

**TAS France Enterprise License Agreement (ELA) – Master Agreement**

**Contents**

- 1 Parties ..... 2
- 2 Preamble..... 2
- 3 Definitions ..... 3
- 4 Purpose of this Agreement ..... 4
- 5 License ..... 4
- 6 ELA Maintenance/Support..... 5
- 7 Duration..... 5
- 8 Communication ..... 5
- 9 Intellectual Property Rights (« IPR »)..... 6
  - 9.1. Ownership of IPR on the ELA Software..... 6
  - 9.2. Ownership of the Customer's data..... 6
  - 9.3. Specific Contract for development of new software ..... 6
  - 9.4. Indemnification ..... 7
- 10 Compliance..... 7
  - 10.1. Supplier’s compliance ..... 7
  - 10.2. Customer’s compliance ..... 8
- 11 Processing of personal data ..... 8
  - 11.1. Processing of personal data by the Customer..... 8
  - 11.2. Processing of personal data by the Supplier..... 8
- 12 Warranty..... 12
- 13 Specific provisions for Software as a Service (“SaaS”)..... 12
- 14 Assignment..... 13
- 15 Subcontracting..... 13
- 16 Security..... 14
  - 16.1. Commission decisions ..... 14
  - 16.2. Software as a Service (SaaS)..... 15
- 17 Confidentiality..... 15
- 18 Termination ..... 16
- 19 Institutional aspect..... 16
- 20 Applicable law..... 16

21 Order of precedence ..... 17

22 Entire agreement – Implementation caveat ..... 17

23 List of Annexes ..... 17

**1 PARTIES**

The parties to this Agreement are, on the one hand:

**TAS France SASU**

*Statutory registration number*  
382525541

*Address*  
15 traverse des BRUCS, 06560 VALBONNE – SOPHIA ANTIPOLIS, FRANCE

*VAT Registration number*  
FR93 382 525 541

represented for the purposes of signing this agreement by Francesco DE SIMONI, Directeur Général.

As the "**Supplier**"

And on the other hand,

**The European Union**, represented by the European Data Protection Supervisor (“**EDPS**”) as the lead contracting authority and European Union institutions, agencies or other bodies (the “**EUIs**”), all listed in Annex I;

represented for the purposes of signing this agreement by Leonardo CERVERA NAVAS, Director.

As the "**Customer**", as further specified in Article 3

Together referred to as the “**Parties**”.

**2 PREAMBLE**

TAS Group is specialised in software solutions for electronic money, payment systems, capital markets and extended enterprise.

Its subsidiary TAS France SASU offers hosting and Cloud Computing services to all types of companies wishing to outsource all or part of their information system.

The present and its Annexes (“**Agreement**”) are the result of the negotiation with reference "2022-0561 - EDPS - TAS France SASU - FWC DI 07722 SIDE II - Purchase of an off-premise solution" initiated

in October 2021.

The subject matter of the Agreement is to set the conditions under which the Customer may order licences on a variety of ELA Software, as well as ELA Maintenance/Support and Professional Services, as set out in the Annexes.

The Agreement does not confer on the Supplier any exclusive right to supply the products and to provide the services referred to in the above paragraph. The Customer takes no commitment to purchase any software products or services, and no direct purchases with the Supplier can be made through this Agreement. Instead, purchases and implementation of the Agreement may only be done through a Reseller.

### 3 DEFINITIONS

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

<b>Term</b>	<b>Definition</b>
ELA	This Enterprise License Agreement.
ELA Maintenance/Support	Any modification of the ELA Software products after delivery, reactive or pro-active, to correct faults, to improve performance or other attributes (e.g. updates, patches, bugfixes etc.), as well as ELA Maintenance/Support services for the ELA Software as described in Annex VI.
ELA Software	The Supplier software products covered by the ELA, as described in Annex V as well as any modification thereof delivered under the ELA Maintenance/Support.
EUI	European Union Institution, Body, Office or Agency.
Intra muros	Within the Customer's premises.
Order Form / Specific Contract	Document signed by the Customer and the Reseller, ordering ELA Software, ELA Maintenance/Support or Professional Services pursuant to a framework contract and to this Agreement. References to Order Forms and Specific Contracts are interchangeable.
Professional Services	All services related to information technology, such as training, consultancy, integration work, engineering and development as specified in the Annexes. All requests for Professional Services will be based on a Statement of Work.
Reseller	Any authorised reseller which has a direct framework contract with the Customer (e.g. any of the contractors of the SIDE II framework contracts (i.e. DI/07720, DI/07721, DI/07722 and DI/07723)).
Service Level Agreement	Agreement on applicable service levels, describing the quality of the services and the penalties for total or partial non-performance, as laid down in Annex VII.
Statement of Work	Description of the tasks requested from the Supplier, and laid down as part of the Specific Contract.
Customer's internal business purposes	Non-commercial use, including via on-line remote access from outside the premises of the contracting authority, by the Customer's staff or by other persons acting in fulfilment of a direct or indirect contractual obligation

	towards the Customer, be it as a contractor, a subcontractor or personnel of such (sub)contractor, within the context of the fulfilment of their mission for the Customer’s exclusive benefit, and as subject to the license conditions.
--	--

Furthermore, any references to the Customer in this Agreement shall be understood, as required by the context, as referring to one of the following concepts:

- a) all the EUIs covered by the Agreement, listed in Annex I, in relation to their collective rights and obligations with the Supplier, as one of the parties to the Agreement, and as the contracting authorities;
- b) any one of the participating EUIs acting in its own capacity, in particular for matters related to the conclusion, execution or termination of Specific Contracts between itself and the Reseller;
- c) the EDPS acting in its capacity as lead contracting authority and agent for the other participating EUIs or in its capacity as a contracting authority.

#### **4 PURPOSE OF THIS AGREEMENT**

During the Term, as defined in Article 7, and subject to the terms of this Agreement, the Customer and the Supplier agree to determine terms and conditions under which the Customer may:

- license ELA Software; and/or
- enter into ELA Support/Maintenance agreements; and/or
- enter into Specific Contracts for related Professional Services.

No direct transactions between the Supplier and the Customer are permitted under this Agreement.

Instead, all orders for ELA Software, ELA Maintenance/Support and Professional Services shall be placed through a Reseller. All requests for quotation, orders, invoices and payments will be dealt with exclusively between the Customer and the Reseller. This Agreement shall apply to any Order Form / Specific Contract between the Customer and the Reseller which makes reference to this Agreement.

Each Order Form / Specific Contract between the Customer and a Reseller under this Agreement will be agreed in writing by means of a proposal from the Supplier to the Reseller, in conformity with the licensing and pricing conditions agreed in the present Agreement. The Parties agree that no additional terms and conditions will be added through the ordering process or in the Order Form / Specific Contract, and that any such added terms and conditions will be void, unless additional terms and conditions are necessary to comply with legal obligations to which the Parties are subject that are laid down in EU law. In such a case, the Parties will add additional terms and conditions by modifications to the Agreement, as per Article 22. New Annexes to cover new software, maintenance/support or services may be added to this Agreement in mutual agreement of the Parties.

#### **5 LICENSE**

Order Forms / Specific Contracts on the basis of this Agreement shall grant to the Customer the right to use the ELA Software and benefit from ELA Maintenance/Support as described in the relevant Annexes.

Unless otherwise specified in the Annexes, the license granted to the Customer shall include the non-exclusive, transferable and irrevocable right to install/access, execute and use the ELA Software. The license shall be granted for all territories in which the Customer is active and for the entire duration of the intellectual property rights on the ELA Software.

Unless otherwise specified in the Annexes, the Customer may make copies of the software for backup and archival purposes, provided that the Supplier's copyright and other proprietary notices are preserved on each copy.

Unless otherwise specified in the Annexes, the Supplier shall provide the Customer with a complete and comprehensible documentation for the installation, configuration and use of the ELA Software.

## **6 ELA MAINTENANCE/SUPPORT**

Without prejudice to the Service Level Agreement and unless otherwise provided in the ELA Maintenance/Support of Annex VI, the following services shall be performed by the Supplier and are included in the ELA Maintenance/Support pricing:

- (1) diagnosing errors or faults encountered by the Supplier or the Customer affecting the ELA Software and making any necessary corrections as soon as practically possible and at the latest within thirty (30) working days of the discovery of the error or fault; the Supplier shall be obliged to effect corrections only if the error can be reproduced or if the Customer provides the Supplier with sufficient information from which the error can be diagnosed.
- (2) providing the Customer with successive ELA Software versions and releases and the relevant reference documentation.

## **7 DURATION**

This Agreement will be effective as of signature of both Parties and for a period of four (4) years (the "**Term**"). Even within the Term, no Order Form / Specific Contract under this Agreement may be renewed automatically or tacitly.

Commercial terms and conditions agreed in the Annexes may have shorter durations than the Term.

After the end of the Term,

- (1) this Agreement shall remain applicable to the Order Forms / Specific Contracts which were signed during the Term, until the last Order Form / Specific Contract expires. However, no Order Form / Specific Contract under this Agreement may be renewed, whether expressly or tacitly, after the Term;
- (2) any provision of this Agreement that expressly or by implication is intended to continue in force after the Term shall remain in full force and effect, including the confidentiality and indemnification obligations.

## **8 COMMUNICATION**

All notices to be given under this Agreement shall be made via the following contact details:

Supplier contact details:

TAS France SASU  
15 traverse des BRUCS  
06560 VALBONNE – SOPHIA ANTIPOLIS  
FRANCE  
[contact@tasgroup.fr](mailto:contact@tasgroup.fr)  
+33 4 92 94 56 90

Customer contact details:

European Data Protection Supervisor  
Unit Technology and Privacy  
Rue Wiertz 60  
1047 Brussels  
BELGIUM  
[edps-procurement@edps.europa.eu](mailto:edps-procurement@edps.europa.eu)  
+32 2 283 19 00

Specific contact details per product family may be included in the respective Annexes.

## **9 INTELLECTUAL PROPERTY RIGHTS (« IPR »)**

### **9.1. Ownership of IPR on the ELA Software**

The Supplier represents and warrants that it is the holder of all rights to the ELA Software covered by the present Agreement and shall notify the Customer of any changes in ownership of the ELA Software during the Term.

The Customer acknowledges that it will not become the owner of the licensed ELA Software, which will remain the ownership of the Supplier.

To the extent that the ELA Software contains third party materials, the Supplier shall disclose in writing such third party materials to the Customer and warrants that it has acquired from such third parties all necessary rights on the third party materials for granting the license under this Agreement.

### **9.2. Ownership of the Customer's data**

The Supplier acknowledges that all data provided by the Customer to the Supplier or generated through the use by the Customer of the ELA Software shall remain the ownership of the Customer. The Supplier shall acquire no right in such data other than the right to use such data for the purpose of and in compliance with this Agreement – with the understanding that personal data is excluded.

### **9.3. Specific Contract for development of new software**

In the cases that the Supplier has agreed to create software (including customizations) for the Customer under a Specific Contract, the Supplier shall provide the Customer with the software in both source and object codes. The Customer shall be the owner of all intellectual property rights on such software.

## **9.4. Indemnification**

The Supplier will defend and/or settle any claims against the Customer alleging that ELA Software infringes the intellectual property rights of a third party. In addition, the Supplier will hold the Customer harmless, by paying infringement claim defence costs, other possibly negotiated settlement amounts, court awarded damages and all other costs resulting from the alleged infringement. The Customer shall promptly inform the Supplier of any claim. The Supplier shall, at no cost to the Customer, modify the ELA Software so as to be non-infringing and materially equivalent, or shall procure a license from the third party. If these options are not available, the Supplier will refund to the Customer the amount paid for the ELA Software, or, for ELA Maintenance/Support services, the balance of any pre-paid amount or, for Professional Services, the amount paid, in addition to other amounts which may have to be paid in order to hold the Customer harmless.

## **10 COMPLIANCE**

### **10.1. Supplier's compliance**

- 1) Customer may check or require an audit on the implementation of the Agreement. This may be carried out by any outside body authorised to do so on its 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 Agreement. The audit procedure is initiated on the date of receipt of the relevant letter sent by the Customer. Audits are carried out on a confidential basis.
- 2) The Supplier must keep all original documents stored on any appropriate medium, including digitised originals if authorised under national law, for a period of five (5) years starting from the payment of the balance of the last Specific Contract issued under this Agreement.
- 3) The Supplier must grant the Customer's staff and outside personnel authorised by the Customer the appropriate right of access to sites and premises where the Agreement is implemented and to all the information, including information in electronic format, needed to conduct such checks and audits. The Supplier 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.
- 4) On the basis of the findings made during the audit, a provisional report is drawn up. The Customer or its authorised representative must send it to the Supplier, who has thirty (30) days following the date of receipt to submit observations. The Supplier must receive the final report within sixty (60) days following the expiry of the deadline to submit observations. On the basis of the final audit findings, the Customer may recover all or part of the payments made and may take any other measures which it considers necessary.
- 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 Agreement and up to five years starting from the payment of the balance of the last specific contract issued under this Agreement.

- 6) The Court of Auditors and the European Public Prosecutor's Office established by Council Regulation (EU) 2017/1939 ('the EPPO') and, for the processing of personal data, the European Data Protection Supervisor acting as the data protection supervisory authority have the same rights as the Customer, particularly right of access, for the purpose of checks, audits and investigations.

## **10.2. Customer's compliance**

In application of the principles of inviolability of premises and archives of the European Union institutions, bodies, offices and agencies, which are established by the "Protocol (7) on Privileges and Immunities of the European Communities", consolidated version of the Treaty on the Functioning of the European Union (OJ C 326, 26.10.2012), the Supplier may not audit the Customer.

## **11 PROCESSING OF PERSONAL DATA**

### **11.1. Processing of personal data by the Customer**

For the purpose of this Article 11.1:

- (a) the data controller for the personal data contained in this ELA is the EDPS;
- (b) the data protection notice is available at [https://edps.europa.eu/data-protection/our-work/publications/data-protection-notice/12-edps-data-protection-notice\\_en](https://edps.europa.eu/data-protection/our-work/publications/data-protection-notice/12-edps-data-protection-notice_en)

Any personal data included in or relating to the Agreement, 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 Agreement by the data controller.

The Supplier or any other person whose personal data is processed by the data controller in relation to this Agreement 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 Supplier or any other person whose personal data is processed in relation to this Agreement 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 as the data protection supervisory authority.

### **11.2. Processing of personal data by the Supplier**

For the purpose of this Article 11.2,

- (a) the Customer, listed in Annex I to this Agreement, is the data controller (the controller) for the processing of personal data in that Customer's respective use of the services provided to or procured by that Customer under this Agreement;



- (b) the Supplier is the data processor (the processor) for the processing of personal data on behalf of the controller under this Agreement;
- (c) the subject matter and purpose of the processing of personal data by the Supplier are the provision of a cloud collaboration workspace allowing amongst others conference calls, collaborative document editing and file sharing and related services (e.g. storage and backup) provided to or procured by the Customer under this Agreement as further specified in Annexes II, IV and V;
- (d) The localisation of and access to the personal data processed by the Supplier shall comply with the following:
  - i. the personal data shall only 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. no access shall be given to such data outside of the European Union and the European Economic Area;
  - iv. the Supplier may not change the location of data processing without the prior written authorisation of the Customer as the controller for the processing;
  - v. any transfer of personal data under the Agreement to third countries or international organisations shall fully comply with the requirements laid down in Chapter V of Regulation (EU) 2018/1725, in the exceptional event that the Customer as the controller for the processing allows a specific transfer to take place.

The processing of personal data by the Supplier on behalf of the controller shall meet the requirements of Regulation (EU) No 2018/1725 and be processed solely for the purposes set out by the controller. The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, as well as the location of data processing, are specified in Annex II.

The Supplier 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 Agreement as laid down in Chapter III (Articles 14-25) of Regulation (EU) No 2018/1725. The Supplier shall inform the controller about such requests within 48 hours after receiving such requests and shall take no action to respond to any such requests unless and until authorised by the controller to do so.

The Supplier 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 Supplier shall grant personnel access to the data to the extent strictly necessary for the implementation, management and monitoring of the Agreement. The Supplier 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 17 of this Agreement.

The Supplier 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 Parties shall set out in Annex III to this Agreement the appropriate technical and organisational measures, including technical and organisational measures to ensure the security of the data, to be implemented by the Supplier to ensure that the processing will meet the requirements of Regulation (EU) 2018/1725 and that the rights of the data subject will be protected.

The Supplier shall notify relevant personal data breaches to the controller without undue delay and at the latest within 48 hours after the Supplier becomes aware of the breach. In such cases, the Supplier 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 Supplier 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.

The Supplier 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 acting as the data protection supervisory authority;
- (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 Parties shall set out in Annex III to this Agreement the appropriate technical and organisational measures by which the Supplier is required to assist the Customer (as the controller for the processing) in the application of this Article 11.2 as well as the scope and the extent of the assistance required.

The Supplier 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 Customer is subject to Protocol (No 7) of the Treaty on the Functioning of the European Union (TFEU) on the privileges and immunities of the European Union, including as regards the inviolability of archives (including the physical location of data and services as set out in this Article 11.2) and data security, which includes personal data held on behalf of the Customer in the premises of the Supplier or subcontractor / sub-processor.

The personal data processed in context of the Customer's use of the services provided shall not be disclosed to third parties prior to consulting the Customer (as the controller for the processing) and without the Customer's agreement on the specific access or disclosure request. This includes requests received by the Supplier, its parent companies or any establishments of the corporate group and any sub-processors from the US authorities or any other third country authority.

The Supplier shall ensure compliance with legal obligations pursuant to Article 49 under Regulation (EU) 2018/1725 and Article 48 of Regulation (EU) 2016/679 where a court, tribunal or an administrative authority of a third country orders to transfer or disclose personal data processed in context of the controller's use of the services. Such order shall not be recognized or enforced unless it is issued on the grounds of a valid international agreement between the relevant third country and the Union or a Member State and in compliance with Protocol (No 7) to the TFEU and specific Member State law provisions, in particular the laws of France (e.g. the French blocking statute<sup>1</sup>).

The Supplier shall in every case notify the Customer (as the controller for the processing) within 24 hours of any legally binding request for access or disclosure of the personal data processed on behalf of the Customer, in particular those made by any national public authority, including an authority from a third country. Should such a request be received by the Supplier, its parent companies or any establishments of the corporate group and any sub-processors, the Supplier shall immediately submit to the Customer the request received, any supplemental information and a summary of the facts related to the request. The Supplier may not give such access without the prior written authorisation of the Customer.

The duration of processing of personal data by the Supplier will not exceed the period referred to in Article 10.1, point 2). Upon expiry of this period, the Supplier 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 Supplier shall not subcontract any of its processing operations performed on behalf of the Customer in accordance with this Agreement to a third party (the sub-processor), without the Customer's prior specific written authorisation and in line with this Article 11.2 of this Agreement and in compliance with Article 29(2) and (4) of Regulation (EU) 2018/1725. The Supplier shall submit the request for specific authorisation at least two (2) months prior to the engagement of the sub-processor in question, together with the information necessary to enable the Customer to decide on the authorisation. The Customer shall issue such an authorisation of the use of the sub-processor in writing. The list of sub-processors authorised by the Customer (as the controller for the processing) can be found in Annex II. The Parties shall keep Annex II up to date. For the purpose of Article 15, if part or all of the processing of personal data is subcontracted to a third party, the Supplier shall pass on the obligations referred to in Article 11.2 in writing in a legally binding document under Union or Member State law to those parties, including subcontractors / sub-processors. At the request of the Customer, the Supplier shall provide a document providing evidence of this commitment. The Customer may request the Supplier to

---

<sup>1</sup> Law No 68-678 of 26 July 1968 on the communication of economic, commercial, industrial, financial or technical documents and information to foreign natural or legal persons amended by Law 80-538 1980-07-16 Article 2 I JORF 17 July 1980 Creation of Law 80-538 1980-07-16 Article 2 II JORF 17 July 1980 amended by Law 80-538 1980-07-16 Article 3 of the Official Journal of the French Republic of 17 July 1980 amended by Order No 2000-916 of 19 September 2000 — Article 3 (V) JORF 22 September 2000 in force on 1 January 2002. Latest update of the data in this text: 01 January 2002 Version in force on 08 February 2022

replace a subcontractor / sub-processor or intended subcontractor /sub-processor found to be in a situation provided for in Article 0 of this Agreement.

## **12 WARRANTY**

The Supplier warrants that the ELA Software will be free from any viruses or other malicious code at the time of receipt by the Customer. Such warranty shall be repeated at the time of receipt by the Customer of any update or upgrade.

The Supplier warrants that the ELA Software does not and shall not include or contain any clock, timer, counter, or other limiting or disabling code, design or routine which causes the ELA Software to be erased, inoperable or otherwise incapable of being used in the full manner for which it was designed and licensed pursuant to this Agreement. This includes, without limitation: (a) after being used or copied a certain number of times, or after the lapse of a certain period of time, or after the occurrence or lapse of any triggering factor or event; or (b) because the ELA Software has been installed on or moved to hardware different to that on which the ELA Software was originally installed.

The Supplier warrants that the ELA Software will materially conform to its specifications and will be free of defects at the time of delivery and for a period of *ninety (90) days* thereafter ("**Warranty Period**").

In case of malfunction during the Warranty Period, the Supplier warrants to make its best efforts to remedy the malfunction. When the Supplier receives a warranty claim for an ELA Software, the Supplier will either repair the relevant defect or replace the ELA Software. Failure to remedy a default for a period longer than *thirty (30) days* shall entitle the Customer to a full refund of the ELA Software and ELA Maintenance/Support fee and to all related costs and damages for the Customer.

The Supplier does not warrant that the operation of ELA Software will be uninterrupted or error-free, or that the ELA Software will operate in hardware and software combinations other than as authorized by the Supplier. However, if the Supplier recommends that the Customer runs the ELA Software on specified hardware or equipment, the Supplier shall be responsible if the ELA Software does not function on such hardware or equipment.

The Supplier warrants that it shall give a notice of at least three (3) months before implementing any change to the unique identifier (or SKU) of the ELA Software.

## **13 SPECIFIC PROVISIONS FOR SOFTWARE AS A SERVICE (“SAAS”)**

The following provisions shall apply if the ELA Software is licensed in the form of a software as a service.

The Supplier may not suspend the provision of the ELA Software for any reason other than the existence of a serious risk for the security of the service. In this case, the Supplier may suspend the provision of the ELA Software only if it notifies the Customer of the interruption and makes all commercially reasonable efforts to restore the service as soon as possible.

The Supplier warrants that it has an operational business continuity plan to ensure the continued

provision of the ELA Software and will provide the details of such business continuity plan upon request from the Customer.

The Supplier will promptly retrieve and deliver to the Customer a copy of all data uploaded by the Customer in the ELA Software or generated through the use by the Customer of the ELA Software (or only those portions specified by the Customer) in the format and on the media reasonably specified by the Customer at any time upon the Customer reasonable request and, in any case, at the expiration of this Agreement. If requested by the Customer, the Supplier shall securely erase such data from its systems within seven (7) days and provide the Customer with a written confirmation thereof.

## **14 ASSIGNMENT**

The Supplier shall notify the Customer at least thirty (30) days in advance of any intended transfer or assignment of its rights and obligations arising from the Agreement. In such cases, the Supplier must provide the Customer with the identity of the intended assignee and obtain the Customer's consent prior to such assignment. The Customer shall not unreasonably withhold or delay such consent. Any right or obligation assigned by the Supplier without notification to the Customer and its consent will not be enforceable against the Customer. The Supplier shall defend and/or settle any claims against the Customer in this regard. The Customer reserves the right to terminate the present Agreement and to claim reimbursement from the Supplier.

The Customer has the right to terminate this Agreement, should the assignee not have access to procurement, or be in one of the exclusion situations listed in the 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 (the “Financial Regulation”).

The Customer may assign any of the rights and obligations arising from the Agreement to any other EUI, without prior consent from the Supplier.

## **15 SUBCONTRACTING**

Subcontracting is the situation where the Supplier, in order to carry out the ELA, enters into legal commitments with other entities for performing part of this Agreement. No prior authorisation from the Customer is necessary. The Customer has no direct legal commitment with the subcontractor(s). In case of subcontracting, the Supplier remains bound by its contractual obligations and is solely responsible for the implementation of this Agreement.

The Supplier ensures that the obligations and administrative requirements (including but not limited to confidentiality and security) under this Agreement are understood and respected by its subcontractors. In addition, the Supplier must ensure the subcontractors 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. 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 Customer, the Supplier must submit any relevant information, including evidence for the compliance with these obligations.

This clause is without prejudice to authorisations for subcontracting which are required under the applicable law (e.g. in case of data processing by the subcontractor). Where the subcontractor is or will be engaged by the Supplier for carrying out specific processing activities on behalf of the Customer that involve personal data the relevant data protection provisions of this Agreement, in particular Article 11.2 shall apply, including the obligation to obtain prior specific written authorisation of the Customer.

Any *Intra muros* deployment of personnel or subcontractors will be subject to specific provisions to be agreed by the Parties in accordance with Article 22.

## **16 SECURITY**

### **16.1. Commission decisions**

The Supplier undertakes to comply with the obligations laid down in the 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 standards and guidelines, as well as the Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on the security in the Commission, and the Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information, its implementing rules and the corresponding security notices.

These documents (as adapted from time to time) are available for consultation at the following address: [https://ec.europa.eu/info/files/security-standards-information-systems\\_en](https://ec.europa.eu/info/files/security-standards-information-systems_en).

Should the Supplier, during the implementation of the Agreement, need remote access to any communication and information system of the Commission or of other EUIs or data sets processed therein, the Supplier shall be requested to comply with security rules referred to in Article 6(5) of the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017.

This entails prior authorisation which shall be granted on the basis of a formal request for network access service “Remote Access for Companies” and approval process which takes in average 4-6 weeks. The outcome of the approval, i.e. the security convention, shall be valid for a specified duration linked to the contract and shall be obtained before the connection is activated. The formal request is initiated by the concerned DG or service of the Commission and based on the risk assessment with the focus on nature and sensitivity of the tasks to be performed remotely and the security needs of each accessed communication and information system.

During the authorisation process the Supplier is asked to describe relevant organisational, physical, logical and network security measures in order to provide reasonable assurance that the risks are adequately and systematically covered at a level equivalent to the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017, its implementing rules and corresponding security standards. The authorisation process may impose additional security requirements as a prerequisite for approval, in order to protect the Commission’s communication and information system and networks from the risks of unauthorised access or other security breaches.

Any financial burden for any security vetting procedure and security background check will be at charge of the Supplier and not the Customer.

## **16.2. Software as a Service (SaaS)**

Supplier confirms it will provide all requested information with regard to SaaS-products, and will voluntarily share any useful information it may have in this regard. It will fill in any questionnaire on SaaS products, or any replacing document, in good faith, if requested by the Customer, either directly or through the Reseller. Any quotation from the Supplier to the Reseller regarding SaaS products shall be accompanied by such filled-in SaaS questionnaire. Such filled-in SaaS questionnaire shall be included in the Supplier's proposal (Annex V to this Agreement).

## **17 CONFIDENTIALITY**

The Parties must treat with confidentiality any information or documents, in any format, disclosed in writing or orally relating to this Agreement, which is either identified in writing as confidential or which can reasonably be presumed to be confidential. Each Party must:

- (a) not use confidential information or documents for any purpose other than to perform its obligations under the Agreement 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.

The confidentiality obligations are binding upon the Parties during the implementation of the Agreement 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.

The Supplier must obtain from any natural person with the power to represent it or take decisions on its behalf, as well as from subcontractors or third parties involved in the implementation, a commitment that they will comply with this Article or have confidentiality obligations in place that are similar or higher than those in this Article. At the request of the Customer, the Supplier must provide a document with evidence of this commitment.

Each Party undertakes to treat in absolute confidentiality and not make use of or disclose to third parties any information or documents linked to this Agreement.

The Parties explicitly agree that the contents of this Agreement may be disclosed to the Resellers and to other EUIs on a strict need-to-know basis.

Any press releases or public statements relating to the present Agreement shall be presented to the Commission for review prior to such release.

## **18 TERMINATION**

The Customer may terminate the Agreement and/or any of its on-going Order Forms / Specific Contracts in the following circumstances:

- (a) if the Supplier is in breach of the data protection obligations of Article 11.2;
- (b) if the Supplier does not comply with the applicable data protection obligations resulting from Regulation (EU) 2016/679;
- (c) where the Customer has evidence that the Supplier or any related entity or person has violated any provisions on security and/or confidentiality included in the Agreement.

Termination may either be immediate, or enter into force at a date specified by the Customer in the termination notice.

## **19 INSTITUTIONAL ASPECT**

The European Union has legal personality under Article 47 of the consolidated version of the Treaty on the European Union (OJ C 326, 26.10.2012), including all its bodies, institutions, services and departments. Within the European Union, several people, bodies, institutions, services and departments will be authorized to initiate the order process through the Reseller. Therefore, any Order Form / Specific Contract relating to this Agreement which is concluded between the Reseller and any of these bodies, institutions, services and departments forming part of the European Union legal entity shall be in the name of the European Union and shall result in entitlements for the Union, rather than entitlements specific to a body, institution, service or department.

The Supplier accepts that the EDPS (acting as defined under Article 3, point c) of this Agreement) and the European Commission (as the lead contracting authority for the SIDE II framework contracts (i.e. DI/07720, DI/07721, DI/07722 and DI/07723)), are also authorised to order and purchase ELA Software, ELA Maintenance/Support and Professional Services centrally and for the benefit of other EUIs.

Any other EUI than the Customers listed in Article 1 and Annex I can join the Agreement at a later time by means of a notification letter sent by the EDPS or the European Commission to the Supplier. Following such notification, all references to the Customer in this Agreement shall be understood as also including such other participating EUIs and therefore entitling such other EUI to the Customer's rights under this Agreement.

## **20 APPLICABLE LAW**

The Agreement is governed by Union law, complemented by the law of Belgium. The courts of Brussels and the Court of Justice of the EU at the choice of the Customer have exclusive jurisdiction over any dispute regarding the interpretation, application or validity of the Agreement.

This includes compliance 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.



## **21 ORDER OF PRECEDENCE**

This Agreement consists of the ELA terms, included in the present document, and its Annexes.

If there is a conflict between any provision in the terms of the ELA and the terms of its Annexes, the terms of the ELA will prevail, unless the conflicting Annex (a) references the specific terms of the ELA with which it conflicts; (b) summarizes such terms; (c) states the different terms that shall apply; and (d) provides the rationale for the application of the different terms.

## **22 ENTIRE AGREEMENT – IMPLEMENTATION CAVEAT**

This ELA and its Annexes represent the entire understanding of the Parties with respect to its subject matter and supersedes (i) any previous communication or agreements that may exist and (ii) any additional terms that Supplier may provide after signature of this Agreement. Modifications to the Agreement will be made only through a written amendment, signed by both Parties, with the exception of adding new EUIs, as per Article 19, and sub-contractors / sub-processors, as per Article 11.2. New Annexes to cover new software, maintenance/support or services may be added to this Agreement in mutual agreement.

## **23 LIST OF ANNEXES**

The Parties have agreed to the conditions set out in this Agreement and in the following Annexes to this Agreement, which form an integral part of the Agreement:

- I. List of all EUIs covered by the Agreement
- II. Description of the processing and list of sub-processors authorised by the Customer
- III. Technical and organisational measures including technical and organisational measures to ensure the security of the data
- IV. Customer specifications for the software products and services to be provided by the Supplier
- V. Supplier's proposal
- VI. ELA Maintenance/Support
- VII. Service Level Agreement
- VIII. Commercial conditions
- IX. Cloud Terms and Conditions of the European Commission
- X. ICT Systems Baseline Security Requirements of the European Parliament

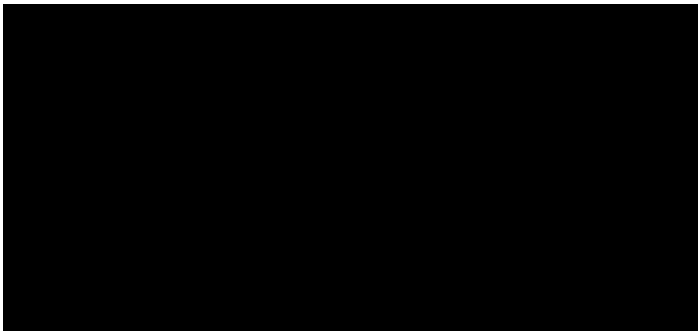
**SIGNATURES**

For the Supplier,

TAS France SASU,

Francesco DE SIMONI,  
Directeur Général

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



Done at \_\_\_\_\_, on \_\_\_\_\_ 2022

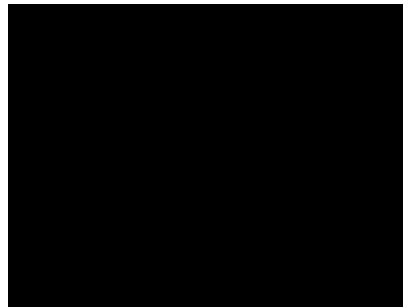
In duplicate in English.

For the Customer,

European Data Protection Supervisor,

Leonardo CERVERA NAVAS,  
Director

Signature:



Done at Brussels, on 18 May 2022

**Annex I**

**List of all EUIs covered by the Agreement**

The following EUIs are covered by the Agreement as the Customers:

#	European Union institutions, agencies or other bodies		Main Location
1	EDPS	European Data Protection Supervisor	(BE) Brussels
2	European Council		(BE) Brussels

Other EU institutions, bodies, offices or agencies may join the Agreement at any time by way of an amendment of the Agreement as provided under Article 19 of the Agreement. In such a case, the Parties will update the list of all EUIs covered by the Agreement.

For the purpose of Article 11.2 of this Agreement, each EUI listed in this Annex I is the controller for the processing of personal data in that EUI's respective use of the services provided or procured by the that EUI under this Agreement.

## Annex II

### Description of the processing and list of sub-processors authorised by the Customer

#### A) Description of the processing

The processing of personal data on behalf of the Customer in the Supplier's provision and Customer's use of the services provided under this Agreement and referred to under Article 11.2 is described as follows. Further information on the processing can be found in the Customer specifications for the software products and services to be provided by the Supplier under Annex IV to this Agreement.

#### Categories of data subjects whose personal data is processed

The categories of data subjects whose personal data is processed are:

- staff of the Customer using or managing the provided services,
- recipients of communications by the Customer included in provided services,
- individuals included in the documents handled by the Customer in provided services,
- individuals involved in collaborations lead or supported by the Customer,
- individuals participating in conference calls and chats.

Further information on the categories of data subjects whose personal data is processed in the different services and service components provided under this Agreement can be found in the tables in document "Nextcloud-Database-Tables" included in the Supplier's proposal under Annex V to this Agreement.

#### Categories of personal data processed

The categories of personal data processed are: name, surname, email address, telephone number, user ID information and hashed password of users, user status message, user notification preferences, user location and time zone, user language, user profile data (organisation, role, headline, biography, working hours); name, surname, email address, telephone number and/or other contact details of contacts; display names, emails, comments, chat message details and other content provided by a user; user interactions with another user or contact, user interactions with a service (e.g. user opened, shared, changed or received a file, item of a user was shared; user created or was added into or interacted with a conversation, call or email); IP addresses; group memberships, tasks allocations, tasks progress; audio and video conference data (e.g. audio and video stream, shared screens), account security data (two-factor devices, special-use passwords, log-in session tokens, open log-in sessions), internet connectivity data (device type, user agent, IP address).

Further information on the categories of personal data processed in the different services and service components provided under this Agreement can be found in the tables in document "Nextcloud-Database-Tables" included in the Supplier's proposal under Annex V to this Agreement.

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No processing of sensitive data by the Supplier on behalf of the Customer is currently foreseen under this Agreement. Should the Customer instruct the Supplier to process sensitive data on its behalf, the Parties will accordingly update this Annex and where necessary other Annexes to this Agreement.

#### Nature of the processing

Personal data are processed by the Supplier for the provision of a cloud collaboration workspace allowing amongst others conference calls, cloud calendars and address books, collaborative document editing and file sharing, kanban project management, and related services (e.g. storage and backup) provided to or procured by the Customer under this Agreement as specified in this Annex and Annexes IV and V to this Agreement. As part of the processing, the Supplier will perform the following operations to the Customer: provide infrastructure and platform to host and manage cloud services provided to the Customer; store and backup information, including personal data, uploaded and created in the Customer's use of the provided services; user accounts; secure information, including personal data, stored in, transmitted to and processed on the cloud services provided to the Customer; provide maintenance, updates and support for the services provided to the Customer.

#### Purpose(s) for which the personal data is processed on behalf of the controller

In providing the services provided to or procured by the Customer, personal data will be processed for the purposes of: storing and backing up information; access management with user accounts; enabling file sharing, document creation and editing, calendar, contact and appointment setup, kanban project management, communication and other interaction by users and between users; preventing and detecting unauthorised access to, use of and disclosure of information, including personal data, ensuring its security and confidentiality; providing maintenance, software update and troubleshooting support.

#### Duration of the processing

In accordance with Article 11.2 of this Agreement, the maximum duration of the processing by the Supplier on behalf of the Customer is the duration of the Agreement plus a period of five (5) years starting from the payment of the balance of the last Specific Contract issued under this Agreement.

Further information on the retention of different categories of personal data processed in the different services and service components provided under this Agreement can be found in the tables in document "Nextcloud-Database-Tables" included in the Supplier's proposal under Annex V to this Agreement.

#### Location of data processing

Personal data processed by the Supplier under this Agreement is carried out in accordance with Article

11.2, point (d) of this Agreement in the European Union and European Economic Area, in particular in France and Belgium and in case of activated disaster recovery option also in Italy.

B) List of sub-processors authorised by the Customer (if applicable)

No sub-processors are currently authorised by the Customer. A Customer (as the controller for the processing) may authorise the use of a sub-processor by way of an amendment of the Agreement as provided under Article 11.2 of the Agreement. In such a case, the Parties will use the template below to list the sub-processors authorised by the Customer in this Annex. The Parties will keep this list of sub-processors authorised by the Customer up to date.

[The Customer as the controller for the processing has authorised the use of the following sub-processors:

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Subject matter, nature and duration of the processing: ...

Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): ...

2. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Subject matter, nature and duration of the processing: ...

Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): ...

...]

### **Annex III**

#### **Technical and organisational measures including technical and organisational measures to ensure the security of the data**

The Parties have agreed that the Supplier implements at least the technical and organisational measures, including technical and organisational measures to ensure the security of the data, as detailed in the document “EDPS\_NEXTCLOUD\_Data Security Measures” included as Annex III to this Agreement. The Parties will update Annex III to this Agreement where necessary. The Customer (as the controller for the processing) will reassess these measures before a production system is deployed and the Parties will adjust the measures for the production system in accordance with the Customer’s assessment.

Further details of technical and organisational measures to be put in place by the Supplier can be found in the Supplier’s proposal (Annex V to this Agreement).

### **Annex IV**

#### **Customer specifications for the software products and services to be provided by the Supplier**

The EDPS’ specifications as detailed in the document “EDPS\_NEXTCLOUD\_Customer Specifications” for the software products and services to be provided by the Supplier are included as Annex IV to this Agreement. The Parties will update Annex IV to this Agreement where necessary with further Customer specifications for the software products and services to be provided by the Supplier.

### **Annex V**

#### **Supplier’s proposal**

The Supplier’s proposal as detailed in the document “TASFrance\_hosting-proposal” (including any documentation, questionnaires, tables, correspondence with and guarantees provided to the contracting authority during the procurement process) and the technical documentation “Nextcloud-Database-Tables” is included as Annex V to this Agreement.

### **Annex VI**

#### **ELA Maintenance/Support**

The Parties may decide to enter into ELA Maintenance/Support agreement at any time by way of an amendment of the ELA Master Agreement. In such a case, ELA Maintenance/Support agreement will be included as Annex VI to this Agreement.

## **Annex VII**

### **Service Level Agreement**

The Service Level Agreement for the provision of the services under this Agreement that has been agreed by the Parties are set out in the Supplier's proposal (Annex V to this Agreement)..

## **Annex VIII**

### **Commercial conditions**

Commercial conditions for the provision of the services under this Agreement that have been agreed by the Parties are set out in the Supplier's proposal (Annex V to this Agreement).

## **Annex IX**

### **Cloud Terms and Conditions of the European Commission**

The Supplier agrees to abide by the Cloud Terms and Conditions of the European Commission which is incorporated in this Agreement by reference. A copy of the Cloud Terms and Conditions of the European Commission is included as Annex IX to this Agreement.

## **Annex X**

### **ICT Systems Baseline Security Requirements of the European Parliament**

The Supplier agrees to abide by the ICT Systems Baseline Security Requirements of the European Parliament which is incorporated in this Agreement by reference. A copy of the ICT Systems Baseline Security Requirements of the European Parliament is included as Annex X to this Agreement.



# Annex III to the Global ELA

Technical and organisational measures including technical and organisational measures to ensure the security of the data

The Supplier implements the following technical and organisational security measures (including any relevant certifications) as agreed with the Customer to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. For this purpose, the Supplier will ensure that the corresponding technical and organisational measures remain up to date and that it remains informed of any developments that may affect the measures. It shall notify the Customer at least one month in advance in case of necessary changes that could affect the Customer (e.g. blocking of weak ciphers). In case of changes that are urgent to ensure the effectiveness of the measures, i.e. high-risk vulnerabilities, the notice period shall be at least 24 hours.

In case the Supplier employs another supplier in accordance with Article 11.2 of the Global ELA to process personal data on behalf of the Customer (sub-processing), the requirements in this Annex III to the Global ELA and in any documents incorporated by reference shall apply *mutatis mutandis* to this or these other supplier(s) with respect to the specific sub-processing carried out by that or those other supplier(s).

## 1 INFORMATION SECURITY MANAGEMENT

The Supplier shall manage its overall information security i.e. periodically analyse its existing practices, determine points of improvement, plan for these improvements (prioritising the most critical issues first), implement and monitor the effectiveness of the improvements.

The process to improve the overall information security shall be documented and regularly reviewed in order to improve its effectiveness.

The Supplier shall provide the Customer with its information security policy.

## 2 CERTIFICATIONS

The Supplier maintains a valid certification ISO 27001 that covers the design provision and management of data centre hosting and housing services including data management in general and personal data including health data (IAF 33).

The Supplier maintains a valid certification ISO 9001 that covers the design provision and management of data centre hosting and housing services (IAF 33).

The Supplier maintains a valid certification PCI DSS for its data centres.

The ~~s~~Supplier maintains a valid certification according to the HDS Certification Standard that covers the provision and maintenance of housing and hosting, the physical infrastructure, the information system's application hosting platform, backups, and the virtual infrastructure of the information system as well as the administration and operation of these components.

Those certifications cover IT security governance and management processes and the physical security of locations at which Customer data and other data from the Customer's use of the services provided to the Customer is processed.

The Supplier commits to provide to the Customer the annual full up-to-date certification audit reports issued by the competent certification authorities.

### **3 MEASURES FOR USER IDENTIFICATION AND AUTHORISATION**

The Supplier supports the SAML 2.0 standard to allow the Customer the use of Single-Sign-On with customer-controlled identification and authorisation services (e.g. EU Login).

The Supplier supports also authorisation with username and password and with one-off codes sent to mailboxes controlled by the Customer.

### **4 SUPPLIER STAFF ACCESS CONTROLS**

The Supplier ensures physical and logical access control for its staff to the devices and the platform providing the service. Such access shall be limited strictly to the requests made by the Customer or to ensuring the continuity of the service. For these cases, the number of staff being granted access shall follow the principle of as few as possible and as many as necessary and shall be clearly logged and documented (see section on logging).

Only duly authorised staff with a need to know, i.e. for whom access to EDPS information is necessary for the conduct of their tasks, shall be able to access Customer data (on any of the environments) and its backups. In this respect, the principle of least privilege shall be applied, according to which staff accounts shall receive only the privileges that are essential for the work they need to do. Customer data shall also be protected from access by system administrators.

Any and all access to Customer data shall be appropriately logged so as to be able to trace back the access to an individual.

These logs shall be managed securely and maintained for at least 6 months.

The Supplier provides the Customer with a list of generic (privileged) user accounts implemented on the system. The Supplier deactivates generic user accounts immediately that are not in use. The Supplier informs the Customer on every use of generic (privileged) user accounts on the Customer's system.

### **5 TECHNICAL VULNERABILITY MANAGEMENT**

Given the particular use case of the Customer, the Customer requests the level of maintenance to be provided by the Supplier. Corrective and preventive maintenance as defined in Annex IX are particularly relevant for technical vulnerability management.

Upon Customer request, the Supplier will carry out corrective maintenance including the installation of critical security patches without undue delay and in any event not later than 1 working day upon explicit written request of the Customer. For this, the Supplier subscribes to and monitors security-related distribution lists, most importantly of the software vendors, to be notified about such patches as they become available.

Upon Customer request, the Supplier will carry out preventive maintenance. This involves monitoring the equipment actively for vulnerabilities using appropriate scans and reporting tools. The supplier provides reports to the Customer on their request.

Upon Customer request, the Supplier will carry out adaptive and/or evolutive maintenance. This involves installing feature updates without undue delay and not later than one month after release date.

## **6 MEASURES FOR THE PROTECTION OF DATA DURING TRANSMISSION**

The Supplier ensures that data transmissions between the Supplier's infrastructure and the Customer are always encrypted according to current state-of-the-art, such as Transport Layer Security.

## **7 MEASURES FOR THE PROTECTION OF DATA DURING STORAGE**

The physical security of the Supplier's computing equipment employed for Customer data is all certified (see above). The Customer can activate Nextcloud server-side encryption (with private keys processed on the server, but not stored permanently). The Supplier ensures regular integrity checks on the system hardware caused by technical malfunction (for example malfunction of storage equipment or corrupted data blocks).

## **8 SECURE DISPOSAL**

Upon Customer request, at the end of the contract, or at disposal or reuse of hardware containing Customer data, the Supplier shall perform the secure deletion of Customer data from any of the Supplier's environments including the backups, i.e. data shall be erased using a software certified by at least one EU Member State National Information Security Service. Within 24 hours after deletion, the Supplier shall notify the deletion to the Customer, informing the Customer of the reason for the deletion and certifying to the Customer that the data was securely deleted using a specific software.

## **9 MEASURES FOR ENSURING BACK-UPS AND DISASTER RECOVERY**

The Supplier ensures that back-ups (snapshots) of all data of the production environment are created as below:

- Daily within the last 15 days;
- Monthly for the last 3 months.

The daily and monthly back-ups shall be the ones taken at 6:00 UTC+1, and back-ups falling outside these periods shall be deleted.

The Supplier's optional disaster recovery offer ensures that these back-ups are stored at two separate physical locations. These locations shall be at least 300km apart.

The Supplier ensures that the daily backups are kept separated from the production system (e.g. air gapped) to avoid scenarios such as compromised networks or ransomware attacks. The Supplier ensures a target recovery time in case of an incident of 24h.

## **10 MEASURES FOR ENSURING EVENTS LOGGING**

The Supplier ensures to keep audit logs for activities linked to the server provision, operation and maintenance, which shall be accessible to the Customer.

The service integrates audit logs to cover admin-level operations carried out by the Customer.

These logs shall be kept for a period of 30 days. Upon request of the Customer, the Supplier ensures that log files can be neither accessed nor changed by the Supplier.

The Supplier deletes personal data, such as IP addresses, through anonymisation in web service access log entries older than 14 days.

## **11 MEASURES FOR ENSURING LIMITED DATA RETENTION**

The Customer is responsible for organisational measures to implement data retention in the production environment. The Supplier provides the component Nextcloud Files Retention to enable the Customer tagging files for later automatic deletion.

## **12 SECURITY INCIDENTS**

In case of a security incident (as defined in Annex IX), the Customer shall be informed at latest 4 hours after detection of the security incident with details on the security incident, its impact on the security of Customer data and with a plan to implement controls in order to mitigate the impact or correct the situation.

In case this information is not available after 4 hours, the Supplier will provide the available information and complement the communication as soon as more elements become available.

Sharing information with outside parties on security incidents that affect the Customer is subject to prior approval (by the Customer).

The Supplier carries out analysis and diagnosis of system alerts and corrects anomalies.

## **13 MEASURES FOR ENSURING AVAILABILITY AND RESILIENCE OF THE SERVICE**

The Supplier ensures total redundancy of all the server components (N+1/N+2 redundancy) and synchronous copy of data and virtual machines on two separate nodes in real time.

The Supplier ensures private and dedicated cloud resources available to the virtual machines used to provide the service.

The Supplier provides for an automatic migration of virtual machines without any data loss.

The Supplier shall ensure an availability target of 99.99%. This means that unplanned availability shall not exceed 52,56 minutes per year. This excludes administrator-level operations actions carried out by the Customer causing the loss of availability. The Supplier shall inform the Customer about planned maintenance work at least 7 days in advance.

## **14 MEASURES FOR ENSURING ACCOUNTABILITY**

The Supplier shall, upon request, provide the Customer with the current documentation on its implemented IT security and data protection measures relevant to the provided service. This documentation shall cover in particular measures used to meet the requirements of this Annex III to the Global ELA and any documents incorporated by reference, including documentation on the certification processes.

As provided by Article 10 'Compliance' of the Global ELA, the Customer may audit the implementation of the Agreement at any moment during the provision of the service. The audit may include on-site visits at the Supplier and any sub-processors.

The Supplier maintains a data processor record in accordance with Article 31(2) of Regulation (EU) 2018/1725<sup>1</sup> for the processing activities carried out on behalf of the Customer.

## **15 MEASURES FOR ENABLING COMPLIANCE WITH DATA SUBJECT RIGHTS REQUEST**

The Supplier provides tools that enable and/or facilitate the Customer's compliance with data subject rights requests as stipulated in Chapter III of Regulation (EU) 2018/1725. In particular, this shall include the possibility to export, delete and amend in bulk all personal data referring to an individual user.

## **16 MEASURES FOR ALLOWING DATA PORTABILITY AND INTEROPERABILITY**

As provided by Article 9.2 'Ownership of the Customer's data' of the Global ELA, the Supplier provides on the reasonable request of the Customer a full database and application-level configuration export containing all Customer data.

The Supplier employs solely Free and Open Source Software (FOSS software) on application-level, in particular Nextcloud and LibreOffice/Collabora Office Online, to allow the Customer's independent reuse of the database using a similar service.

---

<sup>1</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018R1725>




May 2022

**EUROPEAN  
DATA  
PROTECTION  
SUPERVISOR**

The EU's independent data  
protection authority

*Piloting  
Nextcloud and Collabora Office*

Customer Specifications (Annex IV)

  
EDPS Technology and Privacy Unit

## Contents

<b>1. Project Description .....</b>	<b>2</b>
<b>2. Software Description .....</b>	<b>2</b>
<b>3. Hardware Environment Description .....</b>	<b>3</b>

# 1. Project Description

The EDPS wants to carry out a pilot of the collaborative working cloud suite *Nextcloud Hub* and *Collabora Office Online* for a limited period of one year to assess the utility of software solutions offering high security and privacy safeguards through the use of free software (FOSS).

This action contributes to the EDPS strategy 2020-2024<sup>1</sup> on sovereignty:

*The EDPS is interested in policy initiatives to achieve ‘digital sovereignty’, where data generated in Europe is converted into value for European companies and individuals, and processed in accordance with European values. At the same time, we are committed to overcome the detrimental vendor’s lock-in syndrome in EUI.*

The pilot shall

- inform the EDPS for a revision of its own IT environment planned for the near future and
- inform the EDPS for its policy and supervision activities.

The platform shall offer a basic configuration with 100 user accounts and offer in total 100 GB storage.

# 2. Software Description

- **Nextcloud** with subscription to Nextcloud Files Premium, Groupware, and Talk
  - Nextcloud Deck
  - Nextcloud Talk with at best the possibility to test both
    - peer-to-peer talks (WebRTC, requires TURN server)
    - high performance backend (requires also a server)
  - Nextcloud Calendar
  - Nextcloud Files
  - Nextcloud Circles
  - Collabora Online (with license subscription)
  - Edit Files with LibreOffice (third-party plugin)
  - Files automated tagging
  - Approval Workflow
  - SAML 2.0 single-sign-on
  - Two-factor authentication with login code sent to user by email (if SAML is not activated)
  - Nextcloud Data Request

---

<sup>1</sup> [https://edps.europa.eu/sites/edp/files/publication/20-06-30\\_edps\\_shaping\\_safer\\_digital\\_future\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/20-06-30_edps_shaping_safer_digital_future_en.pdf)



- Nextcloud Files Retention
- **ElasticSearch:**
  - full-text search in documents
  - Ingest plugin to cover also PDF, docx, pptx, xlsx, odt, odp, ods, etc.<sup>2</sup>

To allow Customers other than the EDPS to employ Nextcloud for their own purposes, the offer should consist of one or more base-line configurations and options that can be selected to extend the base-line configuration.

### 3. Hardware Environment Description

The EDPS is the supervisory authority to the EU institutions and has to lead by example. Due to the use of production data, the EDPS requires a high level of security and data protection compliance.

The following measures are examples and may be substituted by other appropriate measures.

- hosting in the EU
- certified server hosting and housing environment
- either no sub-processors/sub-contractors or only those with no links to subsidiaries outside of the EU
- private and dedicated resources
- redundant hardware components and migration without data loss
- high availability 99.99% SLA
- backups
  - o daily with retention of 15 days
  - o monthly with retention of 3 months
- security updates
- updates to the latest stable version of Nextcloud (to be discussed)
- optional increase of user base
- optional increase of storage

---

<sup>2</sup> <https://www.elastic.co/guide/en/elasticsearch/plugins/current/ingest-attachment.html>, <https://tika.apache.org/2.3.0/formats.html>

- optional booking of disaster recovery with 2nd location at min. 300km distance
- optional booking of preventive, adaptive and evolutive maintenance



# **SIDE-II Negotiated Package (Group S) for EU institutions, bodies and agencies**

## **Private cloud and Nextcloud hosting proposal**

Date

2 May 2022

### **TAS France**

15 traverse des Brucs, 06560 Valbonne – Sophia Antipolis, France

SIREN 382 525 541 – VAT n. FR 93382525541

#### **Confidentiality**

*This document is strictly confidential. It may not be disclosed in whole or in part to a third party, by any means and for any purpose whatsoever, without the prior consent of TAS France. These restrictions do not concern the elements contained in the documents made public by TAS France or the communication of which would have been made compulsory by a regulatory authority*

# SOMMAIRE

<b>1</b>	<b>HOSTING PROPOSAL .....</b>	<b>3</b>
1.1	HOSTING INFRASTRUCTURE .....	3
1.2	PROPOSED PLATFORMS .....	3
1.3	PLAN A.....	5
1.3.1	<i>Installation and configuration</i> .....	5
1.3.2	<i>Hosting</i> .....	5
1.4	PLAN B.....	6
1.4.1	<i>Installation and configuration</i> .....	6
1.4.2	<i>Hosting</i> .....	6
1.4.3	<i>Monitoring, supervision and administration</i> .....	7
1.5	AVAILABLE HOSTING OPTIONS AND UPGRADES .....	8
1.6	SOFTWARE OPTIONS .....	10
<b>2</b>	<b>BILLING AND PAYMENT TERMS.....</b>	<b>11</b>
<b>3</b>	<b>SERVICE LEVEL AGREEMENT (“SLA”).....</b>	<b>12</b>
<b>4</b>	<b>CUSTOMER SUPPORT .....</b>	<b>17</b>

# 1 HOSTING PROPOSAL

## 1.1 Hosting infrastructure

Each Customer will use distinct private and dedicated cloud platforms.

Each platform will be hosted in TAS France datacenter in Sophia Antipolis - France (<https://youtu.be/EF6F6r6hPSE>), of Tier4 level, certified ISO:9001, ISO:27001, [PCI-DSS](#) and [HDS](#).

TAS France private cloud hosting service relies on a hyperconverged hardware infrastructure with following characteristics:

- [DELL / EMC / VMWARE VxRail technology](#)
- Total redundancy of all the components of each node
- N+1 / N+2 redundancy of nodes
- Native and synchronous copy of data and VMs on two separate nodes, in real time
- Automatic migration of VMs without any data loss
- Full SSD storage
- Inter-VMs network n\*10G
- 99.99% SLA

## 1.2 Proposed platforms

Each Customer platform will be hosted in a distinct dedicated and private cloud, with private, dedicated and guaranteed 24/7 resources (no overbooking).

Backups will be stored on a backup infrastructure distinct from the hosting infrastructure hardware.

In the event of increased needs (i.e. increased number of users) it would be possible to increase the hardware resources allocated to each private cloud, within a very short delay not longer than two weeks.

The initial platform "Plan A" will be composed of one virtual server where will be installed all the software and services.

The initial platform "Plan B" will be composed of:

- **Firewall server:** virtual server where will be installed PFSense firewall. This firewall will protect all the services of the Customer and will also allow to setup VPN if needed (ie. for Nextcloud application administration).

On this firewall will be implemented all the security rules and policies that TAS and the Customer will jointly define.

- **Nextcloud server:** virtual server where will be installed all Nextcloud software and plugins, as for the Customer requirements:
  - Nextcloud Deck
  - Nextcloud Talk
  - Nextcloud Calendar
  - Nextcloud Files
  - Nextcloud Circles
  - Collabora Online
  - Edit Files with LibreOffice
  - Files automated tagging
  - Approval
  - Two-factor authentication with login code sent to the user's mailbox unless Nextcloud SSO & SAML is configured)
  - Nextcloud SSO & SAML
  - Nextcloud Data Request

- Nextcloud Files Retention
  
- **ElasticSearch server:** virtual server where will be installed ElasticSearch, as to allow full-text document search on the Nextcloud database

## 1.3 Plan A

### 1.3.1 Installation and configuration

Service	Non-Recurring Charges
<b>Platform setup</b> Installation and configuration private cloud Installation and configuration of all the applications and services Configuration of private and public networks Configuration of security rules Configuration of all services through a a custom domain chosen and made available by the Customer Backups configuration Tests and adjustments	2 000 €

### 1.3.2 Hosting

Service	Recurring Charges
<b>Private cloud hosting</b> 4 CPU 8 GB RAM 50 GB SSD (OS and software) 100 GB disk space for files	2 000 € / year
<b>Backup</b> Volume source 150 GB Daily backup, retention 7 days	150 € / year
<b>Nextcloud licences</b> Nextcloud Files Standard Subscription 15 users	1 050 € / year

## 1.4 Plan B

### 1.4.1 Installation and configuration

Service	Non-Recurring Charges
<b>Platform setup</b> Installation and configuration of 3 servers: <ul style="list-style-type: none"> <li>- Firewall "PFSense" server</li> <li>- Nextcloud server</li> <li>- ElasticSearch server</li> </ul> Installation and configuration of all the applications and services Configuration of private and public networks Configuration of security rules Configuration of all services through a a custom domain chosen and made available by the Customer Backups configuration Tests and adjustments	<b>€ 6 000</b>

### 1.4.2 Hosting

Service	Recurring Charges
<b>Private cloud hosting</b> 22 CPU 52 GB RAM 200 GB SSD	<b>€ 7 500 / year</b>
<b>Backup</b> Volume source 200GB Daily backup, retention 15 days Monthly backup, retention 3 months	<b>€ 800 / year</b>
<b>Nextcloud licences</b> Nextcloud Files Premium Subscription (100 users) Nextcloud Groupware Subscription (100 users) Nextcloud Talk Subscription (100 users) Collabora Online Subscription (100 users)	<b>€ 11 400 / year</b>



### 1.4.3 Monitoring, supervision and administration

Service	Recurring Charges
<p><b>Monitoring and supervision 24/7, corrective maintenance</b></p> <p>3 servers:</p> <ul style="list-style-type: none"> <li>- Firewall "PFSense" server</li> <li>- Nextcloud server</li> <li>- ElasticSearch server</li> </ul> <p>Monitoring 24/7 of servers' resources (CPU, RAM, disk space, ping, private and public networks etc.)</p> <p>Monitoring 24/7 of services (PHP, MySQL, etc.)</p> <p>Alerts handling 24/7</p> <p>Analysis and diagnosis 24/7</p> <p>Corrective actions 24/7</p> <p>Corrective maintenance: corrective security updates/patches 24/7 (this includes installation of critical security updates/patches without undue delay)</p> <p>Access to TAS France support (based in Sophia Antipolis), 24/7, without any limitation or overcharging based on the number of interventions, nor the number of requests, nor the total duration of the intervention</p>	<p><b>€ 8 000 / year</b></p>
<p><b>Firewall administration 24/7</b></p> <p>Administration 24/7 of the firewall PFSense dedicated to the Customer platform:</p> <ul style="list-style-type: none"> <li>- Security rules management: analysis and diagnosis, creation, modification etc.</li> <li>- Users and VPN management: creation, modification, deletion</li> <li>- Access and security requirements definition and implementation</li> <li>- Access to TAS France support (based in Sophia Antipolis), 24/7, without any limitation or overcharging based on the number of interventions, nor the number of requests, nor the total duration of the intervention</li> </ul>	<p><b>€ 3 000 / year</b></p>

## 1.5 Available hosting options and upgrades

Service	Non-Recurring Charges	Recurring Charges
<b>TURN and HPB server</b> Virtual server for TURN and Talk High Performance Back-end Server resources: - 6 CPU - 10 GB RAM - 100 GB SSD		
Installation and configuration	€ 1 500	
Hosting		€ 1 500 / year
Monitoring and supervision 24/7		€ 3 000 / year
<b>Cloud resources upgrade</b>		
2 CPU		€ 150 / year
4 GB RAM		€ 300 / year
100 GB SSD		€ 350 / year
<b>Separate Recovery site (TAS datacenter, Milan-Italy)</b>		
Installation and configuration	€ 2 000	
2 CPU		€ 100 / year
4 GB RAM		€ 200 / year
100 GB HDD		€ 300 / year
Veeam licences (for virtual servers replication)		€ 100 / year / VM
Backup Volume source 200GB Daily backup, retention 15 days Monthly backup, retention 3 months		€ 800 / year

<b>Virtual server “Monitoring and supervision 24/7, corrective maintenance” (option for Plan A)</b>		
<p>Monitoring 24/7 of server’s resources (CPU, RAM, disk space, ping, private and public networks etc.)</p> <p>Monitoring 24/7 of services (PHP, MySQL, etc.)</p> <p>Alerts handling 24/7</p> <p>Analysis and diagnosis 24/7</p> <p>Corrective actions 24/7</p> <p>Corrective maintenance: corrective security updates/patches 24/7 (this includes installation of critical security updates/patches without undue delay)</p> <p>Access to TAS France support (based in Sophia Antipolis), 24/7, without any limitation or overcharging based on the number of interventions, nor the number of requests, nor the total duration of the intervention</p>		<p><b>€ 3 000 / year / VM</b></p>
<b>Preventive, Adaptive and Evolutive maintenance (option for Plan B)</b>		
<p>Preventive maintenance</p> <p>Acronis Advances Security license</p> <p>Acronis Advanced Management license</p> <p>Vulnerability scans</p> <p>Vulnerability remediation following vulnerability assessment (performed by the Acronis solution)</p> <p>Reporting on threats, patches and remediation</p>		<p><b>€ 900 / year / VM</b></p>
<p>Adaptive and Evolutive maintenance</p> <p>New features and releases updates management</p> <p>Installation of software generic new releases and updates (not related to security issues; without undue delay and not later than one month after release date)</p>		<p><b>€ 450 / year / VM</b></p>

## 1.6 Software options

Subscription	Users	User/year €
ONLYOFFICE 50 concurrent users, cluster	100	18,05
Nextcloud Outlook Add-in Premium Subscription	100	6,93
Nextcloud Files Premium Subscription	250	52,12
Nextcloud Groupware Subscription	250	11,14
Nextcloud Talk Subscription	250	15,84
Collabora Online Subscription	250	13,86
ONLYOFFICE 50 concurrent users, cluster	250	7,22
Nextcloud Outlook Add-in Premium Subscription	250	6,44
Nextcloud Files Premium Subscription	1000	30,91
Nextcloud Groupware Subscription	1000	8,35
Nextcloud Talk Subscription	1000	13,86
Collabora Online Subscription	1000	11,39
ONLYOFFICE 50 concurrent users, cluster	1000	6,74
Nextcloud Outlook Add-in Premium Subscription	1000	4,95

## 2 BILLING AND PAYMENT TERMS

TAS France shall commence a service billing as from the service handover date.

Customer will be invoiced quarterly for all amounts due.

The Recurring Fees are payable quarterly in advance.

Late payments hereunder will accrue interest at the official rate of interest.

### 3 SERVICE LEVEL AGREEMENT (“SLA”)

#### I. Service Availability

##### Definitions

- a. Availability of the hosting service: the hosting service is deemed to be “available” from the date of service handover, date to which the service will be provided and maintained in accordance with the specifications.
- b. Availability of IP transit service: a circuit is “available” when it allows signals to be transmitted in both directions. The circuit is “unavailable” when it is not transmitting signals in either one or both directions.
- c. Monthly billing period: refers to the periods of a calendar month starting on the first day of each month for the duration of this contract and used to calculate the Availability of the service.
- d. Downtime: the downtime corresponds to the cumulative duration of incident tickets opened by the Customer during a given month. If two or more incident tickets overlap, the overlap time is only counted once

##### Rate of availability

The following equation will be used to calculate the availability rate of the service. The hours shown refer to the number of hours (rounded to the nearest hour) during the applicable monthly billing period:

$$\frac{\text{(Total hours – Total hours of unavailability)}}{\text{Total hours}} \times 100$$

##### Commitment

TAS France is committed to guaranteeing an availability rate of its services above 99.99%.

##### Service credits

If it occurs that service availability is under 99.99% during a monthly invoicing period, the Customer shall be entitled to the service credits defined below, calculated on the basis of the Monthly Recurring Charge applicable to the service:

<b>Service Availability during the Monthly Invoicing Period</b>	<b>Service Credits: % of Monthly Recurring Charge</b>
99.99 % - 99.90 %	2 %
99.89 % - 99.50 %	4 %
99.49 % - 99.00 %	6 %
98.90 % - 98.00 %	8 %
97.90 % - 96.50 %	10 %
96.49 % - 95.00 %	15 %
< 95.00 %	20 %

## II. Guaranteed response time

### Definition

The guaranteed response time corresponds to the maximum time available to TAS France to intervene following an event for which it is responsible, from the moment when an incident ticket notifying the unavailability of the service has been opened by the Customer.

Scheduled maintenance operations and transmission problems occurring on the Customer's access links are excluded from the guaranteed response time.

### Commitment

TAS France is committed to guaranteeing a maximum response time of 1 hour.

### Service credits

If it occurs that TAS France does not respect this commitment during a monthly invoicing period, the Customer shall be entitled to the service credits defined below, calculated on the basis of the Monthly Recurring Charge applicable to the service:

<b>Response time</b>	<b>Service Credits: % of Monthly Recurring Charge</b>
1h – 1h30	2%
1h30 – 2h	5%
2h – 2h30	10%
> 2h30	20%

## III. Guaranteed fault repair time

### Definition

The guaranteed fault repair time corresponds to the maximum time available to TAS France to restore the availability of a service, following an event for which it is responsible, from the moment when an incident ticket notifying the unavailability of the service has been opened by the Customer.

Scheduled maintenance operations and transmission problems occurring on the Customer's access links are excluded from the guaranteed response time.

### Commitment

TAS France is committed to guaranteeing a maximum fault repair time of 4 hours.

### Service credits

If it occurs that TAS France does not respect this commitment during a monthly invoicing period, the Customer shall be entitled to the service credits defined below, calculated on the basis of the Monthly Recurring Charge applicable to the service:

<b>Fault repair time</b>	<b>Service Credits: % of Monthly Recurring Charge</b>
4h – 6h	2 %
6h – 8h	5 %
8h – 10h	10 %
> 10h	20 %

## IV. Network latency

### Definition

The network latency commitment is measured based on the average network latency over a calendar month for one-way traffic from TAS France network equipment.

### Commitment

TAS France is committed to guaranteeing these network latencies:

- Intra-Europe: 50 ms
- USA and Canada: 80 ms

### Service credits

If it occurs that TAS France does not respect this commitment during a monthly invoicing period, the Customer shall be entitled to the service credits defined below, calculated on the basis of the Monthly Recurring Charge applicable to the service:

Network latency above the commitment	Service Credits: % of Monthly Recurring Charge
0.1 ms – 5 ms	2 %
5.1 ms – 10 ms	4 %
10.1 ms – 15 ms	6 %
15.1 ms – 20 ms	8 %
20.1 ms – 25 ms	10 %
25.1 ms – 30 ms	15 %
> 30.1 ms	20 %

## V. Packet delivery ratio

### Definition

The packets delivery ration commitment is measured according to the average number of IP packets which, during a calendar month, pass through TAS France network to the Customer network equipment.

### Commitment

TAS France is committed to guaranteeing a packets delivery ratio above 99.9%.

### Service credits

If it occurs that TAS France does not respect this commitment during a monthly invoicing period, the Customer shall be entitled to the service credits defined below, calculated on the basis of the Monthly Recurring Charge applicable to the service:

Packets delivery ration	Service Credits: % of Monthly Recurring Charge
99.90 % - 99.80 %	2 %
99.79 % - 99.50 %	4 %
99.49 % - 99.00 %	6 %
98.90 % - 98.00 %	8 %
97.90 % - 96.50 %	10 %
96.49 % - 95.00 %	15 %
< 95.00 %	20 %



## VI. Service credits calculation

The service credits will be calculated monthly.

When the monthly billing period includes an incomplete month, any service credit will be applied on a pro rata basis of the monthly fees.

## VII. Exclusion of Compensation

The Customer shall not be entitled to the service credits in the event of faults or malfunctions caused by the following:

- a. The fault or negligence of the Customer, its employees, representatives or contractors;
- b. The failure of equipment that is owned and/or managed by the Customer or any of its providers other than TAS France;
- c. A fault or problem relating to the equipment connected on the Customer side of the demarcation point of the TAS France Service;
- d. Every event described in article VIII "Force Majeure";
- e. Maintenance during a maintenance scheduled by TAS France, for which the Customer will have been notified at least 1 week (7 days) in advance.

## VIII. Force Majeure

TAS France is not responsible for the payment of compensation for losses or damages that could be incurred by the Customer if the ability of TAS France to meet its commitments has been thwarted or significantly hampered by unforeseen circumstances or circumstances that may be considered reasonably beyond the control of TAS France ("Case of Force Majeure").

The conditions for such an exemption include, as a non-exhaustive list: social conflicts, war, revolution or riot, sabotage, mobilization or other military orders, natural disasters (earthquake, fire, flood etc.), general shortage of goods or transport, laws or official restrictions other than applicable EU legislation and effects from CJEU case law, global failure of Internet.

If any such event, loss, damage or delay shall occur, TAS France will strive to the best of its abilities to prevent or minimize the effects of the said Force Majeure event and to meet its obligations, and will promptly advise the Customer in writing of the extent and estimated duration of this inability to fulfil its obligations.

## IX. Service credits limitations

The total amount that may be credited to the Customer under this agreement in any given month is limited to 20% of the Customer's monthly recurring charge for the affected service.

The total amount that may be credited annually to the Customer is limited to 20% of the total amount of the price payable by the Customer for all services, during a period of 12 months.

The Customer must ask in writing for all service credits applicable due to the insufficient levels of service within twenty-one (21) working days following the date on which the Customer could reasonably be aware of this insufficiency. To be entitled to a service credit, the Customer must make the application in writing to TAS France. If TAS France needs additional information from the Customer the Customer shall be entitled to claim a service credit only when TAS France has received all the information which it has justifiably requested.

## X. Report and duration of faults

### Report of faults

The Customer must ask in writing for all service credits applicable due to the insufficient levels of service within twenty-one (21) working days following the date on which the Customer could reasonably be aware of this insufficiency. To be entitled to a service credit, the Customer must make the application in writing to TAS France. If TAS France needs additional information from the Customer the Customer shall be entitled to claim a service credit only when TAS France has received all the information which it has justifiably requested.

All suspected failures must be reported to TAS France, applying the procedures detailed in the "Customer Support" (chapter 4 of this agreement).

When notifying a failure, the Customer must identify the affected service and provide details of this failure.

### Fault duration

The exact duration of the fault will be calculated based on the time elapsed between the issuing of the default ticket (automatic issuing, following receipt by TAS France of the failure notification sent by the Customer by email), and the time when the service is restored.

## **XI. Liability and compensation**

The service credits will represent the one and only compensation in the event that the commitments of the SLA will not be respected by TAS France.

TAS France excludes all other liability and compensation towards the Customer, for non-respect of SLA commitments.

## 4 CUSTOMER SUPPORT

### Management and escalation of problems

The procedure for problems management and escalation is activated by an alarm generated by the supervision systems, the proactive management procedure or a Customer call or email to the TAS France customer support.

In the event of a service fault Customer may contact TAS France customer support as follows:

- Monday to Friday during working hours (9h00-12h30 and 14h00-18h00 CET): by phone at +33 (0)825 56 34 00 or by email at [support@tasfrance.com](mailto:support@tasfrance.com)
- Monday to Friday outside working hours, Saturday, Sunday and public holidays by phone at +33 (0)6 69 05 55 65 or by email at [noc@tasfrance.com](mailto:noc@tasfrance.com)

After receipt of this call, TAS France customer support shall open, if applicable, an incident ticket, marking the start of the partial or total unavailability of the service. TAS France customer support shall take the necessary measures to resolve the incident.

The incident is treated according to its priority and the corresponding operational procedure.

### Responsiveness

The following times are the references for measuring the responsiveness of TAS France customer support.

Time	Definition	Value
Acknowledgement of receipt time	Time between notification of the fault and the creation of an incident ticket (including initial diagnosis time)	Immediate (automatic creation from the email sent by the Customer)
Reaction time	Time between the creation of the incident ticket by the TAS France customer support operator and the activation of the corrective action (escalation, maintenance, feedback to Customer)	Varies according to the priority of the incident ticket (see following section)

**Priority codes**

TAS France customer support assigns a priority to every incident ticket of the Customers when this ticket is opened.

The following table contains the definitions of the priority codes:

Priority	Definition	Examples	Reaction time
1	<b><u>Service fault</u></b> - Problem affecting critical business processes - Failure without possible bypass	- Server outage - Network outage - Security alert (intrusion, virus)	15 minutes
2	<b><u>Degraded service</u></b> - Degraded performance - Critical business processes operational - Possible workaround	- Poor performances	15 minutes
3	<b><u>Partial failure of service</u></b> - Problem affecting secondary, but important, business processes - Possible workaround	- Loss of redundancy of a system tolerant to faults - Non-critical server outage (i.e. backup)	30 minutes
4	<b><u>Planned maintenance/service interruption</u></b> - Planned maintenance causing service interruption	- Update or installation of software/hardware - Request for minor configuration modification	1 working day
5	<b><u>Request for modification</u></b> - Every request outside the scope of the architecture	- Service level modifications - Request for proposal - Request for consultation	2 working days

The reaction time does not correspond to the recovery time.

**Time slots**

Operational activities depend partially on the time of day, operational coverage will vary according to different time slots.

Time slot	Description	Day	Hours (CET)
24/7	Monitoring and supervision services	7/7	24/24
Working hours	Full service in accordance with the official working hours in Sophia Antipolis. Technical staff available via the customer support	Mon - Fri	9:00 – 18:00
Standbys	Technical staff available via the standby service	Mon – Fri Sat – Sun	18:00 – 9:00 0:00 – 24:00
Event-related standbys	At least one system/server manager or one operator or one service provision specialist is available via the standby service and/or is onsite.	Events	00:00-24:00

**Support service**

A telephone number and an email address are available to manage all types of problems.

TAS France customer support will be in charge of the incident throughout the entire incident resolution cycle.

Reported and detected problems will be logged in the incident ticket management system.

**Service fault**

A service fault is defined as:

- an unavailability of service to end users, due to failure of any component of the system
- general performance outside predefined levels of service

The service may be interrupted in the following circumstances:

**I. Planned maintenance**

The maintenance will be planned jointly with the Customer and a minimum notice of 1 week (7 days) will be given. To the extent possible, scheduled service interruptions will be provided outside of normal business hours.

**II. Risk on data integrity or security**

Systems can be shut down with a very short notice when the integrity or the security of the system or data is at risk due to software or hardware problems or security intrusion or virus etc..



EUROPEAN COMMISSION  
DIRECTORATE-GENERAL INFORMATICS

Directorate A - Strategy & Resources  
DIGIT A3 - ICT Procurement & Contracts

**DYNAMIC PURCHASING SYSTEM  
FOR  
CLOUD SERVICES**

REFERENCE  
**DIGIT/A3/PR/2018/035  
CLOUD II DPS 1**

—

**ANNEX VIII**

**CLOUD TERMS AND CONDITIONS**

## TABLE OF CONTENTS

1	COMMON PROVISIONS .....	3
1.1	Definitions.....	3
1.2	Compliance and Design .....	7
1.3	Service Levels, Quality and Standards .....	9
1.4	Cooperation.....	10
1.5	Integration and Compatibility.....	11
1.6	Product Use and Life.....	12
1.7	Change and replacement management.....	12
1.8	Data Protection.....	14
1.9	Security and Security Incident Management .....	18
1.10	Audit by the Contractor.....	21
1.11	Intellectual property and related rights .....	22
1.12	Documentation .....	24
1.13	Identifiers .....	26
1.14	Confidentiality .....	27
1.15	Third party Initial Vendor or right holder.....	29
1.16	Invoicing .....	30
2	LICENSED SOFTWARE PRODUCTS .....	32
2.1	Delivery.....	32
2.2	Acceptance .....	33
2.3	Guarantee and Maintenance.....	34
2.4	Software trial.....	37
2.5	Intellectual Property Rights .....	38
2.6	Entitlement reporting .....	39
3	CLOUD SERVICES .....	40
3.1	Provision and Service Levels.....	40
3.2	Ownership and Intellectual Property.....	40
3.3	Consequences of termination.....	41
3.4	Data portability .....	41
3.5	Cooperation and information .....	42
3.6	Location .....	42
4	SUPPORT SERVICES.....	43
4.1	Stability and performance of Support Services.....	43

## 1 COMMON PROVISIONS

### 1.1 Definitions

1.1.1 For the purpose of the Contract, the following definitions apply:

**“Acceptance Document”**: Document signed by the Contracting Authority, evidencing conformity of the delivered Products or Deliverables. The Acceptance Document can take the form of a certificate of conformity, a task acceptance form or any other document that, in accordance with the terms of the Contract, is used to evidence conformity of the Products and/or the Deliverables.

**“Adaptive Maintenance”**: All operations as detailed in the Contract undertaken to modify a Product in order to ensure its continued functioning, in normal operating condition, in a changed or changing environment without changing its functionalities.

**“Cloud Services”**: Services which enable ubiquitous, scalable, convenient, on-demand network access to a shared elastic pool of configurable physical or virtual resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or Contractor interaction.

**“Contract”**: All contractual documents (for example, contract and annexes), including these Cloud Terms and Conditions, relating to the relationship between the Contracting Authority and the Contractor formed therein.

Any reference to the Contract should be understood as a reference to any of the remaining contractual documents constituting the Contract, which may include, without being limited to, contract, service level agreement, and tender specifications.

**“Contracting Authority's Staff”**: Staff of the Contracting Authority, whether governed by Regulation No 31 (EEC), 11 (EAEC), which sets out the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community, or otherwise employed or hired by the Contracting Authority.

**“Corrective Maintenance”**: All operations undertaken to detect, isolate and rectify any default, defect, deficiency, malfunctioning or nonconformity in order to restore a failed Product to normal operating condition, or to replace it.

**“Deliverable”**: Result defined in the Contract which must be produced by the Contractor in accordance with the terms of the Contract in the context of the provision of the Services.

**“Delivery Date”**: Date agreed between the Parties on which a Product, Deliverable or Service is to be delivered or provided to the Contracting Authority.

**“Delivery Lead Time”**: Period, starting at the date of receipt of the signed Contract by the Contractor, before the end of which a Product, Deliverable or Service must be delivered or provided to the Contracting Authority.



**“Delivery Note”:** Note in writing which contains the particulars of the delivered Products (including Contract reference(s) and date(s), ordering entity and address, Delivery Lead Time, Delivery Date, actual delivery date, and particulars of delivered Products and their quantities) or Deliverables (including Contract reference(s) and date(s), ordering entity and address, Delivery Date, actual delivery date, and particulars of the delivered Deliverables), to be provided by the Contractor or its carrier along with the delivered Products or Deliverables. The Delivery Note can take the form of a consignment note or any other document that, in accordance with the terms of the Contract, is used to evidence the delivery of the Products and/or Deliverables.

**“Documentation”:** Instructions and manuals relating to the Product(s) and/or Service(s), whether intended for support/technical staff or for end-users, and whether provided in printed or in electronic form.

**“Evolutive Maintenance”:** All operations as detailed in the Contract undertaken to enhance the functionalities of a Product, including but not limited to adding additional functionalities or replacing existing functionalities with other functionalities, in order to increase the Product's performance even in the absence of faults, deficiency, malfunctioning or nonconformity.

**“Hardware”:** Any tangible asset resulting from a manufacturing process and consisting of computer, media, electronic communications or other electronic equipment, whether or not it embeds Software, as well as all accessories related to such equipment.

**“Infrastructure as a Service” or “IaaS”:** Cloud Service that provides the capability to the Contracting Authority to provision processing, storage, networks, and other fundamental computing resources where the Contracting Authority (i) is able to deploy and run arbitrary software, which can include operating systems and applications; and (ii) does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications, and possibly limited control of select networking components (such as host firewalls).

**“Initial Vendor”:** Person who exploits a Product or a Service, which is to be provided under the Contract, under its trademark or sign, or under the trademark or sign of one of its related companies.

**“Internal Use”:** Use, including via on-line remote access from outside the premises of the Contracting Authority, by Contracting Authority's Staff or by other persons acting in fulfilment of a direct or indirect contractual obligation towards the Contracting Authority, be it as a contractor, a subcontractor or personnel of such (sub)contractor, within the context of the fulfilment of their mission for the Contracting Authority.

**“Key Performance Indicators”:** Measurable targets serving as a reference to determine the level of performance of the Services to be provided by the Contractor, as determined in the Contract.

**“Licensed Software Product”:** Software of which intellectual property rights are held by the Contractor or a third party, whether customised or not to meet the Contracting Authority's specific requirements, and licensed to the Contracting Authority under the Contract.

**“Maintenance”**: Corrective Maintenance, Preventive Maintenance, Adaptive Maintenance and Evolutive Maintenance, either alone or in combination with each other.

**“New Release”**: Revision of an existing version of Software, usually amending the reference to the Software’s version from for example version 0.1 to version 0.2.

**“New Version”**: New version of Software, usually amending the reference to the Software’s version from for example version 0.1 to version 1.1.

**“Normal Working Days”**: Monday to Friday inclusive, except for public holidays for the institutions of the European Union held in the place of delivery of the Products or provision of the Services, as published in the Official Journal of the European Union.

**“Normal Working Hours”**: 7 a.m. to 8 p.m. on Normal Working Days.

**“Notification” or “Notify”**: Any form of communication between the Parties made in writing, including by electronic means.

**“Notification of Default”**: Notification by the Contracting Authority to the Contractor of a default in a delivered Product or Deliverable, preventing its conformity with the Contract.

**“Personnel”**: Persons employed directly or indirectly or contracted by the Contractor to implement the Contract.

**“Platform as a Service” or “PaaS”**: Cloud Service that provides the capability to the Contracting Authority to deploy, manage and run onto the cloud infrastructure applications created or acquired by the Contracting Authority using one or more programming languages, libraries, services, execution environments and tools supported by the Contractor. The Contracting Authority does not manage or control the underlying cloud infrastructure including the network, servers, operating systems, or storage, but has control over the deployed applications and possible configuration settings for the application-hosting environment.

**“Preventive Maintenance”**: All operations as detailed in the Contract undertaken to prevent faults, deficiencies, malfunctioning or nonconformities from occurring, or to prevent them from developing into major defects, and to maintain the Product in normal operating condition. Preventive Maintenance includes but is not limited to systematic inspection, tests, measurements, adjustments, correction, parts replacement, and cleaning.

**“Product”**: Product as described in the Contract, consisting of one or more tangible or intangible asset(s) resulting from a manufacturing or development process.

Products include Hardware Products and Licensed Software Products or parts thereof.

Hardware Products and Licensed Software Products are considered as supplies when the latter term is used in the Contract.

**“Security Incident”**: Any event having or threatening to have an adverse effect on the security of network and information systems, including but not limited to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to data, including but not limited to personal data, transmitted, stored or otherwise processed.

**“Service Levels”**: the level of performance of the Services to be provided by the Contractor

**“Services”**: Services as described in the Contract, involving the application of business and technical expertise to enable the Contracting Authority in the creation, management and optimisation of or access to information and business processes.

By default, Services include all Deliverables that are not Products.

**“Software”**: Any intangible asset resulting from a development process and consisting of a computer program or a part thereof.

**“Software as a Service” or “SaaS”**: Cloud Service that provides the capability to the Contracting Authority to use applications provided by the Contractor running on a cloud infrastructure. The applications are accessible from various devices of the Contracting Authority through either an interface, such as a web browser or a program interface. The Contracting Authority does not manage or control the underlying cloud infrastructure including the network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

**“Support Services”**: All standalone or ancillary support, assistance, planning, maintenance, training, consulting, managing, auditing and/or integration Services related to information technology, as further described in the Contract.

**“EU Protected Material”**: Software or other protected material for which the intellectual property rights are the property of the Contracting Authority, or which have been licensed to the Contracting Authority by third parties. EU Protected Material also includes data for which the Contracting Authority or another EU institution, body or agency determines the purposes and means of the processing.

1.1.2 For the purpose of these Cloud Terms and Conditions, capitalised terms which are not defined in Article 1.1 shall have the meaning as defined in the other contractual documents which are part of the Contract.

1.1.3 For the purpose of these Cloud Terms and Conditions, the term **“Contracting Authority”** shall be understood as the legal person(s) constituting the contracting authority, as defined in the other parts of the Contract, or of which such contracting authority is part.

## **1.2 Compliance and Design**

- 1.2.1 The Contractor shall comply with applicable laws, including but not limited to laws in relation to privacy and data protection, (data) security, environmental protection and sustainability, and incident detection and handling, as amended from time to time and interpreted by competent authorities.
- 1.2.2 The Contractor shall comply with fundamental ethical rules and principles recognised at EU and international level.
- 1.2.3 The Contractor shall perform its obligations under the Contract in such a way as to enable the Contracting Authority to comply with the laws applicable to it, including but not limited to Regulation 2018/1725<sup>1</sup>, as amended from time to time and interpreted by competent authorities.
- 1.2.4 The Contractor shall ensure that the Products or Services are designed, developed and provided in compliance with applicable laws. In case of improvements or updates necessary to accommodate the application of any new applicable laws, the Contractor shall ensure that the Products or Services are improved or updated, at no extra cost to the Contracting Authority. The Contractor shall document in an internal file all measures taken to comply and demonstrate compliance with this Article 1.2 and shall make such file available to the Contracting Authority upon the latter's first request, notably for the purpose of checks and audits.
- 1.2.5 The Contracting Authority and the Contractor shall promptly Notify each other of any existing or new legislation applicable to the Contractor preventing it from fulfilling the instructions received from the Contracting Authority and the obligations provided under the Contract as soon as either Party becomes aware of the legislation, even before its entry into force. In such event the Contracting Authority shall be entitled to amend its instructions, or suspend, or terminate the Contract.
- 1.2.6 The Contractor shall protect and indemnify the Contracting Authority against all third party claims or actions alleging a breach of any third party rights and/or infringement of any applicable law, resulting from the provision by the Contractor and/or use by the Contracting Authority of the Products and Services under the Contract.
- 1.2.7 The Contracting Authority reserves the right to conduct its own defence or to negotiate its own settlement, at its own discretion. In such case, the Contractor shall be liable for all reasonable legal expenses, including lawyers and experts fees. Upon first demand of the Contracting Authority, the Contractor shall, at its own and sole expense, voluntarily intervene in any pending litigation resulting from the provision by the Contractor and/or use by the Contracting Authority of the Products and Services under the Contract.

---

<sup>1</sup> Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

- 1.2.8 The Contractor shall be liable for any claim or payment arising out of any judgment, ruling or settlement relating to third party claims or actions alleging a breach of any third party rights and/or infringement of any applicable law, resulting from the provision by the Contractor and/or use by the Contracting Authority of the Products and Services under the Contract, except for the payment of a settlement made by the Contracting Authority without the Contractor's written consent. Such consent shall not be unreasonably withheld, conditioned or delayed.
- 1.2.9 The Contractor shall hold the Contracting Authority harmless from and against any damages suffered by the Contracting Authority caused by a breach of this Article 1.2.

### **1.3 Service Levels, Quality and Standards**

#### *1.3.1 Service Levels*

1.3.1.1 The Service Levels as well as the methods of measuring the performance against such Service Levels are defined in the Contract, usually by reference to Key Performance Indicators.

1.3.1.2 The Contractor shall provide all Services in accordance with the Service Levels and in any event with a level of accuracy, quality, completeness, responsiveness and efficiency that at least meets or exceeds the Service Levels.

1.3.1.3 The Contractor shall provide to the Contracting Authority reports on the Contractor's compliance with the Service Levels on a periodic basis as agreed between the Parties in the Contract.

1.3.1.4 Where relevant and to the extent defined in the Contract, if the Contractor fails to fulfil its obligations under the Contract, including the Service Levels, the Contractor shall make available to the Contracting Authority an equivalent replacement solution. The cost of such equivalent solution shall be borne by the Contractor, unless the latter can demonstrate that the failure is attributable to the Contracting Authority. The Contract shall determine the consequences in the event that the Contractor does not or cannot provide an equivalent solution or continues to fail to meet the Service Levels. Such consequences may include, but are not limited to, the implementation of an improvement plan, credits towards Products or Services, termination of the Contract, or the application of liquidated damages.

#### *1.3.2 Quality management and assurance*

1.3.2.1 The Contractor shall provide the Products and/or Services and perform the Contract in accordance with the state of the art, technical norms, standards and procedures based on best professional practice.

1.3.2.2 Any Product and/or Service provided under the Contract shall be 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 specific request pursuant to which the Contract has been entered into.

**1.4 Cooperation**

- 1.4.1 The Contracting Authority and the Contractor shall cooperate and exchange all data and information necessary and useful for the Contractor to provide the Products and Services under the Contract.
- 1.4.2 Throughout the term of the Contract, the Parties shall maintain the required level of information and make it available to the other Party for the purpose of providing the Products and Services. The updating of information shall not give rise to any payment.
- 1.4.3 The Contractor shall assist and advise the Contracting Authority on the use of the Products and Services provided under the Contract.
- 1.4.4 The Contracting Authority and the Contractor shall Notify each other of any factor likely to impair or delay the proper execution of the Contract.

## **1.5 Integration and Compatibility**

- 1.5.1 The Contractor shall ensure and guarantee that the Products and Services are developed and provided and that the Contract is performed in full knowledge and consideration of the Contracting Authority's evolving multi-manufacturer information technology environment, architecture and physical premises.
- 1.5.2 The Contractor shall be responsible for Product integration as regards its inclusion in the Contract, its operation in the Contracting Authority's environment and the prompt and appropriate introduction of New Versions.
- 1.5.3 The Contractor must perform its obligations under the Contract in such a way as to ensure that the Contracting Authority may add or connect to its information technology environment compatible products or services of any origin
- 1.5.4 Where it has been agreed between the Parties that interfaces need to be implemented, the Contractor shall not modify such interfaces without the Contracting Authority's written agreement, which shall not be unreasonably withheld.
- 1.5.5 Even if a Product or Service is approved by the Contracting Authority, any incompatibility with previous Products or Services 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 Contracting Authority.



## **1.6 Product Use and Life**

### *1.6.1 Product Use*

1.6.1.1 From the date of delivery, the Contracting Authority may make unrestricted use of the Products under normal operating conditions. If the Products are rented, leased or licensed, the right of use applies for the duration specified in the Contract.

1.6.1.2 The Contracting Authority may use any Products provided under the Contract for services it is carrying out for other EU institutions, agencies or bodies.

### *1.6.2 Product Life*

1.6.2.1 As soon as the Contractor becomes aware that one or more Products are or will be declared end-of-life, and will therefore no longer be manufactured, provided or supported, it shall Notify the Contracting Authority of this fact. Unless otherwise agreed in the Contract, in such Notification, the Contractor shall propose a replacement of the Products that are or will be declared end-of-life, subject to the conditions laid down in Article 1.7.3.

1.6.2.2 The Contractor commits that both the originally provided Products and the replacement Products shall remain available for a reasonable period of time before being declared end-of-life, in accordance with the market standards for the relevant category of products or services. The Contract may define the exact duration of the period of minimum availability.

## **1.7 Change and replacement management**

1.7.1 Either Party may, at any time during the duration of the Contract, Notify the other Party of a request to change Products and/or Services originally provided under the Contract, or of a request to replace them with products or services of similar nature. The Contractor shall Notify the Contracting Authority of such request at least 12 months before a change or replacement..

1.7.2 Following a change or replacement request in accordance with Article 1.7.1, the Contractor shall make a change or replacement proposal, which shall at the minimum mention the specification of the proposed changed or replacement products or services, and the price of the changed or replacement products or services.

1.7.3 Any change or replacement in accordance with Article 1.6.2 or this Article 1.7 is subject to the following conditions:

- the changed or replacement products or services can function in the same operational environment as the originally provided Products or Services, with no loss of performance or IT security requirements degradation for the Contracting Authority;

- the changed or replacement products or services shall comply with the technical specifications and the minimum requirements defined in the Contract;
- the change or replacement must not, directly or indirectly, cause a reduction of the functionalities or characteristics of the originally provided Products or Services;
- the change or replacement must not entail any additional cost to the Contracting Authority;
- the price of the changed or replacement products or services shall not be higher than the price of the originally provided Products or Services;
- unless the originally provided Products are declared end-of-life and will therefore no longer be manufactured, provided or supported, the Contractor shall specifically demonstrate that the change or replacement will be beneficial to the Contracting Authority.

1.7.4 In the event the request to change or replace Products and/or Services is made by the Contracting Authority and that the Contractor is unable or unwilling to make a change or replacement proposal, the Contractor shall provide without undue delay a justification for the Contracting Authority to assess.

1.7.5 The Contracting Authority shall, at its own discretion, approve or refuse any change or replacement proposal or justification provided in accordance with Article 1.7.4. The Contracting Authority shall Notify the Contractor of its decision.

1.7.6 Upon request of the Contracting Authority, the Contractor shall provide the Contracting Authority with all necessary information, including but not limited to demonstration Hardware devices, Software trials, price justification, demonstrations, and documentation, required by it to take a decision about whether or not to approve the change or replacement proposal.

1.7.7 In the event the Contractor has Notified a change or replacement in accordance with Article 1.6.2 or Article 1.7.1, the Contractor shall be liable for any expenses made to manage the change or replacement.

## **1.8 Data Protection**

1.8.1 In addition to the obligations related to data protection in the Contract, including but not limited to the details of the personal data processing activities included in the Contract, the Contractor, acting as data processor or subprocessor, shall:

- ✓ not process personal data in any way or any form (including in pseudonymised form and when they have been transformed in the form of anonymous or anonymised data) on its own behalf or on behalf of third parties;
- ✓ not have or exercise any control over the purpose(s) of the processing of personal data or the essential elements of the means of the processing;
- ✓ not independently take decisions regarding the use, the storage or the communication of personal data processed under the Contract, unless and to the extent determined in a data processing agreement or instructed by the Controller;
- ✓ not perform or allow to be performed any processing (including but not limited to copying, printing, forwarding, enriching, modifying, etc.) of or with the personal data processed unless and to the extent necessary for the performance of the Contract, or as agreed in writing between the Parties;
- ✓ deal promptly and properly with all inquiries from the Controller or the Contracting Authority as the case may be relating to the processing of the personal data by the Contractor;
- ✓ ensure that mechanisms are in place for secure logging of processing activities performed on personal data;
- ✓ assist the Controller or the Contracting Authority as the case may be in any cooperation with the competent data protection authority(ies), including the European Data Protection Supervisor, in the performance of the tasks of the foregoing;
- ✓ inform without delay the Controller of any request relating to the exercise of data subjects rights received directly from a data subject, and not reply to such request unless otherwise instructed by the Controller;
- ✓ provide the Controller or the Contracting Authority as the case may be with the necessary information, tools, and assistance to manage any request made by data subjects exercising their rights,
- ✓ inform the Controller without delay of any incident where the confidentiality, integrity or availability of personal data have been compromised or could reasonably be compromised, and provide it with assistance for compliance.

1.8.2 The Contractor and its subprocessors shall not give access to or disclose any personal data processed on behalf of the Contracting Authority or the Controller, actively or passively, intentionally or unintentionally, to any authorities, or legal or natural persons (collectively referred to as third parties) except on instructions from the Controller, unless required to do so by Union or Member State law, as long as the latter is compliant with the

requirements of Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.

- 1.8.3 In case the Contractor and any subprocessor receive a request for disclosure of personal data from a third party, they shall deny the request and redirect the requesting third party to seek access to this data directly from the Controller, in which case the Contractor may provide the Controller's or the Contracting Authority's basic contact information to the third party. In such a case, no other disclosures of personal data by the Contractor and its subprocessors shall take place without being authorised by the affected Controller.
- 1.8.4 The Contractor shall Notify the Controller of any legally binding request for disclosure made by any law enforcement authority, including from non-EU countries, promptly and without undue delay. If the Contractor and its subprocessors are prohibited from notifying the Controller, the Contractor and its subprocessors will use their best efforts to obtain the right to waive this prohibition in order to communicate as much information as they can and as soon as possible, and be able to demonstrate that they did so.
- 1.8.5 To the greatest extent permitted under applicable law, the Contractor shall appeal any legally binding request to disclose the personal data by exhausting all available legal remedies. The Contractor and its subprocessors shall ensure that they are able to demonstrate that they did so.
- 1.8.6 The Controller may request information from the Contractor once a year on whether any disclosures of personal data have taken place and if so, what action was taken in response.
- 1.8.7 In addition to the obligations related to data protection in the Contract, in the event that the Contractor relies on a subprocessor, the Contractor shall:
- ensure that it has previously informed the Controller of its plans to rely on a subprocessor;
  - ensure that it has performed a due diligence in order to ensure that the subprocessor provides sufficient assurance to act on its behalf and to implement the necessary technical and organisational data protection measures;
  - ensure that it has given comprehensive information on the prospective subprocessor, including on its capacity of providing sufficient assurance and its future role in the provision of Products and/or Services;
  - ensure that it has obtained prior specific or general written authorisation from the Controller; and
  - ensure, monitor and control that the subprocessor provides at least the same level of protection for the personal data and the fundamental rights and freedoms of data subjects as the Contractor under the Contract.

- 1.8.8 If the Contractor subcontracts part(s) or all of the processing of personal data to a third party, it warrants that each third party, including subcontractors, is contractually subject to at least the same obligations as those the Contractor is subject to toward the Contracting Authority and other parties as the case may be under this Contract. At the first request of the Contracting Authority, the Contractor shall provide the document(s) providing evidence of this warranty.
- 1.8.9 The Contractor may not transfer any personal data to a country outside the European Economic Area, unless the Controller has given its prior written authorisation to such transfer and the transfer takes place in compliance with the conditions of under Chapter V of Regulation 2016/679 and Chapter V of Regulation 2018/1725.
- 1.8.10 In case of termination of the contractual relationship between the Parties, or in the event that the Contractor is not entitled anymore to process personal data on behalf of the Controller, the Contractor shall, at the choice of the Controller:
- ✓ provide the ability to retrieve all personal data in a structured and widely-used format, to the Controller or to any EU institution or third party selected by the Controller, within a period agreed upon between the Parties; or
  - ✓ delete effectively all personal data, and all copies and extracts thereof.
- 1.8.11 The Contractor shall ensure that the personal data is kept safe and secure until it has been returned or deleted.
- 1.8.12 In the event of deletion or return of personal data as requested by the Controller under this Contract, the Contractor shall deliver a statement certifying that:
- ✓ all personal data and all copies and extracts thereof have been fully and permanently deleted or returned from any hardware or storage media (including but not limited to USB stick, server, and backup copies);
  - ✓ any files or data resulting from the personal data originally communicated by the Controller or the Contracting Authority have also been fully and permanently deleted or returned from any hardware or storage media;
  - ✓ any paper copy of the personal data and any document that contains the personal data has been deleted or returned; and
  - ✓ any subcontractors have been requested to undertake the same measures and have certified in writing that the personal data has been deleted or returned.
- 1.8.13 The Contractor must allow, contribute to and duly cooperate with audits by the Controller or the Contracting Authority of its data processing activities, in accordance with the applicable data protection legislation, including but not limited to Regulation 2018/1725, as amended from time to time. Contribution from the Contractor must be in principle free of charge, unless agreed specifically in the Contract. The audit may be carried out by a third

party selected by the Controller or the Contracting Authority, in possession of the required professional qualifications and bound by a duty of confidentiality. Contribution from the Contractor and its subcontractors is also requested for audits launched by the Controller, the Contracting Authority, or the European Data Protection Supervisor, of the measures taken by the Contractor and its subprocessors to comply with their obligations upon termination of the personal data processing activities.

- 1.8.14 The Contractor acknowledges that the European Data Protection Supervisor has the right to conduct a visit, an audit or an inspection of the Contractor, and of any subcontractor, under the same conditions applicable to an audit of the Controller or the Contracting Authority itself under the applicable data protection legislation, including but not limited to Regulation 2018/1725, as amended from time to time.
- 1.8.15 In the event that the Contractor acts as a reseller for an Initial Vendor which will process personal data as data processor or subprocessor, the Contractor shall ensure that the Initial Vendor concludes a data processing agreement as required by Article 29 of Regulation 2018/1725 directly with the Controller or the Contracting Authority as the case may be, and that all personal data protection requirements set out in the Contract are imposed upon the Initial Vendor. In any event, the Contractor shall indemnify the Controller or the Contracting Authority for any damage and claims that may arise from the non-compliance by the Initial Vendor with such data processing agreement and/or the personal data protection requirements set out in the Contract.
- 1.8.16 Any deviation from or infringement of data protection obligations, including but not limited to the provisions of this Article 1.8, may be a ground for the Contracting Authority to terminate the Contract with immediate effect, without prejudice to possible damages.

## 1.9 Security and Security Incident Management

### 1.9.1 Security

1.9.1.1 When performing tasks for the Contracting Authority in execution of the Contract, the Contractor and its Personnel shall comply with the Contracting Authority's applicable security framework, as may be further defined in the Contract. Where applicable, this may include but is not limited to the following documents, as amended and replaced from time to time<sup>2</sup>:

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

1.9.1.2 In addition, the Contractor shall ensure that an appropriate risk management process for ensuring that the confidentiality, integrity and availability of assets is in place and that all necessary and appropriate technical and organisational security measures have been implemented before commencing its tasks in execution of the Contract, as defined in the Mini-Competition. The Contractor shall appropriately maintain such measures for the duration of the Contract and shall update the measures at regular intervals based on the state of the art and the evolving risks.

1.9.1.3 When determining the appropriate technical and organisational security measures, the Contractor shall notably take into account:

- ✓ the state of the art;
- ✓ the nature, scope, context and purposes of processing, including but not limited to collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of information and/or data; and
- ✓ the risks, including but not limited to those deriving from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to information and/or data transmitted, stored or otherwise processed.

---

<sup>2</sup> These documents are available for consultation at the following address:  
[https://ec.europa.eu/info/files/security-standards-information-systems\\_en](https://ec.europa.eu/info/files/security-standards-information-systems_en).

- 1.9.1.4 Additional security requirements to be taken into account by the Contractor for each individual project shall be described in the Contract.
- 1.9.1.5 If during the performance of the tasks which are the subject of the Contract, the Contractor needs remote access to any communication and information system of the Contracting Authority or to information and/or data processed therein, the Parties shall conclude a specific agreement for remote intervention as an annex to the Contract and the Contractor shall ensure compliance with the Contracting Authority's internal rules on practical and technical security for remote intervention.
- 1.9.1.6 The Contractor shall take all appropriate steps for each Product and Service to ensure that the data and/or information and the media upon which they are stored are safely preserved. The Products and Services supplied shall not contain any vulnerability which could compromise their availability, integrity or confidentiality or that of the Contracting Authority's evolving multi-manufacturer information technology environment, architecture and physical premises. Any cost arising as a consequence of such vulnerability, including but not limited to costs resulting from a loss of data, shall be borne by the Contractor.
- 1.9.1.7 The Contractor shall assist with the management of the security risks by the Contracting Authority and the controller, including risks to the rights and freedoms of individuals when the controller processes their personal data using the contracted services.
- 1.9.1.8 The Contractor shall ensure that all security precautions for each Product or Service are clearly set out in the relevant Documentation supplied to the Contracting Authority.
- 1.9.2 *Security Incident management*
- 1.9.2.1 The Contractor shall implement the necessary organisational and technical measures and mechanisms to prevent, detect, and handle any Security Incident in an appropriate manner. The Contractor shall regularly re-assess and update the implemented measures and mechanisms in light of the state of the art and the risks, which may evolve over time in light of the evolution in the technologies relevant for the Contract.
- 1.9.2.2 In the event a Security Incident occurs or has occurred, the Contractor shall, irrespective of the level of risk, Notify the Contracting Authority thereof without undue delay and not later than 48 hours after becoming aware of the Incident, except in the event the Contractor is made aware by the Contracting Authority.
- 1.9.2.3 In the context of any Notification made in compliance with this Article 1.9 or upon the Contracting Authority's first request, the Contractor shall provide the Contracting Authority with at least the following information:
- ✓ Nature of the Security Incident including where possible, the categories and approximate number of data records concerned and, where applicable, the categories and approximate number of data subjects concerned;



- ✓ Exact date or period of the Security Incident as well as date and time of detection;
- ✓ Explanation on how the Security Incident was detected, its root cause and its likely and/or actual consequences; and
- ✓ Measures taken or proposed to be taken to address the Security Incident, including, where appropriate, measures to mitigate its possible adverse effects.

Further details on the content and format of the Notification may be defined in the Contract.

- 1.9.2.4 The Contractor shall use its best efforts to assist the Contracting Authority with the notification of the Security Incident to the competent authority(ies) and/or the data subject(s) where applicable.
- 1.9.2.5 In the event of a Security Incident attributable to the Contractor, the Contractor shall take all measures necessary and appropriate to limit the negative impact of the Security Incident as much as possible (including but not limited to the provision of forensic assistance to the Contracting Authority) and to mitigate damages. The Contractor shall take upon itself payment of all damages and fines flowing from the Security Incident.
- 1.9.3 The Contractor shall document all measures and mechanisms implemented to comply and demonstrate compliance with this Article 1.9 and shall make such information available to the Contracting Authority upon the latter's first request.
- 1.9.4 Any financial burden for complying with this Article 1.9 shall be at the charge of the Contractor.
- 1.9.5 The Contractor undertakes to impose the security and Security Incident management obligations of this Article 1.9 upon any of its subcontractors and their personnel who perform tasks for the Contracting Authority in execution of the Contract.
- 1.9.6 Non-compliance by the Contractor with the obligations laid down in this Article 1.9 shall be deemed to constitute a breach of substantial contractual obligation by the Contractor and the Contracting Authority shall be entitled to terminate the Contract and/or apply liquidated damages of an amount calculated in accordance with the terms of the Contract.

## **1.10 Audit by the Contractor**

- 1.10.1 The Contractor acknowledges that the Contracting Authority is subject to, or should be interpreted as being subject to, certain privileges and immunities pursuant to Article 343 of the Treaty on the Functioning of the European Union and to Protocol No 7 to this Treaty<sup>3</sup>. In the context of the Contract, the Contractor particularly acknowledges and accepts inviolability of the Contracting Authority's premises and buildings, including but not limited to its assets, as well as the inviolability of its archives, including the physical location and the location in the cloud of its data and services.
- 1.10.2 In view of the EU's supranational nature and its accompanying privileges and immunities, the Contractor shall not exert any right of inspection over the Contracting Authority's use of the Products or Services. In the event that the Contractor is not and does not include the right holder of the licence rights, the Contractor undertakes that said right holder will abide by this Article 1.10 as if the right holder was itself *mutatis mutandis* party to the Contract entered into between the Contractor and the Contracting Authority. The Contracting Authority may request proof of such agreement. In the absence of such proof, the Contractor shall be liable for any compensation requested by the right holder.

---

<sup>3</sup> Given that the ESM is an international organisation under public international law, the ESM is accorded privileges and immunities, in particular with regards to the inviolability of archives, on the basis of the Treaty establishing the European Stability Mechanism.

## **1.11 Intellectual property and related rights**

### *1.11.1 Use, assignment, licensing and sublicensing of licensed rights*

1.11.1.1 The Contracting Authority shall be entitled to use the intellectual property rights under licence pursuant to the Contract for its Internal Use. Licences relating to a limited number of (named) users or devices may be freely reassigned without any limitation to other (named) users or similar devices within the Contracting Authority.

1.11.1.2 The Contracting Authority shall be entitled to assign, license or sublicense all or part of the intellectual property rights under licence pursuant to the Contract to any other EU institution, agency or body, which shall in such event be entitled to use these rights under the same conditions as the Contracting Authority.

1.11.1.3 In the event that the Contractor is not and does not include the right holder of the intellectual property rights under licence, the Contractor undertakes that said right holder will abide by this Article 1.11.1 as if the right holder was itself *mutatis mutandis* a party to the Contract entered into between the Contractor and the Contracting Authority.

### *1.11.2 Third Party Claims relating to the use of Products, Services, Documentation or other protected material delivered under the Contract*

1.11.2.1 Each Party shall Notify the other Party of the existence or threat of any third party claim or action alleging an infringement of its intellectual property rights and/or a non-authorized access to and/or processing of data by the Contracting Authority's use of any Product, Service, Documentation or other protected material delivered under the Contract.

1.11.2.2 In the event of such a dispute or threat of dispute, the Contractor shall promptly provide the Contracting Authority with all assistance requested to mitigate losses, settle the dispute or threat of dispute, enable, facilitate and/or accelerate the clearance of the disputed third party rights. Upon first request of the Contracting Authority, the Contractor shall, at its own and sole expense, voluntarily intervene in any pending litigation relating to the third party right.

1.11.2.3 The Contractor shall proactively Notify the Contracting Authority of any relevant element relating to the dispute or threat of dispute. Upon first request of the Contracting Authority, the Contractor shall, at its own and sole expense, provide the Contracting Authority with all useful and/or reasonable information and assistance in connection with the dispute or threat of dispute.

1.11.2.4 The Contractor shall hold the Contracting Authority harmless from and against any damages suffered by such litigation or threat of litigation and the Contractor shall be liable for any claim or payment arising out of any judgment, ruling or settlement relating to the third party claim or action relating to third party rights, except for the payment of a settlement made by the Contracting Authority without the Contractor's written consent. Such consent may not be withheld without reasonable grounds. In case of

refusal to give such consent, the Contractor shall be bound to submit an alternative reasonable and feasible solution which duly mitigates the losses incurred by the Contracting Authority.

1.11.2.5 If the infringement of a third party right is declared in a judgment, arbitration sentence or party settlement, or if such an event is likely to happen, the Contractor undertakes, at its own and sole cost, to either:

- modify the concerned Products, Services or Documentation in a way that would end the infringement to any third party rights;
- replace the concerned Products, Services or Documentation them with substantially equivalent non-infringing Products, Services or Documentation; or
- obtain any rights from the third party right holders required to allow the Contracting Authority to continue using the concerned Products, Services or Documentation as described in the Contract.

1.11.2.6 If the Contractor fails to remedy the infringement of the third party rights in application of Article 1.11.2.5, the Contracting Authority shall be entitled to take all necessary measures to remedy the infringement at the Contractor's expense.

1.11.2.7 Provided it is not possible to remedy the infringement, the Contracting Authority shall be entitled to terminate the Contract. Without prejudice of Article 1.11.2.5 and without prejudice to the right of the Contracting Authority to claim additional damages, the Contractor shall reimburse to the Contracting Authority the purchase, rental, leasing or licence price of any infringing Product and/or Documentation. The Contracting Authority may, at its own discretion decide to pursue the Contract limited to the use of the non-infringing parts of the Product, Service or Documentation. In the latter case, the Parties will determine in good faith the amount of the reimbursement to the Contracting Authority and/or an adapted price for the further deliveries, rental, leasing or licence of the Product, Service or Documentation.

1.11.2.8 The Contractor will not be responsible under the present guarantee for any third party claiming an infringement of its intellectual property rights based on:

- the Contracting Authority's use of any Product or Service in combination with Hardware or Software not delivered by the Contractor, if such combined use is the only cause of the claimed infringement, and provided that the Contractor did not expressly or implicitly agree with such combined use, or
- the Contracting Authority's use of any Product or Documentation in a form other than the one delivered by the Contractor, if such change in form is the only cause of the claimed infringement, and provided that the Contractor did not expressly or implicitly agree with such use in the other form.

1.11.3 *Use of EU Protected Material*

1.11.3.1 The Contracting Authority may authorise the Contractor to use identified EU Protected Material which the Contractor is likely to use in the execution of its obligations under the Contract.

1.11.3.2 The Contractor shall use the EU Protected Material only to the extent strictly necessary for the execution of the Contract.

1.11.3.3 The Contractor shall not copy any EU Protected Material without prior written authorisation from the Contracting Authority.

1.11.4 *Third Party Claims relating to the use of EU Protected Material*

1.11.4.1 Each Party shall Notify the other Party without undue delay of the existence or threat of any third party claim or action alleging a breach of any third party rights, including intellectual property rights, resulting from the use by the Contractor of EU Protected Material, whether or not in contravention with Article 1.11.3.

1.11.4.2 In the event of such a dispute or threat of dispute, the Contractor shall proactively Notify the Contracting Authority of any relevant element relating to the dispute or threat. Upon first request of the Contracting Authority, the Contractor shall, at its own and sole expense, provide Contracting Authority with all useful and/or reasonable information and assistance in connection with the dispute or threat of dispute.

1.11.4.3 The Contractor shall protect and indemnify the Contracting Authority against all third party claims or actions alleging a breach of any third party rights, including intellectual property rights, resulting from the use by the Contractor of EU Protected Material in contravention with Article 1.11.3. Upon first demand of the Contracting Authority, the Contractor shall, at its own and sole expense, voluntarily intervene in any pending litigation resulting from the use by the Contractor of EU Protected Material in contravention with articles 1.11.3.

1.11.4.4 The Contractor shall be liable for any claim or payment arising out of any judgment, ruling or settlement relating to the third party claim or action alleging a breach of any third party rights resulting from the use by the Contractor of EU Protected Material in contravention with Article 1.11.3, except for the payment of a settlement made by the Contracting Authority without the Contractor's written consent (not unreasonably withheld).

1.11.4.5 The Contractor shall hold the Contracting Authority harmless from and against any damages suffered by the Contracting Authority caused by a breach of this Article 1.11.4.

**1.12 Documentation**

1.12.1.1 The Contractor shall provide the Contracting Authority with the relevant Documentation required for the appropriate and proper operation of the Products and Services, as well as with any update to such Documentation as soon as it becomes available to other customers.

- 1.12.1.2 The Documentation and the updates thereto shall be made available to the Contracting Authority in a reproducible and machine-readable electronic format commonly used by the Contracting Authority.
- 1.12.1.3 The Documentation and the updates thereto shall be available at least in English and, if provided in the Contract, in other language(s).
- 1.12.1.4 The Contracting Authority shall be entitled to reproduce the Contractor's Documentation in full or in part, in electronic form or on paper, for any Internal Use. The Contracting Authority shall reproduce all references to intellectual property rights appearing on the originals.
- 1.12.1.5 The Contracting Authority shall be entitled to modify the Documentation or to translate it to any official language of the European Union in which such Documentation is not made available by the Contractor. The Contractor warrants that the creators of the Documentation will not object to such modification or translation of the Documentation on the basis of their moral rights under copyright. The modified or translated Documentation may only be used by the Contracting Authority for Internal Use.

**1.13 Identifiers**

- 1.13.1 The Contracting Authority may decide to assign an identifier to a unit of a Product. The identifier is an alphanumeric code of 15 characters.
- 1.13.2 The Contracting Authority shall inform the Contractor of the identifier(s) in such manner as shall have been agreed by both Parties. If relevant, the Contractor's original identifier mentioned in its delivery documents is associated with the Contracting Authority's identifier.
- 1.13.3 If the Contracting Authority has assigned an identifier to a unit of a Product, only the Contracting Authority's identifier shall be used in all instances when referred to the unit in question in the communication between the Parties.
- 1.13.4 The format of the identifier or the identifier relating to a unit of a Product may be changed by the Contracting Authority at any time. In that case, the Contractor will be Notified of such change.

## **1.14 Confidentiality**

- 1.14.1 Notwithstanding any other provision of the Contract, any and all data, information and documents shared by the Contracting Authority with the Contractor, or otherwise as submitted by the Contracting Authority to the Contractor, or onto the Contractor's systems in the context of the Contract, including but not limited to EU Protected Material, shall be deemed confidential unless and until an explicit indication to the contrary is made in writing by the Contracting Authority.
- 1.14.2 Data, information and documents shared by the Contractor with the Contracting Authority, shall be deemed confidential if an explicit indication is made in writing by the Contractor on the specific data, information or document and an explanation is provided on the reason why it may not be disclosed.
- 1.14.3 Each Party must:
- ✓ not use confidential data, information or documents for any purpose other than to perform its obligations under the Contract without the prior written agreement of the other Party;
  - ✓ 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;
  - ✓ not disclose directly or indirectly, confidential data, information or documents to third parties without the prior written agreement of the other Party.
- 1.14.4 The Contractor undertakes the obligation to maintain confidentiality on behalf of itself and its Personnel.
- 1.14.5 The confidentiality obligations set out in this Section are directly applicable to the Parties without the need for separate non-disclosure agreements.
- 1.14.6 The confidentiality obligations set out in this Section are binding upon the Contracting Authority and the Contractor for as long as the information or documents remain confidential unless:
- ✓ the disclosing party agrees in writing to release the receiving party from the confidentiality obligation earlier;
  - ✓ the confidential data, information or documents become public through other means than a breach of the confidentiality obligation;
  - ✓ the applicable law requires the disclosure of the confidential data, information or documents.
- 1.14.7 The Contractor understands and acknowledges that the Contracting Authority is subject to transparency rules, including but not limited to those laid down in the Treaty on the Functioning of the European Union, which may require it to provide access to data, information or documents concerning or originating from the Contractor, notwithstanding that such data, information or documents may have been identified by the Contractor in writing as confidential.



- 1.14.8 In derogation of Article 1.14.3, the Contractor understands and acknowledges that the Contracting Authority is entitled to make available (any part of) the confidential data, information or documents to the Contracting Authority's Staff and the staff of other EU Institutions, as well as to other persons and entities working for the Contracting Authority or cooperating with it, including contractors or subcontractors and their personnel provided that they have a reasonable need to know said confidential data, information or documents and are bound by obligations of confidentiality which are no less restrictive than the confidentiality obligations imposed on the Contracting Authority by the Contract.
- 1.14.9 In the event of unauthorised disclosure of confidential data, information or documents by either Party, the other Party shall address it a warning by means of a Notification, requesting the first Party to confirm that it will no longer disclose said data, information or documents, and that measures to contain damages are in place. If no satisfactory response is obtained within the requested time limit, the other Party is entitled to terminate the 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. This is without prejudice to obligations stemming from Regulation 2018/1725 as regards personal data breaches. It is also without prejudice to obligations stemming from other Union law.
- 1.14.10 In the event that the Contract is terminated or in the event that the Contracting Authority requests it, the Contractor shall return all confidential data, information or documents to the Contracting Authority within a reasonable period as agreed between the Parties.
- 1.14.11 In the event of return of confidential data, information or documents as requested by the Contracting Authority under the Contract, the Contractor shall deliver to the Contracting Authority a statement certifying that:
- ✓ all confidential data, information or documents including all copies and extracts thereof have been fully and permanently deleted and/or returned from any hardware or storage media (including but not limited to USB stick, server, and backup copies);
  - ✓ any files or data resulting from the confidential data, information or documents originally communicated by the Contracting Authority have also been fully and permanently deleted and/or returned from any hardware or storage media;
  - ✓ any paper copy of the confidential data, information or documents and any document that contains the confidential data or information has been deleted and/or returned; and
  - ✓ any subcontractors that have received access to and/or copies of the confidential data, information or documents in accordance with this Contract, have been requested to undertake the same measures and have certified in writing that the confidential data, information or documents have been deleted and/or returned.

**1.15 Third party Initial Vendor or right holder**

- 1.15.1 If the Contractor is not the Initial Vendor, the Contractor shall, prior to the provision of any Product or Service, conclude the necessary back-to-back agreements with the Initial Vendor to ensure that the Contractor can fully abide by its obligations under the Contract.
- 1.15.2 If the fulfilment of obligations by the Contractor under the Contract requires the agreement of or the performance of actions by the Initial Vendor, the Contractor undertakes that the Initial Vendor will give the required agreement or perform the required actions.
- 1.15.3 If the Contractor is not and does not include the right holder of intellectual property rights attached to a Hardware Product, Licensed Software Product or Documentation, the Contractor shall either:
- ✓ acquire from the right holder a valid licence or sublicense which allows the Contractor to sublicense to the Contracting Authority, at the latest upon delivery of such Product or Documentation, all rights as specified in the Contract; or
  - ✓ undertake that the right holder shall grant to the Contracting Authority, in a separate licence agreement concluded at the latest upon delivery of such Product or Documentation, all rights as specified in the Contract, as if the right holder was itself *mutatis mutandis* a party to the Contract entered into between the Contractor and the Contracting Authority.
- 1.15.4 The Contractor shall inform the Contracting Authority of applicable licence terms imposed by a third party right holder of intellectual property rights attached to a Hardware Product, Licensed Software Product or Documentation before a corresponding purchase, rental, leasing or licence is effectuated. Unless agreed in writing by the Contracting Authority, these licence terms shall not derogate from the Contract.
- 1.15.5 The Contractor shall hold the Contracting Authority harmless from and against any damages suffered by the Contracting Authority caused by a breach of this Article 1.15.

**1.16 Invoicing**

- 1.16.1 The manner in which invoices are sent, received and paid shall be agreed upon in the Contract.
- 1.16.2 If the use of an electronic invoicing system has been agreed between the Parties in relation with the Contract and there is a conflict between the terms of use of the electronic invoicing system and this Article 1.16, the terms of use of the electronic invoicing system shall have precedence on this Article 1.16.
- 1.16.3 Invoices for the delivery of Products or the provision of Services are to be sent to the address or in the manner stated in the Contract. The payment period shall not be binding on the Contracting Authority if any invoice is sent to a different address or manner.
- 1.16.4 One-off payments (for the acquisition of Products, the provision of Services consisting in a single performance, etc.) shall be invoiced when the relevant Delivery Note, or, where applicable, the Acceptance Document has been Notified to the Contractor. If neither a Delivery Note nor an Acceptance Document is to be issued under a Contract, the one-off payments shall be invoiced when the Products or Services have been fully delivered or provided by the Contractor and accepted by the Contracting Authority.
- 1.16.5 Payments for rental and leasing of Products or for continuous Services (Maintenance, Cloud Services, etc.) shall be invoiced at the end of the calendar quarter unless otherwise agreed in the Contract. The first invoice shall cover the period from the date of Notification to the Contractor of the Delivery Note, or, where applicable, the Acceptance Document of the Products or from the start date of the Services indicated in the Contract to the last day of the current calendar quarter. When the total value of a Contract relates to an amount of less than €25,000, payment for rental and leasing of Products or for continuous Services shall be invoiced when the Products or Services have been fully delivered or provided by the Contractor and accepted by the Contracting Authority.
- 1.16.6 In exceptional cases, on request by the Contractor, and subject to a prior approval by the Contracting Authority, payments referred to in Article 1.16.5 may be invoiced per calendar year and in advance for the whole period, irrespective of the amount involved. If the amount to be paid is variable, only the certain amount shall be invoiced in advance and the variable part shall be invoiced at the end of the calendar year.
- 1.16.7 Subscription fees (for licences, Support Services, Maintenance, etc.) may be invoiced per subscription period, and in advance for the whole subscription period, provided that they are accompanied by the Delivery Note. Annual instalments will be made for subscription periods covering more than twelve (12) months. Those subscriptions will be invoiced and paid annually. Invoices cannot cover periods exceeding twelve (12) months, or exceed the duration of the Contract. If the amount of the subscription fee is variable, only the certain amount shall be invoiced in

advance and the variable part shall be invoiced at the end of the period covered by the advanced payment.

## **2 LICENSED SOFTWARE PRODUCTS**

### **2.1 Delivery**

#### *2.1.1 Delivery Date*

2.1.1.1 The Licensed Software Products shall be delivered on the Delivery Date and before the end of the Delivery Lead Time.

2.1.1.2 Unless otherwise agreed in the Contract, the Delivery Lead Time for the provision of Licensed Software Products shall be seven (7) Normal Working Days.

2.1.1.3 Unless otherwise agreed in the Contract, the Contractor shall Notify the Contracting Authority of a proposed Delivery Date at least two (2) Normal Working Days before such proposed Delivery Date. The proposed Delivery Date for physical deliveries must be a Normal Working Day. The Parties may at all times agree in writing to modify the above notification period for a specific delivery.

2.1.1.4 Unless the Contracting Authority Notifies the Contractor of its refusal of the proposed Delivery Date no later than one (1) Normal Working Days after the Notification referred to in Article 2.1.1.3, the proposed Delivery Date shall be deemed accepted by the Contracting Authority. The Contracting Authority shall not refuse the proposed Delivery Date without reasonable grounds. In case of refusal of the proposed Delivery Date, the Contractor shall Notify the Contracting Authority of a new proposed Delivery Date in accordance with Article 2.1.1.3.

2.1.1.5 Any liquidated damages provided for in the Contract for failure of the Contractor to deliver the Licensed Software Product within the applicable time limits are without prejudice to the right for the Contracting Authority to claim additional damages under applicable law. If the Contracting Authority has incurred costs in relation to a third party by reason of a failure to deliver the Licensed Software Products on the Delivery Date or before the end of the Delivery Lead Time, the Contractor shall reimburse these costs immediately upon production of supporting document.

2.1.1.6 If the Licensed Software Products are not delivered no later than ten (10) Normal Working Days after the expiration of the Delivery Lead Time, the Contracting Authority shall be entitled to immediately terminate the Contract.

#### *2.1.2 Delivery Terms*

2.1.2.1 The manner in which a Licensed Software Product shall be delivered shall be agreed upon in the Contract.

2.1.2.2 When it is agreed that the Licensed Software Product shall be downloaded by the Contracting Authority, the Contractor shall Notify the Contracting Authority, on the Delivery Date, of the accurate and complete instructions, including access codes, enabling the Contracting Authority to download the

Licensed Software Product. The Licensed Software Product shall be available for download on the indicated download area as from the Delivery Date and for at least sixty (60) Normal Working Days.

- 2.1.2.3 A Delivery Note shall be Notified to the Contracting Authority together with the downloading instructions. The Contracting Authority shall Notify the Contractor of its acknowledgment of receipt of the Delivery Note within two (2) Normal Working Days. Acknowledgement of receipt of the Delivery Note by the Contracting Authority is simply an acknowledgment of the fact that the delivery took place and in no way implies conformity of the Licensed Software Product with the Contract.
- 2.1.2.4 When it is agreed that the Licensed Software Product shall be delivered on a tangible medium, the Licensed Software Product shall be delivered on (a) machine-readable medium(s) (disk or other) as determined in the Contract, reproducing the Licensed Software Product.
- 2.1.2.5 The machine-readable medium(s) containing the Licensed Software Product shall be delivered at the exact place or places and under the conditions determined in the Contract. Unless otherwise agreed in the Contract, the machine-readable medium(s) containing the Licensed Software Product shall be delivered under the conditions of Incoterms 2010 Delivery Duty Paid. Unless otherwise agreed in the Contract, the delivery may be made at any time during Normal Working Hours on the Delivery Date.
- 2.1.2.6 Unless expressly requested or agreed by the Contracting Authority, partial delivery of the machine-readable medium(s) containing the Licensed Software Product ordered in a Contract is not allowed.
- 2.1.2.7 Each delivery of (a) machine-readable medium(s) of a Licensed Software Product shall be accompanied by a Delivery Note in duplicate, duly dated and signed by the Contractor or its carrier. One copy of the Delivery Note must be countersigned by the Contracting Authority upon delivery and returned to the Contractor or its carrier. Signature of the Delivery Note by the Contracting Authority is simply an acknowledgment of the fact that the delivery took place and in no way implies conformity of the Licensed Software Product with the Contract.

## **2.2 Acceptance**

- 2.2.1 The acceptance period for Licensed Software Products shall run up to thirty (30) Normal Working Days from the date of signature or Notification of the acknowledgement of receipt of the Delivery Note by the Contracting Authority.
- 2.2.2 During the acceptance period, the Contracting Authority shall Notify the Contractor of any defaults in the Licensed Software Product preventing its conformity with the Contract. As from the date of such Notification of Default, the acceptance period shall be interrupted. A new acceptance period of thirty (30) Normal Working Days shall commence on the date on which the Contractor Notifies the Contracting Authority that the default has been remedied.

- 2.2.3 At the latest upon the expiration of the acceptance period, acceptance of a Licensed Software Product shall be recorded in an Acceptance Document, which shall indicate at least the detailed nature of the accepted Licensed Software Product and the reference number of the Contract(s) concerned.
- 2.2.4 If no Acceptance Document has been issued at the end of the acceptance period and if no Notification of Default is pending, the Contracting Authority is considered as having accepted the Licensed Software Product.
- 2.2.5 If, due to a default of the Licensed Software Product, acceptance cannot be completed after two attempts of acceptance or within a maximum time limit of thirty (30) Normal Working Days from the signature or acknowledgment of receipt of the Delivery Note by the Contracting Authority, and where a different time limit has not been specified in the Contract, the Contracting Authority shall be entitled to terminate the Contract after Notifying the Contractor with thirty (30) Normal Working Days' notice to meet its obligations. This provision is without prejudice to the Contracting Authority's other rights as provided for in the Contract.

## **2.3 Guarantee and Maintenance**

- 2.3.1 *Guarantee*
- 2.3.1.1 The Contractor warrants that the Licensed Software Product will be free from any viruses, backdoors or other malicious code at the time of receipt by the Contracting Authority. Such warranty shall apply anew to any update or upgrade delivered to the Contracting Authority.
- 2.3.1.2 The Contractor warrants that the Licensed Software Product does not and shall not include or contain any clock, timer, counter, or other limiting or disabling code, design or routine which causes or may cause the Licensed Software Products to be erased, inoperable or otherwise incapable of being used in the full manner for which it was designed and licensed pursuant to the Contract. This includes, without limitation: (a) after being used or copied a certain number of times, or after the lapse of a certain period of time, or after the occurrence or lapse of any triggering factor or event; or (b) because the Licensed Software Product has been installed on or moved to Hardware different to that on which the Licensed Software Product was originally installed.
- 2.3.1.3 The Contractor warrants that the Licensed Software Product will materially conform to its specifications and will be free of defects at the time of delivery and for a guarantee period of one (1) year.
- 2.3.1.4 In case of malfunction during the guarantee period, the Contractor shall ensure that the malfunction is remedied without undue delay. When the Contractor receives a guarantee claim for any Licensed Software Product, the Contractor shall either repair or have repaired the relevant defect, or replace the Licensed Software Product. Failure to remedy a default for a period longer than twenty (20) Normal Working Days shall entitle the Contracting Authority to a full refund of the price of the Licensed Software Product including the fees for Maintenance or Support Services relating to the Licensed Software Product, as well as the indemnification of all related

costs and damages. The Contractor shall pay for the shipment of repaired or replaced Licensed Software Products to the Contracting Authority.

2.3.1.5 The Contractor does not warrant that the Licensed Software Product will operate in combination with Hardware and/or Software other than those described in the Contract or in the Licensed Software Product Documentation. However, if the Contractor expressly or implicitly agreed with the operation of the Licensed Software Product in combination with specific Hardware and/or Software, the Contractor shall be responsible during the guarantee period if the Licensed Software Product does not perform in conformity with its specifications in combination with such Hardware and/or Software.

2.3.1.6 The Contractor warrants that it shall give a notice of at least three (3) calendar months before the implementation of any change to the unique identifier or SKU of a Licensed Software Product.

2.3.1.7 The guarantee provided for in this Article 2.3.1 replaces any other guarantee of the Licensed Software Product provided for in any other set of general conditions that would be part of the Contract.

### 2.3.2 *Maintenance*

2.3.2.1 The fees for the Maintenance of Licensed Software Products are either expressed as a percentage of the licence fees or are calculated at a fixed price.

2.3.2.2 Subscriptions to Maintenance of Licensed Software Products shall only be renewed if the Contracting Authority expressly consents with such renewal. The express consent of the Contracting Authority is required for each renewal of a Maintenance subscription (no automatic or tacit renewal).

2.3.2.3 On the part of the Contracting Authority, without prejudice to the Contract, Maintenance of a Licensed Software Product shall involve:

- ✓ preparing and sending to the Contractor all documents and additional available information which the Contractor might reasonably request in order to detect and correct errors in the Licensed Software Product;
- ✓ testing and accepting, when it is reasonable to do so, New Versions or New Releases of the Licensed Software Product, as proposed by the Contractor. One (1) year after the date of such an acceptance, the Contractor is no longer required to provide Maintenance for previous versions or releases of the of Licensed Software Product and any dependent products;
- ✓ installing any preventive corrections provided by the Contractor as long as it is agreed that such corrections are necessary.

2.3.2.4 On the part of the Contractor, without prejudice to the Contract, Preventive Maintenance of a Licensed Software Product shall involve:



- ✓ identifying potential security weak spots of the Licensed Software Product, amongst others based on the evolution of the Software environment;
- ✓ fixing potential security weak spots of the Licensed Software Product that are identified.

2.3.2.5 On the part of the Contractor, without prejudice to the Contract, Corrective Maintenance of a Licensed Software Product shall involve:

- ✓ diagnosing errors or faults encountered by the Contractor or the Contracting Authority in the content of the Licensed Software Product and making any corrections required in order to have the Licensed Software Product perform in conformity with its specifications and the rules of art; the Contractor shall make corrections only if the error can be reproduced or if the Contracting Authority provides the Contractor with sufficient information from which the error can be diagnosed;
- ✓ make all the corrections (including patches) to the Licensed Software Product to ensure that such Licensed Software Product and any system it interacts with operate as specified in the Documentation within thirty (30) Normal working days of receipt of a Notification from the Contracting Authority providing details of a problem;
- ✓ rewriting the Licensed Software Product where necessary in order to correct all known problems or faults diagnosed by the Contractor;
- ✓ providing telephone support for the Contracting Authority in order to advise it on the use of Licensed Software Product;
- ✓ providing remote "hotline" support to resolve urgent problems and failures relating to the Licensed Software Product.

2.3.2.6 On the part of the Contractor, without prejudice to the Contract, Adaptive Maintenance of a Licensed Software Product shall involve:

- ✓ adapting the Licensed Software Product to developments in the Software environment;
- ✓ providing the Contracting Authority with successive versions and releases of the Licensed Software Product and the relevant Documentation;
- ✓ installing New Releases and New Versions of the Licensed Software Product free of charge on existing Hardware at the Contracting Authority's request;
- ✓ where necessary, adapting products that were using the previous version of the Licensed Software Product, free of charge.

2.3.2.7 On the part of the Contractor, without prejudice to the Contract, Evolutive Maintenance of a Licensed Software Product shall involve:

- ✓ improving performance of the Licensed Software Product;
- ✓ implementing new or changed user requirements in the Licensed Software Product.

2.3.2.8 If the Contractor is not the Initial Vendor of the Licensed Software Product, the Contractor undertakes that the Initial Vendor will, where agreed in the Contract or where required to ensure that the Maintenance is in conformity with the state of art, provide the Maintenance Services described in the Contract on behalf of the Contractor.

## **2.4 Software trial**

2.4.1 Upon request of the Contracting Authority, the Contractor shall grant to the Contracting Authority a trial period for Software under the conditions as set out in this Article 2.4.

2.4.2 The Contracting Authority shall be entitled to request a trial period during which New Versions of Licensed Software Products or other Software in the catalogue of the Contractor, or of an Initial Vendor for which the Contractor acts as a reseller, shall be available to the Contracting Authority in order to assess whether such (New Version of the) Software is adapted to the needs and the environment of the Contracting Authority. This includes, but is not limited to, testing substitute Licensed Software Products proposed by the Contractor under Article 1.7 on Change and replacement management. The Contracting Authority's request shall be motivated and shall describe the precise purpose of the request, the duration of the trial period, the intended use of the Software and the maximum number of users.

2.4.3 The Contractor may refuse to grant the trial period for Software if the Contracting Authority's request is patently unreasonable or if the purpose of such request is not legitimate under Article 2.4.2.

2.4.4 The Contractor shall make the requested Software available to the Contracting Authority and grant it a licence to use the Software under the conditions set in the in the Contracting Authority's request. The licence shall be granted free of charge and for the period included in the Contracting Authority's request. It shall cover all intellectual property rights attached to the requested Software. In the event that the Contractor is not and does not include the right holder of intellectual property rights attached to the requested Software, the Contractor shall either:

- ✓ acquire from the right holder a valid licence or sublicense allowing the Contractor to sublicense to the Contracting Authority all rights as stipulated in this Article 2.4.4; or
- ✓ commit that the right holder shall grant to the Contracting Authority, in a separate licence agreement concluded no later than at the time that the requested Software is made available to the

Contracting Authority, all rights as stipulated in this Article 3.4.4, as if the right holder was itself *mutatis mutandis* a party to the Contract entered into between the Contractor and the Contracting Authority.

- 2.4.5 The Contracting Authority shall be entitled to use the Software only for Internal Use, irrespective whether such use is productive or not.
- 2.4.6 Upon termination of the trial period, the Contractor shall promptly uninstall and destroy all copies of the requested Software.
- 2.4.7 The grant of a trial period for Software to the Contracting Authority shall in no way result in an obligation for the Contracting Authority to purchase (a licence on) the tested Software.

## **2.5 Intellectual Property Rights**

- 2.5.1 The Contractor shall grant and the Contracting Authority shall accept, as from the delivery of the Licensed Software Product, a non-exclusive licence to use the Licensed Software, for all modes of exploitation inherent to the normal use of the Software and to any other use as specified in the Contract, under the conditions as specified in the Contract. The licence shall cover all intellectual property rights attached to the Licensed Software Product. Unless otherwise agreed in the Contract, the licence shall be granted worldwide, for the entire duration of protection, including if need be the right to sublicense the rights to any third party. The payment of the price for the Licensed Software Product shall include all fees payable to the Contractor for the acquisition by the Contracting Authority of the licensed rights for all modes of exploitation inherent to the normal use of the Software and to any other use as specified in the Contract.
- 2.5.2 Temporary licences relating to Licensed Software Products shall only be renewed if the Contracting Authority expressly consents in writing to such renewal. The express consent of the Contracting Authority is required for each renewal of the temporary licence (no automatic or tacit renewal).
- 2.5.3 The Contracting Authority shall be entitled to reproduce the Licensed Software Product to the extent necessary to make normal use of the Software or any other use of the Software as specified in the Contract, as well as for the purposes of back-ups and archiving.
- 2.5.4 The Contracting Authority shall take all measures necessary in relation to its end user personnel and persons having access to the Licensed Software Product and its Documentation, to ensure that the confidentiality of the Software is observed.
- 2.5.5 The Contracting Authority shall not pledge, assign, sub-license, transfer or lend, for payment or otherwise, the Licensed Software Product except in the manner set out under the Contract.

## **2.6 Entitlement reporting**

2.6.1 The Contractor shall keep records of licence transactions with the Contracting Authority and shall, upon request, provide reports of such transactions in order to allow the Contracting Authority to prove its entitlements to a Licensed Software Product. Such records and reports shall at least contain the following information:

- ✓ the unique identifier or SKU of the Licensed Software Product;
- ✓ the licence metric unit and the number of licensed units;
- ✓ the recipient of the licence in full name with address; and
- ✓ if applicable, the licence period.

2.6.2 If the Contractor is not and does not include the holder of the rights attached to the Licensed Software Product, it shall record relevant information required to identify any entitlements towards the rights holders.

2.6.3 The Contractor undertakes to transmit the corresponding licensing information electronically without undue delay to any software and licence asset management system used by the Contracting Authority and which is in accordance with standard commercial practice.

### **3 CLOUD SERVICES**

#### **3.1 Provision and Service Levels**

- 3.1.1 The Contractor shall make available on the Delivery Date (or before the end of the Delivery Lead Time, if more appropriate) the Cloud Services to the Contracting Authority and the Contracting Authority shall have the right to use them, in accordance with the terms and conditions of the Contract.
- 3.1.2 The Contractor may not suspend the provision of the Cloud Services for any reason other than the existence of a serious risk for the security of the Cloud Service. In such event, the Contractor may only suspend the provision of the Cloud Services following a Notification to the Contracting Authority of the interruption. The Contractor shall use all commercially reasonable efforts to restore the Cloud Service as soon as possible.
- 3.1.3 The Service Levels as agreed upon in the Contract shall include, but are not limited to, availability (uptime), customer support response time, and publication of relevant technical metrics (computing/storage/network metrics etc.).
- 3.1.4 The Contractor shall provide or make available to the Contracting Authority standardised reports, including at least performance and availability metrics of the Cloud Services.
- 3.1.5 In the event the Contractor provides a Cloud Service for the exclusive use by the Contracting Authority (e.g. private cloud, managed services), the Contractor shall (i) provide or make available, on a regular basis, to the Contracting Authority a report including the applicable Service Levels, Service Level objectives accomplished, and Service Level objectives not-accomplished; and (ii) establish a disaster recovery plan and define the corresponding recovery time in the Contract if applicable.

#### **3.2 Ownership and Intellectual Property**

- 3.2.1 Unless otherwise agreed in the Contract, the Contracting Authority shall retain intellectual property and/or ownership rights to all information, data, inputs, and outputs, related to the use of the Cloud Services.
- 3.2.2 The Contractor shall retain intellectual property and/or ownership rights to the cloud infrastructure underlying the Cloud Services provided by the Contractor.
- 3.2.3 The Contractor warrants for any use of the Cloud Services that the Contracting Authority may envisage for the purposes and within the limits as set out in the Contract, that (i) any material provided by the Contractor in the context of the Cloud Services, including but not limited to third party software or applications, is free of claims from right holders or in general from any other third parties; (ii) the necessary rights and authorisations to provide such material to the Contracting Authority have been obtained by

the Contractor; and (iii) all the necessary intellectual property rights have been cleared.

### **3.3 Consequences of termination**

3.3.1 In case of termination of the Cloud Services and upon request of either Party, the Parties shall agree on a portability plan, which may include terms on data or information retrieval or transfer methods and formats, and deletion protocols.

3.3.2 In any event, the Parties acknowledge and agree that in case of termination of the Cloud Services, the Contractor shall not delete the data or information of the Contracting Authority until the data or information has been retrieved or transferred, at the choice of the Contracting Authority, as follows:

- ✓ in case the Contracting Authority requests retrieval of the data or information, it shall be entitled to retrieve the data or information in a structured and widely-used format capable of ensuring portability of the data or information, within a period agreed upon between the Parties; or
- ✓ in case the Contracting Authority requests transfer of the data or information, the Contractor shall transfer the data or information in a structured and widely-used format capable of ensuring portability of the data or information, as agreed with the Contracting Authority at the time of the request, to the Contracting Authority or to any third party selected by the Contracting Authority within a period as agreed between the Parties.

3.3.3 Once the Contractor has confirmed with the Contracting Authority that data or information has been retrieved or transferred successfully, and after informing the Contracting Authority, the Contractor shall ensure definitive destruction of copies of, and erasure of, all data and information of the Contracting Authority and shall certify the same to the Contracting Authority.

3.3.4 In any event, the Contracting Authority has the right to request deletion of the data or information irrespective of any request for retrieval or transfer of the data or information.

3.3.5 Upon termination of the Cloud Services, the Contracting Authority will cease using the cloud infrastructure underlying the Cloud Services.

### **3.4 Data portability**

3.4.1 The Contractor shall ensure and must be able to demonstrate the ability to port the data or information of the Contracting Authority from its infrastructure within a period agreed upon between the Parties in a structured and widely-used format as agreed with the Contracting Authority. The Contractor must ensure that the Contracting Authority is fully provided with the Cloud Services and access to the data or information during this period.

3.4.2 If data portability is required, the Contractor agrees to cooperate with other suppliers of the Contracting Authority to ensure that the data can be ported onto the Services of other suppliers. It agrees to attend meetings called by the Contracting Authority for that purpose.

### **3.5 Cooperation and information**

3.5.1 The Contractor shall not disclose any data or information issued by the Contracting Authority and processed through the Cloud Services, actively or passively, intentionally or unintentionally, to any authorities, legal or natural persons. The Contractor shall Notify the Contracting Authority of any legally binding request for disclosure made by any law enforcement authority, including from non-EU countries, promptly and without undue delay. The Contractor shall not give access or disclose the data or information unless authorised by the Contracting Authority. To the largest extent permitted under applicable law, the Contractor shall appeal any legally binding request to disclose the data.

3.5.2 The Contractor shall inform the Contracting Authority, within a reasonable period of time, about (i) future changes concerning the Cloud Services such as the implementation of additional functions; (ii) future changes in the infrastructure and procedures with a potential impact on the Cloud Services; and (iii) the results of relevant security audits, under guarantee of confidentiality.

### **3.6 Location**

3.6.1 The Contractor warrants that the Cloud Services are fully hosted in the territory of the European Economic Area, unless otherwise agreed in the Contract.

3.6.2 The Contractor undertakes that it shall not move data, whether at rest or in transit, from the Contracting Authority outside the European Economic Area, unless otherwise agreed in the Contract or unless the Contracting Authority has given its prior written authorisation.

3.6.3 The Contractor warrants that the Cloud Services are designed and shall be maintained in such a way that the Contracting Authority is clearly aware of the location(s) where the Cloud Services are physically hosted, and of the laws applicable thereto. The degree of precision with which the location is established may be further defined in the Contract.

3.6.4 The Contractor shall provide the Contracting Authority with comprehensive information on the physical location of the physical assets (e.g. servers, storage, devices, etc.) used by the Contractor and its subcontractors for the provided Cloud Services (including for backup, business continuity purposes and transit) as well as locations from where remote operations are performed.

3.6.5 The Contracting Authority shall be in control of determining the physical location of its data at rest. Any change of location shall be subject to the prior express written consent of the Contracting Authority, except if the new location was already permitted in the Contract.

## **4 SUPPORT SERVICES**

### **4.1 Stability and performance of Support Services**

- 4.1.1 Throughout the term of the Contract, the Contractor shall ensure that stable Support Services are maintained as required for the proper implementation of the Contract and to ensure service continuity for the Contracting Authority.
- 4.1.2 The Contractor shall not take any action that may adversely affect the functioning or performance of, or effect a decrease in the resource efficiency of the Support Services, without the approval of the Contracting Authority.
- 4.1.3 The timetable for the performance of the Support Services shall be set out in the Contract. If such a timetable cannot be prepared for more complex projects or projects of longer duration, the Parties shall first agree a provisional timetable. The final timetable shall be agreed at a date stated in the Contract.





STD-01-BSR  
Cybersecurity Framework  
Security Standard  
ICT Systems Baseline Security Requirements

## Document history

Date	Version	Author	Description
24/03/2020	2.6	CISO	Draft for Approval
15/04/2020	2.6	CISO	Validated by TCIS
15/10/2020	2.7	CISO, Inter-DG	Validated by Inter-DG Steering Group on Information Systems Security.
24/11/2020	2.7	Resource Directors	Document endorsed in the meeting held the 24/11/2020
09/12/2020	2.7	ISSB	Document endorsed in the meeting held the 09/12/2020

## Table of Contents

Document history.....	2
Table of Contents .....	3
General references .....	4
References.....	4
1. Introduction.....	5
1.1. Adoption procedure.....	5
1.2. Introduction.....	5
1.3. Objective and Methodology. How to use this standard .....	6
1.4. Applicability.....	6
1.5. Terminology.....	7
1.6. Glossary and Acronyms .....	7
2. List of Baseline Security Requirements .....	10
2.1. Security by Design .....	10
2.2. Network Security .....	11
2.3. Identity and Access Management .....	12
2.4. Asset Protection .....	14
2.5. Application Security .....	16
2.6. Security Logging and Monitoring.....	17
2.7. Change Management.....	17
2.8. Data Backup and Recovery .....	19
2.9. Third Party Security.....	19

## General references

- **European Parliament Security Policies**  
<https://itecnet.in.ep.europa.eu/home/ict-security/governance--policies/ict-security-governance-and-policies.html>
- **Information Security Policy in the European Parliament**  
Geda Note D (2020) 14287 dated 02/06/2020
- **PCI DSS – Payment Card Industry Requirements and Security Assessment Procedures**  
[https://www.pcisecuritystandards.org/document\\_library](https://www.pcisecuritystandards.org/document_library)
- **ENISA baseline security requirements for the procurement of secure ICT products and services**  
<https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services>

## References

1. **European Parliament Security Standards**  
<https://itecnet.in.ep.europa.eu/home/ict-security/governance--policies/ict-security-standards-guidelines-and-procedures.html>
2. **EU Trusted List of Service providers**  
<https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers>
3. **EP Application development standards**  
<https://ep-foundry.in.ep.europa.eu/standards/>
4. **OWASP ASVS for web applications**  
<https://owasp.org/www-project-application-security-verification-standard/>
5. **Java Secure Coding Guidelines**  
<https://www.oracle.com/technetwork/java/seccodeguide-139067.html>
6. **Common Vulnerability Scoring System Version 3.0 Calculator**  
<https://www.first.org/cvss/calculator/3.0>

# 1. Introduction

## 1.1. Adoption procedure

Bureau decision concerning the "EUROPEAN PARLIAMENT INFORMATION AND COMMUNICATION TECHNOLOGY SYSTEMS SECURITY POLICY", adopted on 07/09/2015.

This document is part of the set of documented standards, guidelines and procedures that support the implementation of the different domains of the Cybersecurity Policy.

## 1.2. Introduction

The definition of a minimal set of controls and security to tackle cybersecurity is one of the guiding principles of the European Parliament (EP) Cybersecurity policy. Chapter 10 of the framework is centred about a minimal level of security and emphasize the need for a standardised and shared approach for baselined security requirements.

The procurement, development and operation of ICT systems may result in the introduction of cybersecurity risks and incidents.

To prevent this situation, it is important to define a common set of minimum mandatory security requirements that will cover the whole lifecycle of the ICT systems at the EP in order to contribute to an appropriate level of security and resilience for those ICT systems. This list of requirements that any ICT system in the EP must implement will be called Baseline Security Requirements and it is based on commonly agreed best practices and standards.

It is understood that this list is not a comprehensive list of all possible security controls that must be implemented for a given ICT system. Additional more specific controls for a given ICT system must be defined based on the results of a formal risk assessment. Certain requirements have been suggested as recommended, and compliance with them may be evaluated on a case-by-case basis, based on a risk assessment.

The security requirements listed in this document can be mapped to security-specific features and capabilities that must be built into a given system. The EP has defined a set of additional standards and guidelines oriented to define and support the implementation of these security features. The right list of standards and guidelines to be applied for every system must be identified on a case-by-case basis, depending on the features implemented (e.g., EP logging and monitoring standard or EP TLS secure configuration standard).

### 1.3. Objective and Methodology. How to use this standard

This requirements document must be included in every EP external tender and internal project.

Every tender or project at the EP must produce in its preliminary phase a statement of compliance to the Baseline Security Requirements. Any failure to comply with one or more of these requirements must be logged and reported in order to analyse the risks related to this non-compliance.

Compensating controls may be considered when a requirement cannot be explicitly met as stated, due to legitimate technical or business constraints. Compensating controls must be documented and assessed for their effectiveness.

The residual risks related to the non-compliance with the mandatory baseline requirements must be reported by the system Owner to the DG/PG risk manager.

A checklist with the baseline security requirements is available to assist staff working in the statement of compliance reporting. This checklist<sup>1</sup> must be used to indicate the level of compliance for each of the requirements in this document (Compliant, Partially Compliant, Not Compliant), the list of compensating controls in case of non-compliance and a plan and deadline to implement those controls.

### 1.4. Applicability

This standard is applicable to any ICT system (“system”) or ICT system components (“system components”) in the EP IT environment storing, processing or transmitting any information categorised as Parliament Use Information or Other Confidential Information (non-classified) whether these environments are developed, provided and hosted on-premises or in the cloud.

This standard does not apply to systems storing, processing or transmitting EU Classified information.

System components include network devices, servers, computing devices, and applications. Examples of system components include but are not limited to the following:

- Server types including but not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), Domain Name System (DNS) and PaaS.

---

<sup>1</sup> (ref 1) The checklist can be found in the page of the European Parliament Security Standards <https://itecnet.in.ep.europa.eu/home/ict-security/governance--policies/ict-security-standards-guidelines-and-procedures.html>

- Applications including all purchased and custom applications, including internal and external (e.g., Internet, SaaS) applications.
- Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.
- Network components used to build a system including but not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- Any other component or device located within or connected to the EP network.

External service providers who may participate in the procurement, development or operation of an EP system are responsible for demonstrating their compliance with the EP Baseline Security Requirements.

## 1.5. Terminology

The following terms are defined to qualify the security statements listed in the rest of the document and in all the other chapters of the standard:

**MUST:** This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the policies.

**MUST NOT:** This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the policies.

**SHOULD:** This word, or the adjective "RECOMMENDED", mean that valid reasons may exist in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

**SHOULD NOT:** This phrase, or the phrase "NOT RECOMMENDED", mean that valid reasons may exist in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

## 1.6. Glossary and Acronyms

The following terms have significant meanings throughout the document:

<b>Public Information</b>	European Parliament information category defined in the Information Security Policy of the European Parliament. Public information is intended to be, or already has been, released to the public.
<b>Parliament Use</b>	European Parliament information category defined in the Information Security Policy of the European Parliament.

<b>Information</b>	Parliament use information is primarily intended for internal use within the European Parliament, although it may, in some cases, be communicated to external entities when required for parliamentary activities; preferably with instructions not to distribute outside their organisation.
<b>Other Confidential Information (non-classified)</b>	European Parliament information category defined in the Information Security Policy of the European Parliament.  This category encompasses information that is of sensitive nature and limited for use within the European Parliament, and/or a limited number of DGs or services within the Parliament administration, other EU Institutions, bodies, offices and agencies established by virtue or on the basis of the Treaties, EU Member States and public administrations.
<b>Information Asset Classification / Information Classification / Data Classification</b>	Classification of information based on the levels of confidentiality, integrity and availability required to protect it.
<b>Password</b>	Secret credential that ensures secure authentication of an account or a user.
<b>Risk Management</b>	Processes and methods used to identify risks and reduce their likelihood and impact. EP Risk assessment methodology
<b>Security standard</b>	Document that list mandatory security requirements, controls, settings and processes. EP security standards form part of the EP Cybersecurity policy framework and ICT security governance.
<b>System Documentation</b>	This sentence refers to any applicable mandatory documentation artefact set out in any of EP methodologies and practices.
<b>Trusted Certificate Authority</b>	Member States maintains a list of qualified trust service providers.  <a href="https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers">https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers</a>
<b>Vulnerability Management Process</b>	Process oriented to identify security vulnerabilities (e.g., weaknesses)

**Acronyms**

<b>ASVS</b>	Application Security Verification Standards
<b>CA</b>	Certification Authority
<b>CSA</b>	Cloud Security Alliance
<b>CIS</b>	Center for Internet Security
<b>CVE</b>	Common Vulnerabilities and Exposures
<b>CVSS</b>	Common Vulnerability Scoring System
<b>DG</b>	Directorate general
<b>DNS</b>	Domain Name System
<b>EP</b>	European Parliament
<b>GSM</b>	Global system for Mobile Communications



<b>HSM</b>	Hardware Security Module
<b>ICT</b>	Information and communications Technology
<b>NTP</b>	Network Time Protocol
<b>OWASP</b>	Open Web Application Security Project (see ASVS)
<b>PKI</b>	Private Key Infrastructure
<b>RDP</b>	Remote Desktop Protocol
<b>SNMP</b>	Simple Network Management Protocol
<b>SSL</b>	Secure sockets Layer
<b>TLS</b>	Transport Layer Security
<b>TPM</b>	Trusted Platform Module

## 2. List of Baseline Security Requirements

### 2.1. Security by Design

**Functionalities are based on well-established security practices and are reduced to the strict minimum required for system operations.**

**Systems and networks must be configured following well-defined standards to function as required and securely. EP is developing and maintaining documented security configuration standards, including standardized operating system and application images.**

#### **General requirements**

1. A risk assessment identifying the main Cybersecurity risks and the Security Controls implemented to mitigate those risks must be conducted for every system in all stages of its lifecycle and its outcome shall be documented early in the system documentation (e.g., architecture or design documents);
2. All system interfaces, components and data flows must be justified and documented (e.g., in architecture or design documents);
3. Functionalities that are not needed (because they do not implement a business or security requirement) must be removed (e.g., scripts, drivers, process, services, daemons, unnecessary web servers, file shares, games ...);
4. Functionalities that are or to be installed must not have undocumented capabilities, especially not those that run against the security and privacy interests of the institution (they must be free from malware, spyware, hidden functionalities, un-documented backdoors or any other unapproved or unwanted functionalities such as non-authorized data forwarding);
5. Only one primary function per server must be implemented in order to prevent functions that require different security levels from co-existing on the same server (e.g., web servers, database servers, DNS should be implemented in different servers);
6. Technologies, protocols and functionalities that are outdated or already recognised as insecure (e.g., TLS 1.1, SSL 3.0, SNMPv2 ...) must not be used;
7. Data from production environments must not be used in other environments;

### **Secure Configurations**

8. EP security standards<sup>2</sup> must be applied and implemented throughout the system. EP standardized operating system and images implementing EP security configuration standards must be used when deployed in the EP environment;
9. Security configurations defined in industry accepted standards (e.g., CIS-CAT, CSA or specific manufacturer hardening standard) must be applied when specific EP security configurations and EP security standards are not available;
10. Vendor-supplied default settings before installing a system (e.g., default passwords, unnecessary default accounts, SNMP community strings, Apache default web server...) must always be changed or disabled;

## **2.2. Network Security**

11. Only network ports, protocols, and services with validated business needs must run on each system;
12. IP forwarding and port forwarding capabilities must be disabled in all hosts unless explicitly needed;
13. Systems components must be segregated according to different trust levels (based on a risk assessment) using existing infrastructure security layers (e.g., firewall rules, gateways, reverse proxies, virtualization security groups or similar mechanisms);
14. Systems must not have direct connectivity to the Internet and must use the EP gateways that provide security controls (e.g., EP proxies/reverse proxies);
15. Host-based firewalls or port filtering tools must be configured on end systems;
16. All firewalls deployed in the solution (host-based, appliances) must use a default reject rule that drops all traffic except those services and ports that are explicitly allowed;
17. Production and non-production systems must be segmented;

### **Wireless Access Control**

18. Wireless peripheral access of devices (e.g., Bluetooth, Wi-Fi) must be disabled, unless such access is required for a documented business need;

---

<sup>2</sup> (ref 1) European Parliament Security Standards <https://itecnet.in.ep.europa.eu/home/ict-security/governance--policies/ict-security-standards-guidelines-and-procedures.html>

## 2.3. Identity and Access Management

**If authentication is unsuccessful, the system must not allow any user specific activities to be performed. Provide and support strong authentication mechanisms for some specific scenarios. Design and pre-configure the solution according to the least privilege and need to know principles, whereby administrative rights are only used when necessary, sessions are technically separated and all accounts are manageable.**

### **General Access Control Design**

19. Access control mechanisms for accessing protected data and resources must be described in details in the system documentation (e.g., architecture or design documents);
20. Access to data and system resources must only be given after successful authentication and authorisation. Without successful authentication and authorisation, the system must not allow any activity;

### **Authentication**

21. Any system requiring user authentication for the purpose of access control must rely on the standard authentication services in place at the EP, in particular, when possible, the solution must be integrated with existing SSO (Single-Sign-On) services;
22. Systems must have the capability to enforce rules or policies for identification and authentication of users that access them (e.g., multi-factor authentication);
23. The system should incorporate multi-factor authentication for all administrative and privileged access and when required according to the risk level of the user authenticated;
24. The system must incorporate multi-factor authentication for all remote network access;
25. Roles and privileges must be properly segregated and managed in the system (e.g., a basic list of roles could be system administrator, user, data base administrator, backup operator, security administrator ...);

### **Passwords**

26. The system must be able to issue initial temporary random passwords for first use. Users must be requested to change this initial temporary password after first use;
27. Initial temporary passwords and recovery tokens must be sent through a secure channel;
28. Passwords must be modifiable in all cases by the user;
29. Modifications of user passwords must require a secured logged session, and the user to enter the old password, new password and a confirmation of the new password;

30. The password rules must be configurable only by the administrator and comply with EP password standard:
- minimal length (8 characters or more)
  - password length (128 characters or longer)
  - minimal complexity (at least 3 of either; both cases, letter, number or special character)
  - reuse (12 last passwords or more)
  - maximal validity (120 days or shorter)
  - maximum number of changes for a given period of time (1 per day);

### **Least Privilege and need-to-know**

31. Every account and every resource (e.g., processes) must have by default only the minimal rights that are required to perform their tasks (e.g., the database administrator or backup administrator accounts should not be assigned the same privileges as the overall systems administrator account); access to system components (e.g., functions, data, URLs, controllers, services ...) must be limited with this approach;
32. Applications and all underlying components and middleware must run with minimal privileges and must **not** use administration accounts shipped with systems;
33. Administration functionality and/or interfaces must **not** be accessible to unauthorized users (also low level interfaces e.g. ILO ...);
34. Administration functionality and/or interfaces must **not** be directly accessible from Internet except for specific source IP addresses (and using when needed a jump host or bastion server);
35. Access controls must ensure the segregation between the different environments (development, pre-production and production);

### **Account Provisioning, Monitoring and Control**

36. An administrator must be able to manage all accounts (including technical and service accounts) without support from the provider or the project team;
37. The system must implement the possibility to inventory all accounts and to audit the use of administrative privileged functions;
38. The system must issue a log entry and alert when an account is added or removed;
39. Every user must have his/her own nominative user account;
40. Shared or default accounts must **not** be used in the system (e.g., "admin" ...);
41. User accounts that cannot be associated with a business process or business owner in the functional and security requirements must be removed;
42. Service accounts and accounts supporting automated application functionalities must prevent interactive login;

43. All users with administrative account access must use a dedicated account for elevated activities. This account should only be used for administration activities and not internet browsing, email, or similar activities;
44. Inactive accounts must be disabled after a configurable amount of time defined in EP standards (e.g. 120 days);
45. Session idle timeouts (e.g., user session, server session) must be configurable as defined in the system documentation (e.g., architecture or design documents); after an idle timeout, the user must re-authenticate or to re-activate the terminal or session;
46. Repeated access attempts to the system must be limited by locking out the user identifier after not more than a configurable number of attempts (defined in the system documentation e.g., architecture or design documents). Set the lockout duration to a configurable value (e.g., 60 minutes) or until an administrator enables the user identifier;
47. Attempts to access deactivated accounts must be logged and monitored;

## 2.4. Asset Protection

### **Provide adequate level of protection for critical information assets during storage and transmission.**

48. An accurate and up-to-date list of all system components (physical and logical) with the potential to store, transmit or process information must be inventoried in the dedicated EP inventories. Physical assets include equipment of any kind, documentation, and premises; logical assets are the system components and the information generated by applications, stored, and communicated between components of the system;
49. An identification and classification of Other Confidential Information (non-classified), Parliament Use Information and Personal Data must be performed for every system; when needed, specific protection requirements (e.g., encryption, integrity, retention, privacy, and other confidentiality requirements) must be defined for these data, based on the risk assessment of the system;
50. Data storage amount and retention time must be limited to that which is required for legal, regulatory and/or business requirements;
51. Security secrets used in the system (e.g., authentication credentials, passwords, API keys, encryption keys ...) must **not** be included in the source code;
52. All security secrets used in the system must be managed and stored securely to resist offline attacks (e.g., salting and hashing passwords using a strong cryptographic function, secure software key storage, TPM or HSM...) and cannot be accessed without root or administrator privileges. All access to password files in the system must be audited and documented;
53. All account user names and authentication credentials must be transmitted only in encrypted form (e.g., HTTPS);

54. All administrative access to a system must use encrypted channels (e.g., protocols such as RDP or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel);
55. Communications between systems and underlying services (e.g. web services, database services) should be encrypted (e.g. HTTPS);
56. Sensitive data (i.e., Other Confidential Information) transmitted between systems and underlying services (e.g. web services, database services) must be encrypted;
57. Any data transmitted over public or open networks (e.g. data in transit from/to cloud providers, Internet, Wi-Fi, GSM...) must be transmitted only in encrypted form;
58. The authenticity of the server and client in a communication link must be verified in order to prevent man-in-the-middle attacks (e.g., application components should validate server certificates and chains; clients requested for authentication);

### **Cryptography**

59. All keys and certificates used in the system must be replaceable;
60. The minimum key length requirement for certificates (and other asymmetric keys) must be 2048 bits;
61. Strong, non-deprecated algorithms, ciphers and protocols must be used throughout the whole certificate hierarchy<sup>3</sup>;
62. Proprietary encryption algorithms must **not** be used;
63. Cryptography implementation must be done based on well-established encryption libraries (e.g., OpenSSL) to avoid implementation weaknesses;
64. No cryptographic means must be used if there are indications that they have been vulnerable to cryptanalysis;
65. The EP PKI Certification Authorities (CA) must be trusted across all systems and applications;
66. Web facing applications must use valid certificates from a trusted Certificate Authority in the EU Trusted Lists<sup>4</sup>; internal applications should use EP Certification Authority TLS certificates;

---

<sup>3</sup> (ref 1) TLS Standard in <https://itecnet.in.ep.europa.eu/home/ict-security/governance--policies/ict-security-standards-guidelines-and-procedures.html>

<sup>4</sup> (ref 2) <https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers>

### **Malware Protection**

67. Anti-malware software must be deployed on all systems commonly affected by malicious software (particularly personal computers and servers);
68. The system must be compatible with the standard anti-virus agent installed at the EP. In case of incompatibility with the standard EP anti-virus, alternative anti-virus solutions must be proposed and validated by EP;

## **2.5. Application Security**

**The application layer is high-risk and may be targeted by both internal and external threats.**

69. Every application must comply with the following applicable standards and methodologies:
  - EP Web Application Security Standard<sup>5</sup>;
  - EP application development standards (only applicable to applications developed at the EP)<sup>6</sup>;
  - recognized applicative security frameworks (e.g., OWASP ASVS for web applications)<sup>7</sup>;
  - specific language secure coding guidelines (e.g., Java Secure coding guidelines)<sup>8</sup>;
70. Information provided in error messages must be generic: it must **not** reveal technical details about the underlying security or any other system internal mechanisms, except for a unique identifier which can be used in troubleshooting;
71. Authentication error messages must **not** provide information about the existence of an account on the application (e.g., valid user-id messages);
72. All newly developed systems must undergo security testing based on their risk level (e.g., application security testing for internet facing web applications or for systems containing Other Confidential Information (non-classified) ...);

---

<sup>5</sup> (ref 1) see <https://itecnet.in.ep.europa.eu/home/ict-security/governance--policies/ict-security-standards-guidelines-and-procedures.html>

<sup>6</sup> (ref 3) <https://ep-foundry.in.ep.europa.eu/standards/>

<sup>7</sup> (ref 4) <https://owasp.org/www-project-application-security-verification-standard/>

<sup>8</sup> (ref 5) <https://www.oracle.com/technetwork/java/seccodeguide-139067.html>



## 2.6. Security Logging and Monitoring

**Logging enables anomaly detection as well as investigation and response to incidents. This section summarizes the most important logging requirements for applications, but for a complete list of requirements, please refer to the EP Logging and Monitoring Standard<sup>9</sup>.**

73. Logging and auditing functions must be included and supported by design (for all components of the system and applications). They must be based on common logging formats in order to feed existing EP Security Information and Event Management (SIEM) and logging and monitoring systems;
74. At least following logs must be capable of being aggregated to the central logging system:
  - Authentication (successful/failed);
  - Creation, deletion, modifications of accounts and permissions;
  - Access to Other Confidential Information (non-classified);
  - Event data identified in the risk assessment as a required mitigation control to an existing risk (e.g., access to the system resources and data, systems activity or modifications of security configurations).
75. Logs must **not** include sensitive information (e.g. passwords, Other Confidential Information (non-classified), personal or financial data like IBAN ...);
76. The system that store logs must have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals;
77. The system must use the EP standard time source in order to achieve exactness of system time. The time source must be authenticated;

## 2.7. Change Management

**Support throughout the lifetime of the system must be such that the system can work as agreed and is secure. Change management shall offer comprehensive and understandable documentation about the overall design of the system, describing its cybersecurity risk, architecture, functionalities and protocols, their realisation in hardware or software components, the interfaces and interactions of components with each other and with internal and external services, the security controls implemented to mitigate the security risks, in order to be able to implement and use the product in the most secure way possible.**

---

<sup>9</sup> (ref 2) <https://itecnet.in.ep.europa.eu/home/ict-security/governance--policies/ict-security-standards-guidelines-and-procedures.html>

### **Support and Maintenance**

78. Support for the system and its components must be guaranteed during a minimum period. If it is not the case, all unsupported system components must be subject to an obsolescence management plan and must be updated to the most current supported version;
79. All system components must be updated timely after publication of security patches;
80. All system components should be updated timely after publication of functional patches;

### **Vulnerability Management**

81. The complete system with all its components, including extensions and enhancements, must be included in the EP vulnerability management standard<sup>10</sup>;
82. Research for potential vulnerabilities for all the components used to develop the solution must be guaranteed;
83. Timely provisioning of security patches or other appropriate risk mitigation measures, when new vulnerabilities are discovered must be guaranteed. As a first remediation step, the provider should at least respond with a remediation plan at the latest within 48 hours for “Critical” severity vulnerabilities (CVSS between 8.0-10.0)<sup>11</sup>. The plan must indicate the timeframe for resolving the vulnerability;

### **Supply Chain Security**

84. The authenticity checking method(s) of the product must be capable of checking the integrity and tracing back software and/or hardware components to their genuine sources;

### **Document Transparency**

85. The system documentation must be compliant with EP Project Management Methodology (ENGAGE) and will be updated when there are major changes to design or functionality;

---

<sup>10</sup> (ref 1) EP vulnerability management standard in <https://itecnet.in.ep.europa.eu/home/ict-security/governance--policies/ict-security-standards-guidelines-and-procedures.html>

<sup>11</sup> <https://www.first.org/cvss/calculator/3.0>

## 2.8. Data Backup and Recovery

**For a variety of reasons, the data stored in the system might not be accessed in a normal way. In that case, the data shall be retrieved from a different storage.**

- 86. Every system components and data must be backed up on a predefined frequency;
- 87. Backup media must be tested on a regular basis by performing a data and system restoration process to ensure that the backup is working properly;
- 88. All back-ups must have an off-line version allowing the restore of information systems at a certain moment in time;
- 89. Backups must be properly protected via physical security or encryption when they are stored, as well as when they are moved across the network (e.g., remote backups and cloud services);

## 2.9. Third Party Security

**Provide evidence that a managed security by design approach has been adopted, including documented secure software development, quality management and information security management processes.**

- 90. The provider must possess a current valid security certification (e.g., ISO27001 or corresponding) in the relevant area (e.g., development, production, cloud);
- 91. Relevant information security directives that are applicable to its product (e.g., regulation EC 2018/1725 with regard to the processing of personal data by the European Union institutions) must be provided;