarchical link

- Consultants are employed by the contractor, not by the EU Institution. Accordingly, any matters directly related to the hierarchical link (career development, supervision of work quality, planning of leaves, etc.) must be dealt with the contractor, not with the EU Institution.

- In addition, consultants must not, under any circumstances, convey the impression that they are employed by the EU Institution, or that they are authorised to represent the EU Institution. In particular, when signing documents or e-mails, or whenever their name appears in a document related to their work for the EU Institution, clear reference must be made to the fact that they work for the contractor. The EU Institution can issue more detailed instructions to this end.

Relations with the EU Institution and with the EU Institution’s personnel

- Consultants shall not seek to obtain any information (be it political, judicial, contractual, commercial, budgetary or financial affairs, or the management of the EU Institution, the personnel or data processing, or other sensitive information) which is not necessary for performing the Framework Contract. If — for whatever reason — such information is in fact obtained, they shall refrain from using or disclosing it, unless the EU Institution...

---

2 This definition applies as well to Contractor’s Personnel hosted outside Commission premises with a "replicated" environment: i.e. using Commission IT equipment and having received a Commission IT account.

3 Delete as appropriate.
explicitly authorises them to do so. The above does not apply to information that is already publicly available.

– Consultants shall not exert any pressure on the EU Institution’s officials. In particular, they shall not seek to obtain any information on on-going or forthcoming procurement procedures that is not already in the public domain.

– Consultants shall refrain from making any gifts or offers of hospitality to the EU Institution’s officials.

Confidentiality

– Consultants must treat the facts, information and/or documents, what ever their source, that are made available to them or generated during the course of their provision of service to the Commission in the context of the implementation of the above-mentioned contract with the strictest confidentiality.

– Without prejudice to the general obligation of professional secrecy, no such information and/or documents acquired in the course of their service provision under the above mentioned contract, will be disclosed to any third parties, in any way and by any means, directly or through others, without the prior authorisation of the EU Institution. This restriction covers, in particular, all notes, analyses, opinions, compilations, studies, interpretations, summaries, extracts, data or other documents or records in original or in copy containing, regarding, reflecting or otherwise deriving from any confidential, sensitive or secret information that consultants prepared or became aware of in the exercise of their functions in the context of the work as a service provider and that is not yet public or accessible to the public without any restriction (e.g. published on the internet, Europa or any other media, accessible for consultation).

– Consultants are aware that tasks carried out in view of the implementation and/or performance of this contract are also governed by this principle of confidentiality.

– Consultants shall refrain from exploiting insights of a confidential nature in policy, strategy or internal processes that they may have acquired during their provision of service and that have not yet been made public or are not commonly available in the public domain.

– Consultants are aware of the fact that the principle of confidentiality pointed out in the first paragraph will continue to apply after their period of service provision to the Commission under the above mentioned contract.

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

Contacts with other parties and publications

– During service provision, Consultants shall not have any professional connections with third parties which might be incompatible with providing a service in the Commission (e.g.
must not work for lobbyists, legal attachés, other firms or entities involved in EU-related matters in their field of work etc.).

- Consultants shall not have contact with the Press on matters relating to their work as a service provider in the Commission unless their employer and the Commission have agreed it beforehand.

- Consultants must not, alone or with others, publish or cause to be published any matter dealing with the work of the European Commission without the written permission of their employer and the Commission. Such permission is subject to the conditions in force for all Commission staff.

- All rights, for any articles or other work done, as part of their service provision to the Commission remain the property of the Commission in accordance with the contract signed by the Contractor and the Commission.

**Duty of loyalty**

- Consultants should carry out the provision of service solely with the interests of their employer and their client, the European Commission, in mind.

- Consultants should neither seek nor take instructions from any other party in the context of their provision of service to the Commission.

- Consultants shall carry out the duties of service provision assigned to them objectively, impartially and in keeping with their duties of loyalty to their employer as a contractor with the Commission.

**Conflict of interests during the period of service provision**

- Consultants shall not, in the performance of their duties, deal with a matter in which, directly or indirectly, they have any personal interests such as to impair their independence, and, in particular, family and financial interests.

**Safety and security**

- Consultants must follow all safety and security requirements and procedures laid down by the EU Institution, in particular (but not limited to) the following:
  
  - Consultants must willingly comply with the requirements of the EU Institution’s security services, including the inspection of the personal goods (by scanner or physical inspection).
  
  - When on the EU Institution’s premises, consultants shall wear at all times the access card issued to them by the relevant EU Institution services. They must return the access card(s) before they leave, at first request by the EU Institution.
- Consultants must never jeopardise the good functioning, the security or the confidentiality of the systems or data, which they may have access to within the framework of their functions.
- Consultants may not bring in, or let in, any unauthorised person to the EU Institution’s premises.
- If, at the EU Institution’s discretion, consultants are entitled to use the parking lots available in the EU Institution’s buildings, they must respect strictly the applicable rules and regulations. Failure to do so will result in the removal of the authorisation.
- Consultants must keep secret the safety and security requirements and procedures as well as protection mechanisms which they may come to gain knowledge about in the process of their activities.
  - Consultants must familiarise themselves, and comply strictly with, all security guidelines issued by DG HR’s “Security” Directorate, which will be made available to them at the start of their assignments, and in particular with the security guidelines outlined in Annex XIII to the FWC: “Appendices for Security baseline for external connections – remote service delivery”.

**Use of equipment and infrastructure**

- Consultants must ensure that the equipment and infrastructure provided to them by the EU Institution and/or by the contractor remains in good working order and report any incidents to this effect. Use of this equipment and infrastructure, including software and access to information systems, must be limited to professional purposes related to the performance of contractual obligations.
  - However, where applicable, use of standard computer equipment (including e-mail and Internet access) and fixed telephones for private purposes is tolerated under the same conditions as for the EU Institution’s personnel, i.e. (in summary) as long as such use (i) is on a purely occasional basis and does not amount to extensive use; and (ii) is not for illegal or irregular purposes, in any way that might disrupt the functioning of the service itself or in any manner contrary to the interests of the EU Institution.
  - In case consultants receive a device or IT account from the Commission for work purposes, they should be the sole users of that device/IT account. Consultants should protect it at any time and notify immediately to the local security officer (LSO) of any breach of security of a device or IT account.
  - Consultants must never copy illegally, carry, transmit nor destroy data, documentation, software or application programs, nor any material (even when obsolete). They must never access, nor even try to access data, locations or systems to which they have not been granted access or which they do not need to access for the implementation of their tasks.
Conduct at work

- When on the EU Institution’s premises, consultants must not perform any professional tasks that are not linked to the framework contract.
- Consultants may not make use of the EU Institution premises for marketing or recruitment purposes.
- Consultants must be aware that, where applicable, the EU Institution reserves the right to check the accuracy of any declarations about presence at the workplace, and to undertake corrective actions whenever necessary.
- Consultants are strongly expected to show EMAS awareness in their daily behaviour at the workplace. This includes, for instance, printing on both sides of the paper, switching off the lights and other equipment, using appropriate bins for waste recycling, etc.

Intellectual property rights

- Consultants declare to have been informed, by the contractor, of the Framework Contract, especially Articles I.13 and II.23 thereof concerning intellectual property rights and exploitation of the results, and acknowledge that the Union acquires ownership of the results as defined in the Framework Contract. As a consequence, consultants acknowledge that the European Union acquires ownership of the results as defined in the Framework Contract, including all intellectual property rights, such as copyright on software developments made by them, for all territories worldwide and for the whole duration of the intellectual property rights concerned, at no additional price to the European Union and with no additional compensation for the consultants than their salary or fees received from the contractor.
- If consultants want to use open source software for their assignments, they must first provide all relevant information (e.g. on licences) both to the EU Institution and the contractor, as well as seek the prior authorisation of the contractor.
- As creators, consultants also confirm that they do not object to the following:
  
  (a) that their name be mentioned or not mentioned when the results are presented to the public;
  
  (b) that the results be divulged or not after they have been delivered in their final version to the contracting authority;
  
  (c) that the results be adapted provided that this is done in a manner that is not prejudicial to their honour or reputation.

Declaration of intent by contractor’s personnel without employment contract (Framework Contract Art. I.22.2.d – only applicable to this case)

- Consultants pertaining to this category declare that they agree to participate with the contractor in the request for services of the latter’s contracts issued by the EU Institution.
They further declare that they are able and willing to work within the overall execution period defined by the EU Institution, as foreseen in the technical annex attached to the request for the position for which their CV has been submitted.

– Consultants pertaining to this category confirm that they do not have a confirmed engagement\(^4\) as expert in another EU-funded project, or any other professional activity incompatible in terms of capacity and timing with the above engagements and that they shall avoid such conflicting assignments. Should any such conflict seem probable, they shall notify without delay the respective contractor. They will not charge the same working day to more than one project.

– Consultants pertaining to this category declare that they are aware of their obligations deriving from the legislation in force of the country(ies) in which they will provide their services under the present contract. These obligations may include, amongst others, any obligation to be registered for VAT purposes and or in an enterprise database (e.g. Banque-Carrefour des Entreprises in Belgium). They are aware that, upon request of the contractor or the EU Institution, they should be able to submit, at any time, evidence of their compliance with their aforementioned obligations.

– Consultants pertaining to this category declare that they will comply with all the rights and obligations included in the contractual provisions governing the implementation of the contract under which their CV is proposed.

– Consultants pertaining to this category also declare that in case their CV is accepted under this request for services, they have signed or will sign a resulting contract with the contractor in their capacity as:

- [an individual (self-employed natural person)];

- a representative of a company (legal person) having at the date of signature of the present declaration:
  - only one owner/administrator who is also the only active person (employee or not) providing IT services in that company;
  - several company owners or administrators, but in which only one person (employee or not) is active in providing IT services;
  - one or several company owners or administrators, in which maximum two persons (employees or not) with family ties are active in providing IT services\(^5\).

– Consultants pertaining to this category commit to provide, should they be requested by the EU, any document (including one issued by an independent third-party, like Office for Social Security, National Revenue Service, etc.) evidencing the above capacity.

\(^4\) The engagement of an expert is confirmed where such expert is committed to work as an expert under a signed contract financed by the EU general budget or the EDF or where he/she is an expert in a tender which has received a notification of award. The date of confirmation of the engagement in the latter case is that of the notification of award to the consultant.

\(^5\) Delete as appropriate.
Termination of service provision

The consultants are aware that the employer and/or the Commission reserve their legal right to terminate or request the termination of the consultants’ service provision and to pursue any person who does not respect the above-mentioned obligations and requirements.

<table>
<thead>
<tr>
<th>Consultant’s name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consultant’s own company:</td>
</tr>
<tr>
<td>name, legal address and</td>
</tr>
<tr>
<td>VAT no.</td>
</tr>
<tr>
<td>[To be filled only by</td>
</tr>
<tr>
<td>consultants without</td>
</tr>
<tr>
<td>employment contract</td>
</tr>
<tr>
<td>with the contractor]</td>
</tr>
<tr>
<td>Consultant’s signature</td>
</tr>
<tr>
<td>Place, date</td>
</tr>
</tbody>
</table>
Overview technical and organisational security measures within Proximus

1. Proximus Security organization

The Security Governance and Investigation department, under Group Corporate Affairs is entitled with the organization’s Security Governance, Security Management and Cyber Security Monitoring and Response responsibilities.

Security Governance is responsible for the Information Security Framework of Proximus, which includes the definition and management of the Information Security Policies, as well as of the Security Architecture.

Security Management is responsible to evaluate the alignment of the different company projects with the security policies, to execute information security risk assessments on projects, to execute vulnerability management and pentest management activities and to measure and report compliance to information security policies.

Under Cyber Security Intelligence & Incident Response there are two teams:

- Cyber Defense Center - The Cyber Defense Center is the central monitoring team for cyber security incidents on Proximus Group infrastructure and services. With a 24x7 capability using the global Network Operations Center, the Cyber Defense Center aims to detect and contain attacks and intrusions on the shortest possible timeframe.
- Proximus CSIRT - The Proximus CSIRT provides information and assistance to reduce the risks of cyber security incidents as well as responding effectively to such incidents when they occur. They strive to be an international example for Cyber Security Intelligence and Expertise throughout all areas of Incident Response. The Proximus CSIRT gathers, filters, analyses and disseminates threat intelligence in order to
proactively communicate about upcoming attacks against the Proximus Group.

For each of Proximus core divisions a liaison Security Officer has been appointed to directly coordinate within Security Governance and Investigation, ensuring their division compliance with established Security Framework

2. **Proximus Security policy framework**

Proximus maintains a Proximus Security Policy Framework which contains comprehensive controls and coverage of current and emerging information security topics that enable the organisation to respond to the rapid pace at which threats, technology and risks evolve. Throughout the established Security Policy Framework, Proximus ensures that information risks associated with its services are kept within acceptable levels, responding to rapidly evolving threats, including sophisticated cyber security attacks and complying with applicable regulations at all times.

Proximus Security Policy Framework is adhering to the best practices of ISF Standard of Good Practice for Information Security providing complete coverage of the topics set out in ISO/IEC 27002:2013, COBIT 5 for Information Security, NIST Cybersecurity Framework, CIS Top 20 Critical Security Controls for Effective Cyber Defence and Payment Card Industry Data Security Standard (PCI DSS), acting as an enabler for continuously improving information security within the organization and helping the organisation to prepare for and manage major incidents that may have a significant impact on Proximus business.

Proximus Security Policy Framework is consistent with the structure and flow of the ISO/IEC 27000 ‘suite’ of standards, and acting as an enabler to multiple ISO 27001 certification programs within the Organization, via the implementation of an Information Security Management Systems (ISMS).

Proximus Security Policy Framework indicatively addresses topics in the areas of:


3. **Proximus Security Risk management**

The Security Risk Assessment process is a core element in safeguarding security and data privacy at Proximus.
The SRA process guarantees for all projects and systems the implementation of Proximus security controls and an approval by security experts before bringing in service.

The Proximus Risk Assessment Methodology is aligned with the IRAM2 methodology from ISF. IRAM2 is the standard corporate methodology to be used across all Proximus wide Information Security Projects and Proximus applied Information Security Management Systems based on ISO27001. IRAM2 is aligned with the ISF Standard of Good Practice for Information Security.

4. Human resource

The objective of Human Resource security controls are to:

- To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.
- To ensure that employees and contractors are aware of and fulfil their information security responsibilities.
- To protect the organization’s interests as part of the process of changing or terminating employment.

5. Asset Management

Proximus asset management and data classification is in place to ensure traceability and auditability.

The objective of Asset Management security controls are to:

- To identify organizational assets and define appropriate protection responsibilities.
- To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.
- To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

6. Access control

Proximus has established methods of restricting access to business applications, systems, computing devices and networks by requiring users to be authorized before being granted access privileges, authenticated using access control mechanisms and subject to a rigorous sign-on process before being provided with access.
Proximus has dedicated Identity and Access Management platforms for its customers, partners and employees to ensure segregation of duties and also a specific infrastructure for privileged access management.

The objective of Access control security controls are to:

- To limit access to information and information processing facilities.
- To ensure authorized user access and to prevent unauthorized access to systems and services.
- To make users accountable for safeguarding their authentication information.

To prevent unauthorized access to systems and applications.

7. **Cryptography**

Encryption brings an even higher level of security and privacy to our services.

As the data you create moves between your device, Proximus services, and our datacenters, it is protected by security technology like HTTPS and Transport Layer Security.

Proximus encrypts highly confidential and sensitive personal data whenever it is necessary.

Proximus security policies also include the use of pseudonymization (replacing personally identifiable material with artificial identifiers) and encryption (encoding messages so only those authorized can read them).

The objective of cryptographic controls are to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

8. **Physical and environmental security**

The objective of Physical and environmental security controls are to:

- To prevent unauthorized physical access, damage and interference to the organization’s information and information processing facilities.
- To prevent loss, damage, theft or compromise of assets and interruption to the organization’s operations.
9. Operations security

The objective of Operations security controls are to:

To ensure correct and secure operations of information processing facilities.

- To ensure that information and information processing facilities are protected against malware.
- To protect against loss of data.
- To record events and generate evidence.
- To ensure the integrity of operational systems.
- To prevent exploitation of technical vulnerabilities.
- To minimise the impact of audit activities on operational systems.

Specifically, to the exploitation of technical vulnerabilities, Proximus has established a Vulnerability Management process to complete the security cycle involving the projects lifecycle (preventive controls) and the incident response management (detective controls) using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration testing, quality assurance processes, software security reviews, and external audits.

Proximus Vulnerability Management process identifies and classifies vulnerabilities, and coordinates remediation and mitigation actions for vulnerabilities which can be caused by

1. design mistakes,
2. coding mistakes or malicious code, or
3. configuration mistakes

and affect elements from

- a) operating systems components or network components
- b) middle components (interpreters, JRE,...) or
- c) daemons, applications, firmwares,...

When vulnerabilities are identified, a corrective path is triggered, involving changes in network, installation of security patches, correction of misconfigurations, correction of applications code or design. This lets Proximus detect and respond to threats to protect products from spam, malware, viruses, and other forms of malicious code.
10. **Communications security**

The objective of Communications security controls are to:

- To ensure the protection of information in networks and its supporting information processing facilities.
- To maintain the security of information transferred within an organization and with any external entity.

11. **System development and maintenance**

Proximus design with security in mind. Our security and privacy experts work with development teams, reviewing code and ensuring products utilize strong security protections.

The objective of System development and maintenance controls are to:

- To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.
- To ensure that information security is designed and implemented within the development lifecycle of information systems.
- To ensure the protection of data used for testing.

12. **Supplier relationships**

The objective of Supplier relationships controls are to:

- To ensure protection of the organization’s assets that is accessible by suppliers.
- To maintain an agreed level of information security and service delivery in line with supplier agreements.

In detail, Proximus limits access to your business’s data to Proximus personnel who need it to do their jobs; for example, when a customer service agent assists you in managing your data.

Strong access controls are enforced by organizational and technical safeguards. And when we work with third parties, like customer support vendors, to provide Proximus services, we have them signed a security schedule document which highlights Proximus security requirements and we audit them randomly to ensure they provide the appropriate level of security and privacy needed to receive access to your business’s data.
13. **Information security incident management**

The objective of Information security incident management controls are to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Security Monitoring and Response is one of the core services provided by Proximus Cyber Defense Center and the CSIRT team.

The Security Monitoring and Response Process has been established within Proximus to achieve the following key objectives:

- Provide guidance during decision-making associated with security incidents.
- Provide a process framework for effective 24x7 security monitoring (Level 1) and on-call response service (Level 2 and above) within Proximus, focused on initial detection, analysis and response.
- Provide guidance regarding prioritization and escalation of security incidents.
- Ensuring the Proximus and its customers have the following benefits:
  - Improved overall incident resolution through consistent and timely handling of the security incidents monitoring, analysis, identification and escalation.
  - Improved service through defined work interfaces with all teams involved in handling incidents.
  - Improved and consistent reporting to facilitate continuous improvement of security at Proximus.

Proximus in compliance with international security standards and requirements, has a security logging policy defining all relevant data to be sent to Proximus SIEM platform to perform accurate monitoring of security events.

14. **Compliance**

The objective of Compliance controls are to:

To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

- To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.
Annex XII to FwC DI-07910

List of sub-processors (Lot 1)

1. Service desk
   - 
   - 
   
2. Billing
   - 
   - 
   -
Annex XIII.1

SECURITY BASELINE FOR EXTERNAL CONNECTIONS – REMOTE SERVICE DELIVERY

APPENDIX 1 - RULES FOR CONTRACTORS
APPENDIX 1 - RULES FOR CONTRACTORS

This section details all of the controls that are required for the security baseline. Each control includes its NIST ID and the title of the control area, and the specific security measures that are required by the Commission for this scenario. Contractors are advised to refer to the full NIST documentation for further information about the controls.

The technical controls in this appendix apply to the relevant network equipment owned by the contractor from where the connection to Commission systems is established, including any supporting systems, except where specified otherwise.

If the service providers do not work from contractor premises, the rules for working from a home office must be applied (see appendix 2).

The NIST Special Publication distinguishes the following security and privacy control families:

<table>
<thead>
<tr>
<th>ID</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>Access Control</td>
</tr>
<tr>
<td>AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td>AU</td>
<td>Audit and Accountability</td>
</tr>
<tr>
<td>CA</td>
<td>Security Assessment and Authorisation</td>
</tr>
<tr>
<td>CM</td>
<td>Configuration Management</td>
</tr>
<tr>
<td>CP</td>
<td>Contingency Planning</td>
</tr>
<tr>
<td>IA</td>
<td>Identification and Authentication</td>
</tr>
<tr>
<td>IR</td>
<td>Incident Response</td>
</tr>
<tr>
<td>MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td>MP</td>
<td>Media Protection</td>
</tr>
<tr>
<td>PE</td>
<td>Physical and Environmental Protection</td>
</tr>
<tr>
<td>PL</td>
<td>Planning</td>
</tr>
<tr>
<td>PM</td>
<td>Program Management</td>
</tr>
<tr>
<td>PS</td>
<td>Personnel Security</td>
</tr>
<tr>
<td>PT</td>
<td>Personally Identifiable Information Processing and Transparency</td>
</tr>
<tr>
<td>RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>SA</td>
<td>System and Services Acquisition</td>
</tr>
<tr>
<td>SC</td>
<td>System and Communications Protection</td>
</tr>
<tr>
<td>SI</td>
<td>System and Information Integrity</td>
</tr>
<tr>
<td>SR</td>
<td>Supply Chain Risk Management</td>
</tr>
</tbody>
</table>
I.1. GENERAL RULES

(1) The contractor must cooperate with the Commission or any third party appointed by the Commission for the verification of compliance with these rules. The verification process may include on-site inspections in the contractor's premises.

(2) The contractor must have security policies covering all of the control families shown above.

(3) The contractor must nominate a single point of contact for security issues relating to the contract and to liaise with the Commission’s security teams.

(4) The specific controls listed in this appendix must be implemented, and their implementation must be documented. Any exceptions must be documented and reported during any verification of compliance.

(5) Where a service delivery security plan is required in the contract, this baseline must be used as additional input for the security requirements.

(6) Contractors and their staff must be aware of the EC’s security rules relating to their activities, the level of confidentiality of the information that they handle, and any relevant handling instructions (notably for sensitive non-classified information).

(7) Contractors must ensure that all service providers sign the applicable Acceptable Use Policy for the Commission IT equipment and follow any specific policies or rules for acceptable use relating to the CISs used.

(8) Commission information must not be stored or processed on any non-Commission devices or services without written authorisation from the Commission. Any such use is out of scope of this baseline and may be subject to different rules.

(9) The use of any online tools that are not authorised for use by the EC, such as instant messaging services or file storage/exchange platforms, is forbidden for handling, discussing or exchanging Commission information.

(10) Commission equipment and services must only be used for the fulfilment of services contracted for the Commission. All Commission equipment and information must be returned upon completion of the contracted services.

(11) In line with the standard contractual obligations, any non-disclosure or secrecy obligations continue to be binding after the completion of the contracted services.

I.2. ACCESS CONTROL

<table>
<thead>
<tr>
<th>AC-2</th>
<th>Account Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>All user accounts must be assigned to identified individuals. Shared accounts are not permitted.</td>
</tr>
</tbody>
</table>

For relevant network equipment owned by the contractor:

(2) Maintain an inventory of each of the organization's authentication systems, including those located on-site or at a remote service provider.

(3) Configure access for all accounts through as few centralised points of authentication as possible, including network, security, and cloud systems.

(4) Encrypt or hash with a salt all authentication credentials when stored.
(5) Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

(6) Maintain an inventory of all accounts organized by the authentication system.

(7) Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.

(8) Disable any account that cannot be associated with a business process or business owner.

(9) Automatically disable dormant accounts after a set period of inactivity.

(10) Ensure that all accounts have an expiration date that is monitored and enforced.

(11) Monitor attempts to access deactivated accounts through audit logging.

For equipment/environment/CIS owned by the EC, the contractor must:

(12). Apply the Commission’s procedures for requesting and reviewing access to Commission resources.

(13) Require approvals by EC account managers for requests to create accounts.

(14) Notify EC account managers when accounts are no longer required/users are terminated or transferred/system usage or need-to-know changes for an individual.

AC-5 \hspace{1cm} Separation of Duties
Contractors must respect any segregation that is imposed by the CISs accessed.

AC-17 \hspace{1cm} Remote Access

For remote access into the contractor’s network environment (not using EC laptops):

(1) Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed

(2) Authorise each type of remote access to the system prior to allowing such connections

(3) Route remote accesses through authorised and managed network access control points

(4) Require all remote login access to the organization's network to encrypt data in transit

(5) Use multi-factor authentication for remote access connections

(6) Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.

(7) Protect information about remote access mechanisms such as authentication methods from unauthorised use and disclosure.
AC-18  Wireless Access

For contractor sites:

(1) Maintain an inventory of authorised wireless access points connected to the wired network.
(2) Implement measures to detect and alert on unauthorised wireless access points.
(3) Disable wireless access on devices that do not have a business purpose for wireless access.
(4) Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.
(5) The Advanced Encryption Standard (AES) must be used to encrypt wireless data in transit.
(6) Ensure that wireless networks use secure authentication protocols based on the access scenario (i.e. which client is connecting and which network domains are accessed)
(7) Disable wireless peripheral access of devices [such as Bluetooth and Near Field Communication (NFC)], unless such access is required for a business purpose.
(8) Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted, and filtered and audited accordingly.

I.3. AWARENESS AND TRAINING

AT-2  Literacy Training and Awareness

(1) The contractor must provide and keep records of security awareness training to its personnel, covering fundamental security issues.
(2) Service providers must also follow any security-related training required by the Commission, including initial briefings on information security and acceptable use of EC CIS and information.

I.4. AUDIT AND ACCOUNTABILITY

AU-2  Event Logging

(1) Ensure that local logging has been enabled on all systems and networking devices.
(2) Log records must be made available to the Commission's security investigators in HR.DS in the event of a security incident.

AU-3  Content of Audit Records

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.
AU-4 Audit Log Storage Capacity
Ensure that all systems that store logs have adequate storage space for the logs generated.

AU-6 Audit Record Review, Analysis, and Reporting
(1) Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.
(2) Deploy log analytic tools for log correlation and analysis
(3) On a regular basis, review logs to identify anomalies or abnormal events.

AU-8 Time Stamps
Use at least two time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

AU-9 Protection of Audit Information
Protect audit information and audit logging tools from unauthorised access, modification, and deletion

AU-11 Audit Record Retention
Logs must be retained for at least six months.

I.5. SECURITY ASSESSMENT AND AUTHORISATION

CA-2 Control Assessments
The security measures defined in this baseline must be assessed by the contractor or an independent assessor at least every three years. The results of this assessment must be made available to the contracting authority upon request.

I.6. CONFIGURATION MANAGEMENT

CM-2 Baseline Configuration
A secure configuration must be established for all relevant network devices.

CM-3 Configuration Change Control
A formal change control process must be in place for all relevant network devices.
### CM-5  Access Restrictions for Change
Access to change configuration settings must be logged and restricted to qualified network administrators.

### CM-8  System Component Inventory
All relevant network devices for the Commission access services must be identified.

## I.7. IDENTIFICATION AND AUTHENTICATION

### IA-1  Policy and Procedures
See rule (1) in section 6.1.
Contractors must ensure the identity of their staff through suitable procedures.

### IA-2  Identification and Authentication (organizational Users)
1. Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorised individuals have elevated privileges.
2. Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.
3. Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account must only be used for administrative activities and not Internet browsing, email, or similar activities.
4. Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.
5. Use multi-factor authentication and encrypted channels for all administrative account access.

### IA-5  Authenticator Management
1. Credentials for access to the Commission must only be issued via a formal procedure including verification of the user's identity by the Commission.
2. Credentials for access to contractor network devices must be issued via a formal procedure including verification of the user's identity.
3. Strong passwords (including requirements for minimum length and complexity) or multi-factor authentication must be enforced on the contractor's network.
4. Users must change passwords on first use (including default passwords for generic accounts, e.g. root, admin...)
5. Passwords used to access the Commission's assets must be different from any other passwords of the user.
(6) Users must protect all authenticators (passwords, laptops with digital certificate, tokens...) from unauthorised access, particularly when outside office premises (e.g. while working in home offices or travelling)

(7) Encrypt or hash with a salt all authentication credentials when stored.

(8) Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

### I.8. INCIDENT RESPONSE

<table>
<thead>
<tr>
<th>IR-1</th>
<th>Policy and Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>The contractor must have a documented incident response procedure.</td>
</tr>
<tr>
<td>(2)</td>
<td>The contractor must appoint a single point of contact for communicating security incidents with the Commission.</td>
</tr>
<tr>
<td>(3)</td>
<td>The contractor must report any relevant security incidents to the Commission’s IT Helpdesk as soon as possible and cooperate with any security investigations.</td>
</tr>
<tr>
<td>(4)</td>
<td>The contractor must ensure that any relevant evidence is preserved and made available to the Commission’s security investigators in HR.DS.</td>
</tr>
</tbody>
</table>

### I.9. MAINTENANCE

<table>
<thead>
<tr>
<th>MA-3</th>
<th>Maintenance Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security updates must be applied in a timely manner to any relevant network equipment (OS and third party software)</td>
<td></td>
</tr>
</tbody>
</table>

### I.10. MEDIA PROTECTION

<table>
<thead>
<tr>
<th>MP-2</th>
<th>Media Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>The use of removable media for Commission information must be generally discouraged and restricted as much as possible. Where this is necessary, there must be specific rules over the handling and storage of the media, and the secure deletion of information when no longer needed. At a minimum:</td>
<td></td>
</tr>
<tr>
<td>(1) Media must not be used for both Commission information and non-Commission information.</td>
<td></td>
</tr>
<tr>
<td>(2) Malware protection on Commission IT equipment must not be disabled or changed.</td>
<td></td>
</tr>
<tr>
<td>(3) Any Commission information at the level of Commission Use or above must be encrypted.</td>
<td></td>
</tr>
<tr>
<td>(4) Media must be physically protected when stored or transported.</td>
<td></td>
</tr>
<tr>
<td>(5) Any non-public Commission information must be securely deleted from removable media when no longer needed, or at latest at the termination of the contract.</td>
<td></td>
</tr>
</tbody>
</table>
(6) Users shall not connect media from unknown or suspicious sources to Commission IT equipment (e.g. media that are found unattended or received from unknown people)

MP-7  Media Use

Media that are not provided by the contractor or the EC must not be used for Commission information.

I.11. PHYSICAL AND ENVIRONMENTAL PROTECTION

PE-1  Policy and Procedures

The physical security policy must cover (as relevant):
- Office spaces in contractor premises
- Home offices
- Data centres (for related network equipment)

Remote access to the EC environment is not permitted from any other locations.

PE-2  Physical Access Authorisations

Office spaces
(1) Office spaces must be designed to reduce physical risks such as eavesdropping, unauthorised observation of activities and loss or theft.
(2) Access must be restricted to authorised personnel (for visitor access see PE-7)
(3) There must be a formal process for granting access and revoking it when no longer justified
(4) Offices used for Commission work should be segregated from other offices, e.g. with access control or physical locks

Data centres
(5) As above, with access restricted only to relevant technical staff.

PE-3  Physical Access Control

Office spaces + Data centres
(1) All entrances and exits must be controlled (e.g. by access control systems or guards)
(2) Physical access control measures must be implemented as appropriate for both working and non-working hours
(3) Physical access logs must be retained for at least six months and made available to the Commission during security investigations.
### PE-4  Access Control for Transmission
Physical network components including cables should be protected from unauthorised access.

### PE-6  Monitoring Physical Access
1. Office spaces and data centres on contractor sites must be monitored with intrusion alarms.
2. Entrances to data centres must be under video surveillance.
3. All alarms must be investigated as soon as possible.

### PE-7  Visitor Control
Visitors to office spaces and data centres must be formally registered, with verification of their identity, and accompanied by an authorised user.

### PE-8  Visitor Access Records
Records of visitor access must be maintained for at least six months and made available to the Commission during security investigations.

### I.12. PLANNING

**PL-2  System Security and Privacy Plans**
The contractor must have up-to-date documentation covering:
1. the network architecture used for connecting to the EC's CISs
2. the provision of the contracted services.

### I.13. PROGRAM MANAGEMENT

**PM-1  Information Security Program Plan**
See rule (1) in section 6.
The contractor must have an information security management system in line with an appropriate security framework.

### I.14. PERSONNEL SECURITY

**PS-2  Position Risk Designation**
The contracting authority in the Commission must inform the contractor which roles are considered to be sensitive, and therefore what sort of screening is required. The options are:
i. Standard;
ii. Highly sensitive (tasks requiring a security clearance).

### PS-3 Personnel Screening

The contractor must provide the appropriate level of screening in line with the sensitivity of the tasks to be performed (see §4.1 above): The options are:

i. Standard: contractor should have formal recruitment processes to verify the service provider’s identity, education and work experience, including a criminal records check or equivalent (alternatively the EC can perform a background screening, where available - currently only in Belgium)

ii. Highly sensitive: additionally, the contractor must apply for a national security clearance for the service provider as soon as possible.

NB the Commission can only recognise security clearances for non-EU nationals of countries with which the EU has a Security of Information agreement or from a Member State that can clear non-EU nationals on their territory.

### PS-4 Personnel Termination

(1) The EC must be informed of the termination of a service provider’s contract to ensure that all user IDs are removed and any Commission assets are returned (laptop, hardware tokens, access badges etc.).

(2) The service provider may be asked for a handover process &/or an exit interview and must be reminded of the continuing obligation to respect the confidentiality of Commission information.

### PS-5 Personnel Transfer

When a service provider is transferred to a different role for the EC, the contractor must inform the EC to ensure that all access rights are modified accordingly. Transfer within the contractor to a non-EC role requires the same procedure as termination.

### PS-7 External Personnel Security

Any relevant security requirements from the Commission must be included in the contract between the contractor and external personnel.
### I.15. Personally Identifiable Information Processing and Transparency

<table>
<thead>
<tr>
<th>PT-1</th>
<th>Policy and Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If there are any GDPR-related requirements in the contract, these must be covered by the policy and any required security measures (e.g. if the contractor is acting as a data processor).</td>
</tr>
</tbody>
</table>

### I.16. Risk Assessment

<table>
<thead>
<tr>
<th>RA-1</th>
<th>Policy and Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For equipment/environment/CIS owned by the contractor:</td>
</tr>
<tr>
<td></td>
<td>The contractor must have an ISMS in line with an appropriate security framework, including risk assessment in line with the requirements in the Call for Tender.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RA-5</th>
<th>Vulnerability Monitoring and Scanning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Vulnerability scanning must be performed regularly on the network equipment used for connecting to the Commission's infrastructure and a process must be in place to remediate any vulnerabilities identified.</td>
</tr>
</tbody>
</table>

### I.17. System and Services Acquisition

<table>
<thead>
<tr>
<th>SA-4</th>
<th>Acquisition Process</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Relevant network devices must be procured through a formal process that includes security requirements</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SA-5</th>
<th>System Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Relevant network devices must be documented, including security requirements and configuration.</td>
</tr>
</tbody>
</table>

### I.18. System and Communications Protection

<table>
<thead>
<tr>
<th>SC-7</th>
<th>Boundary Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(1) Perform regular scans from outside each trusted network boundary to detect any unauthorised connections which are accessible across the boundary.</td>
</tr>
</tbody>
</table>
|      | (2) Deny communications by default, particularly incoming connections and known malicious or unused Internet IP addresses, and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries.
(3) Deny communication over unauthorised TCP or UDP ports or application traffic to ensure that only authorised protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.

(4) Deny communications to/from unauthorised devices on the internal network.

(5) Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.

(6) Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.

(7) Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.

(8) Follow the control practices for external telecommunications services (see SC-7(4)).

(9) Boundary protection devices must fail closed / secure.

(10) Route traffic through authenticated proxy servers where possible.

(11) Secure network devices against unauthorised physical connections.

(12) Locate EC devices in a separate subnet / VLAN with restrictions on communications to/from the internal network.

---

**SC-28 Protection of Information at Rest**

EC information may only be handled on the provided EC equipment.

**SC-35 External Malicious Code Identification**

The contractor must have anti-malware protection at multiple levels (network, host…)

**SC-43 Usage Restrictions**

(1) Usage restrictions must be applied by the contractor in line with EC requirements. The contractor must ensure that all service providers sign and return the acceptable use policy provided by the Commission for the equipment provided.

(2) Only personnel employed on EC contracts may use EC equipment.

**SC-45 System Time Synchronization**

Contractor network equipment must be synchronised to a recognised external time source (and at least one other independent source for verification).
### 1.19. **SYSTEM AND INFORMATION INTEGRITY**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SC-46</strong></td>
<td><strong>Cross Domain Policy Enforcement</strong></td>
</tr>
<tr>
<td></td>
<td>The VLAN in which the EC laptops reside must be restricted to communicating only with the EC, and protected from incoming communications from any other internal or external sources.</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SI-2</strong></td>
<td><strong>Flaw Remediation</strong></td>
</tr>
<tr>
<td></td>
<td>A process must be in place for the timely identification and remediation of security vulnerabilities on relevant network devices.</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SI-3</strong></td>
<td><strong>Malicious Code Protection</strong></td>
</tr>
<tr>
<td></td>
<td>(1) The network environment must be protected from malware, including protection at the network perimeter.</td>
</tr>
<tr>
<td></td>
<td>(2) Anti-malware software must be centrally managed and regularly updated.</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SI-4</strong></td>
<td><strong>System Monitoring</strong></td>
</tr>
<tr>
<td></td>
<td>(1) The contractor must have intrusion detection and prevention on the network used for connections to the Commission, with central management and alerting.</td>
</tr>
<tr>
<td></td>
<td>(2) The service must be regularly updated.</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SI-5</strong></td>
<td><strong>Security Alerts, Advisories, and Directives</strong></td>
</tr>
<tr>
<td></td>
<td>The contractor must monitor relevant security alerts for their environment.</td>
</tr>
</tbody>
</table>
Annex XIII.2

SECURITY BASELINE FOR EXTERNAL CONNECTIONS – REMOTE
SERVICE DELIVERY

APPENDIX 2 - RULES FOR SERVICE PROVIDERS WORKING FROM
HOME
APPENDIX 2: RULES FOR SERVICE PROVIDERS WORKING FROM HOME

This subset of the rules is applicable for service providers connecting from home offices. The home office for a service provider must be located in an EU Member State and may be his/her own home or a similar location such as the residence of a relative or partner where the relevant security measures can be applied.

I.1. GENERAL RULES

(1) The specific controls listed in this appendix must be implemented. Any exceptions must be documented by the contractor and accepted by the EC as the contracting authority.

(2) Where a service delivery security plan is required in the contract, this baseline must be used as additional input for the security requirements.

(3) Service providers must be aware of the EC’s security rules relating to their activities, the level of confidentiality of the information that they handle, and any relevant handling instructions (notably for sensitive non-classified information).

(4) Service providers must sign the applicable Acceptable Use Policy for the Commission IT equipment and follow any specific policies or rules for acceptable use relating to the CISs used.

(5) Commission information must not be stored or processed on any non-Commission devices or services without written authorisation from the Commission. Any such use is out of scope of this baseline and may be subject to different rules.

(6) The use of any online tools that are not authorised for use by the EC, such as instant messaging services or file storage/exchange platforms, is forbidden for handling, discussing or exchanging Commission information.

(7) Commission equipment and services must only be used for the fulfilment of services contracted for the Commission. All Commission equipment and information must be returned upon completion of the contracted services.

(8) In line with the standard contractual obligations, any non-disclosure or secrecy obligations continue to be binding after the completion of the contracted services.

I.2. ACCESS CONTROL

<table>
<thead>
<tr>
<th>AC-2</th>
<th>Account Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>All user accounts must be assigned to identified individuals. Shared accounts are not permitted.</td>
</tr>
<tr>
<td>(2)</td>
<td>Apply the Commission’s procedures for requesting and reviewing access to Commission resources.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AC-5</th>
<th>Separation of Duties</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Service providers must respect any segregation that is imposed by the CISs accessed.</td>
</tr>
</tbody>
</table>
**AC-18 Wireless Access**

1. Users must be aware of the security of the digital environment used for remote access and take appropriate steps to reduce risks, including unauthorised access and malware infection.
2. Network devices that are used to access the Commission’s resources must be protected by secure access control mechanisms.
3. Default passwords on network devices must be changed.
4. Users must not share the personal Wi-Fi Access Point with any unknown third parties.

### I.3. AWARENESS AND TRAINING

**AT-2 Literacy Training and Awareness**

Service providers must follow any security-related training required by the Commission, including initial briefings on information security and acceptable use of EC CIS and information.

### I.4. IDENTIFICATION AND AUTHENTICATION

**IA-1 Policy and Procedures**

Contractors must ensure the identity of their staff through suitable procedures.

**IA-5 Authenticator Management**

1. Credentials for access to the Commission must only be issued via an agreed procedure including verification of the user’s identity by the Commission.
2. Users must change passwords on first use (including default passwords for generic accounts, e.g. root, admin...).
3. Passwords used to access the Commission's assets must be different from any other passwords of the user.
4. Users must protect all authenticators (passwords, laptops with digital certificate, tokens...) from unauthorised access, particularly when outside office premises (e.g. while working in home offices or travelling).

### I.5. INCIDENT RESPONSE

**IR-1 Policy and Procedures**

1. The service provider must report any relevant security incidents to the Commission’s IT Helpdesk as soon as possible and cooperate with any security investigations.
2. The service provider must preserve any logs or other evidence of security incidents on Commission equipment.
1.6. MEDIA PROTECTION

MP-2 Media Access

The use of removable media for Commission information is generally discouraged and restricted as much as possible. Where this is necessary, there must be specific rules over the handling and storage of the media, and the secure deletion of information when no longer needed.

At a minimum:

(1) Media must not be used for both Commission information and non-Commission information.

(2) Malware protection on Commission IT equipment must not be disabled or changed.

(3) Any Commission information at the level of Commission Use or above must be encrypted.

(4) Media must be physically protected when stored or transported.

(5) Any non-public Commission information must be securely deleted from removable media when no longer needed, or at latest at the termination of the contract.

(6) Users shall not connect media from unknown or suspicious sources to Commission IT equipment (e.g. media that are found unattended or received from unknown people)

MP-7 Media Use

Media that are not provided by the contractor or the EC must not be used for Commission information.

1.7. PHYSICAL AND ENVIRONMENTAL PROTECTION

PE-2 Physical Access Authorisations

(1) Users must be aware of the physical security of the environment where they are using remote access and take appropriate steps to reduce risks such as eavesdropping, unauthorised observation of their activities, and loss or theft of their equipment or credentials.

(2) Users must not store sensitive non-classified (SNC) information on non-Commission devices. Paperless working is recommended; printed documents containing SNC must be locked away when not in use.

(3) Users must not allow unauthorised people to use the device used for the Commission’s remote access services, including friends and family members.

(4) Users must be attentive to signs of unauthorised use of endpoint devices. They must promptly report any suspected security breaches such as unrecognised access attempts via the appropriate channels.
## I.8. PERSONNEL SECURITY

<table>
<thead>
<tr>
<th>PS-3</th>
<th>Personnel Screening</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The service provider must agree to the appropriate level of screening.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PS-4</th>
<th>Personnel Termination</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(1) The EC must be informed of the termination of a service provider’s contract to ensure that all user IDs are removed and any Commission assets are returned (laptop, hardware tokens, access badges etc.).</td>
</tr>
<tr>
<td></td>
<td>(2) The service provider may be asked for a handover process &amp;/or an exit interview and must be reminded of the continuing obligation to respect the confidentiality of Commission information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PS-7</th>
<th>External Personnel Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Any relevant security requirements from the Commission must be included in the contract between the contractor and external personnel.</td>
</tr>
</tbody>
</table>

## I.9. SYSTEM AND COMMUNICATIONS PROTECTION

<table>
<thead>
<tr>
<th>SC-28</th>
<th>Protection of Information at Rest</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EC information may only be handled on the provided EC equipment.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SC-43</th>
<th>Usage Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(1) Usage restrictions must be followed by the service provider in line with EC requirements. The service provider must sign the acceptable use policy provided by the Commission for the equipment provided and return it via the contractor.</td>
</tr>
<tr>
<td></td>
<td>(2) Only personnel employed on EC contracts may use EC equipment.</td>
</tr>
</tbody>
</table>
Annex XIII.3

SECURITY BASELINE FOR EXTERNAL CONNECTIONS – REMOTE SERVICE DELIVERY

APPENDIX 3 - ACCEPTABLE USE POLICY
APPENDIX 3: ACCEPTABLE USE POLICY

All service providers must sign and return the acceptable use policy (AUP) shown below. The signed AUPs must be collected by the contractor and submitted to the contracting authority at the start of the contract.

Acceptable Use of European Commission Information and IT Resources

All service providers in the PXE (Provider-eXternal-IT Equipment) category must sign this document to indicate their agreement and return it to the relevant contracting authority in the Commission.

General Principles

1. The Commission provides information communication and technology (ICT) services for Commission business. The use of Commission IT resources for personal use or other business purposes is forbidden.
2. Service providers must be aware of the level of confidentiality of the information that they handle. Non-public Commission information must not be stored or processed on any non-Commission devices or services without written authorisation from the Commission.
3. Commission information that is not publicly available may not be shared with any personnel without a need-to-know to fulfil their contracted tasks for the Commission.
4. Paperless working is recommended where possible and particularly while teleworking from home. Printed documents containing sensitive information must be locked away when not in use.
5. Authentication mechanisms must be protected from use by unauthorised persons at all times. User IDs and authentication credentials are individual and must not be shared.
6. Service providers must use different passwords for accessing Commission CISs from any other passwords.
7. Service providers remain fully responsible for the supplied equipment and for the actions taken in their name. Service providers must inform the Commission immediately via the IT Helpdesk of any suspected or confirmed security incident or weakness. They must not test or exploit any security weaknesses, or seek to circumvent the security measures put in place by the Commission.

End user devices (workstations, laptops or other personal computing devices)

8. All Commission devices must be protected from access or theft by unauthorised persons at all times including during transport. In shared offices or homes, working in common areas is discouraged and Commission equipment must not be left unlocked or unattended.
9. Software from non-Commission sources must not be installed or used on Commission IT equipment. Service providers must not change the security configuration of the operating system and any other installed software.
10. Commission devices may only connect to authorised networks for the purpose of connecting to the Commission’s remote access services. Authorised networks include:
    • the Commission’s internal network or guest wi-fi when on Commission premises;
• the contractor’s internal network;
• the service provider’s home network while teleworking;
• any authorised network service contracted by the Commission.

11. Service providers must not use any unauthorised online services for Commission purposes in the event that the Commission’s teleworking solutions are unavailable.
12. Security measures installed on end user devices, including anti-malware software and firewalls, must not be disabled or their configuration changed.
13. Service providers must not allow unauthorised people to use the Commission’s equipment or services, including friends and family members.

Commission communication and information systems (CISs)

14. The Commission’s CISs must only be used for the provision of the services described in the contract and in line with the Commission’s IT security policy and any rules or guidelines on acceptable use issued by the system owner.
15. Service providers must not access CISs for which they have not been explicitly granted authorisation.
16. Privileged access rights such as system administration must be used with extreme care. Service providers with administrative privileges must use a dedicated account for administrative tasks, and administrative accounts must not be used for any other activities.
17. Service provider must be vigilant of attacks such as phishing or scams.
18. Service providers must always encrypt sensitive non-classified emails with SECEM2.

Use of removable media and online services

19. The use of removable media for Commission information is strongly discouraged. All files must be securely deleted as soon as they are no longer needed.
20. Users shall not connect media from unknown or suspicious sources to Commission IT equipment.
21. Removable media containing Commission information must be protected against unauthorised disclosure, loss and theft. Security incidents involving removable media containing Commission information must be reported to the Commission via the IT Helpdesk.
22. Separate removable media must be used for Commission information and for other purposes.
23. Sensitive non-classified information must be encrypted on removable media.
24. Online services that are not provided or authorised by the Commission must not be used for communicating (videoconferencing / teleconferencing), storing or transferring Commission information.

Teleworking

25. Teleworking must only be performed from the service provider’s home office which must be located in an EU Member State and may be his/her own home or a similar location such as the residence of a relative or partner where the relevant security measures can be applied. Teleworking is not permitted from public spaces such as hotels, restaurants, airports, train stations or social clubs.
26. When using home networks for teleworking, the following measures must be in place:
   • Home networks must not be shared with unknown persons;
   • Wireless networks must be encrypted and protected with a strong password;
Passwords used to access home networks, such as for wireless networks, must be changed from the default passwords;
Commission devices must not be connected to other home computing devices;
Commission devices must not be used to connect to the Internet except through the Commission’s authorised networks.

Logging and monitoring

27. The service provider must accept that the supplied equipment will be subject to regular checks by the Commission; these may take the form of physical verification, user surveys and log consultation.

28. The service provider consents to the Commission logging and monitoring activities on its end user devices and CISs for security purposes. All such logs will be handled in accordance with the relevant privacy statements.

Termination

29. At the end of the contracted services, all Commission IT resources including end user devices, physical authentication mechanisms and information must be returned to the Commission.

30. All non-disclosure or secrecy obligations continue to be binding after the completion of the contracted services.

Confirmation

I hereby confirm that I have read, understood and will abide by the rules in this acceptable use policy.

<table>
<thead>
<tr>
<th>Contractor company:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Service provider</td>
<td></td>
</tr>
<tr>
<td>(last name, first name):</td>
<td></td>
</tr>
<tr>
<td>Signature:</td>
<td></td>
</tr>
<tr>
<td>Date:</td>
<td></td>
</tr>
</tbody>
</table>