Implementation analysis regarding the technical specifications and other key elements for a future EU system for traceability and security features in the field of tobacco products

Final Report

Annex III – Model Contract

Service Contract N° 2015 71 05

everis
April 2017

Public Health

EUROPEAN COMMISSION

Consumers, Health, Agriculture and Food Executive Agency
Health Unit

Directorate-General for Health and Food Safety
Directorate B-Health systems, medical products and innovation
Unit B2- Health in all policies, global health, tobacco control

E-mail: *CHAFEA-HP-TENDER@ec.europa.eu*

SANTE-B2-Tobacco-Control@ec.europa.eu

European Commission
B-1049 Brussels

Implementation analysis regarding the technical specifications and other key elements for a future EU system for traceability and security features in the field of tobacco products

Final Report

Annex III – Model Contract

Service Contract N° 2015 71 05

Consumers, Health, Agriculture and Food Executive Agency
Health Programme

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*)**:**

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

This report was produced under the health Programme (2014-2020) in the frame of a specific contract with the Consumers, health, Agriculture and Food Executive Agency (Chafea) acting under the mandate of the European Commission. The content of this report represents the views of the contractor and is its sole responsibility; it can in no way be taken to reflect the views of the European Commission and/or Chafea or any other body of the European Union. The European Commission and/or Chafea do not guarantee the accuracy of the data included in this report, nor do they accept responsibility for any use made by third parties thereof.

More information on the European Union is available on the Internet (http://europa.eu).

Luxembourg: Publications Office of the European Union, 2018

PDF	ISBN 978-92-9200-876-5	doi:10.2818/751591

TABLE OF CONTENTS

INTRODUCTION

The following document serves as the Final Report to the European Commission´s Consumers, Health, Food and Agriculture Executive Agency (Chafea) in response to the request for service Chafea/2015/health/40 for the implementation of Framework Contract FWC DIGIT/R2/PO/2013/004 ABC III Lot 2, concerning the implementation analysis regarding the technical specifications and other key elements for a future EU system for traceability and security features in the field of tobacco products.

The present document is the Annex III of the study carried out, and is complemented by:

- Main Report
- Annex I – Evaluation of Policy Options
- Annex II – Technical Specifications of the Tracking and Tracing System and the Security Features

All these documents are made public, and can be requested under the following publication numbers:

Volume	Catalogue number	ISBN	DOI
Main Report	EB-02-17-895-EN-N	978-92-9200-770-6	10.2818/453932
Annex I – Evaluation of Policy Options	EB-02-17-896-EN-N	978-92-9200-874-1	10.2818/628162
Annex II – Technical Specifications of the Tracking and Tracing System and the Security Features	EB-02-17-897-EN-N	978-92-9200-875-8	10.2818/343517

MODEL CONTRACT FOR THE THIRD PARTY DATA STORAGE

This Agreement is signed

Between

[*Name of the Contractor*], [*legal form*] with its registered office at [_____], and registered in the [*Legal Entities' Registry or equivalent*] under N° [_____] and with VAT N° [_____];

Hereinafter referred to as "the **Contractor**";

Represented by [*name*], *[function*];

And

[*Name of the Manufacturer/Importer*], [*legal form*] with its registered office at [_____], and registered in the [*Legal Entities' Registry or equivalent*] under N° [_____] and with VAT N° [_____];

Hereinafter referred to as "the **Manufacturer/Importer**";

Represented by [*name*], [*function*];

The Contractor and the Manufacturer/Importer shall hereinafter be referred to jointly as "the **Parties**" or individually as "the **Party**".

This Agreement (hereinafter: the "Agreement") includes:

- General Terms of Service
- Annex 1: Requirements Specification
- Annex 2: Service Level Agreement
- Annex 3: Price Conditions
- Annex 4: Definitions

WHEREAS

1. Directive 2014/40/EU (hereinafter: "the **Directive**") aims to improve the functioning of the internal market for tobacco and related products, while ensuring a high level of health protection for European citizens. The Directive entered into force on 19 May 2014 and became applicable in the EU Member States on 20 May 2016.

2. The Commission has developed the requirements of the Directive in the provisions set out in:

- Commission Implementing Decision (EU) XXXX/2017 and its annex on technical standards for security features applied to tobacco products,

- Commission Implementing Regulation (EU) XXXX/2017 and its annexes on technical standards for the establishment and operation of a traceability system for tobacco products, and
- Commission Delegated Regulation (EU) XXXX/2017 on key elements of data storage contracts to be concluded as part of a traceability system for tobacco products,

which form the basis for this Agreement.

3. Article 15(5) of the Directive requires that all economic operators involved in the trade of tobacco products, from the manufacturer to the last economic operator before the first retail outlet, record the entry of all unit packets into their possession, as well as all intermediate movements and the final exit of the unit packets from their possession.

4. For the purpose of hosting the data storage facility for all relevant data generated by the abovementioned obligation, Article 15(8) requires Member States to ensure that manufacturers and importers of tobacco products conclude data storage contracts with an independent third party. The data storage facility shall be physically located within the territory of the European Union.

5. The resulting data storage of the Tracking and Tracing System shall be composed of

i) a group of independent Primary Data Storage solutions, where each Primary Data Storage solution shall host data exclusively related to a single manufacturer/importer or a specific group of manufacturer(s)/importer(s);

ii) a central Surveillance Data Storage solution, which shall host a global copy of the distributed data. The Surveillance Data Storage solution shall be able to offer a comprehensive logical view of all relevant data based on its local data, which could be further exploited for the enforcement activities required by the Directive. Also, the Surveillance Data Storage solution shall provide a secure Repository Router component, as defined in Annex 1 (Requirements Specification), to facilitate distributors and wholesalers transmitting their reports seamlessly through a single point.

6. Pursuant to Article 15(8) of the Directive, the European Commission must approve the suitability of the Contractor, in particular its independence and technical capacities, as well as the data storage contract.

7. The present Agreement regulates the relationship between the Parties.

The Parties have agreed as follows:

GENERAL TERMS OF SERVICES

Table of Contents

1. Definitions

1.1. In this Agreement, all terms shall have the same meaning as defined in Article 2 of the Directive and Article 2 of Implementing Regulation XXX/2017, unless specifically provided in the Agreement. Such terms and their definitions are set out in Annex 4 (Definitions).

1.2. Unless specifically defined in the Agreement, capitalised terms or expressions shall have their meaning indicated in Annex 4.

2. General scope and structure of the Agreement

2.1. The Agreement is structured as follows:

- General Terms of the Service (hereinafter: "GTS")
- Annex 1: Requirements Specification (hereinafter: "RS")
- Annex 2: Service Level Agreement (hereinafter: "SLA")
- Annex 3: Price Conditions (hereinafter: "PC")
- Annex 4: Definitions

2.2. The GTS describes the general content of the commitments that the Parties assume with regard to the provision of Service by the Contractor, and further details the specific content of the commitments that the Parties respectively assume.

The "Service" relates to the services required to be carried out in accordance with art.25 and 26 of Implementing Regulation XXXX/2017, and means any and all services to be provided by the Contractor under the Agreement, including:

(i) the deployment and operation of the Data Storage;
(ii) the deployment and operation of testing interfaces to support the connectivity with the economic operators and the other solutions of the System described in the RS in Annex 1;
(iii) the obligation to carry out patches, fix bugs, or perform other maintenance on the Service, in compliance with the RS in Annex 1 and the SLA in Annex 2; and
(iv) the deployment and operation of all necessary services to accomplish the functional and technical requirements as described in Annex 1.

2.3. The Service to be provided by the Contractor to the Manufacturer/Importer is described in detail in Annex 1.

3. Duration of the Service

3.1. The Agreement shall enter into force on the date on which it is signed by the last Party and shall continue and remain in full force for a minimum period of five (5) years (hereinafter: "the Term") unless and until it is terminated sooner in accordance with the Agreement.

3.2. The Manufacturer/Importer shall have the right to extend the Term by giving the Contractor written notice of its intention to do so at least six (6) months before the end of the Term or extended term (as the case may be). All extensions to the Term shall be carried out in accordance with the same terms and conditions set out in this Agreement.

4. Main duties and warranties of the Contractor

4.1. The Contractor shall provide the Services as described in the RS. The Contractor and the Manufacturer/Importer may agree to include additional services in the RS.

4.2. The Contractor warrants that the Service shall be provided in compliance with the Agreement. It also warrants that it shall be implemented at latest by the date specified in the Agreement.

4.3. The Contractor warrants that the Service shall be provided in compliance with the applicable law and Implementing Regulation XXX/2017 and Delegated Regulation XXX/2017 adopted under the Directive.

4.4. The Contractor warrants its independence from the tobacco industry, in accordance with the requirements set out in Article 35 of Implementing Regulation XXX/2017, and its technical capacities with respect to the provision of the Service referred to in Article X of this Agreement. The independence and technical capacities of the Contractor shall be maintained throughout the full duration of the Agreement. The Manufacturer/Importer may terminate the Agreement, in accordance with Part XY of Implementing Regulation XXX/2017, if those conditions are no longer fulfilled.

4.7. The Contractor agrees to provide the Manufacturer/Importer with information on maintenance, as defined in the RS in Annex 1, throughout the execution of the

Agreement. This information shall be provided upon request by the Manufacturer/Importer.

4.8. The Contractor shall make support services available to the Manufacturer/Importer, pursuant to the specifications set forth in the SLA in Annex 2.

4.9. The Contractor shall maintain the operability, availability and performance of the Service for the duration of this Agreement, in accordance with the requirements set forth in the RS in Annex 1.

4.10. The Service may be interrupted by the Contractor for the performance of corrective or preventive maintenance.

4.11 The Contractor shall notify the Manufacturer/Importer in advance of scheduled ordinary maintenance. The Contractor shall make all reasonable efforts to forewarn the Manufacturer/Importer of extraordinary maintenance and to minimise the inconvenience resulting from such interventions.

5. Change control procedure

5.1. The Manufacturer/Importer may at any time propose or request changes, modifications, or additions to the scope of the Service. The Contractor may also propose changes.

5.2 Any amendment of this Agreement that relates to provisions linked to any of the key elements listed in the Delegated Regulation XXXX/2017 shall be communicated and approved by the European Commission.

5.3. Any amendment of this Agreement that does not related that relates to provisions linked to any of the key elements listed in the Delegated Regulation XXXX/2017 shall be communicated to the European Commission.

5.4 The Contractor shall not take any action or implement any decision which may affect the Service or decrease the resource efficiency to a level below the agreed SLA, without first obtaining the approval of the Manufacturer/Importer and the European Commission.

6. Confidentiality and announcements

6.1. The Recipient Party shall hold all confidential information in strict confidence and specifically shall:

(i) use confidential information only for the purposes of the performance of its obligations under this Agreement;

(ii) notify the Disclosing Party immediately upon suspecting or becoming aware of any unauthorised disclosure, access or use of confidential information and take all measures necessary to prevent any (further) unauthorised disclosure, access or use thereof.

6.2 In duly justified cases, the European Commission or the Member States may grant manufactures or importers access to a defined set of stored data, as provided for by Article 15(8) of the Directive. The Manufacturer/Importer shall:

(i) restrict disclosure of or access to confidential information to its representatives, advisors, auditors, members and users who require such information for the performance of the Agreement, and not divulge confidential information to any other third parties or give any other third party access to confidential information without the Disclosing Party's prior written consent;

(ii) subject any person having access to confidential information for the performance of the Agreement to confidentiality and non-use obligations at least as restrictive as the ones set out in the Agreement, and make such persons aware, prior to any disclosure or access, of the confidential nature of this information. Upon request, the Recipient Party shall provide the Disclosing Party with the names of the persons having access to confidential information;

(iii) make copies of confidential information only when strictly necessary for the performance of the Agreement, and not alter, modify, dissemble, reverse engineer, or decompile any confidential information.

6.3. Neither Party shall issue any media release, public announcement, or other disclosure relating to the existence, purpose or content of the Agreement or use the name, trademark or logo of the other Party without that Party's prior written consent. This shall include, without limitation, use in promotional or marketing material, provided that nothing in this article shall restrict any disclosure to the extent required by a legislative, administrative or judicial action as mentioned under article above.

6.4. The obligations and restrictions set forth in this article shall remain in force for the full Term of the Agreement and shall remain in force for ten (10) years after the expiration or termination of the Agreement for any reason whatsoever.

7. Data protection

7.1. In this article, the terms "process", "data processor", and "data subject" shall have the meanings indicated in the EU Data Protection Directive 95/46/EC and, from 25 May 2018, shall be in compliance with Regulation EU 679/2016, and national implementing legislation in EU Member States, as well as other applicable data protection and privacy laws and regulations (hereinafter: "Data Protection Laws").

7.2. The Contractor agrees to perform all Services under this Agreement, including and without limitation the collection, use, processing, storage, and maintenance of any data, in accordance with Data Protection Laws and the terms of this article.

7.3. The Contractor shall:

(i) ensure that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(ii) respect the conditions referred to in Article 7.2 of this Agreement for engaging another processor;

(iii) taking into account the nature of the processing, assist the European Commission by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the EC's obligation to respond to requests for exercising the rights of data subjects;

(iv) observe the provisions of article 19 of Delegated Regulation XXXX/2017 in terms of Data portability;

(v) make available to the European Commission all information necessary to demonstrate compliance with the obligations laid down in this article and allow for and contribute to audits, including inspections, conducted by the European Commission, competent authorities of Member States and auditors mandated by the European Commission.

7.4. To the extent that any data is processed under the Agreement, or if the Contractor receives or has access to any data under or in relation to this Agreement, the provisions of this article shall apply. To the extent that the Contractor receives and/or processes data under or in relation to this Agreement on behalf of the Manufacturer/Importer, the Contractor, as data processor and with respect to this data, shall:

(i) process data only to the extent and in such a manner that is necessary for the provision of the Service and for no other purpose;

(ii) ensure that all necessary or appropriate technical and organisational measures are taken to (a) protect the security and confidentiality of data processed; (b) protect the data against unauthorised or unlawful processing and against accidental loss, destruction, or damage; and (c) implement the security measures imposed under applicable law or adopted by competent authorities;

(iii) not disclose any data to any of its employees, directors, agents or affiliates or any third party, except as necessary for the performance of the Service;

(iv) take reasonable steps to ensure the reliability and integrity of any staff who have access to the data and, if sensitive data is processed, draft a list of the categories of persons having access to such data with a description of their function, ensure that such persons are subject to a statutory or contractual obligation to maintain the confidentiality of such data, and keep a list of such persons at the disposal of the Manufacturer/Importer or competent authorities;

(v) not cause or permit data to be transferred outside the territory of the European Union;

(vi) provide, at no charge, any assistance that the Manufacturer/Importer may reasonably require in order to deal with any request for data subject access in compliance with applicable Data Protection Laws; or any request, inquiry or investigation initiated by any relevant competent authority in respect to data;

(vii) comply with all relevant provisions of applicable Data Protection Laws.

8. Data access rights

8.1. Parties agree that access to the recorded data shall be given only to the European Commission, the competent authorities of the Member States, and the external auditor in accordance with Article 15.8 of the Directive. Neither the Manufacturer/Importer nor the Contractor shall have access to the data recorded.

8.2. Only in duly justified cases, the European Commission or the competent authorities of the Member States may grant the Manufacturer/Importer access to the data stored, provided that commercially sensitive information remains adequately protected in conformance with relevant Union and Member State law, and subject to the requirements

of the legal framework of [EU country of Manufacturer/Importer]. For this purpose, the Manufacturer/Importer shall request access, in writing, from the European Commission or, as applicable, the competent authority of the Member State concerned.

8.3. The Contractor shall process data supplied by the Manufacturer/Importer only for the purposes of this Agreement, pursuant to the Directive and the Delegated Regulation (EU) XXXX/2017 on key elements of data storage contracts to be concluded as part of a traceability system for tobacco products. The Contract shall not receive from the Manufacturer/Importer any guidance on the processing of the data recorded.

9. Prices, billing and payments

9.1. In consideration for Contractor carrying out the Services, the Manufacturer/Importer shall pay to the Contractor the charges set out in Annex 3 upon receipt of a valid invoice corresponding to those charges.

9.2. Except for VAT, the Contractor shall be responsible for all tax liabilities in respect to any amounts payable. The Contractor hereby agrees to indemnify the Manufacturer/Importer in respect to any claims that may be made against the Manufacturer/Importer by the relevant competent authorities, in respect to tax or similar charges, and any costs, interest and penalties that may be found due in respect to such charges.

9.3. All sums due to the Contractor under this Agreement shall be payable by the Manufacturer/Importer by electronic bank transfer upon receipt of a correct, undisputed and properly due invoice which shall state, at minimum:

(i) a short description of the relevant Services;

(ii) the period to which the invoice corresponds;

(iii) the Contractor's bank account for payment; and

(iv) all charges and applicable taxes.

9.4. If the Manufacturer/Importer has a bona fide dispute in relation to an entire invoice or any parts of an invoice submitted by the Contractor, the Manufacturer/Importer may withhold payment of the amount in dispute. In this event, the Contractor shall continue to perform its obligations under the Agreement and shall not suspend the provision of any Service or other obligations under the Agreement.

9.5. If any amount, in the absence of a dispute, is not paid on or before the due date and remains unpaid for a period of fifteen (15) days after receipt by the Manufacturer/Importer of a written reminder from the Contractor sent by registered mail, the penalties included in Directive 2011/07/EU on late payments shall apply.

9.6. Suspension of services in case of late payments by a manufacturer or importer to the provider shall be prohibited, unless the delay exceeds the final payment deadline by thirty days or more.

10. Location and subcontracting

10.1. The Contractor facilities providing the Service and the data storage facilities must be located on the territory of the European Union. In the case that the borders of the European Union change during the execution of the Service, the Contractor shall ensure that the facilities providing the Service remain on or are relocated to the territory of the European Union.

10.2. Changes to the physical location of the Contractor's facilities during the Term of the Agreement may take place only with the written approval of the Manufacturer/Importer.

10.3. The Contractor may subcontract parts of the Service to third parties. The subcontract shall not affect the primary responsibility of the Contractor for the performance of the Agreement.

10.4. In case of subcontract, the Contractor shall:

(a) ensure that the proposed subcontractor has the necessary technical expertise and meets the requirements of independence laid down in Article 35 of Implementing Regulation XXXX/2017.

(b) submit to the Commission a copy of the declaration referred to in Article 8 of the Delegated Regulation signed by the respective sub-contractor(s).

11. Intellectual Property Rights

11.1. Unless otherwise expressly agreed elsewhere in this Agreement, no Intellectual Property Rights (IPR) are intended to be transferred as a result of the Agreement and nothing in the Agreement shall result in the Manufacturer/Importer having any right, title, licence to or interest in any pre-existing IPR of the Contractor, in respect of which all rights are hereby expressly reserved.

11.2. The Manufacturer/Importer shall grant the Contractor, as of the effective date, a non-exclusive, royalty-free, sub-licensable, non-transferrable and worldwide licence to use the pre-existing IPR of the Manufacturer/Importer for the entire duration and exclusive purpose of the provision of Services under this Agreement. If the Contractor uses pre-existing IPR of the Manufacturer/Importer, the Contractor shall be responsible for verifying and ensuring that:

(i) the pre-existing IPR is fit for purpose; and

(ii) none of the licence types or terms applicable to pre-existing IPR (if any), as provided to the Contractor, restrict the Contractor's ability to transfer ownership and/or grant the licences to pre-existing IPR as provided for in this Agreement.

11.3. The Contractor shall grant the Manufacturer/Importer, as of the effective date, a non-exclusive, royalty-free, sub-licensable, transferrable, irrevocable and worldwide licence to use the pre-existing IPR of the Contractor, if and to the extent necessary or useful for the Service provided and in order to use the system, for any purpose. For the avoidance of doubt, this shall include without being limited to the right to execute, display, install, test, reproduce, distribute, sub-licence, modify, maintain, enhance, commercially exploit and create derivative works of, grant sub-licences to third parties, and further develop the pre-existing IPR (and any third party IPR incorporated or delivered by Contractor):

- contained in the system; and

- otherwise delivered to the Manufacturer/Importer by the Contractor or required in order to use, maintain or develop the system.

12. Business Continuity Plan

12.1. The Contractor shall develop a Business Continuity Plan, based on ISO 22301:2012, prior to the commencement date.

12.2. This Business Continuity Plan (hereinafter: "BCP") shall include, at minimum, the following structure:

(i) Introduction

(ii) Plan activation: Detail who shall be responsible for activation of the BCP, when, and what are the subsequent control mechanisms to ensure that all aspects are efficiently and effectively covered.

(iii) Responsibilities: Identify the specific responsibilities for key roles and teams within the organisation, highlighting the responsibilities of Emergency Response Teams and key staff.

(iv) Risk mitigation activities and processes: A series of identified potential risks, the planned mitigation of each risk, and the processes/procedures that shall be followed in the event that the specific risks occur.

(v) Emergency processes and procedures: Identify all processes and procedures that may be required to fully and effectively handle emergency situations. Unless specifically mentioned, the assumption shall be that the entire content of the BCP is applicable when any emergency situation arises. This section shall also address:

- Emergency alert and escalation;
- Evacuation;
- Handling of insurance;
- Handling of media and press releases, if required;
- Financial and legal considerations.

13. Auditing

13.1. In the case of announced and unannounced audit visits, the Contractor shall grant the European Commission, the competent authorities of the Member States, and any external auditor appointed by the European Commission access to the Contractor facilities and all locations that are otherwise relevant to this Agreement. In this regard, the Contractor shall provide reasonable support as required throughout the Term of this Agreement in order for the following actions to be undertaken:

(i) access the build and test environments of the Contractor to verify compliance with the Contractor's obligations under this Agreement;

(ii) verify Contractor compliance with legal and regulatory requirements;

(iii) verify the accuracy of the charges in connection with the Services, and any other amounts payable or receivable by the Manufacturer/Importer under this Agreement;

(iv) verify that the Contractor's systems protect the integrity, operational availability, and security of data and confidential information; and

(v) verify that the Services are being provided and the Contractor's obligations are being fulfilled, in accordance with this Agreement.

14. Liability

14.1. The Contractor shall be liable for and shall hold harmless, defend and indemnify the Manufacturer/Importer from and against any direct damages arising out of or relating to its performance under this Agreement, whether based on an action or claim, in contract, equity, negligence, tort, or otherwise, for all events, acts or omissions.

14.2. Liability of either of the Parties shall not be limited in case of breach of confidentiality and/or data protection rules, wilful misconduct, or gross negligence.

14.3. Without prejudice to the article of this Agreement, neither Party shall be liable for any claims, proceedings, damages, expenses, costs or losses that are indirect or consequential, including third parties' claims, regardless of whether the damages were foreseeable or arose in connection with the Party's participation in the Services, and/or performance of the Party's obligations under this Agreement.

14.4. Liability provisions set in this article applicable without prejudice to the applicable law set in article 20 of this Agreement.

15. Force Majeure

15.1. A "Force Majeure Event" shall be understood in accordance with the laws of [EU country of Manufacturer/Importer].

15.2. Any failure or delay by the Manufacturer/Importer or the Contractor in the performance of obligations under this Agreement due to a Force Majeure Event shall not be deemed a breach of the Agreement or a ground for termination, provided that the non-performing Party attempts to recommence performance whenever and to whatever extent possible without undue delay. Upon the occurrence of a Force Majeure Event, the non-performing Party shall be excused from the performance of those obligations under this Agreement that are affected by the Force Majeure Event for as long as the Force Majeure Event continues.

16. Insurance and guarantee

16.1. The Contractor shall provide the Manufacturer/Importer with evidence of insurance against all insurable risks of damage, loss or injury caused by the Contractor in the performance of the Agreement, including any act by its staff or by any person acting on the Contractor's behalf under the Agreement.

16.2 The insurance shall be the type that is customary for the industry sector in which the Contractor operates and shall include insurance coverage for professional and corporate liability, providing coverage for at least the amount defined in the STS. In any case, the minimum amounts stipulated shall not prevent the Contractor from complying with the obligation to insure itself for higher amounts, where deemed necessary, as provided in statutory provisions. Furthermore, the amounts of insurance stipulated shall in no way limit or diminish the obligation of the Contractor to compensate the Manufacturer/Importer for damages incurred.

16.3. The Contractor shall provide at its own expense and as security for due performance of the Agreement, including the obligation to pay a contractual penalty, a guarantee for the amount to be secured, issued by an established credit institute of good standing registered the European Union. This guarantee must in all cases be directly enforceable, unconditional, irrevocable, and issued for the duration of the Service set forth in the Agreement and according to the applicable law.

16.4. At the Contractor's request, the Manufacturer/Importer shall return to the former or to the guarantor any guarantee deeds provided to it, as soon as it is established that the Manufacturer/Importer can no longer invoke any of the rights secured by the guarantee.

17. Termination

17.1. The Agreement may be terminated for cause by the Manufacturer/Importer without prejudice to any right or remedy the Manufacturer/Importer may have against the Contractor for breach or non-performance of this Agreement. The Manufacturer/Importer may terminate this Agreement for cause if:

(i) the Contractor commits a material breach of any of its obligations or of the terms and conditions set out in this Agreement, provided that where such breach is capable of remedy, the Contractor has been notified in writing of the breach and has not remedied it within thirty (30) days of receipt of the notice;

(ii) any of the representations, warranties and undertakings given by the Contractor have become materially inaccurate during the term of the Agreement;

(iii) following an independent review by a qualified external party, it is determined that Contractor is not or shall not be able to complete the Services within the timescale contemplated in this Agreement;

(iv) the Contractor is in breach of its obligations relating to confidentiality, security and/or data protection;

(v) the Contractor or any of its staff are in breach of any anti-corruption laws, as defined in Annex 4; and/or

(vi) the Manufacturer/Importer exercises its right to terminate all or part of the Agreement under Article 9 (“Prices, billing and payments”) of this Agreement.

17.2. The Agreement may be terminated for cause by the Contractor if the Manufacturer/Importer fails to pay any undisputed charges invoiced for Services under the Agreement, exceeding the due date for payment by three (3) months. In this case, the Contractor may give the Manufacturer/Importer notice of its intention to terminate the Agreement if payment is not received within thirty (30) days of that notice.

17.3. In connection with Part C of Annex 1 to the Implementing Regulation (EU) XXXX/2017, the following requirements apply:

1. Where, at any time after the appointment of a provider of a primary repository, the Commission determines that such a provider no longer possesses the independence or capacity requirements as provided for in Article 15(8) of Directive 2014/40/EU, it shall inform the parties to the data storage contract who shall initiate the termination of that contract.

2. Where the contractual relationship between a manufacturer and importer and the provider of a primary repository is terminated, or expected to be terminated, by any of the parties to the contract, for any reason, including for the reasons referred to in paragraph 1, the manufacturer or importer shall immediately inform the Commission of such termination, or expected termination, and as soon as it is known, the date of the notification of termination and the date at which the termination is to take effect. The manufacturer or importer shall propose and notify to the Commission a replacement provider as soon as practicable, and at the latest, three months prior to the termination date of the existing contract.

3. The appointment of the replacement provider shall take place in accordance with paragraphs 3 to 7 of Part A of Annex 1 to the Implementing Regulation (EU) XXXX/2017.

4. In the event that the operator of the secondary repository gives notice of its intention to cease operating that repository in accordance with the contract entered into pursuant to Part B of Annex 1 to the Implementing Regulation (EU) XXXX/2017, it shall immediately inform the Commission thereof and of the date at which the termination is to take effect. The providers of the primary repository system shall nominate and notify to the Commission a replacement operator as soon as practicable, and at the latest, three months prior to the termination date of the existing contract.

5. Where the finding referred to in paragraph 1 applies to the provider who has been appointed to operate the secondary repository, the parties to the contract for the operation of that secondary repository shall, in turn, be terminated.

6. The termination of the contract for the operation of the secondary repository system and the appointment of the replacement operator of the secondary repository shall take place in accordance with termination and appointment provisions set out in Part B of Annex 1 to the Implementing Regulation (EU) XXXX/2017.

18. Termination assistance, data and knowledge transfer

18.1. Following notice of termination of this Agreement for any reason, the Contractor shall provide termination assistance as is reasonably required for the period of time that is reasonable for an orderly disengagement and (where applicable) seamless transition to the next Contractor.

18.2. Contractor shall perform the termination assistance services described in this Agreement. In particular, the Contractor shall:

(i) transfer the services, the system, and/or the work products to the next Contractor within a reasonable timeframe; and

(ii) assist with the handover of operational responsibility to the next Contractor.

18.3. The Contractor shall provide an interim and a final Termination Assistance Plan following the guidelines of this Agreement. Within sixty (60) days of the notice of termination of the Agreement, the Contractor shall deliver a copy of its initial Termination Assistance Plan to the European Commission.

18.4. Upon written request during the Termination Assistance Period, the Contractor shall provide data regarding:

(i) consumption and utilisation of resources;

(ii) business process procedures and work flow;

(iii) business process volumes and statistics;

(iv) business process training modules;

(v) performance histories;

(vi) current and projected work volumes; and

(vii) any other data reasonably requested by the European Commission about the services deemed necessary for the next Contractor to assume responsibility for continued performance of the services.

18.5. The Contractor shall provide a transfer of knowledge regarding the services and related topics (which may be specified in the Termination Assistance Plan) to facilitate the provision of replacement services by the next Contractor. This shall include:

(i) participation in workshops, meetings, and "hands-on" activities;

(ii) providing the next Contractor with information about the Service that is necessary to implement the Termination Assistance Plan; and

(iii) providing the next Contractor with information about the Service in order for the next Contractor to assume responsibility for the continued performance of the Service in an orderly manner, thereby minimising disruption to operations.

18.6. The Contractor shall deliver to the next Contractor an up-to-date backup of the data stored during the performance of the Service. Any maintenance after this delivery and any additional data received or created shall be migrated to the next Contractor without undue delay.

18.7. The Contractor shall have no right of retention with respect to any data, information and/or other necessary material to be delivered to the next Contractor and shall allow full data portability in accordance with this Agreement.

18.8. The Contractor shall not retain in any way any data or copies of provided data longer than necessary for the performance of the Agreement. Upon request by the Manufacturer/Importer, the European Commission, or a competent authority of a Member State, the Contractor shall deliver a certificate executed by one of its duly authorised officers, confirming compliance with destruction obligations.

19. Amendments to the Agreement

19.1 Pursuant to Article 15(8) and (10) of the Directive, and Article 5 of this Agreement, the Parties do not have the right to amend this Agreement without previous approval by the European Commission if the amendment relates to provisions linked to any of the key elements listed in the Delegated Regulation (EU) XXXX/2017.

20. Applicable law and disputes

20.1. In the event of any dispute arising out of or in connection with this Agreement, the Parties agree, without prejudice to the rights of either Party, to immediately seek an interim or final remedy before the court, as set forth in Sub-article 20.3 of the Agreement to attempt in good faith to resolve the dispute amicable and without undue delay.

20.2. If either Party does not agree with any dispute referred for determination in accordance with Sub-article 20.1, then the dispute shall be determined by the [EU country of Manufacturer/Importer] courts in accordance with the sub-article.

20.3. The construction, validity and performance of this Agreement and all non-contractual obligations arising from or connected with this Agreement shall be governed by, and construed in accordance with, the Laws of [EU country of Manufacturer/Importer]. Any dispute arising out of this Agreement shall be subject to the exclusive jurisdiction of the courts of [courts of the seat of the Manufacturer/Importer], to which both Parties hereby agree to submit irrevocably for these purposes.

21. Miscellaneous

21.1 This Agreement constitutes the entire agreement between the Parties. There are no oral agreements or understandings. Any amendment or addition to the Agreement that relates to provisions linked to any of the key elements listed in the Delegated Regulation XXXX/2017, must be pre-approved by the European Commission.

21.2 Should a clause of the Agreement be or become invalid, the remainder of the Agreement shall remain in force. The invalid clause must be replaced by a valid clause that achieves the object and purpose of the invalid clause to the greatest extent possible.

21.3 If the Agreement contains any gap or ambiguity, it shall be interpreted in light of the object and purpose of the Directive.

On behalf of the Contractor:
Name (written in full):
Position:
Address:
Signature…….
(Stamp of organisation)

On behalf of the Manufacturer/Importer:
Name (written in full):
Position:
Address:

Signature…….
(Stamp of organisation)

ANNEX 1 – REQUIREMENTS SPECIFICATIONS ("RS")

1. Primary Data Storage

a. Requirements specifications

i. Functional

Functional Requirements – Tracking and Tracing System – Primary Data Storage		
ID	**Name**	**Priority**
RQ_TTPR_FU_1	Unique identifier at unit packet level – information to be determined	Must have
The Primary Data Storage solution shall ensure that the following information can be determined for a unique identifier: • the date of manufacturing; • the place of manufacturing; • the manufacturing facility; • the machine used to manufacture the tobacco products; • the time of manufacture; • the product description; • the intended market of retail sale; • the intended shipment route; • where applicable, the importer into the Union; • the serial number; • the actual shipment route from manufacturing to the first retail outlet, including all warehouses used as well as the shipment date, shipment destination, point of departure and consignee; • the identity of all purchasers from manufacturing to the first retail outlet; and • the invoice, order number and payment records of all purchasers from manufacturing to the first retail outlet This shall be accomplished through the processing of the data transmitted by the economic operators.		
RQ_TTPR_FU_2	Unique identifier at aggregation packaging level – information to be determined	Must have
The Primary Data Storage solution shall ensure that the following information is determined for a unique identifier at aggregation packaging level: • the date of manufacturing; • the location of the aggregation activities; and • a serial number. This shall be accomplished through the processing of the data transmitted by the economic operators.		
RQ_TTPR_FU_3	All relevant transactions – storage	Must have
The Primary Data Storage shall ensure that all relevant transactions of all natural and legal persons engaged in the supply chain of tobacco products that are received into the system are stored properly.		
RQ_TTPR_FU_4	All relevant transactions – support at aggregation packaging level	Must have
The Primary Data Storage shall support relevant transactions that have been recorded at aggregation packaging level.		
RQ_TTPR_FU_5	All relevant transactions – transmission interface for manufacturers and importers	Must have
The Primary Data Storage shall provide a secure interface for the manufacturers and importers to allow the transmission of all relevant transactions.		
RQ_TTPR_FU_6	Shipment and trade information available through an electronic link	Must have

Functional Requirements – Tracking and Tracing System – Primary Data Storage		
ID	**Name**	**Priority**
The Primary Data Storage shall provide a secure interface to make available shipment and trade information through a link to the unique identifier.		
RQ_TTPR_FU_7	Stored data - prevent data access	Must have
The Primary Data Storage shall prevent access by any party other than the competent authorities of the Member States, the Commission, and the external auditors, thereby ensuring that economic operators or any other party involved in the trade of tobacco products are forbidden to read, update or delete any data stored in the system.		
RQ_TTPR_FU_8	Stored data – global copy	Must have
Once the Primary Data Storage has successfully processed and stored any relevant transaction reported from the manufacturer(s)/importer(s), a copy of this same record shall be transmitted to the Surveillance Data Storage.		
RQ_TTPR_FU_9	Recall of messages	Must have
The Primary Data Storage shall accept the recall of messages in such a way that any report transmitted by the economic operators can be recalled. There shall be no time limitation in accepting the recall of messages.		
RQ_TTPR_FU_10	Data query – visual query tool	Must have
The Primary Data Storage shall provide a visual query tool to allow auditors, competent authorities and the Commission to make manual queries without technical knowledge of any specific query language. The queries that shall be supported by the tool are illustrated in the use case section of WP3.		
RQ_TTPR_FU_11	Data query – API query tool	Should have
The Primary Data Storage should provide an API (Application Programming Interface) query tool to allow auditors, competent authorities and the Commission to programmatically interface with the solution to query data. The queries that shall be supported by the tool are illustrated in the use case section of WP3.		
RQ_TTPR_FU_12	Bulk data extraction	Should have
The Primary Data Storage should provide an interface for human interaction for auditors, competent authorities and the Commission to perform bulk data extraction, using the data formats most commonly used for this purpose, such as CSV, flat file format, etc.		
RQ_TTPR_FU_13	All relevant transactions – transmission interface for the Surveillance Data Storage	Must have
The Primary Data Storage shall provide an interface to allow data exchange with the Surveillance Data Storage in order to enable the acquisition of the records transmitted by the distributors and wholesalers through the Surveillance Data Storage router.		
RQ_TTPR_FU_14	System maintenance	Must have
The Primary Data Storage shall provide a user interface to allow system maintenance.		
RQ_TTPR_FU_15	Data auditing access	Must have
The Primary Data Storage shall provide an interface to allow authorised users access to audit data.		
RQ_TTPR_FU_16	Data audit trail	Must have
The Primary Data Storage shall provide a functional audit trail for every data entry.		
RQ_TTPR_FU_17	Data access authorisation	Must have

Functional Requirements – Tracking and Tracing System – Primary Data Storage		
ID	**Name**	**Priority**
The Primary Data Storage shall provide and limit data access to authorised users only.		
RQ_TTPR_FU_18	Logic data deletion	Must have
The tracking and tracing data records may only be logically deleted until the moment of the definitive data purge, in accordance with the required data retention period.		
RQ_TTPR_FU_19	Data retention period	Must have
The Primary Data Storage shall provide a retention period of at least ten (10) years after the reception of the reported event. Data records must be kept accessible during this period.		
RQ_TTPR_FU_20	Operations audit trail	Must have
The Primary Data Storage shall keep audit trails (logs) for every operation performed, including any data access or manipulation. Every data change must be logged, including the original value. The audit trail shall contain at least the following information: • Audit ID: A unique unchangeable auto-number containing the audit's key • Edit Date: A date/time containing the timestamp of the change • User: The user ID of the user who made the change • Record ID: The value that uniquely identifies the changed record • Source: The name of the object (table/view/document) that contains the changed record • Field: The name of the changed field • Before Value: The value before the change		
RQ_TTPR_FU_21	Lookup tables for offline verification - interface	Must have
The Primary Data Storage shall provide an interface to allow offline applications to download the lookup tables to verify the unique identifier information.		
RQ_TTPR_FU_22	User authentication and authorisation	Must have
The Primary Data Storage shall establish an authentication mechanism, to ensure that only authenticated users have access to the system, and an authorisation mechanism, to ensure that the authenticated user has authorisation to access the system.		
RQ_TTPR_FU_23	Change the user password	Must have
The Primary Data Storage provider shall establish a mechanism to allow the user to change his/her own password.		
RQ_TTPR_FU_24	Recover the user password	Must have
The Primary Data Storage provider shall establish a mechanism to allow the user to recover his/her own password.		
RQ_TTPR_FU_25	Deactivate user	Must have
The Primary Data Storage provider shall establish a mechanism to allow System Administrators to deactivate a user.		
RQ_TTPR_FU_26	Re-activate user	Must have
The Primary Data Storage provider shall establish a mechanism to allow System Administrators to re-activate a user.		
RQ_TTPR_FU_27	Provisioning of additional capabilities laid down in future updates of the	Must have

Functional Requirements – Tracking and Tracing System – Primary Data Storage		
ID	**Name**	**Priority**
	Implementing Acts	
The Primary Data Storage provider shall accommodate any additional capability or system update that could be laid down in future amendments to the relevant EU legislation.		

ii. Technical

1. System qualities

System Qualities – Tracking and Tracing System – Primary Data Storage		
ID	**Name**	**Priority**
RQ_TTPR_RE_1	Data reception acknowledgment	Must have
The Primary Data Storage shall acknowledge the sender of a successful data receipt, otherwise failing with a consistent error code.		
RQ_TTPR_RE_2	Business continuity and disaster recovery	Must have
The Primary Data Storage provider shall provide data resilience and disaster recovery capabilities across multiple sites.		
RQ_TTPR_RE_3	Data backups	Must have
The Primary Data Storage provider shall take periodic full and/or incremental snapshots of the data store to mitigate the risk of system/storage failure.		
RQ_TTPR_RE_4	Outbound channel redundancy	Must have
The Primary Data Storage shall be able to change automatically to additional outbound communication channels (at least one shall be established) in case the message submission fails due to a communication error with the Surveillance Data Storage.		
RQ_TTPR_RE_5	Message replay-ability	Must have
The Primary Data Storage shall persist the outgoing messages until the messages are successfully delivered. When trying to transmit the outgoing messages, the Primary Data Storage shall handle transient failures by transparently retrying a failed operation.		
RQ_TTPR_PE_1	Storage size	Must have
The Primary Data Storage shall be able to support storage size of at least 25 Terabytes per instance yearly.		
RQ_TTPR_PE_2	Messaging throughput	Must have
The Primary Data Storage shall support rates of message throughput for input/output operations in the range of fifty thousand (50,000) messages per second per instance.		
RQ_TTPR_PE_3	Query request throughput	Must have
The Primary Data Storage shall be able to support at least five hundred (500) concurrent query requests per instance.		
RQ_TTPR_PE_4	Network uptime	Must have
The Primary Data Storage facility shall be able to meet the network uptime target: 99.982% (Tier III data centre).		

System Qualities – Tracking and Tracing System – Primary Data Storage		
ID	**Name**	**Priority**
RQ_TTPR_PE_5	Server uptime	Must have
The Primary Data Storage facility shall be able to meet the server uptime target: 99.982% (Tier III data centre).		
RQ_TTPR_PE_6	Latency intra data centre	Must have
The Primary Data Storage facility shall be able to meet the latency target: less than 100 milliseconds latency between physical servers in the same data centre.		
RQ_TTPR_PE_7	Inter data centre speed	Must have
The Primary Data Storage facility shall be able to meet the speed target: at least 100 Mbps between the different data centres involved, namely the Surveillance Data Storage solution and ID Issuer solutions.		
RQ_TTPR_PE_8	Support response time	Must have
The Primary Data Storage provider shall be able to meet the support response time target: 30 minute support response time for emergency incidents.		
RQ_TTPR_PE_9	Hardware break/fix	Must have
The Primary Data Storage provider shall be able to meet the hardware break/fix target: subject to the vendor-backed support.		
RQ_TTPR_PE_10	Data archiving	Must have
The Primary Data Storage provider shall securely archive data that is no longer required by the system, in compliance with the required retention period, thus reducing the size of the data store.		
RQ_TTPR_PE_11	Separate physical data storage areas	Must have
The Primary Data Storage provider shall create a tiered storage environment utilising multiple media types delivering the required combinations of performance, capacity and resilience.		
RQ_TTPR_PE_12	Data centre efficiency	Should have
The Primary Data Storage provider should be compliant with the European Code of Conduct for Energy Efficiency in Data Centres, and use best practices for data centre energy efficiency.		
RQ_TTPR_SU_1	Scalability	Must have
The Primary Data Storage facility shall be scalable and technically upgradeable to maintain performance against threat growth. This includes I/O performance, storage and network capacity, and licences.		
RQ_TTPR_SU_2	Unlimited by design	Must have
The Primary Data Storage shall have growth potential beyond the figures given in this section in order to host all relevant data for at least the totality of the retention period. Therefore, the data storage capacity and the database size shall not deem any limitation on design.		
RQ_TTPR_SU_3	Notification of storage limit	Must have
The Primary Data Storage provider shall notify the system administrator and the correspondent manufacturer(s)/importer(s) when the allocated storage reaches 75% of its total capacity.		
RQ_TTPR_SU_4	Support to connectivity tests with economic operators connectivity	Must have
The Primary Data Storage provider shall provide the manufacturer(s) or importer(s), which have established this repository, with the necessary support (e.g. credentials, configuration information, documentation, sample data, test sets, etc.) to verify the compliance of their event reporting implementations (e.g. Temporary Buffer component) with the system requirements prior to the connection to production.		

System Qualities – Tracking and Tracing System – Primary Data Storage		
ID	**Name**	**Priority**
RQ_TTPR_SU_5	Operational support to economic operators	Must have
The Primary Data Storage provider shall provide to the manufacturer(s) or importer(s), which have established this repository, the necessary operational support (e.g. credentials, configuration information, documentation, sample data, connectivity verification, issues monitoring, test sets, etc.) to facilitate a smooth production functioning of their reporting implementations (e.g. Temporary Buffer component).		
RQ_TTPR_SU_6	Support to connectivity tests with the Surveillance Data Storage solution	Must have
The Primary Data Storage provider shall provide to the Surveillance Data Storage provider the necessary support (e.g. credentials, configuration information, documentation, sample data, test sets, etc.) to verify the compliance of his implementation with the system requirements prior to the connection to production.		
RQ_TTPR_SU_7	Operational support to Surveillance Data Storage solution	Must have
The Primary Data Storage provider shall provide to the Surveillance Data Storage provider the necessary support (e.g. credentials, configuration information, documentation, sample data, connectivity verification, issues monitoring, test sets, etc.) to facilitate a smooth production functioning of both solutions.		
RQ_TTPR_SU_8	Support to interface versioning	Must have
The Primary Data Storage provider shall support any data model or functionality evolution through the release of a new interface version in accordance with the new features.		

2. Security

Security – Tracking and Tracing System – Primary Data Storage		
ID	**Name**	**Priority**
RQ_TTPR_SE_1	Data isolation	Must have
The Primary Data Storage provider shall provide economic operators with a secure and segmented hosting environment with server, storage, and network elements that are logically isolated from other economic operators running on the same infrastructure.		
RQ_TTPR_SE_2	User access authorisation	Must have
The Primary Data Storage shall provide a user authorisation mechanism in order to ensure the segregation of responsibilities and restrict access to data.		
RQ_TTPR_SE_3	Auditability	Must have
The Primary Data Storage provider shall provide auditing, an audit trail with change recording, and an activity logging mechanism with timestamps for all data-related activities.		
RQ_TTPR_SE_4	Audit logging	Must have
The Primary Data Storage shall record important events together with the user who performs the operation in an audit log, which shall be centrally maintained. The list of events that the Primary Data Storage shall record in the audit log shall include but not be limited to the following: • Database activities • Technical events, like data synchronisation and data replication • Accessing of data		
RQ_TTPR_SE_5	Error logging	Must have
All errors and faults in the Primary Data Storage shall be recorded in an error log, which shall be centrally maintained.		

Security – Tracking and Tracing System – Primary Data Storage		
ID	**Name**	**Priority**
RQ_TTPR_SE_6	Completeness of logs	Must have
The error log and audit log shall contain all required information in order to provide the authorised user with interpretable and comprehensive information about the cause of the error, as well as the audit traceability for the actions taken by an authorised user.		
RQ_TTPR_SE_7	Auditing and monitoring plan	Must have
The Primary Data Storage provider shall implement an auditing and monitoring plan. The plan shall address, but not be limited to, the following topics: • Auditing of vulnerabilities and threats • Auditing of data access • Auditing of database baseline • Monitoring of suspicious activities • Monitoring of systems health • Anomalies detection • Implementation of server hardening guidelines for securing the system		
RQ_TTPR_SE_8	End-to-end traceability	Must have
The Primary Data Storage shall ensure that any data/action can always be traced to its original source (i.e. Temporary Buffer of manufacturer(s)/importer(s)/distributor(s)/wholesaler(s)).		
RQ_TTPR_SE_9	Auditor support	Must have
The Primary Data Storage provider shall provide full access and any requested evidence to the independent external auditor to ensure that s/he can monitor the activities of the Primary Data Storage provider and the accesses to the Primary Data Storage solution.		
RQ_TTPR_SE_10	Log preservation	Must have
The Primary Data Storage shall archive the error and audit logs, using integrity checking countermeasures to ensure that the log file has been archived successfully after each archiving process.		
RQ_TTPR_SE_11	Log retention period	Must have
Access logs shall be immutable and kept for at least four (4) years. Error logs shall be immutable and kept for at least two (2) years.		
RQ_TTPR_SE_12	Sender tracking	Must have
The Primary Data Storage shall resolve and authenticate the sender's identity against a trusted identity provider. Messages sent from an unauthenticated sender shall not be accepted.		
RQ_TTPR_SE_13	Checksum verification	Must have
The Primary Data Storage shall verify the message checksum to ensure that the data was not tampered with. Messages where the checksum is not valid shall not be accepted.		
RQ_TTPR_SE_14	Secure coding practice	Must have
The Primary Data Storage provider shall provide a system implementation compliant with common secure coding practices, such as OWASP.		
RQ_TTPR_SE_15	User access authentication	Must have
The Primary Data Storage shall provide a user authentication mechanism prior to any access to system resources and data.		

Security – Tracking and Tracing System – Primary Data Storage		
ID	**Name**	**Priority**
RQ_TTPR_SE_16	Password strength	Must have
The Primary Data Storage shall ensure the enforcement of password standards (e.g. minimum length and use of alpha, numeric and special characters) and, when applicable, establish a specified period for password expiration and prohibit the user from reusing recent passwords.		
RQ_TTPR_SE_17	Password protection	Must have
The Primary Data Storage shall ensure that user passwords are non-printing and non-displaying.		
RQ_TTPR_SE_18	Integration with the European single sign-on mechanism	Should have
The Primary Data Storage should provide integration with the European access control mechanism (i.e. "EU Login") to allow competent authorities to use a single sign-on to the system, when applicable.		

3. Data protection

Data Protection – Tracking and Tracing System – Primary Data Storage		
ID	**Name**	**Priority**
RQ_TTPR_DP_1	Data protection rules	Must have
The Primary Data Storage provider shall be compliant with and ensure that personal data is processed and protected in accordance with EU Regulation 2016/679 (European Commission - REGULATION (EU) 2016/679, 2016), which repeals Directive 95/46/EC.		
RQ_TTPR_DP_2	Antitrust	Must have
The data confidentiality must follow all the necessary safeguarding measures, respecting the current ruling of antitrust, in order to prevent the leak or access of any sensitive data of an economic operator by any other economic operator.		
RQ_TTPR_DP_3	Confidentiality treatment	Must have
The Primary Data Storage provider must treat with confidentiality any information, or documents disclosed, in any format exchanged or stored in the system.		

4. System constraints

System Constraints – Tracking and Tracing System – Primary Data Storage		
ID	**Name**	**Priority**
RQ_TTPR_SC_1	Facility location	Must have
The Primary Data Storage facility shall be physically located within the territory of the European Union, and any maintenance on the servers shall be carried out within the European Union.		
RQ_TTPR_SC_2	Extension of guarantees	Must have
Any additional exchange of data and metadata that might occur in the Primary Data Storage facility with the objective to implement or support the Tracking and Tracing System shall be guaranteed the same level of data protection and quality as defined for the rest of the system.		
RQ_TTPR_SC_3	Non-limiting throughput for economic operators	Must have

System Constraints – Tracking and Tracing System – Primary Data Storage		
ID	**Name**	**Priority**
The overall throughput of the Primary Data Storage shall not be a limiting factor for the speed of the manufacturing production lines or for the logistics activities of importers, distributors or wholesalers.		
RQ_TTPR_SC_4	Data dictionary compatibility	Must have
The Primary Data Storage solution shall ensure that the physical storage of the Tracking and Tracing data is conformant with the data dictionary described in the Final Report "Implementation analysis regarding the technical specifications and other key elements for a future EU system for traceability and security features in the field of tobacco products" (Annex II, Section 3.10).		
RQ_TTPR_SC_5	Data validation rules	Must have
The Primary Data Storage solution shall implement Tracking and Tracing data validation rules conformant with the common validation rules in the Final Report "Implementation analysis regarding the technical specifications and other key elements for a future EU system for traceability and security features in the field of tobacco products" (Annex II, Section 3.11).		
RQ_TTPR_SC_6	Messaging compatibility	Must have
The Primary Data Storage solution shall exchange messages conformant with the specifications in the Final Report "Implementation analysis regarding the technical specifications and other key elements for a future EU system for traceability and security features in the field of tobacco products" (Annex II, Section 3.5.1).		
RQ_TTPR_SC_7	Decoupling of operations	Must have
The Primary Data Storage must decouple data acquisition from data processing, avoiding unnecessary coupling between independent processes.		
RQ_TTPR_SC_8	Event-driven design	Must have
The Primary Data Storage shall be designed based on an event-driven architectural pattern for the data acquisition and data processing components.		
RQ_TTPR_SC_9	Fault isolation	Must have
The main components of the Primary Data Storage shall be designed to support fault isolation, in order to not propagate its errors to other components of the solution and to limit the impact of any problem to the minimum.		
RQ_TTPR_SC_10	Designed for monitoring	Must have
The Primary Data Storage solution shall be designed for monitoring in order to help the provider in the identification of current, potential or future issues (e.g. performance, code bugs, application errors, security threats, etc.). The monitoring should be applied at the following levels: hardware, software, infrastructure and application (the latter aiming at reporting on "what is the problem").		
RQ_TTPR_SC_11	Idempotent messages	Must have
The Primary Data Storage message management shall be designed to avoid acquiring and reprocessing the same message multiple times, since messages of the Tracking and Tracing System are not idempotent.		
RQ_TTPR_SC_12	Usage of an agnostic query language to retrieve the canonical data model	Should have
The Primary Data Storage should provide an interface compliant with some agnostic query language to retrieve data from the Tracking and Tracing canonical data model. As such, the Resource Query Language (RQL), which is an open language (apsstandard - RQL, 2014) for querying collections of resources, could be a potential solution.		

5. System interfaces

Interface PR2MI	
ID	**Name**
▪ PR2MI	▪ Primary Data Storage to manufacturers and importers
Owner System	
▪ Primary Data Storage solution	
Data Source	**Data Target**
▪ Component established at the facilities of the manufacturers or importers (e.g. Temporary Buffer)	▪ Primary Data Storage
Data Type	
▪ Operational event messages ▪ Transactional event messages	
Interface Trigger	
▪ Push upon request by the client systems of the economic operators.	
Access Control	
▪ Only authorised manufacturers and importers have access to this interface.	
Description	
▪ This interface provides the event information reporting channel to the manufacturers and importers.	

Interface PR2CA	
ID	**Name**
▪ PR2CA	▪ Primary Data Storage to competent authorities
Owner System	
▪ Primary Data Storage solution	
Data Source	**Data Target**
▪ Primary Data Storage	▪ Competent authorities
Data Type	
▪ Operational event messages ▪ Transactional event messages ▪ Data extraction messages ▪ Lookup tables ▪ Notifications	
Interface Trigger	
▪ Push execution on demand.	
Access Control	
▪ Only the competent authorities have access to this interface.	
Description	
▪ This interface provides the channel to give competent authorities full access to the Primary Data Storage.	

Interface PR2AU	
ID	**Name**
▪ PR2AU	▪ Primary Data Storage to auditors
Owner System	

▪ Primary Data Storage solution	
Data Source	**Data Target**
▪ Primary Data Storage	▪ Auditors
Data Type	
▪ Operational event messages ▪ Transactional event messages ▪ Data extraction messages ▪ Lookup tables ▪ Notifications	
Interface Trigger	
▪ Pull execution on demand.	
Access Control	
▪ Only the auditors have access to this interface.	
Description	
▪ This interface provides the channel to give auditors access to the auditing data of the Primary Data Storage.	

Interface PR2SU	
ID	**Name**
▪ PR2SU	▪ Primary Data Storage to Surveillance Data Storage
Owner System	
▪ Primary Data Storage solution	
Data Source	**Data Target**
▪ Surveillance Data Storage	▪ Primary Data Storage
Data Type	
▪ Operational event messages ▪ Transactional event messages ▪ Replication of lookup tables	
Interface Trigger	
▪ Push execution on demand.	
Access Control	
▪ Only the Surveillance Data Storage has access to this interface.	
Description	
▪ This interface provides the channel to the Repository Router to update the Primary Data Storage.	

iii. Applicable standards

Applicable Standards – Tracking and Tracing System – Primary Data Storage		
ID	**Name**	**Priority**
RQ_TTPR_AS_1	ISO 27001 compliant hosting	Must have
The Primary Data Storage shall be hosted in an ISO 27001 compliant hosting. This provider is expected to deliver a highly available, scalable, and flexible system.		
RQ_TTPR_AS_2	Character set content	Must have
The Primary Data Storage shall store content using the ISO/IEC 8859-15:1999 character set.		

2. Surveillance Data Storage

a. Requirements specifications

i. Functional

Functional Requirements – Tracking and Tracing System – Surveillance Data Storage		
ID	**Name**	**Priority**
RQ_TTSU_FU_1	Unique identifier at unit packet level – information to be determined	Must have
The Surveillance Data Storage solution shall ensure that the following information is determined for a unique identifier at unit packet level: • the date of manufacturing; • the place of manufacturing; • the manufacturing facility; • the machine used to manufacture the tobacco products; • the time of manufacture; • the product description; • the intended market of retail sale; • the intended shipment route; • where applicable, the importer into the Union; • the serial number; • the actual shipment route from manufacturing to the first retail outlet, including all warehouses used as well as the shipment date, shipment destination, point of departure and consignee; • the identity of all purchasers from manufacturing to the first retail outlet; and • the invoice, order number and payment records of all purchasers from manufacturing to the first retail outlet This shall be accomplished through the processing of the data transmitted by the economic operators.		
RQ_TTSU_FU_2	Unique identifier at aggregation packaging level – information to be determined	Must have
The Surveillance Data Storage solution shall ensure that the following information is determined for a unique identifier at aggregation packaging level: • the date of manufacturing; • the location of the aggregation activities; and • a serial number. This shall be accomplished through the processing of the data transmitted by the economic operators.		
RQ_TTSU_FU_3	All relevant transactions – global copy	Must have
The Surveillance Data Storage shall ensure that all relevant transactions of all natural and legal persons engaged in the supply chain of tobacco products that are received into the Tracking and Tracing System are stored properly.		
RQ_TTSU_FU_4	All relevant transactions – support at aggregation packaging level	Must have
The Surveillance Data Storage shall support relevant transactions that have been recorded at aggregation packaging level.		
RQ_TTSU_FU_5	All relevant transactions – transmission interface for Primary Data Storage	Must have
The Surveillance Data Storage shall provide a secure interface to the Primary Data Storage to allow the transmission of all relevant transactions reported from manufacturers and importers.		
RQ_TTSU_FU_6	Shipment and trade information available through an electronic link	Must have
The Surveillance Data Storage shall provide a secure interface to make available shipment and trade information through a link to the unique identifier.		
RQ_TTSU_FU_7	All relevant transactions – transmission interface for distributors and wholesalers	Must have

Functional Requirements – Tracking and Tracing System – Surveillance Data Storage		
ID	**Name**	**Priority**
The Surveillance Data Storage shall provide a secure interface to distributors and wholesalers to allow the transmission of all relevant transactions reported from such sources.		
RQ_TTSU_FU_8	All relevant transactions – routing of distributors and wholesalers records	Must have
The Surveillance Data Storage shall provide a routing service for the records transmitted by the distributors and wholesalers, which shall also be processed by the manufacturer(s)/importer(s) that they refer to.		
RQ_TTSU_FU_9	Stored data - prevent data access	Must have
The Surveillance Data Storage shall prevent access by any party other than the competent authorities of the Member States, the Commission, and the external auditors, thereby ensuring that economic operators or any other party involved in the trade of tobacco products are forbidden to read, update or delete any data stored in the system.		
RQ_TTSU_FU_10	Recall of messages	Must have
The Surveillance Data Storage shall accept the recall of messages in such a way that any report transmitted by the economic operators can be recalled. There shall be no time limitation in accepting the recall of messages.		
RQ_TTSU_FU_11	Data query – visual query tool	Must have
The Surveillance Data Storage shall provide a visual query tool to allow auditors and competent authorities to make manual queries without technical knowledge of any specific query language. The queries that shall be supported by the tool are illustrated in the use case section of WP3.		
RQ_TTSU_FU_12	Data query – API query tool	Should have
The Surveillance Data Storage should provide an API (Application Programming Interface) query tool to allow auditors and competent authorities to programmatically interface with the solution to query data. The queries that shall be supported by the tool are illustrated in the use case section of WP3.		
RQ_TTSU_FU_13	Bulk data extraction	Should have
The Surveillance Data Storage should provide an interface for human interaction for auditors, competent authorities, and the Commission to perform bulk data extraction for further analysis, using the data formats most commonly used for this purpose, such as CSV, flat file format, etc.		
RQ_TTSU_FU_14	Data query – data grouping	Must have
The Surveillance Data Storage shall provide the capability to perform queries, retrieving any information containing data aggregation, such as grouping and having.		
RQ_TTSU_FU_15	Data query – data calculation	Must have
The Surveillance Data Storage shall provide the capability to perform queries, retrieving any information that is calculated and not stored, such as sums or averages.		
RQ_TTSU_FU_16	Data query – data sorting	Must have
The Surveillance Data Storage shall provide the capability to perform queries, retrieving sorted information.		
RQ_TTSU_FU_17	Lookup tables - data maintenance	Must have
The Surveillance Data Storage shall provide a mechanism to allow the maintenance of the lookup tables.		
RQ_TTSU_FU_18	System maintenance	Must have

Functional Requirements – Tracking and Tracing System – Surveillance Data Storage		
ID	**Name**	**Priority**
The Surveillance Data Storage shall provide a user interface to allow system maintenance.		
RQ_TTSU_FU_19	Auditing data access	Must have
The Surveillance Data Storage shall provide an interface to allow access to audit data.		
RQ_TTSU_FU_20	Data audit trail	Must have
The Surveillance Data Storage shall provide a functional audit trail for every data entry.		
RQ_TTSU_FU_21	Data access authorisation	Must have
The Surveillance Data Storage shall provide and limit data access to authorised users only.		
RQ_TTSU_FU_22	Logic data deletion	Must have
The Tracking and Tracing data records may only be logically deleted until the moment of the definitive data purge, in accordance with the required data retention period.		
RQ_TTSU_FU_23	Data retention period	Must have
The Surveillance Data Storage shall provide a retention period of at least ten (10) years after the reception of the reported event. Data records must be kept accessible during this period.		
RQ_TTSU_FU_24	Operations audit trail	Must have
The Surveillance Data Storage shall provide and keep audit trails (logs) for every operation performed, including any data access or manipulation. Every data change must be logged, including the original value. The audit trail shall contain at least the following information: • Audit ID: a unique unchangeable auto-number containing the audit key • Edit Date: A date/time containing the timestamp of the change • User: The ID of the user that made the change • Record ID: The value that uniquely identifies the changed record • Source: The name of the object (table/view/document) that contains the changed record • Field: The name of the changed field • Before Value: The value before the change		
RQ_TTSU_FU_25	Lookup tables for offline verification - interface	Must have
The Surveillance Data Storage shall provide an interface to allow offline applications to download the lookup tables and verify the unique identifier information.		
RQ_TTSU_FU_26	User authentication and authorisation	Must have
The Surveillance Data Storage shall establish an authentication mechanism to ensure that only authenticated users have access to the system, and an authorisation mechanism, to ensure that the authenticated user has authorisation prior to any system access.		
RQ_TTSU_FU_27	Change the user password	Must have
The Surveillance Data Storage provider shall establish a mechanism to allow the user to change his/her own password.		
RQ_TTSU_FU_28	Recover the user password	Must have

Functional Requirements – Tracking and Tracing System – Surveillance Data Storage		
ID	**Name**	**Priority**
The Surveillance Data Storage provider shall establish a mechanism to allow the user to recover his/her own password.		
RQ_TTSU_FU_29	Deactivate user	Must have
The Surveillance Data Storage provider shall establish a mechanism to allow System Administrators to deactivate a user.		
RQ_TTSU_FU_30	Re-activate user	Must have
The Surveillance Data Storage provider shall establish a mechanism to allow System Administrators to re-activate a user.		
RQ_TTSU_FU_31	Data analytics capabilities	Must have
The Surveillance Data Storage shall provide data analytics capabilities in order to provide information tools to support national enforcement activities and the Commission. Each authorised user (i.e. competent authorities and the Commission) shall have his/her own data analytics environment in which to configure his/her own rules. See the risk-based surveillance use case for further details.		
RQ_TTSU_FU_32	Key indicators tool	Could have
The Surveillance Data Storage could provide a tool acting as a dashboard, where key indicators of the system could be configured.		
RQ_TTSU_FU_33	Notification tool	Must have
The Surveillance Data Storage shall provide a tool for automatic notifications to be triggered based on configurable parameters and criteria. The tool should provide the possibility of configuring different notification channels and recipient stakeholders. Each authorised user (i.e. competent authorities and the Commission) shall have his/her own environment in which to configure his/her own notifications and channels. See the notify use case for further details.		
RQ_TTSU_FU_34	Query notification	Must have
The Surveillance Data Storage shall provide a visual interface to allow competent authorities, external auditors, and the Commission to query notifications generated.		
RQ_TTSU_FU_35	Control access of data extraction	Must have
The Surveillance Data Storage shall ensure that any data extraction shall be compliant with the data access level of the requestor.		
RQ_TTSU_FU_36	Data view format	Must have
The Surveillance Data Storage shall provide the capability to present data in a row and column format, with information vertically listed in column-by-column headings and in horizontal bands, and with each band having its own content possibly spanning multiple lines.		
RQ_TTSU_FU_37	Data drill down	Should have
The Surveillance Data Storage should provide the capability to present data at specific level, and drill down to other levels of information for a selected value (e.g. Pallet > Master Case > Carton > Unit Packet).		
RQ_TTSU_FU_38	Data drill up	Should have
The Surveillance Data Storage should provide the capability to present data at specific level, and drill up to other levels of information for a selected value (e.g. Unit Packet > Carton > Master Case > Pallet).		

Functional Requirements – Tracking and Tracing System – Surveillance Data Storage		
ID	**Name**	**Priority**
RQ_TTSU_FU_39	Provisioning of additional capabilities laid down in future updates of the Implementing Acts	Must have
The Surveillance Data Storage provider shall accommodate any additional capability or system update laid down in future amendments to the relevant legislation.		

ii. Technical

1. System qualities

System Qualities – Tracking and Tracing System – Surveillance Data Storage		
ID	**Name**	**Priority**
RQ_TTSU_RE_1	Data reception acknowledgment	Must have
The Surveillance Data Storage shall send acknowledgement of a successful data receipt to the sender, otherwise failing with a consistent error code.		
RQ_TTSU_RE_2	Business continuity and disaster recovery	Must have
The Surveillance Data Storage provider shall provide data resilience and disaster recovery capabilities across multiple sites.		
RQ_TTSU_RE_3	Data backups	Must have
The Surveillance Data Storage provider shall take periodic full and/or incremental snapshots of the data store to mitigate the risk of system/storage failure.		
RQ_TTPR_RE_4	Outbound channel redundancy	Must have
The Surveillance Data Storage shall be able to change automatically to additional outbound communication channels (at least one shall be established) in case the message submission fails due to a communication error with the Primary Data Storage.		
RQ_TTSU_PE_1	Storage size	Must have
The Surveillance Data Storage shall be able to support a storage size of at least 100 Terabytes per instance yearly.		
RQ_TTSU_PE_2	Messaging throughput	Must have
The Surveillance Data Storage shall support rates of message throughput for input/output operations in the range of 750 thousand (750,000) messages per second per instance.		
RQ_TTSU_PE_3	Query request throughput	Must have
The Surveillance Data Storage shall be able to support at least five hundred (500) concurrent query requests per instance.		
RQ_TTSU_PE_4	Network uptime	Must have
The Surveillance Data Storage facility shall be able to meet the network uptime target: 99.982% (Tier III data centre).		
RQ_TTSU_PE_5	Server uptime	Must have
The Surveillance Data Storage facility shall be able to meet the server uptime target: 99.982% (Tier III data centre).		
RQ_TTSU_PE_6	Latency intra data centre	Must have

System Qualities – Tracking and Tracing System – Surveillance Data Storage		
ID	**Name**	**Priority**
The Surveillance Data Storage facility shall be able to meet the Latency Target: Less than 100 millisecond latency between physical servers in the same data centre.		
RQ_TTSU_PE_7	Inter data centre speed	Must have
The Surveillance Data Storage facility shall be able to meet the Speed Target: more than 100 Mbps between the different data centres involved, namely the ID Issuer solutions and Primary Data Storage solutions.		
RQ_TTSU_PE_8	Support Response Time	Must have
The Surveillance Data Storage provider shall be able to meet the support response time target: 30 minute support response time for emergency incidents.		
RQ_TTSU_PE_9	Hardware break/fix	Must have
The Surveillance Data Storage provider shall be able to meet the hardware break/fix target: subject to the vendor-backed support.		
RQ_TTSU_PE_10	Data archiving	Must have
The Surveillance Data Storage provider shall archive data that is no longer required by the system, in compliance with the maximum retention period required, thereby reducing the size of the data store.		
RQ_TTSU_PE_11	Separate physical data storage areas	Must have
The Surveillance Data Storage provider shall create a tiered storage environment utilising multiple media types delivering the required combinations of performance, capacity and resilience.		
RQ_TTSU_PE_12	Data centre efficiency	Should have
The Surveillance Data Storage provider should be compliant with the European Code of Conduct for Energy Efficiency in Data Centres, and use best practices for data centre energy efficiency.		
RQ_TTSU_SU_1	Scalability	Must have
The Surveillance Data Storage facility shall be scalable and technically upgradeable to maintain performance against threat growth. This includes I/O performance, storage and network capacity, and licences.		
RQ_TTSU_SU_2	Unlimited by design	Must have
The Surveillance Data Storage shall have growth potential beyond the figures given in this section to indicate data storage capacity, database or list sizes, and shall not deem any limitation on design.		
RQ_TTSU_SU_3	Notification of storage limit	Must have
The Surveillance Data Storage provider shall notify the authorised user when the allocated storage reaches 75% of its total capacity.		
RQ_TTSU_SU_4	Support to connectivity tests with economic operators	Must have
The Surveillance Data Storage provider shall provide the distributor(s) and wholesaler(s) with the necessary support (e.g. credentials, configuration information, documentation, sample data, etc.) to verify the compliance with the system requirements of their event reporting implementations (e.g. Temporary Buffer component) prior to the connection to production.		
RQ_TTSU_SU_5	Operational support to economic operators	Must have
The Surveillance Data Storage provider shall provide the distributor(s) and wholesaler(s) with the necessary operational support (e.g. credentials, configuration information, documentation, sample data, connectivity verification, issues monitoring, test sets, etc.) to facilitate a smooth production functioning of their reporting implementations (e.g. Temporary Buffer component).		

System Qualities – Tracking and Tracing System – Surveillance Data Storage		
ID	**Name**	**Priority**
RQ_TTSU_SU_6	Support to connectivity tests with the Primary Data Storage solutions	Must have
The Surveillance Data Storage provider shall provide the different Primary Data Storage providers with the necessary support (e.g. credentials, configuration information, documentation, sample data, test sets, etc.) to verify compliance of their client implementations with the system requirements prior to the connection to production.		
RQ_TTSU_SU_7	Operational support to Primary Data Storage solutions	Must have
The Surveillance Data Storage provider shall provide the different Primary Data Storage providers with the necessary operational support (e.g. credentials, configuration information, documentation, sample data, connectivity verification, issues monitoring, test sets, etc.) to facilitate a smooth production functioning of the solutions involved.		
RQ_TTSU_SU_8	Support to connectivity tests with ID Issuer solutions	Must have
The Surveillance Data Storage provider shall provide the ID Issuer solution providers with the necessary support (e.g. credentials, configuration information, documentation, sample data, test sets, etc.) to verify the compliance of their client implementations prior to the connection to production.		
RQ_TTSU_SU_9	Operational support to ID Issuer solutions	Must have
The Surveillance Data Storage provider shall provide the ID Issuer solution providers with the necessary operational support (e.g. credentials, configuration information, documentation, sample data, connectivity verification, issues monitoring, test sets, etc.) to facilitate a smooth production functioning of the solutions involved.		
RQ_TTSU_SU_10	Support to interface versioning	Must have
The Surveillance Data Storage provider shall support any data model or functionality evolution through the release of a new interface version compliant with the new features.		

2. Security

Security – Tracking and Tracing System – Surveillance Data Storage		
ID	**Name**	**Priority**
RQ_TTSU_SE_1	Data isolation	Must have
The Surveillance Data Storage provider shall provide economic operators with a secure and segmented hosting environment with server, storage, and network elements that are logically isolated from other economic operators running on the same infrastructure.		
RQ_TTSU_SE_2	User access authorisation	Must have
The Surveillance Data Storage shall provide a user authorisation mechanism in order to ensure the segregation of responsibilities and restrict access to data.		
RQ_TTSU_SE_3	Auditability	Must have
The Surveillance Data Storage shall provide auditing, an audit trail with change recording, and an activity logging mechanism with timestamps for all data-related activities.		
RQ_TTSU_SE_4	Audit logging	Must have

Security – Tracking and Tracing System – Surveillance Data Storage		
ID	**Name**	**Priority**
The Surveillance Data Storage shall record important events together with the user who performs the operation in an audit log, which shall be centrally maintained. The list of events the Surveillance Data Storage shall record in the audit log shall include but not be limited to the following: • Database activities • Technical events, like data synchronisation and data replication • Accessing of data		
RQ_TTSU_SE_5	Error logging	Must have
All errors and faults in the system shall be recorded in an error log, which shall be centrally maintained.		
RQ_TTSU_SE_6	Completeness of logs	Must have
The error log and audit log shall contain all required information in order to provide the authorised user with interpretable and comprehensive information about the cause of the error, audit traceability for the actions taken by an authorised user.		
RQ_TTSU_SE_7	Auditing and monitoring plan	Must have
The Surveillance Data Storage provider shall implement an auditing and monitoring plan. The plan shall address, but not be limited to, the following topics: • Auditing of vulnerabilities and threats • Auditing of data access • Auditing of database baseline • Monitoring of suspicious activities • Monitoring of systems health • Anomalies detection • Implement server hardening guidelines for securing the system		
RQ_TTSU_SE_8	End-to-end traceability	Must have
The Surveillance Data Storage shall ensure that any data/action can always be traced to its original source (i.e. Temporary Buffer of an economic operator or ID Issuer).		
RQ_TTSU_SE_9	Auditor support	Must have
The Surveillance Data Storage provider shall provide full access and any requested evidence to the independent external auditor to ensure that s/he can monitor the activities of the Surveillance Data Storage provider and the accesses to the system.		
RQ_TTSU_SE_10	Log preservation	Must have
The Surveillance Data Storage shall archive the error and audit logs, using integrity checking countermeasures to ensure that the log file has been archived successfully after each archiving process.		
RQ_TTSU_SE_11	Log retention period	Must have
Access logs shall be immutable and kept for at least four (4) years. Error logs shall be immutable and kept for at least two (2) years.		
RQ_TTSU_SE_12	Sender tracking	Must have
The Surveillance Data Storage shall resolve and authenticate the sender's identity against a trusted identity provider. Messages sent from an unauthenticated sender shall not be accepted.		
RQ_TTSU_SE_13	Checksum verification	Must have

Security – Tracking and Tracing System – Surveillance Data Storage		
ID	**Name**	**Priority**
The Surveillance Data Storage shall verify the message checksum to ensure that the data was not tampered with. Messages where the checksum is not valid shall not be accepted.		
RQ_TTSU_SE_14	Secure coding practice	Must have
The Surveillance Data Storage provider shall provide a system implementation compliant with common secure coding practices such as OWASP.		
RQ_TTSU_SE_15	User access authentication	Must have
The Surveillance Data Storage shall provide a user authentication mechanism prior to any access to system resources and data.		
RQ_TTSU_SE_16	Password strength	Must have
The Surveillance Data Storage shall ensure the enforcement of password standards (e.g. minimum length and use of alpha, numeric and special characters.) and, when applicable, establish a specified period for password expiration and prohibit the user from reusing recent passwords.		
RQ_TTSU_SE_17	Password protection	Must have
The Surveillance Data Storage shall ensure that user passwords are non-printing and non-displaying.		
RQ_TTSU_SE_18	Integration with the European single sign-on mechanism	Should have
The Surveillance Data Storage should provide integration with the European access control mechanism (i.e. "EU Login") to allow, when applicable, competent authorities to use single sign-on to the system.		

3. Data protection

Data Protection – Tracking and Tracing System – Surveillance Data Storage		
ID	**Name**	**Priority**
RQ_TTSU_DP_1	Data protection rules	Must have
The Surveillance Data Storage provider shall be compliant with and ensure that personal data is processed and protected in accordance with EU Regulation 2016/679 (European Commission - REGULATION (EU) 2016/679, 2016), which repeals Directive 95/46/EC.		
RQ_TTSU_DP_2	Antitrust	Must have
The data confidentiality must follow all the necessary safeguarding measures respecting the current ruling of antitrust, in order to prevent leak or access of any sensitive data of an economic operator by any other economic operator.		
RQ_TTSU_DP_3	Confidentiality treatment	Must have
The Surveillance Data Storage provider must treat with confidentiality any information or documents disclosed, in any format exchanged or stored in the system.		

4. System constraints

System Constraints – Tracking and Tracing System – Surveillance Data Storage		
ID	**Name**	**Priority**

System Constraints – Tracking and Tracing System – Surveillance Data Storage		
ID	**Name**	**Priority**
RQ_TTSU_SC_1	Facility location	Must have
The Surveillance Data Storage facility shall be physically located within the territory of the European Union, and any maintenance on the servers shall be carried out within the European Union.		
RQ_TTSU_SC_2	Extension of guarantees	Must have
Any additional exchange of data and metadata that might occur in the Surveillance Data Storage facility with the objective to implement or support the Tracking and Tracing System shall be guaranteed the same level of data protection and quality defined for the rest of the system.		
RQ_TTSU_SC_3	Non-limiting throughput for economic operators	Must have
The overall throughput of the Surveillance Data Storage shall not be a limiting factor for the speed of the manufacturing production lines or for the logistics activities of the importers, distributors or wholesalers.		
RQ_TTSU_SC_4	Data dictionary compatibility	Must have
The Surveillance Data Storage shall ensure that the physical storage of the Tracking and Tracing data conforms to the data dictionary in the Final Report "Implementation analysis regarding the technical specifications and other key elements for a future EU system for traceability and security features in the field of tobacco products" (Annex II, Section 3.10).		
RQ_TTSU_SC_5	Data validation rules	Must have
The Surveillance Data Storage solution shall implement Tracking and Tracing data validation rules conformant with the common validation rules in the Final Report "Implementation analysis regarding the technical specifications and other key elements for a future EU system for traceability and security features in the field of tobacco products" (Annex II, Section 3.11).		
RQ_TTSU_SC_6	Messaging compatibility	Must have
The Surveillance Data Storage solution shall exchange messages conformant with the specifications in the Final Report "Implementation analysis regarding the technical specifications and other key elements for a future EU system for traceability and security features in the field of tobacco products" (Annex II, Section 3.5.1).		
RQ_TTSU_SC_7	Decoupling of operations	Must have
The Surveillance Data Storage must decouple data acquisition from data processing, avoiding unnecessary coupling between independent processes.		
RQ_TTSU_SC_8	Event-driven design	Must have
The Surveillance Data Storage shall be designed based on an event-driven architectural pattern for the data acquisition and data processing components.		
RQ_TTSU_SC_9	Fault isolation	Must have
The main components of the Surveillance Data Storage shall be designed to support fault isolation, in order not to propagate its errors to other components of the solution and limit the impact of any problem to the minimum.		
RQ_TTSU_SC_10	Designed for monitoring	Must have
The Surveillance Data Storage solution shall be designed for monitoring in order to help the provider in the identification of current, potential or future issues (e.g. performance, code bugs, application errors, security threats, etc.). The monitoring should be applied at the following levels: hardware, software, infrastructure and application (the latter aiming at reporting on "what is the problem").		
RQ_TTSU_SC_11	Idempotent messages	Must have
The Surveillance Data Storage message management shall be designed to avoid acquiring and reprocessing the same message multiple times, since messages of the Tracking and Tracing System are not idempotent.		

System Constraints – Tracking and Tracing System – Surveillance Data Storage		
ID	**Name**	**Priority**
RQ_TTSU_SC_12	Usage of an agnostic query language to retrieve the canonical data model	Should have
The Surveillance Data Storage should provide an interface compliant with some agnostic query language to retrieve data from the Tracking and Tracing canonical data model. As such, the Resource Query Language (RQL), which is an open language (apsstandard - RQL, 2014) for querying collections of resources, could be a potential solution.		

5. System interfaces

Interface SU2DW	
ID	**Name**
▪ SU2DW	▪ Surveillance Data Storage to distributors and wholesalers
Owner System	
▪ Surveillance Data Storage solution	
Data Source	**Data Target**
▪ Component established at the facilities of the manufacturers or importers (e.g. Temporary Buffer)	▪ Surveillance Data Storage
Data Type	
▪ Operational event messages ▪ Transactional event messages	
Interface Trigger	
▪ Push upon request by the client systems of the economic operators.	
Access Control	
▪ Only authorised wholesalers and distributors have access to this interface.	
Description	
▪ This interface provides the event information reporting channel for wholesalers and distributors.	

Interface SU2CA	
ID	**Name**
▪ SU2CA	▪ Surveillance Data Storage to competent authorities
Owner System	
▪ Surveillance Data Storage solution	
Data Source	**Data Target**
▪ Surveillance Data Storage	▪ Competent authorities
Data Type	
▪ Operational event messages ▪ Transactional event messages ▪ Data extraction messages ▪ Lookup tables ▪ Notifications	
Interface Trigger	
▪ Pull execution on demand ▪ Push execution on demand ▪ Push scheduled execution	

Access Control
▪ Only the competent authorities have access to this interface.
Description
▪ This interface provides the channel to give competent authorities full access to the Surveillance Data Storage.

Interface SU2AU	
ID	**Name**
▪ SU2AU	▪ Surveillance Data Storage to auditors
Owner System	
▪ Surveillance Data Storage solution	
Data Source	**Data Target**
▪ Surveillance Data Storage	▪ Auditors
Data Type	
▪ Operational event messages ▪ Transactional event messages ▪ Data extraction messages ▪ Lookup tables ▪ Notifications	
Interface Trigger	
▪ Pull execution on demand	
Access Control	
▪ Only the auditors have access to this interface.	
Description	
▪ This interface provides the channel to give auditors access to the auditing data of the Surveillance Data Storage.	

Interface SU2PR	
ID	**Name**
▪ SU2PR	▪ Surveillance Data Storage to Primary Data Storage
Owner System	
▪ Surveillance Data Storage solution	
Data Source	**Data Target**
▪ Primary Data Storage	▪ Surveillance Data Storage
Data Type	
▪ Operational event messages ▪ Transactional event messages	
Interface Trigger	
▪ Push execution on demand ▪ Push scheduled execution	
Access Control	
▪ Only the Primary Data Storage has access to this interface.	
Description	
▪ This interface provides the channel to update the Surveillance Data Storage with Primary Data Storage data.	

Interface SU2II	
ID	**Name**
▪ SU2II	▪ Surveillance Data Storage to ID Issuer
Owner System	
▪ Surveillance Data Storage solution	
Data Source	**Data Target**
▪ ID issuer	▪ Surveillance Data Storage
Data Type	
▪ Issuance of serial numbers messages	
Interface Trigger	
▪ Push execution on demand	
Access Control	
▪ Only the ID Issuers have access to this interface.	
Description	
▪ This interface provides the channel for ID Issuers to report the issuance of serial numbers.	

iii. Applicable standards

Applicable Standards – Tracking and Tracing System – Surveillance Data Storage		
ID	**Name**	**Priority**
RQ_TTSU_AS_1	ISO 27001 compliant hosting	Must have
The Surveillance Data Storage shall be hosted in an ISO 27001 compliant hosting. This provider is expected to deliver a highly available, scalable, and flexible data storage platform.		
RQ_TTSU_AS_2	Character set content	Must have
The Surveillance Data Storage shall store content using the ISO/IEC 8859-15:1999 character set.		

3. Repository Router

a. Requirements specifications

i. Functional

Functional Requirements – Tracking and Tracing System – Repository Router		
ID	**Name**	**Priority**
RQ_TTRR_FU_1	Event acquisition	Must have
The Repository Router shall provide one endpoint through which a distributor or a wholesaler may deliver one or more messages at a time.		
RQ_TTRR_FU_2	Event recording	Must have

Functional Requirements – Tracking and Tracing System – Repository Router		
ID	**Name**	**Priority**
The Repository Router shall ensure that all events are validated and recorded in the Surveillance Data Storage.		
RQ_TTRR_FU_3	Submission to interested parties	Must have
The Repository Router shall ensure that all events received from distributors and wholesalers are submitted to the Primary Data Storage of the manufacturer/importer of the items referred to in the event.		
RQ_TTRR_FU_4	Storage of orphan events	Must have
The Repository Router shall store orphan events for which the manufacturer/importer of the items referred to in the event is unknown, until this information becomes available and the event is submitted to a Primary Data Storage.		

ii. Technical

1. System qualities

System Qualities – Tracking and Tracing System – Repository Router		
ID	**Name**	**Priority**
RQ_TTRR_RE_1	Message replay-ability	Must have
The Repository Router shall persist the outgoing messages until the messages are successfully delivered. When trying to transmit the outgoing messages, the Repository Router shall handle transient failures by transparently retrying a failed operation. A durable queue could be a cost-effective implementation alternative.		
RQ_TTRR_RE_2	Data reception acknowledgment	Must have
The Repository Router shall return an acknowledgement of a successful data receipt to the sender, otherwise failing with a consistent error code.		
RQ_TTRR_RE_3	High availability	Must have
The Repository Router shall be available for use with an uptime target of 99.982% (Tier III data centre).		
RQ_TTRR_PE_1	Messaging throughput	Must have
The Repository Router shall support rates of message throughput for input/output operations in the range of 750 thousand (750,000) messages per second per instance.		
RQ_TTRR_PE_2	Minimum concurrency level	Must have
The Repository Router shall support one thousand (1,000 simultaneously connected clients.		
RQ_TTRR_PE_3	Minimum scalability	Must have
The Repository Router shall support traffic spikes up to an average of 20% higher than normal demand.		

2. Security

Security – Tracking and Tracing System – Repository Router		
ID	**Name**	**Priority**
RQ_TTRR_SE_1	Sender tracking	Must have

Security – Tracking and Tracing System – Repository Router		
ID	**Name**	**Priority**
The Repository Router shall resolve and authenticate the sender's identity against a trusted identity provider. Messages sent from an unauthenticated sender shall not be accepted.		
RQ_TTRR_SE_2	Checksum verification	Must have
The Repository Router shall verify the message checksum to ensure that the data was not tampered with. Messages where the checksum is not valid shall not be accepted.		

3. System constraints

System Constraints – Tracking and Tracing System – Repository Router		
ID	**Name**	**Priority**
RQ_TTRR_SC_1	Messaging compatibility	Must have
The Repository Router shall exchange messages conformant with the specification in the Final Report "Implementation analysis regarding the technical specifications and other key elements for a future EU system for traceability and security features in the field of tobacco products" (Annex II, Section 3.5.1).		
RQ_TTRR_SC_2	Decoupling of operations	Must have
The Repository Router must decouple the data acquisition from data processing, avoiding unnecessary coupling between independent processes.		
RQ_TTRR_SC_3	Event-driven design	Must have
The Repository Router shall be designed based on an event-driven architectural pattern for the data acquisition and data processing components.		
RQ_TTRR_SC_4	Fault isolation	Must have
The main components of the Repository Router shall be designed to support fault isolation, in order not to propagate its errors to other components of the solution and limit the impact of any problem to the minimum.		
RQ_TTRR_SC_5	Idempotent messages	Must have
The Repository Router message management shall be designed to avoid acquiring and reprocessing the same message multiple times, since messages of the Tracking and Tracing System are not idempotent.		

ANNEX 2 – SERVICE LEVEL AGREEMENT ("SLA")

1. Data Storage service operation

1.1. Definitions

- "**SaaS**" means Storage as a Service.
- "**DSaaS**" means dedicated SaaS, operated from a remote platform within < Contractor NAME> premises.
- "**DSaaS Failure**" means the duration of time when the user attempts but is unable to access or use, to a material extent, the end-user functionality of the SaaS infrastructure.
- "**Downtime**" and "**Outage**" means the loss of connectivity or persistent access for all running instances that are hosted by the Contractor, combined with the inability to access the external connectivity due to the failure of the Contractor's systems.
- "**RecpS**" means reception service. It is the service provided by the Data Storage to the economic operators, enabling the communication between them.
- "**DEMsg**" means data exchange message. Economic operators send DEMsg to the Data Storage by using RecpS.
- "**AckMsg**" means acknowledgement message. The RecpS always sends an acknowledgement message after receiving a DEMsg.
- "**PSA**" means one or more dedicated private storage arrays (each comprised of a selection of disk drives together with one or more engines), created through the DSaaS in accordance with the service description provided in the RS.
- "**Planned System Downtime**" means a scheduled outage of the Service for the purpose of system maintenance or updates, such as but not limited to a release, patch or hot fix.
- "**Service Level**" means the standards set forth in the Service Level Agreement.
- "**Service Credit**" means the remedy the Contractor will provide for a validated claim. The service credit shall be applied in the form of credit or a discount towards a future invoice of subscription charges for the service.
- "**Availability**" means that the systems shall be promptly available and the agreed service shall not be denied to authorised users.

1.2. Service uptime commitment

1.2.1. For the purpose of measuring the quality of the Service provided, the Contractor commits:

- To provide user access to the DSaaS production application on a twenty-four hour, seven days a week (24/7) basis at a rate of 99.982%[1].
- To commence the DSaaS Services Uptime Metric on the Go Live Date. The Go Live Date is the date upon which the Contractor concludes the successful end-user testing.
- That the Go Live Date shall start to count after the production environment is prepared and released and with a defined point at which end-users access the production environment with production data.

1.3. Measurements method

1.3.1. The DSaaS Services Uptime Metric shall be measured using the service availability process monitoring software provided.

1.3.2. On a monthly basis, the DSaaS Services Uptime Metric will be measured using the measurable hours of the period.

1.4. Setup and deployment

1.4.1. In order to set up the DSaaS, the Contractor shall:

- Provide a RecpS link upon receipt of an order for the same in accordance with paragraph 3.3 of this Annex.
- Provide specific access to this link with secure login authentication, ensuring that each login shall belong to and used by only one specific user.

1.4.2. The Manufacturer/Importer shall procure and configure its own connection to the RecpS link provided by this Service. For the avoidance of doubt, unless otherwise agreed, the Contractor shall not be responsible for any setup obligations other than those set out in paragraph 2.2.1 of this Annex.

1.5. On-going management

- The functionality of the RecpS will enable the user to send any previously agreed DEMsg.
- In order to confirm the reception of a DEMsg, RecpS will send an AckMsg to the Manufacturer/Importer, following the previously agreed rules.
- The Contractor shall:
  a. Be responsible for maintenance of the RecpS infrastructure, including but not limited to replacing failed disks and upgrading any part of the DSaaS infrastructure in accordance with the Manufacturer/Importer' recommendations;

[1] This corresponds to a maximum combined unavailability of 94 minutes per year.

b. Proactively monitor the RecpS infrastructure.
c. Provide troubleshooting assistance for each Manufacturer/Importer and user to ensure the agreed availability.

2. Manufacturer/Importer dependencies

2.1. Where applicable, the Manufacturer/Importer shall ensure that any firewalls operated by the Manufacturer/Importer are functional, and are configured so that the Manufacturer/Importer is able to utilise RecpS.

2.2. The Manufacturer/Importer shall notify DSaaS of any problem with RecpS.

3. Service levels

3.1. For the purposes of this paragraph 3, the following terms and phrases shall have the following meanings:

"**Affected Components**" means the service(s) affected by the failure to meet a service level objective and includes the initial service that failed plus any additional service(s) that suffer a service outage as a result of the initial service's failure.

"**Non-liability Outage**" means an outage that is not considered a service outage. It shall not attract service credits if it is caused by any one or more of the issues listed below:

a. Force Majeure;
b. An application, or any part of an application layer hosted within the Manufacturer/Importer premises, and / or any problem or issue with the application or application layer;
c. A Manufacturer/Importer's infrastructure without the appropriate capability or sufficient capacity to manage the workload or type of traffic flowing through the service;
d. Any request, act or omission of the Manufacturer/Importer without a previous agreement;
e. Any act or omission of any third parties other than directly by the Contractor's request, including but not limited to a hack, virus attack, or presence of other malware;
f. A suspension of the Service formally requested by the Manufacturer/Importer;
g. Downtime of the Service due to maintenance being carried out. For the avoidance of doubt, this shall apply to both scheduled and emergency maintenance.

3.2. DSaaS shall provide RecpS with all reasonable skills and care and shall use reasonable endeavours to ensure that the Manufacturer/Importer can use, to a material extent, the end-user functionality of the RecpS infrastructure 100% of the time. However, in the event of a RecpS failure, the Manufacturer/Importer shall be entitled to receive the applicable service credit as set out in the table below.

RecpS Failure (listed in minutes)	Service Credit (calculated as a percentage of the Variable Fees due to be paid by the Manufacturer/Importer for the relevant calendar month in which the RecpS Failure occurred)
1 – 60	5%
<adjust the table>	<adjust this table in accordance >
525 or above	75%

3.3. For the purposes of calculating the length of time of a RecpS failure, the failure shall begin either (i) when the Manufacturer/Importer reports the fault to the Contractor; or (ii) when the Contractor independently identifies the fault. A RecpS failure shall end when the Manufacturer/Importer is able to use, to a material extent, the end-user functionality of the RecpS infrastructure.

3.4. The Manufacturer/Importer must make a written request for service credits within seven (7) days after the end of the month in which the service level is not met. The Contractor shall not be liable for service credits where the Manufacturer/Importer notifies Contractor after seven (7) days.

3.5. The Contractor shall only be liable for service credits for the affected components.

3.6. The maximum service credits to be issued per billing period shall be one (1) month's MRC (Monthly Recurring Cost), or a prorated amount if applicable, for the billing period during which the service outage was experienced for each affected component directly impacted by the service outage.

3.7. The Manufacturer/Importer shall choose one of the following SLA plans listed below (when applicable):

	Standard	Premium
Availability	99.5%	99.95%
First Byte Latency	Seconds	Milliseconds

3.8. Technical support

Technical support for the service shall be available during the Term of the Agreement.

Email support and hours of operation shall be as follows:

X:xxa.m. – y:yy p.m. CET zone, Monday – Friday (excluding holidays)

Support hotline: +xx-xxxxx-xxxxx.

Email: xxxxxxxxxxx@xxxxxxxxxxxxxxxxx.xx

After Hours & System Down Support is available only for Severity 1 issues on business days, weekends, and holidays.

Severity	Definition	Response time objective (examples to be adjusted in agreement with the Contractor)	Response time coverage (examples to be adjusted in agreement with the Contractor)
High	**Critical business impact/service down**: Business critical functionality means the service is inoperable or a critical interface has failed. It applies only to a production environment and indicates an inability to access services, resulting in a critical impact on operations. This condition requires an immediate solution.	Within less than 30 minutes	24/7
Medium	**Significant business impact**: A service business feature or function of the service is severely restricted in its use or jeopardises business deadlines.	Within 3 business hours	Working weekdays within business hours
Low	**Minor business impact**: Indicates the service or functionality is usable and has no critical impact on operations.	Within 6 business hours	Working weekdays within business hours
Very low	**Minimal business impact**: An inquiry or non-technical request.	Within 1 business day	Working weekdays within business hours

ANNEX 3 – PRICE CONDITIONS (PC)

1. Price

1.1 The price payable for the provision of the Service shall be the amount specified in the table below.

1.2 A fixed and operational monthly price shall be payable for the Service. This monthly price shall be the sum of the prices specified in in the table below. The price for the Service shall become due in the month following the month of Service provision. The fixed and operational monthly price shall be calculated pro-rata according to the unique identifiers for unit packets stored by the Manufacturer/Importer in the Service.

1.3 The prices stated in this Agreement include the cost of all activities connected with and all measures to be taken by the Contractor in order to fulfil its obligations under this Agreement and the Manufacturer/Importer's requirements to the Service at any time during the term of this Agreement, including but not limited to the provision implementation and testing of the systems on which the Service is based; costs of maintaining those systems as well as any software, hardware and other infrastructure or components that form part of those systems, no matter where they are installed; all costs of remote access, network connectivity, reports, documents and other items to be provided in accordance with this Agreement; and all overheads and costs, such as transportation and accommodation costs, subsistence and other allowances.

1.4 The rates stated in the table below, shall remain fixed during YYYY and YYYY. Thereafter, either Party may request an increase or a decrease of those rates once in respect to any subsequent contract year with effect from DDMM of that year, corresponding to any increase or decrease of 2 % (two per cent) or more of the Euro Area harmonised consumer price index (i.e. Euro Area Monetary Union Index of Consumer Prices – MUICP; published for the first time by the Eurostat monthly 'Data in Focus' publication at http://www.ec.europa.eu/eurostat/), compared to the level of the MUICP in MMYYYY for the first price adjustment, and respectively compared to the level of the MUICP at the time of the last price adjustment for any further adjustments. The Party requesting an increase or a decrease shall demonstrate the increase or decrease to the other Party by providing all necessary information and supporting documentation. If the Contractor requests an adjustment, the Contractor shall show that the revised prices correspond at least to the established prices charged by the Contractor to its other customers.

2. Invoice, price and payment

2.1 The Contractor shall submit one single invoice for all one-off and recurring charges that are due in a particular calendar month within 14 (fourteen) calendar days of

the end of that calendar month. The Contractor's invoices shall be in the language of the Agreement and shall quote the Reference Number of the STS. They shall contain a detailed and auditable account.

2.2 Invoices may be submitted only after the relevant due dates indicated in article 1 of this Annex above. Payment of the prices stated in article 1 shall only become due when the Manufacturer/Importer has received an invoice in the correct form.

2.3 The Manufacturer/Importer shall settle the Contractor's invoice in accordance with in article 4 of this Annex.

2.4 Unless otherwise provided, prices shall be in Euros (EUR).

2.5 Prices must include all taxes (except turnover tax), duties and other charges relating to the Service. Any value added tax (VAT) shall be shown separately.

2.6 The Contractor must afford the Manufacturer/Importer all necessary assistance to ensure that it is exempt from, or reimbursed for, taxes, duties and charges. To this end, the Contractor must comply with the instructions given to him/her by the Manufacturer/Importer and provide in due time the information required.

3. Payment, set-off and security retention

3.1 The Manufacturer/Importer shall make payments within thirty (30) calendar days of the receipt of a duly issued invoice which is in accordance with the specifications provided in the present Annex 3 "PC"

3.2 The Contractor may only set off claims which are undisputed or have been upheld by a final court decision.

4. Price conditions

(…)

Monthly Share:

[TABLE]

CAPEX:

[TABLE]

OPEX:

[TABLE]

Total monthly price:

[TABLE]

ANNEX 4 – DEFINITIONS

"Aggregated packaging" means any packaging containing more than one unit packet of tobacco products;

"Agreement" means the entire agreement entered into between the Parties, which consists of this agreement, and any and all statements of work, exhibits, attachments and other documents incorporated by reference into it;

"Anti-Corruption Laws" means any applicable foreign or domestic anti-bribery and anti-corruption laws and regulations, and any laws intended to implement the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions;

"Anti-tampering device" means the device allowing for recording of the verification process following the application of each unit level unique identifier by means of a video or a log file, which once recorded cannot be further altered by an economic operator;

"Common data dictionary" means a set of information describing the contents, format, and structure of a database and the relationship between its elements, used to control access to and manipulation of the databases common for all primary and secondary repositories;

"Confidential information" means all information of any nature whatsoever, on whatever support and in whatever form, format or medium, that relates to the current or future products, services, business and/or organisation of the Disclosing Party and/or Disclosing Party's Affiliates; and all data collected or stored, whether owned by the Parties or third parties; and any information which, if not otherwise described above, is designated by the Disclosing Party as confidential or is of such a nature that a reasonable person would believe it to be confidential. Confidential information shall not include information that the Recipient Party can prove:

(i) was at the time of disclosure, or thereafter becomes, in the public domain without violation of this Agreement;

(ii) was lawfully obtained from a third party that has lawfully obtained the information;

(iii) was already known and recorded by the Recipient Party prior to disclosure by the Disclosing Party or prior to access by the Recipient Party; or

(iv) was developed by the Recipient Party completely independently of any disclosure by the Disclosing Party and of any access by the Recipient Party.

"Data carrier" means a carrier representing data in a form readable with the aid of a device;

"Disclosing Party" means a Party that discloses confidential information to another Party, or a Party that gives another Party access to confidential information or the confidential information of which is otherwise obtained by the other Party in connection with the Agreement;

"Effective Date" means the date on which this Agreement is signed by both Parties;

"Economic operator" means any natural or legal person who is involved in the trade of tobacco products, from the manufacturer to the last economic operator before the first retail outlet;

"Facility" means any building where tobacco products are manufactured or stored;

"Machine" means machinery which is designed, or adapted, to be used for the manufacture of tobacco products and is integral to the manufacturing process;

"Maintenance" means:

(i) Corrective maintenance: diagnosing and resolving all system incidents and problems, found by the Contractor or the system users;

(ii) Preventive maintenance: performing system tuning, code restructuring, monitoring and other efforts to improve the efficiency and reliability of programs and to minimise on-going maintenance and prevent problems in the future.

"Offline flat-files" means the electronic files that contain data allowing for the extraction of information encoded in the unique identifiers (excluding the timestamp) used at the unit packet and aggregated packaging levels without accessing the repository system;

"Primary repository" means a repository containing data that originate from one manufacturer or importer;

"Recipient Party" means a Party to which confidential information is disclosed, or which has access to or otherwise obtains confidential information in connection with the Agreement;

"Registry" means the record of all the identifier codes generated for economic operators, facilities and machines along with the corresponding information;

"Repository system" means the system consisting of the primary repositories, the secondary repository and the router;

"Router" means a device established within the secondary repository that transfers data between different components of the repository system;

"Secondary repository" means a repository containing a copy of all data stored in the primary repositories;

"Time stamp" means the date and time of occurrence of a particular event recorded in UTC (Coordinated Universal Time) time in a prescribed format;

"Unique identifier" means the alphanumeric code enabling the identification of a unit pack or an aggregated packaging of tobacco products;

"Working day" means any day from Monday to Friday except legal holidays in the Member State for which the ID issuer is competent.

EB-02-17-898-EN-N

Publications Office

doi:10.2818/751591