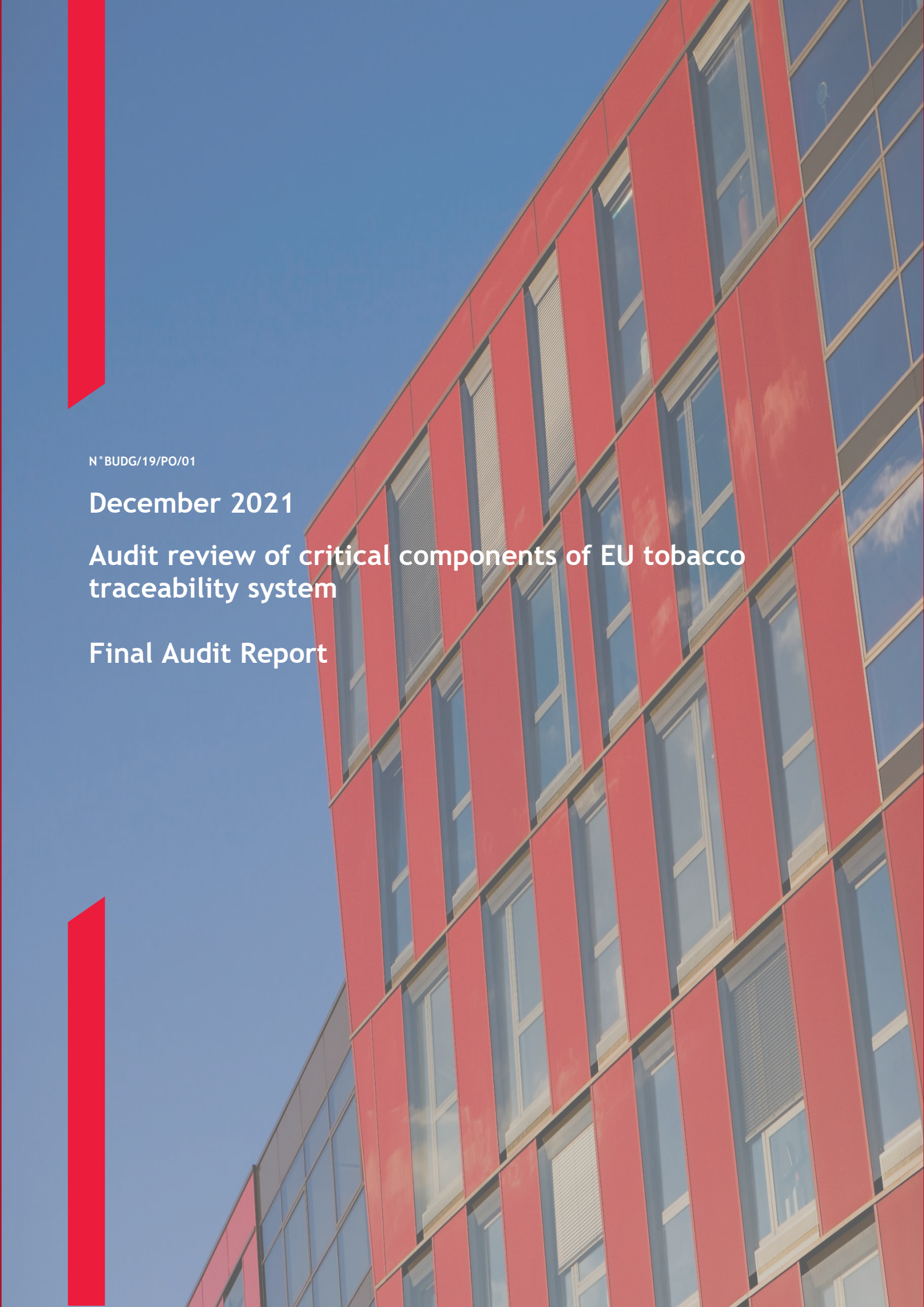


N°BUDG/19/PO/01

December 2021

Audit review of critical components of EU tobacco traceability system

Final Audit Report

Table of Contents

1. Executive Summary

1.1. Introduction

On 3 April 2014, the European Parliament and the Council adopted the Tobacco Products Directive 2014/40/EU ('TPD'). Article 15 of the TPD aims to address the illicit trade in tobacco products by introducing a system of traceability for these products. The EU system contributes to reducing the circulation of tobacco products not compliant with the TPD and other tobacco control legislation. Its purpose is to reduce artificially cheap supplies of illegal tobacco products that affect the uptake and general prevalence of smoking. It therefore plays an important role in protecting public health, state budgets and legal economic operators.

As part of the overall legislative framework and to compliment the TPD, the EU has also defined and adopted the following additional legislation:

- Commission Implementing Regulation (EU) 2018/574 on technical standards for the establishment and operation of a traceability system for tobacco products
- Commission Delegated Regulation (EU) 2018/573 on key elements of data storage contracts to be concluded as part of a traceability system for tobacco products.

The Implementing Regulation sets out the various components that are required to be implemented as part of the system of traceability to manage and monitor tobacco products. These include:

- repositories which are established for the purpose of storing data relating to tobacco products of individual manufacturers and importers ('primary repositories')
- a repository which contains a copy of all data stored in the primary repositories system ('secondary repository')
- a routing service ('router') set up and managed by the provider of the secondary repository system.

In addition to the components as mentioned above, the EU legislation provides various technical and non-technical requirements for the primary and secondary repositories and router.

In December 2018, a concession contract was established between the EU Commission and Dentsu Aegis Network Switzerland AG (hereafter referred to as 'Dentsu') to provide the secondary repository and router for a period of 5 years and the systems went live on 20 May 2019.

1.2. Objectives and Scope

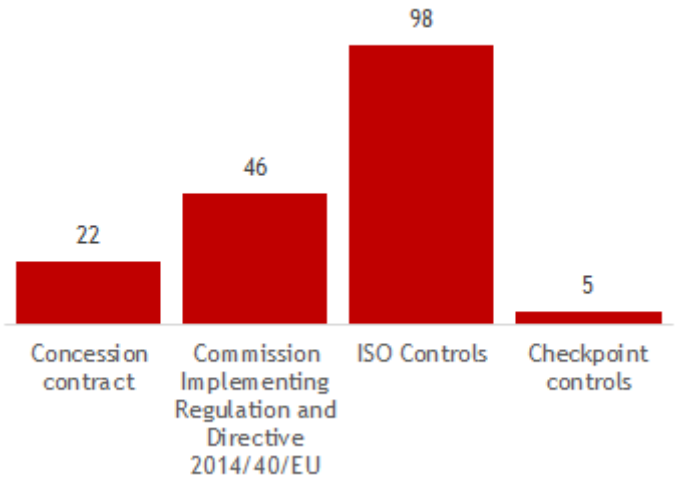
The Tobacco Products Directive 2014/40/EU foresees that an external audit must be conducted of the primary repositories. To structure this process, the EU Commission adopted Guidelines on annual audit reports to be submitted in accordance with Article 15(8) of Directive 2014/40/EU in the context of the EU traceability system for tobacco products.

In order to complete the audits of the primary repositories, the EU Commission, through an RFP process, required the services of an external services provider to perform an audit of the secondary repository and router provided by Dentsu Aegis Network Switzerland AG ('Dentsu').The objective of the audit was to provide a review of the controls that the contractor, Dentsu, is currently operating and ensure that it is in line with its contractual requirements, as well as ascertaining whether the router and secondary repository is configured and managed in line with the information security management standards and including the domains as set out by the abovementioned Guidelines.

Our engagement approach can be found in Appendix 1.

1.3. Summary of Key Findings

68 requirements from the Concession Contract, Commission Implementing Regulation (EU) 2018/574 and Directive 2014/40/EU that are within the scope of this audit are listed in this report. 98 ISO controls (across 6 areas) and 5 categories of validation controls – or checkpoints – are also covered. Graph 1 shows the split of requirements and controls reviewed. Where a control satisfies the requirements for the Concession contract, the legislation, ISO controls and Checkpoint controls, control testing was not duplicated, and our observations were only reported within one section of the report and referenced where appropriate.



Graph 1: Number of requirements and controls reviewed

Our review also highlighted the following areas of leading practice implemented by Dentsu which are considered relevant to the services provided to the European Commission:

- Dentsu is currently ISO 27001 certified and conduct compliance audits as and when required
- Access to the secondary repository and router are limited to the team within Dentsu responsible for providing this service to the European Commission
- The organisation has adopted a cloud first strategy and have utilised the services of an established Infrastructure-As-A-Service provider to host the secondary repository and router
- Redundancy and backup solutions have been designed and implemented in line with the availability requirements of the European Commission services contract
- Monitoring solutions are in place to detect and respond to security related incidents
- Contract management activities, such as meetings and performance reviews are regularly conducted, with resulting actions assigned and distributed
- Risk registers are maintained and discussed and contains risks that are categorised, and impact assessed
- Management policies and guidelines are in place to govern areas such as Conflict of Interests, Data Retention Storage, Privacy Principles, Supplier Assurance and Third-Party Management
- Responsibilities and roles of resources assigned to the operation of the EU secondary repository are defined, with backup personnel allocated to specific roles
- Although the obligation has not been triggered, an Exit Strategy has been drafted by Dentsu
- Dentsu have provided additional services not considered part of the scope of the Concession Contract and regulation, this includes:
  - Creating a test environment for the primary repository providers
  - Supporting the primary providers

- Contracts with primary repository providers are in place based on a consistent template.

The results of our assessment highlighted one finding and four observations. 'Findings' relate to errors in delivering the relevant requirements, whereas 'observations' are defined as not relating to non-compliance, but opportunities for improvement or areas to note for the European Commission and Dentsu. The findings and observations are:

Finding:

- For the months of Aug – Sept 2019, Oct – Nov 2019 and Feb – Mar 2021, there was a clerical error relating to the updating of SLA and performance reports. This has been identified as a known error and was communicated to Dentsu by the European Commission. The European Commission confirmed that, due to the size of the error, the impact was not deemed significant or material.

Observations:

- The approval of the resulting and non-resulting information from the European Commission is required before Dentsu is obligated to submit its Exit Strategy within 30 days of the aforementioned approval. As the approval had not yet been formally provided at the time of our fieldwork, this is not a non-compliance observation; however, there is a contractual obligation that cannot be fulfilled due to a dependency that should be noted.
- Not all seven of the originally approved primary repository provider contracts and had been submitted to the European Commission within one month of the appointment of Dentsu per Clause 7.6 of the Concession Contract (see section 2.2.1 for further details). This has been noted as an observation as, while the timing was not formally or contractually amended per best practice both parties agreed there was no impact when assessing Dentsu's ability and obligations in providing the services, due to:
  - The European Commission's acknowledgement that the timeline was ambitious and that there is a reliance on legal negotiations being concluded, of which Dentsu may not have full control
  - Email confirmation from the European Commission to extend the deadline
  - The shared responsibility with the primary repository providers for the submission per points 4 and 5 of Part B of Annex I within the Implementing Regulation
  - The reduced access risks due to the lack of connection to the tobacco traceability system
  - Submission of the contracts was ultimately within two months of the appointment date and not significantly delayed.

  It is recommended that adjustments to deadlines are formally agreed where both parties believe it may be unachievable, and ultimate ownership of obligations is clarified by all parties to avoid potential disagreements.
- While Dentsu has implemented Bitlocker to Go, which allows for encryption (encryption is the process of converting information from plain text to ciphertext) of removable media, it is a recommended, but not mandatory control for users. Blocking the use of removable media or mandating that these be encrypted before transferring data can further mitigate the risk of data manipulation and leakage. Dentsu is currently in discussions with its Global IT to determine the best course of action.
- Through the review of the KPIs procedure, the audit team noted that there is an opportunity to consider how the KPI goals are defined, i.e., best practice for goal setting can follow the SMART (Specific, Measurable, Attainable and Time-based) objectives or equivalent. This will facilitate a review of their appropriateness to the services provided.

1.4. Conclusion

With the exception of the finding noted in Section 1.3. Summary of Key findings above *(*amounting to a clerical error) our testing has observed that Dentsu has designed and implemented the controls for the secondary repository and router in line with the requirements set out within the Concession Contract, the Commission Implementing Regulation (EU) 2018/574 and the Commission Delegated Regulation (EU) 2018/573.

2. Detailed Assessment Outcomes

2.1. Our understanding of the tobacco traceability system

The tobacco traceability system is made up of three components namely, the primary repositories, the secondary repository and router. Each manufacturer and importer (economic operators) of tobacco products within the European Union is required to have selected a third-party provider to establish a data storage facility to host data related to the products, also referred to as the primary repository. Currently there are ten approved suppliers of primary repositories that have been approved by the Commission.

To allow for Member States to monitor the tobacco products of the various manufacturers, the secondary repository was established as a data warehouse to consolidate data from the various primary repositories and maintain a copy of the data held within these primary repositories. The router is used to dispatch traceability data received from economic operators to the relevant primary repository and transmit data from ID issuers to the secondary repository.

2.1.1. Description of the secondary repository and router

Within the tobacco traceability system, the secondary repository and router are maintained by Dentsu. The secondary repository acts as a copy of the data held on all primary repositories and allows for the monitoring of activity in relation to tobacco products to take place. The router receives data from ID issuers and economic operators, performs validation checks on the messages sent by these parties, and ensures transmission of this data takes place to the relevant primary repository, and to the secondary repository where required.

Both the secondary repository and router systems are hosted within a third-party cloud hosted infrastructure solution. Interfaces are maintained between the secondary repository and the router, primary repositories, ID issuers, and economic operators, with communications secured using a non-proprietary, open communication standard. Separate interfaces are present between the secondary repository and EU Commission authorities where necessary to allow for auditing of the data held by the secondary repository. Reports around the movement of tobacco products within specific EU member states is also made accessible to competent authorities (the EU Commission and Member States personnel) who are allowed access to this information from the Secondary Repository Portal, which is a graphical interface maintained by Dentsu.

2.2. Detailed assessment outcomes

2.2.1. Contractual Compliance

The following section highlights the contractual requirements stated within the Concession Contract that we have audited Dentsu against:

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	General Scope
Clause/Article Reference:	2.3
Requirement:	The 'Services' relate to the services to be carried out in accordance with Article 15 of the Directive 2014/40/EU2 and Articles 25, 27, 28, 29 and 36 of Commission Implementing Regulation (EU) 2018/574, and means any and all services to be provided by the Contractor under the contract, including: (a) the deployment and operation of the secondary repository (b) the deployment and operation of the router (c) the obligation to carry out patches, fix bugs, or perform other maintenance of the service to ensure the effective operation of the repositories system (d) the deployment and operation of all necessary services to fulfil the functional and technical requirements set out in Annex I.
Evaluation and Documents Reviewed: Based on the review of the architecture diagram and through walkthroughs conducted with Dentsu that a Secondary Repository and Router has been deployed. This is in line with the Concession Contract and the Commission Implementing Regulation (EU) 2018/574 and the Directive. The Secondary Repository and Router are hosted on a third-party Infrastructure-As-A-Service platform and managed internally by the Dentsu team. Dentsu provides a test environment as part of its provision of the secondary repository and router system. While this is not specifically required in the contract and may increase the risk that access to a test system can be terminated without invoking contract non-compliance, it is generally regarded as best practice to include a test environment for this type of services. As such, an explicit contractual requirement may not be necessary.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	General Scope
Clause/Article Reference:	3.1
Requirement:	The Contractor shall provide services of high-quality standards, in accordance with the state of the art in the industry and the provisions of this contract, in particular the technical specifications and the terms of its offer.
Evaluation and Documents Reviewed: The secondary repository and router are hosted on a recognised industry Infrastructure-As-A-Service platform, with regular contract management meetings with the provider that covered the latest changes and potential improvements in operational processes. Through supporting evidence, the audit team confirmed that Dentsu followed best practice in project management (i.e., SCRUM, PRINCE2), operations (ITIL), security (OWASP) and development (SDLC). Dentsu has also obtained and maintained its ISO 27001 certification, in line with the requirements as set out within the Concession Contract and the legislation.	

Findings Noted: *N/A*
Observations Noted: *N/A*

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	General Scope
Clause/Article Reference:	3.2
Requirement:	The Contractor shall comply with the minimum requirements provided for in the technical specifications. This includes compliance with applicable obligations under environmental, social, and labour law established by Union law, national law, and collective agreements or by the international environmental, social, and labour law provisions listed in Annex X to Directive 2014/24/EU.
Evaluation and Documents Reviewed: Processes are in place to monitor legal and compliance risks. The audit team observed evidence of personnel onboarding, and workshops and invitations for sessions in which the legal requirements under the Commission Delegated Regulation (EU) 2018/573 and Commission Implementing Regulation (EU) 2018/574 were discussed and communicated. Evidence also included the weekly steering calls with the European Commission to discuss any new emerging interpretations of existing legal requirements. Through observations, the audit team noted that local legal compliance risks have been formally recognised within Dentsu's Risk Management Framework within the risk register, demonstrating an organisational awareness of meeting these obligations. Additionally, the standard Employment Contract reviewed contained a requirement for committing employees to abide by the Code of Conduct.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	General Scope
Clause/Article Reference:	3.3
Requirement:	The Contractor shall obtain any permit or licence required in the State where the Services are to be provided.
Evaluation and Documents Reviewed: Dentsu provided permits and licenses for software solutions that are used to deliver the services.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	General Scope
Clause/Article Reference:	3.7
Requirement:	The Contractor shall ensure that the personnel performing the contract and any future replacement personnel possess the professional qualifications and experience required to provide the Services.
Evaluation and Documents Reviewed: There is a process in place to assess personnel for professional qualifications and experience required to provide the Services. Evidence was reviewed showing a list of personnel and their roles in the repository service. It was also confirmed that the recruitment process for hiring personnel included a review of their technical capabilities, interviews, candidate screening, background checks and reference checks. An onboarding / offboarding management review process for IT access was also confirmed.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	General Scope
Clause/Article Reference:	3.9
Requirement:	The Contractor shall record and report to the Contracting Authority any problem that affects its ability to provide the Services. The report shall describe the problem, state when it started and what action the Contractor is taking to resolve it.
Evaluation and Documents Reviewed: Reports are collated and provided to highlight service levels and performance, and actions are recorded; however clerical issues were found in the update of the numbers within three of the reports. SLA / availability reports from July 2019 to April 2021 were reviewed by the audit team. These reports provide statistics and graphics demonstrating performance of the contract technical specifications. Of the months tested, SLAs 1, 2 and 3 were reported, with SLA 4 confirmed as a non-reported measure. The audit team observed meeting minutes from an EC status meeting from 25 June 2021 demonstrating the allocation of actions arising from system errors that require resolution. We noted that the performance reported for Aug - Sept 2019, Oct - Nov 2019 and Feb - Mar 2021 were identical. This was confirmed as a clerical error by Dentsu; the European Commission was aware of the error and deemed the materiality low. It was noted as a clerical error and Dentsu has noted that Quality Assurance will be increased. The mitigating control is that KPIs are discussed weekly between Dentsu and the Commission. The audit team also noted through the review of the KPIs procedure that there may be an opportunity to review how the KPI goals are defined, i.e., best practice for goal setting can follow the SMART (Specific, Measurable, Attainable and Time-based) objectives or equivalent.	
Findings Noted: Clerical errors meant that the performance during Aug – Sept 2019, Oct – Nov 2019 and Feb – Mar 2021 had not been correctly updated in the reports.	
Observations Noted: There is an opportunity to include SMART objectives for KPIs.	

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	General Scope
Clause/Article Reference:	3.10
Requirement:	The Contractor shall notify to the Contracting Authority any entity that it wishes to subcontract any parts related to the Performance of the Contract and which was not notified during the approval phase of the Contractor as an operator of a primary repository. Prior written approval of the Contracting Authority shall be required in such cases.
Evaluation and Documents Reviewed: Through a review of evidence provided, the audit team confirmed that subcontractors were notified and approved by the European Commission. Two subcontractors were utilised, with one already included and approved as part of Dentsu's tender process. It was confirmed that the remaining subcontractor was notified to the European Commission with written approval obtained. Additional evidence was also provided demonstrating that legal and technical reviews were undertaken to assess the subcontractor's suitability to perform the services required, such as a completed supplier questionnaire, Information Security assessments, legal and financial independence.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	General Scope
Clause/Article Reference:	3.11
Requirement:	The Contractor shall inform as soon as possible the Contracting Authority of any complaint files lodged by a third party in relation to the performance of the Services, and of the answer or solution provided to such third party.
Evaluation and Documents Reviewed: Complaints are managed as incidents through a review of the incident handling process at Dentsu. Incidents are collected by the Dentsu operational team and stored in the ticketing system. These are managed and reviewed daily by the operational team in order to ensure that a proper response is provided and where necessary the priority of the incident will be increased. Should the complaint not be answered successfully, or should the impact prevent the operation of an economic operator then the below escalation process is to be followed: Level 1: Operation Management Level 2: EU Secondary Program Director Level 3: Dentsu Managing Director Level 4: EU Commission Complaints are also addressed via the weekly operational meetings held between Dentsu and the Commission, as well as during meetings with key stakeholders. Through observations, we noted that the complaints handling procedure outlined how complaints were collected and managed by the operational teams depending on priority and that there is an escalation process for unresolved incidents. The process also covers how resolutions are communicated and how feedback is sought from the party raising the complaint.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	Liability
Clause/Article Reference:	4.2
Requirement:	If required by the relevant applicable legislation, the Contractor shall take out an insurance policy against risks and damage or loss relating to the performance of the contract. It shall also take out supplementary insurance as reasonably required by standard practice in the industry. Upon request, the Contractor shall provide evidence of insurance coverage to the Contracting Authority.

Evaluation and Documents Reviewed:
The audit team confirmed there were in-date insurance policies held by Dentsu for the following risk / insurance categories with limit amounts of at least £10m each:

- General / Public Liability
- Product Liability
- Property Damage and Business Interruption
- Professional Indemnity

A risk assessment is performed annually with the insurance provider to re-evaluate the risks.

Findings Noted:
N/A

Observations Noted:
N/A

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	Conflict of interests
Clause/Article Reference:	5.2
Requirement:	The Contractor shall notify the Contracting Authority in writing as soon as possible of any situation that could constitute a conflict of interest during the performance of the contract. The Contractor shall immediately take action to rectify the situation. The Contracting Authority may do any of the following: (a) verify that the Contractor's action is appropriate (b) require the Contractor to take further action within a specified deadline.

Evaluation and Documents Reviewed:
Evidence of the vetting and conflict of interest checks for staff was reviewed. The audit team noted that employees are also required to periodically sign a declaration to confirm the absence of any conflicts of interest and their compliance with the specific requirements imposed on them by Article 35 of CIR 2018/574.

As part of the onboarding process for staff, staff members are vetted for existing / past conflict of interest activities (e.g., employment with the tobacco industry). Staff members are also required to periodically declare an absence of conflict of interest.

Findings Noted:
N/A

Observations Noted:
N/A

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	General - scope
Clause/Article Reference:	7.1
Requirement:	The Contractor shall provide the Services set out in Annex I. As provided for in Article 27(11) of Implementing Regulation (EU) 2018/574, the Contractor and the Contracting Authority may agree to include additional services for the purpose of contracting the former to carry out additional services not provided for in that Regulation. Additional proportional fees may be charged by the Contractor for providing such additional services.
Evaluation and Documents Reviewed: Dentsu confirmed that no additional scope of work has been agreed with the primary repository operators. However, a mobile app has been added to the scope of the services between Dentsu and the European Commission but was excluded from the scope of this audit.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	General - scope
Clause/Article Reference:	7.5
Requirement:	The Contractor shall maintain the operability, availability, and performance of the Services for the duration of this contract.
Evaluation and Documents Reviewed: The services provided are from the date of the Concession Contract to the current audit period. Dentsu monitor the system on a regular basis to ensure the operability, availability and performance of the system is in line with the requirements as set out within the contract and legislation. The audit team reviewed the SLA / availability reports from July 2019 to April 2021. These reports provide statistics and graphics demonstrating performance of the contract technical specifications. Of the months tested, SLAs 1, 2 and 3 were reported, with SLA 4 confirmed as a non-reported measure. Meeting minutes from an EC status meeting from 25 June 2021 was also reviewed demonstrating the allocation of actions arising from system errors that require resolution.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	General - scope
Clause/Article Reference:	7.6
Requirement:	Pursuant to point 4 of Part B of Annex I to Implementing Regulation (EU) 2018/574, the Contractor shall enter into individual contractual agreements with each provider of a primary repository for the maximum price indicated in point 11.1. The contracts shall be signed and submitted to the Commission within one month from the date of the appointment of the secondary repository.
Evaluation and Documents Reviewed: The nine individual primary repository agreements were reviewed that have been entered with Dentsu and the audit team confirmed that each agreement was based on a contract template drafted by Dentsu to help ensure the relevant Commission Implementing Regulation (EU) 2018/574 requirements were covered, which includes the maximum price. The agreements corresponded to	

those that the European Commission published as notified and approved (the latest issue by the European Commission was reviewed from 24 June 2019). The audit team also reviewed evidence of the draft agreement template sent to the European Commission for comment on 13 January 2019, prior the commencement of the agreements with the primary repository providers. At the time of the appointment of the secondary repository provider (21 December 2018), seven primary repository providers were known. Six of these had their signed agreements submitted to the European Commission within the extended deadline provided (25 January 2019), although the date was not formally updated in the contract. One contract was submitted shortly after.

The European Commission informed the audit team that one month was likely optimistic given that contract negotiations may take longer in reality and, additionally, Dentsu would connect to the primary repository after the relevant legal agreements had been signed and the system had not yet gone live so there was no risk of inappropriate connections.

It was also noted that points 4 and 5 of Part B of Annex I to the Implementing Regulation (mentioned in Clause 7.6) suggest that the submission of the contracts are the joint responsibilities of both the primary and secondary repository providers *("Each primary repository provider appointed in accordance with Part A shall enter into an individual contract with the provider appointed to operate the secondary repository… [and Point 5] The contracts shall be signed and submitted to the Commission within one month from the date of the appointment.")*.

Findings Noted:
N/A

Observations Noted:
While not all seven of the originally approved primary repository provider contracts had been submitted to the European Commission with one month of the appointment of Dentsu, email chains showed that the European Commission acknowledged the delays from the primary repository providers and provided an extension to the deadline for submission. Additionally, the submissions were within two months, and it is recognised by the European Commission and the secondary repository provider that the period specified was not realistic given that contract agreement is subject to negotiation of terms that could take longer than one month to agree in reality - these factors may impact the ability to submit within the deadline and of which Dentsu would not have full control.

Furthermore, connection to the Tobacco Traceability System was dependent on the contracts being formally agreed and the system was not yet live. Therefore, this has been noted as an observation as, while the timing was not formally or contractually amended per best practice:

- The European Commission acknowledged that the timeline was ambitious and that there is a reliance on legal negotiations being concluded, of which Dentsu may not have full control
- Email from the European Commission was provided, extending the deadline
- There is a shared responsibility with the primary repository providers for the submission per points 4 and 5 of Part B of Annex I within the Implementing Regulation
- There is a lack of connection to the tobacco traceability system
- Submission of the contracts was ultimately within two months of the appointment date and not significantly delayed.

It is recommended that adjustments to deadlines are formally agreed where both parties believe it may be unachievable and ultimate ownership of obligations is clarified by all parties to avoid potential disagreements.

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	General - scope
Clause/Article Reference:	7.7
Requirement:	The Contractor shall submit to the Commission within two months from the date of its appointment as the secondary repository the list of specifications and the common data dictionary, referred to in Article 28 of Implementing Regulation (EU) 2018/574. The contractor shall submit to the

	Commission within one month from the date of its appointment as the secondary repository drafts of these documents. Any updates of these documents shall be submitted to the Commission at least two months prior to the date of implementing the update into the system.
Evaluation and Documents Reviewed: Through the review of evidence relating to the communication of the latest specifications and data dictionary, the audit team noted that the specifications were released within two months of the appointment date. Through the review of the data dictionary version history, the draft version (v0.2) was released a month after the appointment date. Discussion with the European Commission and Dentsu confirmed that forums are held to review amendments or updates prior to each version being released. Currently, v1.4.4 is applicable.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	Location
Clause/Article Reference:	12.2
Requirement:	The Contractor shall notify the Contracting Authority about the location, or where applicable locations, of the data storage facilities no later than 19 May 2019.
Evaluation and Documents Reviewed: The secondary repository and router are hosted by a third-party in a location situated within the European Union. The location of the hosting provider was communicated to the European Commission on the 07 March 2019.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	Sub-contracting
Clause/Article Reference:	13.1
Requirement:	In case of subcontracting, the Contractor shall: (a) retain full responsibility vis-à-vis the Contracting Authority for the performance of the contract as a whole during its entire duration (b) ensure that the proposed subcontractor has the necessary technical expertise and meets the requirements of independence laid down in Article 35 of the Implementing Regulation (EU) 2018/574 (c) submit to the Contracting Authority a copy of the declaration referred to in Article 8 of the Delegated Regulation signed by the respective subcontractors
Evaluation and Documents Reviewed: Two subcontractors were utilised, with one already included and approved as part of Dentsu's tender process. The audit team confirmed that the remaining subcontractor was notified to the European Commission with written approval obtained and a declaration completed. Additional evidence was also provided demonstrating that legal and technical reviews were undertaken to assess the subcontractor's suitability to perform the services required, such as a completed supplier questionnaire, Information Security assessments, legal and financial independence.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	Resulting Information
Clause/Article Reference:	16.3
Requirement:	By 20 March 2019, the Contractor shall draw up and submit for the Contracting Authority's approval a list of resulting information and non-resulting information that is necessary for understanding, accessing, or using the resulting information. The Contracting Authority is entitled to organise on-site visits in order to further elaborate this list of resulting information and non-resulting information.

Evaluation and Documents Reviewed:
Evidence was reviewed showing that the required resulting and non-resulting Information list was submitted to the Authority on 20 March 2019, with an updated list submitted on 28 August 2021. The submitted documents are still pending Authority authorisation / approval.

Findings Noted:
N/A

Observations Noted:
The approval of the resulting and non-resulting information from the European Commission is required before Dentsu is obligated to submit its Exit Strategy within 30 days of the aforementioned approval. The obligation under Concession Contract clause 17.1 cannot be fulfilled until the approval is provided.

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	Exit Strategy
Clause/Article Reference:	17.1
Requirement:	Within 30 days from the approval of the list of resulting information referred to in Point 16.3, the Contractor shall submit to the Contracting Authority a draft exit strategy for approval.

Evaluation and Documents Reviewed:
As the Resulting Information has not been formally approved by the Commission, the obligations under this Article had not been triggered at the time of fieldwork. However, Dentsu has a draft Exit Strategy in place which contains some of the following key areas expected:

- Clause 1.2: Dentsu will provide the European Commission with the Exit Information within 14 working days of request.
- Clause 1.3: Data transfer will be performed in a way that ensures the security and protection of personal, commercial, and other sensitive data. Namely the data transfers will take place in accordance with:
  - Data protection rules and standards set out in the EU GDPR
  - Security rules and procedures defined by industry standards, such as ISO 27000, and those that are specified in the Concession Contract.
- Clause 1.6: Dentsu will define and participate in coordination meetings with the Replacement Provider to agree on the terms and modalities of the transfer process.
- Clause 1.7: Dentsu to define and participate in meetings with the European Commission. In the case of termination or failure of the Dentsu business, Dentsu will initiate the first meeting within 5 working days of written notice. In the case of expiry of the Concession Contract, Dentsu will initiate the first meeting no later than 9 months prior to the expiry date or as otherwise requested by the EC.

Findings Noted:
N/A

Observations Noted:
An Exit Strategy exists within Dentsu, which has not been submitted to the Authority. This is due to a dependency on the Authority, where the deadline for submission is triggered when the list of resulting information / non-resulting information has been approved (Concession Contract, 17.1).

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	Liquidated Damages
Clause/Article Reference:	18.1
Requirement:	If the Contractor fails to perform its contractual obligations at any time during the term of the contract, the Contracting Authority may claim liquidated damages for each day of absence of the Services using the following formula: 0.3 x (P x V) / 365 Where P is the price specified in Point 11.1 V is the annual volume of the contract defined as a multiple of 10,000 (ten thousand) unit level unique identifiers, the multiple shall be equal to the total number of unit level unique identifiers introduced into the EU tracking and tracing system for tobacco products in the year preceding the absence of the Services divided by 10,000 (ten thousand); until the end of the first full year in which the EU tracking and tracing system for tobacco products collects the relevant data the annual volume of the contract shall be assumed to account to 2.6 million, i.e. 26 billion divided by 10,000 (ten thousand).
Evaluation and Documents Reviewed: No liquidated damages have been applied to date. The audit team have further noted that there were no liquidated damages over the life of the contract that had been established with the European Commission.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	Liquidated Damages
Clause/Article Reference:	18.2
Requirement:	The Contracting Authority must formally notify the Contractor of its intention to apply liquidated damages and the corresponding calculated amount. The Contractor has 30 days following the date of receipt to submit observations. Failing that, the decision becomes enforceable the day after the time limit for submitting observations has elapsed. If the Contractor submits observations, the Contracting Authority, taking into account the relevant observations, must notify the contractor: (a) of the withdrawal of its intention to apply liquidated damages; or (b) of its final decision to apply liquidated damages and the corresponding amount.
Evaluation and Documents Reviewed: No liquidated damages have been applied to date.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	Invoicing
Clause/Article Reference:	20.1
Requirement:	Invoices shall be issued to providers of primary repositories at the end of each period of reference, to be defined in the individual agreements with the primary repositories, at least once a year.
Evaluation and Documents Reviewed: A sample of invoices for two primary repository providers covering the period June - August 2021 was reviewed and it was noted that they were raised in accordance with the individual agreements each month in the sample.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	Concession contract SANTE/2018/B2/063
Sub-Category:	Checks and Audits
Clause/Article Reference:	21.4
Requirement:	The Contractor must keep all original documents stored on any appropriate medium, including digitised originals if authorised under national law, during the performance of the contract and up to five years after the end of the contract.
Evaluation and Documents Reviewed: Data retention policies are in place. Discussions with Dentsu revealed that the type of information would determine the retention policy applied. The audit team reviewed the Dentsu Retention Storage policy and noted that the document showed a breakdown of document and record types, the associated retention periods and the assigned data owners and locations of storage. • For data in the secondary repository: traceability and audit (described in 25.1.m below) data in the repository is stored for a duration of at least five years. • Information relating to identifier codes (economic operator, facility, machine) are stored for as long as the tobacco traceability system is operational. • For business and client documents such as emails, reports and policies, retention is in accordance with the Dentsu Retention Policy (submitted as additional policy evidence under ref no. 22 of Task 1). • National laws may impose further restrictions on specific document of information, such as accounting, tax records, HR records, in which case the mentioned Dentsu Policy will impose the legal retention periods accordingly.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

2.2.2. Compliance to Legislative Requirements

The section below defines the legislative requirements that Dentsu must comply with:

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	General Requirements
Clause/Article Reference:	17
Requirement:	In order for the traceability system to be able to achieve its objective, it is necessary for it to be capable of enabling easy transmission of all relevant data, providing secure storage of data, and ensuring full access to this data for the Commission, the competent authorities of the Member States and the external auditor. The storage architecture should further allow manufacturers and importers to select independent third-party data storage providers with which to conclude data storage contracts for the purpose of hosting data related exclusively to their tobacco products ('primary repositories'), as provided for by Article 15(8) of Directive 2014/40/EU, whilst ensuring authorities are provided with full access to all stored data for the purpose of carrying out their monitoring and enforcement activities. The effectiveness of such monitoring and enforcement activities requires the presence of a single second-level repository system ('secondary repository'), containing a copy of all the data stored in the primary repositories and providing authorities with a global overview of the functioning of the traceability system. A routing system, operated by the provider of the secondary repository, should be established in order to provide economic operators other than manufacturers and importers with a single-entry point to submit the data recorded by them to the traceability system and thereby ease the data transmission. At the same time, the routing service should ensure that data are transmitted to the correct primary repository.
Evaluation and Documents Reviewed: The audit team confirmed that that the traceability system is capable of enabling the transmission of data, provides secure storage of data and ensures full access of the data when necessary. Through a walkthrough, we covered the flow of data which detailed how the data begins from the economic operators (EOs) requesting and receiving UI codes. UI codes are sent from the router to either the primary repositories (if manufacturers or importers) or to the secondary repository (if distributors or wholesalers). Information sent directly to the primary repositories will be copied instantaneously to the secondary repository. The secondary repository contains a copy of all the data of all the messages sent by the primary repository and router. Data is securely stored within cloud-based infrastructure's database, with the European Commission and Member States being able to access the secondary repository information via the Secondary Repository Portal. External auditors can be provided access only by Dentsu Administrators upon request and approval. The presence of the above secondary repository, router and database was observed during the walkthrough. Furthermore, routing tables are utilised to ensure that the router is sending messages to the correct primary repository. It was described during the walkthrough that messages are split by the router to ensure messages were sent to the appropriate primary repository using routing tables provided by the primary repositories, this is achieved using multiple Lambdas. Lambda is a server-less computing platform used to run various functions of the router.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	General Requirements
Clause/Article Reference:	18
Requirement:	In order to guarantee full access for relevant authorities and to contribute to the efficient functioning of the traceability system, the provider of the secondary repository should develop user interfaces enabling the stored data to be viewed and queried. In accessing the repositories system, the relevant authorities should be able to rely on the eIDAS(4) based reusable solutions provided as building blocks under the telecommunication part of the Connecting Europe Facility. In addition, to facilitate effective surveillance and enforcement, the user interface should allow for the possibility to define individual automatic alerts based on specific reporting events.
Control Checkpoint Objective:	Reporting and Information
Requirement:	Review / assessment of the completeness and accuracy of information presented by the User Interfaces (Standard, Advanced, and Application).
Evaluation and Documents Reviewed: Through walkthroughs, the audit team observed that a user interface is present that allows stored data to be viewed and queried. As observed during a walkthrough, the Secondary Repository Portal allows the European Commission and Member States to view and query stored data. The evidence provided shows a list of current reports generated by the Secondary Repository Portal e.g., authorities can visualise the full history of a certain unique identifier (UI). An example screenshot showing the output for UI summary data has also been provided.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	General Requirements
Clause/Article Reference:	19
Requirement:	To ensure interoperability of the components of the repositories system, technical specifications, based on non-proprietary open standards, should be established for the exchange of data between the primary repositories, the secondary repository, and the routing system.
Evaluation and Documents Reviewed: Technical specifications, based on non-proprietary open standards have been established for the exchange of data between the Primary Repositories, the secondary repository, and the router. A document detailing the list of specifications required to allow the data exchanges with the secondary repository is available. The document covers definitions, system overview, processes descriptions, interfaces, unique identifies, router and messages validation. Moreover, it was confirmed during the walkthrough that all communication between external parties and interfaces and between interfaces is secured using a non-proprietary open protocol.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	General Requirements
Clause/Article Reference:	Recital 24
Requirement:	The protection of personal data processed in the context of a traceability system should be ensured in accordance with Directive 95/46/EC of the European Parliament and of the Council (5).
Evaluation and Documents Reviewed: Dentsu is the data processor, not the data controller. An amendment to the Concession Contract has been provided to confirm the roles and responsibilities as per the General Data Protection Regulation (EU) 2016/679. Our audit confirms that Dentsu have implemented the applicable organisational and technical measures as it relates to the secondary repository and router. The organisational and technical measures can be found in Section 2.2.3 Task 2: Data Security Audit – ISO 27001 Specific Requirements of this report.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	General Requirements
Clause/Article Reference:	25
Requirement:	Recourse to international standards should be possible for the purposes of demonstrating fulfilment of certain technical requirements laid down in this Regulation. Where it is not possible to prove compliance with international standards, it should be the responsibility of the persons to whom the obligations are imposed to prove, by verifiable means, that they comply with those requirements.
Evaluation and Documents Reviewed: Dentsu hold a valid ISO 27001 certificate dated 03 March 2020 for Operations Support over IT Infrastructure.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	25.1. a
Requirement:	It shall allow for functional integration of the repositories system into the traceability system, as well as uninterrupted electronic data exchange between the repositories system and other relevant components of the traceability system.
Evaluation and Documents Reviewed: Functional integration of the repositories system into the traceability system, as well as uninterrupted electronic data exchange between the repository system are in place. A walkthrough of the flow of data was observed and is supported by evidence from the Architecture Diagram. The flow of data starts initially with the economic operators (EOs) and Service Providers who request UI codes to the ID issuer which are then delivered to the EOS and Service Providers as well as the router. The Router routes the codes to the secondary repository (if the EO is a distributor or wholesaler) as well as information such as product movements. If the EO is a manufacturer or importer, information will be sent directly to the primary repository with a copy being sent instantaneously to the secondary repository. The secondary repository contains a copy of all the data of all the messages sent by the primary repository and router. The European Commission and	

Member States can access the secondary repository information via the Secondary Repository Portal.
Findings Noted: *N/A*
Observations Noted: *N/A*

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	25.1. b
Requirement:	It shall allow for electronic identification and authentication of tobacco products, at unit packet and aggregation level, in accordance with the requirements set out in this Regulation.
Evaluation and Documents Reviewed: The electronic identification and authentication of tobacco products, at unit packet and aggregation level takes place. A walkthrough observed confirmed that once UIs have been issued by the ID issuer, the ID issuer then reports a list of UIs to the Router which performs a number of validation checks prior to sending the data to the Primary Repository e.g., the Router validates the aggregation of palettes from different manufacturers prior to sending the information to Primary Repositories and then the Secondary Repository. If checks fail, the transmission will not take place and an error code generated.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	25.1. c
Requirement:	It shall allow for automatic deactivation of unique identifiers in accordance with the rules set out in Article 5.
Evaluation and Documents Reviewed: The audit team confirmed that that automatic deactivation of unique identifiers (UIs) takes place. Discussions during the walkthrough confirmed that requests for unique identifier (UI) deactivations are reported by economic operators directly to the primary repositories for manufacturers and importers and through the router for distributors and wholesalers. The information is automatically routed to the primary repository and then reflected within the secondary repository. It should be noted that the secondary repository will deactivate any UI code generated but not applied to unit packets within 6 months from the date of receipt, and that those deactivations are automatic and not dependent on or require reporting by economic operators.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	25.1. d
Requirement:	It shall ensure electronic receipt and storing of information recorded and sent to the repositories system by economic operators and ID issuers, in accordance with the requirements of this Regulation.
Evaluation and Documents Reviewed: This requirement has been tested during the three controls noted below (25.1.e, 25.1.f and 25.1.g).	

Findings Noted: *N/A*
Observations Noted: *N/A*

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	25.1. e
Requirement:	It shall ensure storage of data for a minimum period of five years as of the moment the data are uploaded into the repositories system.
Evaluation and Documents Reviewed: Through the walkthrough the audit team was able to confirm that data and audit data (described in 25.1.m below) is stored within the database for five years which meets the availability requirements set out by the European Commission. It was also confirmed that Dentsu has a data retention policy, which includes the retention periods, data owners and locations of data storage.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	25.1. f
Requirement:	It shall allow for automatic status messaging to economic operators, and to Member States and the Commission as requested, such as in the event of success, error or changes related to reporting activities, in accordance with the requirements of this Regulation.
Evaluation and Documents Reviewed: Automatic status messaging to economic operators, Member States and the European Commission are in place. Screenshot and descriptive evidence provide timestamped examples of a positive acknowledgement and an example of a negative acknowledgement being sent from the traceability system to an economic operator.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	25.1. g
Requirement:	It shall allow for automatic validation of messages received from economic operators, including refusal of incorrect or incomplete messages, in particular reporting activities related to non-registered or duplicated unique identifiers, whereby the repositories system shall store the information concerning any refused message.
Evaluation and Documents Reviewed: It was observed and confirmed during the walkthrough that if a message contains incorrect information, the full message will be rejected/refused and the error message will indicate the specific component that caused the rejection. Furthermore, if a unique identifier (UI) is a duplicate, it will automatically be rejected.	
Findings Noted: *N/A*	

Observations Noted: *N/A*

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	25.1. h
Requirement:	It shall ensure messaging between all of its components which shall take place instantaneously, in accordance with the requirements of this Regulation, in particular the overall response time of the repositories system in sending acknowledgment messages, not considering the speed of the internet connection of the end user, which shall be no more than 60 seconds.
Evaluation and Documents Reviewed: Messaging between all components takes place instantaneously, in particular the overall response time of the repository system in sending acknowledgement messages are no longer than 60 seconds. It was confirmed during the walkthrough that DataDog is utilised to monitor Key Performance Indicators (KPIs) agreed with by the European Commission for performance and technical KPIs on the secondary repository and router. DataDog monitors metrics such as: • the number of messages in a specific time period • secondary repository API and router API success rates • number of error 500 messages in relation to all messages sent and the latency of the secondary repository and router • the number of positive and negative acknowledgements measured on the router and secondary repository are also monitored using DataDog. The audit team obtained and reviewed a sample of service level/availability reports and confirmed that the overall response time of the repositories system in sending acknowledgement messages were no more than 60 seconds.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	25.1. i
Requirement:	It shall ensure continuous availability of all components and services with a monthly uptime of at least 99,5 % and sufficient back-up mechanisms in place.
Evaluation and Documents Reviewed: The repository components and services meet a monthly uptime of at least 99.5%. Monthly SLA reports were reviewed from July 2019 to August 2021 and confirmed that the monthly uptime did not drop below 99.5% during this period. However, clerical errors in the information within the reports were noted as part of the testing for Article 3.9 of the Concession Contract SANTE/2018/B2/063, of which Dentsu and the European Commission were already aware.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	25.1. j
Requirement:	It shall be guarded by security procedures and systems ensuring that access to the repositories and download of the data stored therein is only granted to persons authorised according to this Regulation.
Evaluation and Documents Reviewed: Security procedures are in place for the access to repositories and to download of data stored within. A walkthrough of the user access process to assign or revoke access rights was observed. The user access process begins during the Starters process, which is tracked using the service request system, and users are assigned access levels based on their job role. Permissions are assigned within the user management section of the Secondary Repository Portal by Dentsu Administrators, who are the only personnel with modification privileges for these permissions. National Administrators are able to create standard users within their respective countries, but they are not able to create or modify users with administrative rights. Revoking user access follows the same process, starting with a Leavers process, user access is removed by Dentsu Administrators. Therefore, access to the repositories and the download of data is granted to specific personnel.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	25.1. k
Requirement:	It shall be accessible by the competent authorities of Member States and by the Commission. National administrators designated by the Member States and Commission services shall be granted access rights enabling them to create, manage, and withdraw user access rights for repositories, and related operations stipulated in this Chapter, via a graphical user management interface. [X1Modes of accessing the graphical user management interface shall be compatible with Regulation (EU) No910/2014, in particular the relevant reusable solutions provided as building blocks under the telecommunication part of the Connecting Europe Facility.] National administrators designated by the Member States shall be able to grant subsequent access rights to other users under their responsibility.
Evaluation and Documents Reviewed: National Administrators designated by the Member States and Commission services have been granted access rights enabling them to create, manage and withdraw user access rights for repositories via a graphical user management interface. This was confirmed during a walkthrough of the Secondary Repository Portal. Permissions and changes must be agreed with by the European Commission and the agreed changes/modifications will be conducted by Dentsu Administrators and not National Administrators themselves, as they are restricted to creating standard users and users within their respective countries	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	25.1. l
Requirement:	It shall enable Member States and the Commission to carry out downloads of full and selected sets of data stored in a repository.
Evaluation and Documents Reviewed: Member States and the Commission are able to download full and selected sets of data stored in a repository system from the Secondary Repository Portal.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	25.1. m
Requirement:	It shall maintain a complete record ('audit trail') of all operations concerning the stored data of the users performing those operations and of the nature of these operations, including the history of users' access. The audit trail shall be created when the data is uploaded for the first time and, notwithstanding any additional national requirements, be maintained until at least five years after.
Evaluation and Documents Reviewed: Although a traditional Security Information and Event Management (SIEM) is not utilised, Dentsu uses a centralised log monitoring tool via the cloud-based infrastructure. Four categories of audit logs are collected: • business audit logs (creation/update/deletion of users within the secondary repository, user access to platform and operations performed when accessing data) • external systems audit logs (logs of all messages, valid or invalid, well-formed, or mal formed received by external systems e.g., primary repository providers, economic operators, service providers or ID issuers) • technical application logs (logs generated by the applications developed by Dentsu) • technical audit logs (logs generated by the infrastructure team to monitor any changes generated, security incidents etc.) Although manual audit log reviews are not regularly performed, the tools perform automatic monitoring which was observed during a walkthrough. A walkthrough of the tool being utilised was observed and discussions with Dentsu confirmed that the tool had preconfigured alerts for specific events. Data within the log monitoring solution will be retained for the entire period of the Concession Contract and as required by the relevant legislation (5 years).	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System - 27.1
Clause/Article Reference:	27.1
Requirement:	A single secondary repository containing a copy of all data stored in primary repositories shall be established. The operator of the secondary repository shall be appointed from among the providers of primary repositories in accordance with the procedure laid down in Annex I, Part B.
Evaluation and Documents Reviewed: A single secondary repository containing a copy of stored data in primary repositories has been established. The architecture diagram evidence provided shows the flow of data from the primary repositories to the secondary repository with a description stipulating that the secondary repository contains a copy of the data of all the messages pushed by the Primary Repositories and Router. Moreover, a walkthrough of the secondary repository was observed which confirmed that the secondary repository obtained data from the primary repositories and stores a copy of the data when required, with the router also directly accessing the secondary repository to store messages when needed.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	27.2. a
Requirement:	The secondary repository shall provide for graphical and non-graphical user interfaces that enable Member States and the Commission to access and query the data stored in the repositories system, using all commonly available database search functions, in particular by remotely carrying out the following operations: a retrieval of any information concerning one or multiple unique identifier(s), including the comparison and cross-checking of multiple unique identifiers and the related information, in particular their location in the supply chain.
Evaluation and Documents Reviewed: The secondary repository provides graphical and non-graphical interfaces that enable Member States and the European Commission to access and query data stored in the repository system. It was confirmed during the walkthrough that a number of interfaces are used for the communication between each of the components of the system. Two interfaces are in place for authorities - one that allows authorities to integrate external applications and one which provides both a standard graphical user interface and an advanced user interface to query information from the secondary repository. Moreover, a walkthrough of the information retrieval process for UIs from within the traceability system was performed by Dentsu. When a UI is queried within the system, the version of the UI generated by the ID issuer, along with the timestamp present when the UI was activated is detailed. Furthermore, additional information such as the date created, ID issuer, intended market and last known location is also present within the system.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	27.2. b
Requirement:	Creation of lists and statistics, such as product stocks and inflow/outflow numbers associated with one or multiple elements of reporting information listed as Data Fields in Annex II.
Evaluation and Documents Reviewed: The system is able to generate reporting information in line with the requirements. We confirmed this through discussions with Member State representatives and also observing aggregated data that showed the movement of UK and destination. A walkthrough also observed that the Secondary Repository Portal allowed the European Commission and Member States to view and query stored data. The evidence provided shows a list of current reports generated by the Secondary Repository Portal e.g., authorities can visualise the full history of a certain unique identifier (UI). *It should be noted that statistics relating to product stocks are not currently available but will be available from the 01 March 2022.*	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	27.2. c
Requirement:	Identification of all tobacco products that have been reported by an economic operator to the system, including the products reported as recalled, withdrawn, stolen, missing, or intended for destruction.
Evaluation and Documents Reviewed: Through discussions with users of the interface system, the audit team confirmed that they are able to access the information on tobacco products. A walkthrough observed that the Secondary Repository Portal allowed the European Commission and Member States to view and query stored data. The evidence provided shows a list of current reports generated by the Secondary Repository Portal e.g., authorities can visualise the full history of a certain unique identifier (UI). An example screenshot showing the output for UI summary data has also been provided. It was also confirmed that Dentsu had made changes to the system to extend its ability to provide further historic data that would enable statistical and trend analyses. It was also confirmed through a review of documentation and walkthroughs of the validation process codes, such as for recalls are generated.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	27.3. a
Requirement:	The user interfaces referred to in paragraph 2 shall enable each Member State and the Commission to define individual rules for: an automatic alerting based on exceptions and specific reporting events, such as abrupt fluctuations or irregularities in trade, attempts to introduce duplicate unique identifiers into the system, deactivation of the identifiers referred to in Articles 15(4), 17(4) and19(4), or where a product is indicated by economic operators as stolen or missing.

Evaluation and Documents Reviewed: Member States receive automatic alerting via email for events such as irregularities in trade, attempts to introduce duplicate identifiers and deactivations of the identifiers. An email to and from the Member State, Belgium, confirmed that it was made aware of data processing issues.
Findings Noted: *N/A*
Observations Noted: *N/A*

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	27.3. b
Requirement:	The receipt of periodic reports based on any combination of the elements of reporting information listed as Data Field in Annex II.
Evaluation and Documents Reviewed: Periodic reports have been provided to the European Commission by Dentsu. Monthly service reports for August 2019, January 2020 and February 2021 have been sent by Dentsu to the European Commission.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	27.7
Requirement:	The overall response time of the repository to any given query or alert trigger, not considering the speed of the internet connection of the end user, shall be no more than 5 seconds for the data stored for less than 2 years and no more than 10 seconds for the data stored for 2 years or more, in at least 99 % of all queries and automatic alerts foreseen under paragraphs 2 and 3.
Evaluation and Documents Reviewed: The overall response time of the repository system to any given query or alert trigger is no more than 5 seconds for data stored for less than 2 years. As the contract has been operating for 2 years, no statistics are available for data stored over 2 years. A walkthrough of DataDog was observed and all metrics were found to have latency of processing averaging under 1 second, meaning that the response times are within the requirements set by the European Commission.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	27.8
Requirement:	The overall time between the arrival of reporting activity data and its accessibility, via the graphical and non-graphical interfaces, in the primary and secondary repositories shall be no more than 60 seconds in at least 99 % of all data transfer activities.

Evaluation and Documents Reviewed: The audit team confirmed that, that the overall time between the arrival of reporting activity data and its accessibility, via the graphical and non-graphical interfaces, in the primary and secondary repositories are no more than 60 seconds in at least 99.5% of all data transfer activities. This was observed during the walkthrough when reporting activity data was retrieved/downloaded from the Secondary Repository Portal.
Findings Noted: *N/A*
Observations Noted: *N/A*

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	27.10
Requirement:	The provider of the secondary repository shall establish and maintain a register of the information transferred to it in accordance with Article 20(3). A record of the information stored in the register shall be kept for as long as the traceability system is operational. The repository shall allow for the receipt, storing and making available of offline flat files for the purpose of updating verification devices used by Member States for offline decoding of unique identifiers. [Art 20(3): ID issuers shall ensure that an up-to-date copy of all offline flat-files, registries and related explanatory notes are electronically provided via the router to the secondary repository]
Evaluation and Documents Reviewed: The audit team confirmed that that a register of information has been established and maintained. A walkthrough confirmed that there is a register of information in place that has been retained throughout the duration of the contract. A cloud-based message storage solution stores all messages received by the router and allows ID issuers to download information from offline flat files without accessing the repository prefix system. The flat files contain data in a plain text format which allows for the extraction of information encoded in the UI used at the unit packet and aggregated packaging levels	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	28.1
Requirement:	The provider operating the secondary repository shall communicate to providers operating primary repositories, ID issuers and economic operators, the list of specifications required for the data exchange with the secondary repository and the router. All specifications shall be based on non-proprietary open standards.
Evaluation and Documents Reviewed: Communications between Dentsu and the primary repository providers and other stakeholders are completed via the ticketing system. The list of specifications and data dictionary is also available publicly and via the Dentsu portal.	

It has been noted that is the responsibility of the primary repository providers to ensure compliance to the Data Dictionary and List of Specifications, according to Article 26(5) of the Implementing Regulation.
Findings Noted: *N/A*
Observations Noted: *N/A*

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	28.2
Requirement:	On the basis of the information listed in Annex II, the provider operating the secondary repository shall establish a common data dictionary. The common data dictionary shall refer to labels of data fields in the human readable format. The common data dictionary shall be communicated to the providers operating primary repositories no later than two months following the date when the provider operating the secondary repository was selected.
Evaluation and Documents Reviewed: A common data dictionary has been established which refers to labels of data fields in human readable formats. The audit team confirmed that the data dictionary is communicated to the providers operating the primary repositories no later than two months following the date when the provider operating the secondary repository was selected.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	28.3
Requirement:	Whenever necessary to ensure the effective operation of the repositories system in accordance with the requirements of this Regulation, the provider operating the secondary repository shall update the list referred to in paragraph 1 and the common data dictionary referred to in paragraph 2. Any such update shall be communicated to the providers operating primary repositories at least two months prior to the date of implementing the update into the system.
Evaluation and Documents Reviewed: The latest version of the Data Dictionary (version 1.4.4) and List of Specifications (version 1.4.4) was communicated to stakeholders two months before being implemented within the system. Consultations with primary repository providers and economic operators were held prior to Dentsu publishing the final versions. Notifications were also sent out prior to the final implementation.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	29.1
Requirement:	The provider of the secondary repository shall set up and manage a router.

Evaluation and Documents Reviewed: Dentsu has set up and is managing a router which is hosted within a third-party hosted data centre. The architecture diagram shows evidence of a router within the system architecture and provides a description of its function.
Findings Noted: *N/A*
Observations Noted: *N/A*

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	29.2
Requirement:	Data exchange between the router and the primary and secondary repositories shall take place using the data format and data exchange modalities defined by the router.
Evaluation and Documents Reviewed: Data exchange between the router and primary and secondary repositories takes place using the data format and data exchange modalities defined by the Router. This was confirmed during a walkthrough of the data exchange between the router and primary/secondary repositories. The router performs a number of validations and checks prior to sending the data to the Primary Repository. If checks fail, the data is not sent, and a list of status messages has also been provided which details a number of error codes. For example, 'MIN_LENGTH_FAILED_VALIDATION' which occurs when the number of characters is not above the minimum length which is required as per the specifications defined in the Data Dictionary.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Repositories System
Clause/Article Reference:	29.4
Requirement:	Economic operators other than manufacturers and importers shall send the information recorded pursuant to Article 15 of Directive 2014/40/EU and in accordance with this Regulation to the router, which shall transfer it to the primary repository serving the manufacturer or importer whose tobacco products are concerned. A copy of those data shall be transferred instantaneously to the secondary repository system.
Evaluation and Documents Reviewed: Controls are in place to ensure that information/messages transferred by the Router are being sent to the correct primary repositories. It was confirmed during a walkthrough that routing tables are utilised to ensure that the Router is sending messages to the correct primary repository. Messages are split by the Router to ensure messages were sent to the appropriate primary repository using routing tables provided by the primary repositories, this is achieved using multiple Lambdas, a server less computing platform used to run various functions of the router.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Costs of the repositories system
Clause/Article Reference:	30.1
Requirement:	All costs related to the repositories system referred to in Article 24(1), including those that arise from its establishment, operation, and maintenance, shall be borne by manufacturers and importers of tobacco products. Those costs shall be fair, reasonable, and proportionate: a) to the services rendered; and b) to the amount of unit level UIs requested over a given period of time
Evaluation and Documents Reviewed: Invoices raised for the agreed primary repository providers are in line with the regulatory requirements. Through review of a sample of invoices, the audit team confirmed that they included a breakdown of the volume of requests by each site and manufacturer in the invoice narratives. The amount charged per invoice was also directly proportionate with the volume of UIs requested over a given period - at a rate of 1.4844 EUR per 10,000 UI requests, which is in line with the contractual requirements. This charging mechanism was also clearly outlined within the invoices for transparency.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Costs of the repositories system
Clause/Article Reference:	30.2
Requirement:	The costs, as applicable, of establishing, operating, and maintaining the secondary repository and the router shall be transmitted to manufacturers and importers of tobacco products through the costs charged to them by the providers of the primary repositories.
Evaluation and Documents Reviewed: The costs relating to the repository system had been passed to the primary repository providers through a review of sampled invoices. The European Commission and Dentsu also confirmed that there have been no additional services agreed that will fall within the scope of this audit.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Independence
Clause/Article Reference:	35.1
Requirement:	ID issuers, providers of repository services and anti-tampering devices as well as, where applicable, their subcontractors shall be independent and exercise their functions impartially.
Evaluation and Documents Reviewed: A process is in place that is followed for the vetting and conflict of interest checks for staff, which are also required to periodically sign a declaration to confirm the absence of any conflicts of interest and their compliance with the specific requirements imposed on them by Article 35 of CIR 2018/574. The audit team confirmed that subcontractors are required to demonstrate legal and financial independence. This is evidenced through a declaration as well as the completion of a supplier questionnaire.	

Findings Noted: *N/A*
Observations Noted: *N/A*

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Independence
Clause/Article Reference:	35.3
Requirement:	Where ID issuers, providers of repository services and providers of anti-tampering devices have recourse to sub-contractors, they shall remain responsible for ensuring compliance by those subcontractors with the independence criteria set out in paragraph 2.
Evaluation and Documents Reviewed: Controls are in place to help ensure subcontractors are compliant to independence terms. Evidence was reviewed that showed subcontractors were required to demonstrate legal and financial independence, through a declaration as well as the completion of a supplier questionnaire.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Final Provisions
Clause/Article Reference:	36.1
Requirement:	All electronic communication provided for under this Regulation shall be carried out using secure means. Applicable security protocols and connectivity rules shall be based on non-proprietary open standards. They shall be established by: a) the ID issuer for communications between the ID issuer and the economic operators registering with the ID issuer or requesting unique identifiers. b) the providers of the primary repositories for communications between the primary repositories and manufactures or importers. c) the provider of the secondary repository for communications between the secondary repository and the router and: i.the ID issuers. ii.the primary repositories; and iii.economic operators using the router, i.e., economic operators other than manufacturers and importers.
Evaluation and Documents Reviewed: All electronic communications provided for under this regulation is carried out using secure means. It was observed during a walkthrough that communication between external parties and interfaces and between interfaces is secured using a non-proprietary open protocol.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Final Provisions
Clause/Article Reference:	36.2
Requirement:	Providers of primary and secondary repositories shall be responsible for the security and integrity of hosted data. Data portability shall be secured in accordance with the common data dictionary set out in Article 28.
Evaluation and Documents Reviewed: The provider of the secondary repository, Dentsu, is responsible for the security and integrity of hosted data. Data portability is also secured. It was discussed during the walkthrough that controls regarding the security and integrity of hosted data are in place. Cloud-based infrastructure is being utilised as the provider to deliver Dentsu's solution in relation to the secondary repository, router, and Apps. The data is encrypted and access to data is limited to certain personnel/job roles who require approval prior to any additional access being granted. MFA is also being utilised as a further security control. Furthermore, an observation of reports being accessed was observed during the walkthrough. Reports were also limited to specific personnel and secured using the cloud-based infrastructure's encryption mechanisms.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Final Provisions
Clause/Article Reference:	36.3
Requirement:	For all transfers of data, the sending party is responsible for the completeness of transferred data. In order for the sending party to discharge this obligation, the receiving party shall acknowledge the receipt of transferred data including a checksum value of actual transmitted data or any alternative mechanism allowing for validating the integrity of transmission, in particular its completeness.
Evaluation and Documents Reviewed: The audit team confirmed that that the receipt of transferred data includes a checksum value. A walkthrough of the checksums was performed by Dentsu and was observed by the audit team. It was confirmed that the repository system verifies the message checksum to ensure that data was not tampered with between parts of the repository system, any messages where the hash is not valid are not accepted. This process ensures that messages making up traffic cannot be altered in transit or within parts of the repository system, nor can they be removed from the sequence without detection. MD5 hash are generated and compared, if there is no match, an invalid signature will return.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	ANNEX I Part B (4)
Requirement:	Each primary repository provider appointed in accordance with Part A shall enter into an individual contract with the provider appointed to operate the secondary repository for the purpose of carrying out the services specified in Chapter V of this Regulation
Evaluation and Documents Reviewed: Individual primary repository agreements that have been entered with Dentsu and that these agreements were based on a contract template drafted by Dentsu to help ensure the Commission Implementing Regulation (EU) 2018/574 requirements were covered. The agreements include a	

clear charging mechanism of 1.4844 Euros per 10,000 UIs processed, monthly SLAs to monitor the continuous availability of services and uptime, overall response times to queries and data storage and back up mechanisms. They also include provisions covering change control, dispute resolution, issue escalation and insurance requirements.
Findings Noted: *N/A*
Observations Noted: *N/A*

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	ANNEX I Part C (3)
Requirement:	Where the finding referred to in paragraph 1 applies to the provider who has been appointed to operate the secondary repository, the contracts for the operation of the secondary repository entered into pursuant to paragraph 4 of Part B shall, in turn, be terminated by the parties. [Part C(1): 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 the failure to comply with the criteria for independence laid down in Article 35, 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. The appointment of the replacement provider shall take place in accordance with paragraphs 2 to 7 of Part A]
Evaluation and Documents Reviewed: Dentsu considers that the contingency and mitigations in these circumstances are covered within the Exit Strategy. In line with Clause 17.1 of the Concession Contract SANTE/2018/B2/063, this should be submitted to the European Commission within 30 days of the approval – which has not yet been provided - of the resulting and non-resulting information.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	COMMISSION IMPLEMENTING REGULATION (EU) 2018/ 574
Sub-Category:	Annex II
Requirement:	The messages required for regulatory purposes shall contain at least the data fields listed in this Annex. Both ID issuers and providers of data repositories (including the router) may decide to extend the message content for strictly technical purposes to secure smooth functioning of the tobacco products traceability system. The messages listed in this Annex do not include the messages to be sent back by ID issuers and providers of data repositories (including the router) to the economic operators, such as acknowledgments of receipt. All the messages generated within the tobacco traceability system shall contain the identification of the originator and a timestamp up to the second (see Data Type: Time(L)). ID

	issuers and providers of data repositories (including the router) shall timestamp each received message up to the second.
Evaluation and Documents Reviewed: Messages within the tobacco traceability system contain the identification of the originator and a timestamp up to the second. Information received from the walkthrough confirms that messages provided by the Router contain identification of the originator and timestamp precision in milliseconds.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	DIRECTIVE 2014/40/EU
Sub-Category:	Traceability
Clause/Article Reference:	15.8
Requirement:	The repository system is exclusively located on the territory of the Union.
Evaluation and Documents Reviewed: The repository system is exclusively located on the territory of the Union. Descriptions of the secondary repository and Router within the architecture diagram document confirm that the secondary repository and router are hosted in Ireland.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Legislation/Contract Requirement:	DIRECTIVE 2014/40/EU
Sub-Category:	Traceability
Clause/Article Reference:	15.8
Requirement:	Access shall be limited to competent authorities of Member States, the Commission and approved external Art. 15(8) of Directive 2014/40/EU; Art. 25(1)(j) of Implementing Regulation (EU) 2018/574 auditors
Evaluation and Documents Reviewed: The system users are provided access to the network and network services that they have been specifically authorised to use. It was confirmed during the walkthrough that access to both the back end and physical data centres for the cloud-based service provider is restricted to Dentsu administrators. Moreover, the list of users provided stipulates that there are 5 Dentsu Administrators with admin access, these include 1 management personnel, 1 Dev Ops personnel, 2 Operations Management personnel and 1 Security Personnel.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

2.2.3. Task 2: Data Security Audit – ISO 27001 Specific Requirements

[redacted]

ISO Domain Requirement:	Organisational and physical security
ISO Sub-Categories	A.6, A.7 and A.11

Evaluation and Documents Reviewed:

A.6 - Organisation of Information Security

[redacted]

A.7 – Human Resources Security

[redacted]

A.11- Physical and Environmental Security

[redacted]

[redacted]

Findings Noted:
N/A

Observations Noted:
N/A

ISO Domain Requirement:	Operations security
ISO Sub-Categories	A.12

Evaluation and Documents Reviewed:
A.12 – Operations Security

[redacted]

Findings Noted:
N/A

Observations Noted:

N/A

ISO Domain Requirement:	Access Control
ISO Sub-Categories	A.9, A.14
Control Checkpoint Objective:	Data / Technical specifications
Requirement:	Change Management controls (including system changes such as outages and maintenance activities), such as: • Impact analysis • Dependency analysis • Communication of changes Changes to data dictionaries and specifications are assessed against the impact on validation controls

Evaluation and Documents Reviewed:
A.9 – Access Control

[redacted]

A.14 - System acquisition, development, and maintenance

[redacted]

[redacted]

Findings Noted:
N/A

Observations Noted:
N/A

ISO Domain Requirement:	Communications Security
ISO Sub-Categories	A.10, A.13, A.15

Evaluation and Documents Reviewed:

A.10 – Cryptography

[redacted]

A.13 – Communications Security

[redacted]

A.15 – Supplier Relationships

[redacted]

Findings Noted:
N/A

Observations Noted:
N/A

ISO Domain Requirement:	Business Continuity
ISO Sub-Categories	A.16, A.17, A.18

Evaluation and Documents Reviewed:

A.16 – Information security incident management

[redacted]

A.17 – Information security aspects of business continuity management

[redacted]

A.18 Compliance

[redacted]

[redacted]

Findings Noted:
Clerical errors meant that the performance during Aug – Sept 2019, Oct – Nov 2019 and Feb – Mar 2021 had not been correctly updated in the reports.

Observations Noted:
N/A

ISO Domain Requirement:	Asset and Data Integrity
ISO Sub-Categories	A.8

Evaluation and Documents Reviewed:
A.8 – Asset Management

[redacted]

Findings Noted:
N/A

Observations Noted:

- While the organisation has implemented Bitlocker to Go, it is not mandatory to encrypt on removable media, but optional based on the user. We recommend that Dentsu either block the use of removable media or mandate that these be encrypted before transferring any data.

2.2.4. Control Checkpoints

As per the audit requirements, BDO has defined a set of control checkpoints that have been evaluated in addition to the requirements stated within the concession contract and various legislation. Where checkpoints were tested as part of previously mentioned controls and requirements (i.e., ISO), they will be documented under those controls.

Control Checkpoint Objective:	Reporting and Information
Requirement:	• Identification and tracking of high-risk activities. • Reports and information are provided to the relevant entities with the sufficient level of detail and are reviewed for accuracy and completeness against the outcomes from the validation controls.
Evaluation and Documents Reviewed: A Risk Register in place to monitor risks and document mitigating actions. Criticality of risks are shown on the Risk Register and the shifting of risk positions across versions demonstrate actions being closed out. We also observed the Dentsu Tracking Risk Management Process document, last updated on 08 July 2021 as part of an annual review, and saw that it contains guidelines on risk identification, category, evaluation, monitoring, review, and reporting. We also observed evidence of actions coming out of the September 2021 Steerco committee relating to the Risk Register update. The audit team confirmed that that the secondary repository provides graphical and non-graphical interfaces that enable Member States and the European Commission to access and query data stored in the repository system. It was confirmed during the walkthrough that interfaces are used for the communication between each of the components of the system. Moreover, a walkthrough of the information retrieval process for UIs from within the traceability system was performed by Dentsu. Further details on reporting can be found under the tests of Article 27(2)a-c. of the Commission Implementing Regulation (EU) 2018/574. In terms of reporting accuracy, a review of Clause 3.9 of the Concession contract SANTE/2018/B2/063 saw clerical errors relating to the update of SLA and performance reports. This was a known error, which was then corrected as a result of the audit. The European Commission confirmed that, due to the size of the error, the impact was not deemed significant or material. For further details of the validation controls review, please see the Control Checkpoint Objective: Validation Controls.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Control Checkpoint Objective:	Notification
Requirement:	Notifications and escalations relating to validation issues exists.
Evaluation and Documents Reviewed: There are notification and escalation processes in place for issue management. The RACI matrix provided by Dentsu outlined the expectation for stakeholder communication for operational and governance activities. Minutes from the European Commission steering committee and status meetings showed actions being allocated to action owners. Dentsu also confirmed that actions on its side that require development or investigation are linked to User Stories or DevOps internally, whilst simple actions such as providing documentation will be carried out by the team within a few days. In terms of issue resolution and complaints handling, the audit team confirmed that that it has reviewed the complaints handling process provided and that it demonstrates how complaints are collected and managed by the operational teams depending on priority and that an escalation process for unresolved incidents is shown. The process also covers how resolutions are communicated and how feedback is sought from the actor / customer who opened in the incident. Dentsu also confirmed that incidents and complaints reported by stakeholders are recorded and managed in the ticketing system; the support portal provides several KPIs and metrics to ensure operational level agreement monitoring.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Control Checkpoint Objective:	Contracting with Primary Repository Operators
Requirement:	Contracts are in place and approvals obtained, in line with timelines per the Regulation, and responsibilities for validations, issues resolutions, scope and obligations are clearly laid out.
Evaluation and Documents Reviewed: Individual primary repository agreements include SLAs to monitor the continuous availability of services and uptime, overall response times to queries and data storage and back up mechanisms. They also include provisions covering change control, dispute resolution, issue escalation and insurance requirements.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Control Checkpoint Objective:	Validation Controls
Requirement:	Collation (including categorisation and prioritisation) of messages and errors or issues, as well as procedures to establish, review, and monitor the validations, e.g., those relating, but not limited to: a) Sequencing and time stamps b) UID duplication c) Multiple activation requests d) Messages affected by planned / unplanned maintenance works / service availability e) Use and allocation of recall codes f) Aggregation errors g) Messages effected by outages / maintenance works h) Missing information (e.g., supplier addresses) i) Mismatched UIDs, facilities and locations

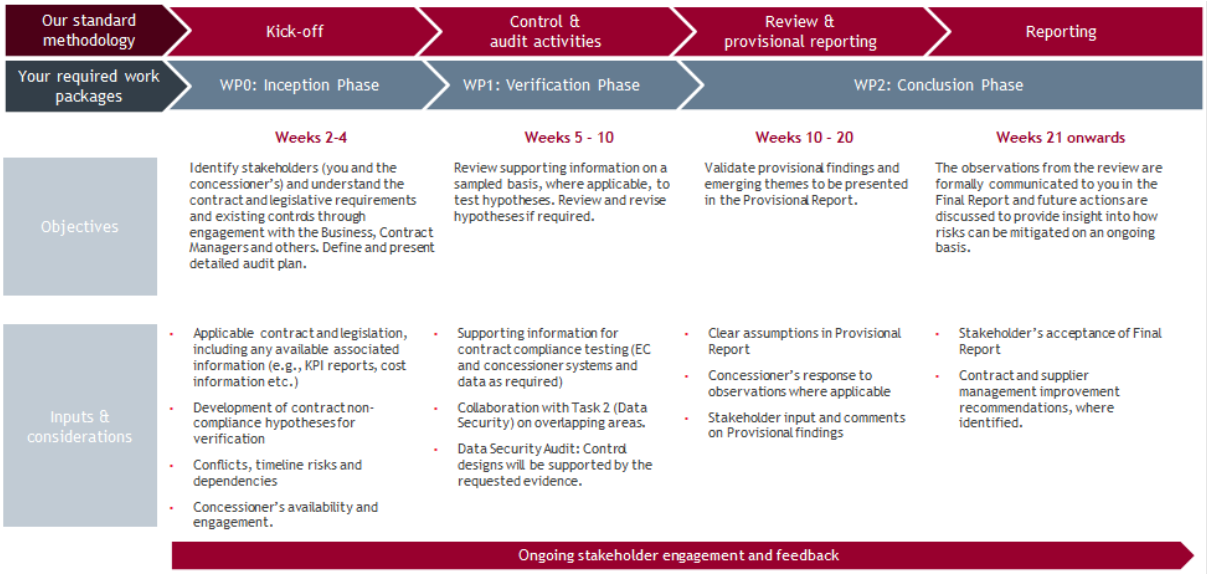
	j) Restoration of messages (e.g., when required, how these messages are identified and restored) k) Volume of messages (e.g., capacity in processing these) l) Deactivated products
Evaluation and Documents Reviewed: Through a review of documentation and walkthroughs, the audit team noted that validation on controls is in place e.g., error codes or recall codes. Validation controls are defined by the European Commission and validated by Dentsu prior to implementation. There are numerous checks to ensure validation controls are working correctly, for example, there are validation checks at both the router and secondary repository which are monitored by DataDog and rejected messages can be viewed through DataDog. Changes will be reported by the European Commission during the weekly meetings, otherwise, no changes will be made. Further there are logging and alerting systems in place to ensure that changes made to the system are recorded and monitored.	
Findings Noted: *N/A*	
Observations Noted: *N/A*	

Appendices

Appendix 1: Engagement Approach

Our approach recognises the challenging environment of managing the illicit trade of tobacco products within the EU and covers the unlawful movement of tobacco products from one jurisdiction to another, without applicable tax being paid. The illicit trade has resulted in the EU losing around €10 billion of public revenue every year. This has resulted in the EU adopting several regulations and implementation of the tobacco traceability system to be used by Member states.

To ensure that we work as efficiently as possible, the team will perform the two tasks as requested by the EU Commission in parallel, namely task 1: contract and legislative compliance and task 2: data security audits. Aligning our four-phase methodology with the EU's requirements, we proposed the following high-level project plan for the overall engagement:



Task 1 Included a review of the concessioner's processes & controls and assessed the relevant supporting information pertaining to:

- Compliance to the complementary primary legislation Tobacco Products Directive 2014/40/EU and the associated secondary legislation Commission Implementing Regulation (EU) 2018/574 and Commission Delegated Regulation (EU) 2018/573
- Compliance to contractual terms surrounding the provision of the services, including
    - Service standards such as quality, operability, availability, performance, and issues resolution
    - Appropriateness of personnel performing the contract
    - Preparation and implementation of an exit strategy
    - Applicable KPIs and MI reporting per the contract
    - The concessioner's controls around the execution of its contract with the primary repository provider, including any liquidated damages and potential risks.

Task 2, which relates to the Data Security audit, assessed:

- compliance to the Guidelines on annual audit reports to be submitted in accordance with Article 15(8) of Directive 2014/40/EU in the context of the EU traceability system for tobacco products
- Contractual items identified in task 1 as items belonging to the security domain will be verified during this task
- compliance in line with ISO/IEC 27001:2013 on Information Security Management Systems.

Appendix 2: List of Stakeholders Engaged

Stakeholder Name	Role
	Directorate-General for Health and Food Safety
	Directorate-General for Health and Food Safety
	Directorate-General for Health and Food Safety
	Directorate-General for Health and Food Safety
	Directorate-General for Health and Food Safety
	Directorate-General for Health and Food Safety
	Danish Safety Technology Authority
	Polish Ministry of Finance
	Irish Office of the Revenue Commissioners
	IBM
	IBM
	Logista
	Logista
	Worldline
	Dentsu
	Dentsu
	Dentsu
	Dentsu
	Dentsu

Restrictions of use

The matters raised in this report are only those that came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. The report has been prepared solely for the management of the organisation and should not be quoted in whole or in part without our prior written consent. BDO LLP neither owes nor accepts any duty to any third party whether in contract or in tort and shall not be liable, in respect of any loss, damage or expense which is caused by their reliance on this report.

Our report is issued in connection with our engagement to provide advisory services to European Commission Any reliance placed on our report or any part thereof by a third party is at their own risk. Findings in this report related to fieldwork carried out between September and November 2021.

www.bdo.co.uk