EUROPEAN
COMMISSION

Brussels, 5.7.2024
C(2024) 4572 final

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of 5.7.2024

laying down common procedures and detailed rules for accessing and processing electronic freight transport information by competent authorities in accordance with Regulation (EU) 2020/1056 of the European Parliament and of the Council

(Text with EEA relevance)

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of 5.7.2024

laying down common procedures and detailed rules for accessing and processing electronic freight transport information by competent authorities in accordance with Regulation (EU) 2020/1056 of the European Parliament and of the Council

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2020/1056 of the European Parliament and of the Council of 15 July 2020 on electronic freight transport information[1], and in particular Article 8 thereof,

Whereas:

(1) Regulation (EU) 2020/1056 requires Member States to ensure that all their competent authorities have access to electronic freight transport information ('eFTI') in line with common procedures and detailed rules, including common technical specifications and procedures for processing regulatory information and for communicating with the economic operators in relation to that information.

(2) In order to lay down these common procedures and rules, pursuant to Article 8 of Regulation (EU) 2020/1056, the Commission should list the main information communication technology ('ICT') components of the eFTI exchange environment to be provided by the Members States and detail their functional and technical specifications.

(3) To ensure flexibility in the application of these common procedures and detailed rules, Member States should be able to decide how to organise the provision of the ICT components, provided those components comply with the respective functional and technical specifications laid down in this Implementing Regulation. More specifically, Member State may decide to set these up as separate components, or integrated in a single component or in several distinct components performing the respective functionalities. They may also set up multiple components performing the same set of functionalities.

(4) Member States should be able to reuse existing ICT components they already developed for other digital public services, insofar as these components already provide or are adjusted to provide the required functionalities in line with the specifications, including technical requirements, where applicable, set out in this Implementing Regulation. Member States should also be able to choose to establish, develop and maintain one or more of the ICT components provided for in this Regulation jointly with other Member States.

[1] OJ L 249, 31.7.2020, p. 33.

(5) Each Member State should be responsible for ensuring the maintenance and security of the ICT components that they set up or for which they are responsible, including for ensuring the security and confidentiality of the information processed within those components. If several Member States decide to set up and manage jointly some of these components, they should ensure that their respective responsibilities are laid down in appropriate agreements or memoranda of understanding.

(6) Pursuant to Regulation (EU) 2020/1056 all communication within the eFTI exchange environment is to take place by means of secure connections between duly identified and authorised parties. Therefore, the common functional and technical specifications laid down in this Implementing Regulation should ensure that such requirements are met for all communication taking place among the participants in the eFTI exchange environment by means of ICT components, including with the eFTI platforms.

(7) The number of participants in the eFTI exchange environment is expected to be high, both at the level of the competent authorities, and at the level of the economic operators concerned, who will be free to use the eFTI platforms of their choice. An adequate number of secure, authenticated and authorised connections would therefore need to be established and maintained between the ICT components of the eFTI exchange environment. To reduce the costs associated with such a high number of connections, some of the ICT components of the eFTI exchange environment to be established by the Member States should mediate this exchange by playing a gateway function, while maintaining a high level of security and compliance with applicable authorisations.

(8) Such gateways, or 'eFTI Gates' should mediate the exchange of regulatory freight transport information between the economic operators concerned and the competent authorities. The eFTI Gates should ensure secure and authenticated connections to the ICT components that mediate the access of individual officers at the level of the competent authorities in a specific Member State, on the one hand, and to the eFTI platforms that hold the data to which these officers would need to have access, on the other hand. They should not store or process eFTI data, except for metadata connected to eFTI data processing such as identifiers or operation logs, and only for legitimate purposes such as routing, format validation or adaptation and for monitoring or statistical purposes.

(9) Furthermore, to reduce the costs involved in establishing connections between eFTI platforms and an eFTI Gate, particularly for the economic operators – but also for the competent authorities, as provided for in Article 8(2) of Regulation (EU) 2020/1056 – eFTI platforms should be required to establish and maintain a secure and authenticated connection to only one eFTI Gate. That eFTI Gate should then mediate the connection to all the competent authorities in all the Member States, by means of a network of secure and authenticated connections between the different eFTI Gates.

(10) In view of the requirement in Article 11 of Regulation (EU) 2020/1056 that Member States maintain an up-to-date list of the eFTI platforms which hold a valid certification issued by a conformity assessment body accredited in their Member State, this single connection of an eFTI platform to the network of eFTI Gates should be established with the eFTI Gate of the Member State where that platform's certification was issued. This would facilitate and make less costly the process of verifying the validity of the certification of an eFTI platform, as part of the process of ensuring the security and authenticity of the communication with an eFTI platform. However, to accommodate situations where no conformity assessment bodies have been accredited to certify eFTI

platforms in a Member State, eFTI platforms should be able to establish their single connection to the eFTI Gate of that Member State, even when they obtained the certification in other Member States.

(11) To ensure a high level of trust in the eFTI exchange environment, Member States should remain responsible for ensuring that all access by their competent authorities to the eFTI exchange environment is duly identified, authenticated and authorised. Member States should ensure that accessing and processing by competent authorities of data made available by economic operators on eFTI platforms is allowed only following due identification and authentication of the identity of the responsible officers, as well as due authorisation based on assigned access and processing rights of the officers, based on their respective responsibilities in relation to the EU and national provisions falling under the scope of Regulation (EU) 2020/1056. For that purpose, Member States should ensure that all competent authorities establish and maintain registries that keep updated records of the access and processing rights of each responsible officer, and that all requests for accessing and processing eFTI data include references to the access and processing rights of the officer responsible for the request. Those access and processing rights should be expressed as coded references to minimise the transfer of the personal data of the officers, as defined by Regulation (EU) 2016/679[2]. Member States should also ensure that their competent authorities take any necessary measures, such as testing, trainings and audits, to ensure that their officers access and process data in compliance with applicable EU and national rules on data privacy and commercial confidentiality.

(12) Regulation (EU) 2020/1056 requires the economic operators concerned to communicate to the competent authorities the 'unique electronic identifying link' to the machine-readable eFTI data corresponding to the regulatory information. Procedurally, this communication should be done in two ways, and the ICT components to be set up by the Member States should support both procedures. The competent authorities should be able to choose either procedure when requesting access to eFTI data to perform regulatory information checks.

(13) Firstly, in line with current paper-based compliance check procedures, the economic operators concerned should be able to communicate directly to the competent authority the unique electronic identifying link during checks performed in physical presence, either during the transport operation or during checks performed at the premises of the economic operator, where applicable EU or national provisions provide for the possibility of checks after the completion of transport operations. To facilitate processing by the competent authorities, the unique electronic identifying link should be communicated in a machine-readable format such as a bar code or QR code, displayed on the screen of an electronic handheld device such as a mobile phone or tablet, or printed on paper. Member States' authorities should be able to decide to accept that, during physical checks of on-going transport operations, the economic operator may on an exceptional basis communicate the unique electronic identifying link by email or other electronic messaging application, in situations where the link could not be directly displayed by the operator on screen or on paper. For checks performed at the premises of the economic operators, when the number of transport

-

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, pp. 1–88)

operations to be inspected is substantially higher, competent authorities should be able to choose to receive the unique electronic identifying links via email or other electronic messaging application, to facilitate and optimise the processing of these links. The choice of these additional communication means should remain with the respective competent authorities.

(14) Secondly, and more compatible with a future where processes are increasingly automated, economic operators should communicate the unique electronic identifying link by publishing it in an electronic repository, or registry, together with certain identifiers, such as the unique identification of the means of transport, derived from the eFTI data set associated with that unique electronic identifying link. Competent authorities could then retrieve that link from the registry by running a query based on those identifiers. . This would enable competent authorities to check the information on the goods being transported on a truck, train or barge without physically stopping or boarding the means of transport and, where relevant, apply follow-up measures in accordance with national law. It would also allow competent authorities to more easily or reliably retrieve the information on multiple transport operations performed by a given means of transport, in a given time period, such as in the case of road cabotage checks, in line with the provisions of Regulation (EC) No 1072/2009 of the European Parliament and of the Council[3].

(15) To ensure the interoperability and security of the information exchange between the eFTI Gates set up by the different Member States, and between the eFTI Gates and the eFTI platforms, a set of harmonised standards and specifications for message exchange, including the configuration of message exchange agreements, business processes, data formats, identifiers and security certificates should be used within the eFTI environment. Member States should also agree on secure procedures for the exchange of the security certificates, such as by means of a custom-built system or secure file transfer protocol.

(16) To reduce the costs and the time taken to set up the eFTI Gates and the other ICT components, Member States should, to the extent possible, rely on open standards maintained by European or international organisations, and on reusable solutions. For message exchange formats, the most widely used, internationally accepted open standards are XML and JSON. While JSON is a more recent and, in certain respects, simpler to implement format, XML is the most common format used by the ICT systems of competent authorities in most Member States. Therefore, to allow Member States to re-use existing solutions and thus reduce their initial implementation costs, all communication between eFTI Gates and between eFTI Gates and eFTI platforms should be done using a single message exchange format, the XML. Similarly, the standards for secure message exchanges maintained by the Commission as part of the eDelivery digital building block[4], and in particular the eDelivery AS4 profile, provide a cost-efficient technical solution that Member States already have experience in implementing.

(17) At the same time, Member States should be able to reuse message exchange standards and solutions already in use for other digital public services for the communication between the eFTI Gate and the eFTI platforms set up in that Member State, in addition

[3] Regulation (EC) No 1072/2009 of the European Parliament and of the Council of 21 October 2009 on common rules for access to the international road haulage market (OJ L 300, 14.11.2009, p. 72).

[4] https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery.

to eDelivery. The detailed requirements and standards underlying those solutions should be made publicly available to enable their implementation by interested eFTI platforms developers, and to enable the accredited conformity assessment bodies to assess their compliance with the specifications.

(18) Similarly, to allow competent authorities' officers to make use of the ICT components that constitute the point of access, or the 'authority access points', to the eFTI environment, Member States should be able to make use of existing electronic solutions that ensure the identification and authentication of the identity of officers when accessing other national digital public services that give access to personal or commercial data of third parties. These solutions should rely, where available, on the means of electronic identification set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council[5].

(19) In the same spirit, Member States should be able to re-use any other existing components of their competent authorities' ICT systems that perform similar functions to those specified in this Implementing Regulation, such as authorisation registries, provided they are adapted in line with the specific requirements laid down in this Implementing Regulation.

(20) To make it as easy as possible for competent authority officers to use the eFTI exchange environment and to facilitate their analysis of the eFTI data made available by economic operators on an eFTI platform, Member States should be able to tailor the user application and its graphical user interface to the needs of their officers. Member States should also be able to introduce additional functionalities to be supported by the user applications, such as the use of smart algorithms that can pre-process the eFTI data, also combining information from other electronic sources, should they so wish.

(21) The continuous and smooth functioning of the eFTI environment requires that any operational issues related to the ICT components set up by the Member States be speedily resolved. To help ensure that, the Member States and the Commission should establish a network of technical support, consisting of dedicated helpdesks at national and, respectively, Union level. This network should establish clear communication procedures and ensure synchronised minimum periods of availability to enable quick reaction to any possible incidents and downtimes which may affect the functioning of the eFTI exchange environment. Those technical support contact points should have the powers and sufficient human and financial resources to enable them to carry out their tasks. Based on activity reports, helpdesks may publish aggregated information on dedicated helpdesk dashboards. The minimum periods of common availability of the helpdesks should be periodically revised, to allow adjusting their activity and efficiently allocate resources.

(22) The ICT components to be set up by the Member States will work as integral components of the wider eFTI exchange environment. That means that the establishment and maintenance of these components should rely on coordinated efforts, based on a harmonised interpretation of the specifications laid down in this Regulation. To this end, Member States should also create a network of operational support, in cooperation with the Commission, in the form of a dedicated group of

[5] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

experts. To harness the expertise and experience developed within the Digital Transport and Logistics Forum (DTLF), the expert group set up by the Commission[6] to assist in the development and implementation of the Union's activities and programmes aimed at the digitalisation of the transport and logistics sector, that group of experts should be set up as a subgroup of the DTLF.

(23) To facilitate Members States' implementation efforts and ensure uniform implementation of these specifications, it is envisaged to complement this Regulation by more detailed, non-binding technical support documents drawn up by the Commission in cooperation with the Member States within this dedicated group of experts.

(24) The measures provided for in this Implementing Regulation are in accordance with the opinion of the Digital Transport and Trade Facilitation Committee,

HAS ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Definitions

For the purpose of this Regulation, the following definitions shall apply:

(1) 'eFTI exchange environment' means the ensemble of ICT components used for the exchange of data in accordance with Regulation (EU) 2020/1056 and the implementing and delegated acts adopted pursuant to that Regulation;

(2) 'ICT component' means a material (hardware) or immaterial (software) unit or set of such units used to perform specific functionalities to enable electronic data communication;

(3) 'competent authority officer' means a physical person entitled to access and process regulatory information requirements referred to in Article 2(1) of Regulation (EU) 2020/1056, on behalf of a competent authority in a Member State;

(4) 'eFTI data' means data corresponding to regulatory information, when made available by economic operators on an eFTI platform in accordance with Regulation (EU) 2020/1056;

(5) 'request for access to eFTI data' means a request on behalf of a competent authority to receive the eFTI data made available by economic operators on an eFTI platform;

(6) 'follow-up communication' means communication between competent authorities and the economic operators concerned on the information made available by the economic operators on an eFTI platform, following a compliance check by a competent authority officer of that information as provided in response to a request for access to eFTI data. This follow-up communication may consist of a request for

[6] Commission Decision C(2018) 5921 of 13 September 2018 setting up the group of experts on digital freight transport and logistics: the Digital Transport and Logistics Forum (DTLF).

missing eFTI data, or information in relation to follow-up action taken by the competent authority in accordance with applicable national provisions;

(7) 'access rights' means the permissions granted to a competent authority officer to perform operations in relation to one or more eFTI data subsets;

(8) 'processing rights' means the operations or sets of operations that a competent authority officer is allowed to perform on a specific eFTI data subset received in response to a request for access to eFTI data;

(9) 'electronic identification means' means a material or immaterial unit, containing person identification data and which is used for authentication for an online service;

(10) 'identification references' means a personal identification number or coded reference that allows the unique identification of a competent authority officer;

(11) 'Authority Access Point (AAP)' means an ICT component or a set of ICT components performing the functionalities set out in Article 4;

(12) 'eFTI Gate' means an ICT component or a set of ICT components performing the functionalities set out in Article 6;

(13) 'requesting Gate' means an eFTI Gate that processes a request for access to eFTI data lodged via an AAP connected to or integrated into that eFTI Gate;

(14) 'receiving Gate' means an eFTI Gate that processes a request for access to eFTI data received from a requesting Gate;

(15) 'eDelivery' means a set of technical specifications and standards for electronic message exchange developed by the Commission under the Connecting Europe Facility programme[7] and continued under the Digital Europe programme[8];

(16) 'eDelivery Access Point' means a communication component that is part of the eDelivery electronic delivery service based on technical specifications and standards;

(17) 'static discovery' means a mechanism for an eDelivery Access Point to obtain the connection details of another eDelivery Access Point without resorting to third party systems;

(18) 'dynamic discovery' means a mechanism for an eDelivery Access Point to obtain the connection details of another eDelivery Access Point by looking up these details in a third-party system;

(19) 'security keys' means pairs of public and private cryptographic keys, generated by cryptographic algorithms in the form of very large numbers that have a unique relationship to each other;

(20) 'security certificate' means a digital document issued by a certificate authority that is used to establish a secure electronic communication channel between two parties; it includes the public security key and information about the subject of the certificate;

(21) 'certificate authority' means an entity that manages the life cycle of digital certificates, which may include enrolment processes and processes for the issuance, delivery, activation, suspension, revocation, renewal or reactivation of the security certificates;

---

7 https://digital-strategy.ec.europa.eu/en/activities/cef-digital

8 https://digital-strategy.ec.europa.eu/en/activities/digital-programme

(22) ‘user application’ means an ICT component performing the functionalities set out in Article 7*;*

(23) ‘technical guidance documents’ means a set of detailed and non-binding technical documents, drawn up by the Commission in cooperation with Member States in the framework of the working group referred to in Article 13.

Article 2

Common measures

1. Member States shall ensure that their competent authorities have access to ICT systems that can process the unique electronic identifying links (UIL) communicated by the economic operators pursuant to Article 4(3) of Regulation (EU) 2020/1056, and that allow their competent authorities’ officers to access and process eFTI data in either of the following procedures:

(a) by directly processing the UIL, when communicated by the economic operator in machine readable format, by displaying it on the screen of an electronic device or printed on a physical support such as paper or, when the competent authority chooses to allow such communication, also by sending it by email or other electronic messaging application;

(b) by retrieving first the UIL, as communicated by the economic operators through publication on a dedicated registry, by means of a unique identifier associated with a transport operation.

2. Member States shall ensure that the ICT systems referred to in paragraph 1 provide at least the following functionalities:

(a) duly authenticated identification and due authorisation of the competent authorities’ officers, each time an officer lodges a request for access to eFTI data;

(b) mediation of the requests for access to eFTI data lodged by the competent authorities’ officers, including retrieval of the information requested from the appropriate eFTI platform or platforms, by means of secure connections to those platforms.

3. To implement the functionalities listed in paragraph 2, those ICT systems shall comprise at least the following components:

(a) authority access points (AAP);

(b) an authorisation registry;

(c) eFTI Gates;

(d) a search mechanism;

(e) a user application.

4. Member States shall ensure that the components listed in paragraph 3 comply with the requirements laid down in Chapter II. Member States shall be responsible for the setting up, hosting, development, availability, monitoring, updating and maintenance of those components and for the security of the information processed within those components. Where two or more Member States set up or develop one or more of

those components jointly, they shall be jointly responsible for their setting up, hosting, development, availability, monitoring, updating, maintenance and security.

5. Member States remain responsible for ensuring that the access and processing by competent authorities of eFTI data is done only for the purposes of checking compliance with the applicable EU and national legal provisions, and in accordance with applicable EU and national provisions laying down the conditions for performing those compliance checks, and rules on respect of personal data privacy and confidentiality of commercial data.

Article 3

Requests for access to eFTI data, responses and follow-up communication

1. Competent authority officers shall lodge all requests for access to eFTI data via the AAP component described in Article 4, by means of the user application described in Article 7.

2. A request for access to eFTI data shall contain the following information:

(a) the UIL of the eFTI data to which access is requested, or one or more identifiers that allow the retrieval of that UIL from the registry of identifiers described in Article 11. This information shall be provided by the competent authority officer responsible for the request;

(b) the references to the access rights of the competent authority officer responsible for lodging the request, as recorded in the authorisation registry described in Article 5. This information shall be automatically added by the user application;

(c) the unique identification number of the request, as issued by the AAP. This information shall be automatically added by the user application.

3. Responses to a request for access to eFTI data may take one of the following forms:

(a) eFTI data, as transmitted by an eFTI platform based on the information contained in a request, and associated message exchange metadata or identifiers, necessary to enable the receiving eFTI Gates or authority access points to map the eFTI data to the respective request,;

(b) error messages, containing coded or brief textual specification of the type of error when an eFTI Gate or an eFTI platform cannot provide the requested eFTI data for technical or business process reasons;

(c) message indicating that no data is available, to be issued by a receiving eFTI Gate when it processes a request that contains identifiers and the search mechanism of the Gate detects no active UIL linked to those identifiers in its registry of identifiers;

(d) ‘no response’ message, transmitted by an eFTI Gate or eFTI platform when that eFTI Gate or platform confirmed receipt of request but did not send a message containing the requested eFTI data within 60 seconds from confirmation of receipt.

4. Where the competent authority officer establishes that the information made available by an economic operator on an eFTI platform, and as retrieved in response to a request for access to eFTI data, is incomplete or fails in other ways to comply with the regulatory information requirements on the basis of which the request was made, the officer may communicate those findings to the economic operator by

lodging a specific follow-up communication for that information. Any such follow-up communication shall comply with applicable national legal requirements on follow-up actions to regulatory compliance checks.

5. Where a specific follow-up communication referred to in paragraph 4 is lodged, the competent authority shall also transmit it via the AAP component, by means of the user application. It shall contain:

(a) the information to be communicated by the competent authority to the economic operator, in free text format, or as an attached document;

(b) the UIL of the eFTI data and the unique identification number of the request for access to that data for which the follow-up communication is lodged.

CHAPTER II

FUNCTIONAL COMPONENTS

Article 4

Authority Access Points

1. The AAP components shall enable the access of the competent authorities' officers to the eFTI exchange environment and shall constitute an officer's sole point of access to that environment.

2. An AAP shall perform the following functionalities:

(a) authenticate the identity of the competent authority officers, or ensure the authentication of the identity of the competent authority officers;

(b) authorise the request for access to eFTI data of the competent authority officers, based on their respective access rights stored in the authorisation registry, or reject the request if the competent authority officer has no active access rights registered;

(c) register the authorised requests for access to eFTI data by issuing a unique identification number for each such request, and record at least the following information for each request:

  (i) identification references of the officer responsible for lodging the request;

  (ii) the UIL of the eFTI data to which access is requested, or the identifier or identifiers provided by the officer when lodging the request;

  (iii) the references to the access rights of the competent authority officer responsible for lodging the request, as recorded in the authorisation registry;

  (iv) the date and time at which the request was lodged;

(d) transmit the authorised requests for access to eFTI data to the eFTI Gate for processing, by providing the following information:

  (i) the unique identification number of the request;

  (ii) the UIL of the eFTI data for which access is requested, or the identifier or identifiers provided by the officer when lodging the request;

  (iii) the references to the processing rights of the competent authority officer responsible for lodging the request, as recorded in the authorisation registry;

(e) receive the responses to requests transmitted by the eFTI Gate and make these responses available to the competent authority officer responsible for that request via the user application;

(f) keep an audit trail of the responses received for each request by logging at least the following information:

(i) the unique identification number of the request for which the response was received;

(ii) the date and time at which the response was received by the AAP;

(iii) the date and time at which the response was forwarded by the AAP to the officer responsible for the respective request;

(g) keep an archive of the requests for access to eFTI data and of the log of the received responses for a period of 2 years or, where national applicable provisions on the availability of evidence for the enforcement of the provisions for which access to eFTI data is required provide for a longer period of time, for that period of time;

(h) when a follow-up communication in accordance with Article 3(4) is lodged, register the follow-up communication by issuing a unique identification number for the follow-up communication and record at least the following information for that follow-up communication:

(i) identification references of the officer responsible for lodging the follow-up communication;

(ii) the UIL of the eFTI data and the unique identification number of the request for access to that data for which the follow-up communication was lodged;

(iii) the date and time at which the follow-up communication was lodged;

(iv) the content of the follow-up communication;

(i) transmit the follow-up communications to the eFTI Gate for processing, by providing the following information:

(i) the UIL of the eFTI data and the unique identification number of the request for access to that data for which the follow-up communication was lodged;

(ii) the content of the follow-up communication.

3. To provide the functionalities set out in paragraph 2, an AAP shall:

(a) use appropriate electronic identification means that allow for reliable identification and authentication of the officers of the competent authorities, or that allow for verifying that the identification and authentication of those officers is ensured by another appropriate ICT component;

(b) use an authorisation registry;

(c) establish and maintain a secure connection to an eFTI Gate;

(d) support a secure connection to the user application.

4. Member States may set up the AAPs either outside of the eFTI Gate, as part of existing ICT systems of their respective competent authorities, or integrated in their respective eFTI Gate.

Article 5

Authorisation registry

Member States shall ensure that the rights of their competent authority officers to access and process eFTI data are recorded and kept up to date in an authorisation registry. The authorisation registry shall include, for each competent authority officer, at least the following:

(a) unique identification references of the officer;

(b) the access rights of the respective officer, expressed as the list of references of the Union and national legal acts that require the provision of regulatory information, in relation to which the respective officer has competences and, more specifically, as the list of the respective identifiers of the eFTI data subsets corresponding to those provisions, as established in Sections 3 and 4 of the Annex to Commission Delegated Regulation [*OP insert reference to delegated act on eFTI common data set and eFTI data subsets];*

(c) the processing rights of the respective officer, expressed as coded references to the processing operations that the officer has the right to perform on each of the respective eFTI data subsets, in line with the applicable Union or national legislation determining the competences of that officer;

(d) a log of the changes to the access and processing rights of that officer.

Article 6

eFTI Gates

1. The eFTI Gates shall ensure, directly or via connection to other eFTI Gates, that:

(a) the authorised requests for access to eFTI data are transmitted to the eFTI platform and contain the specific information requested;

(b) for each such request, the response received from the respective eFTI platform is transmitted to the user application of the competent authority officer responsible for that request, either directly or via an AAP, as applicable; and,

(c) when lodged, the follow-up communication to that request is transmitted to the eFTI platform that contains the eFTI data for which the request had been made and the response provided.

2. An eFTI Gate shall provide the following functionalities:

(a) validate the request for access to eFTI data and, where lodged, follow-up communication, in one of the following ways:

(i) when acting as ‘requesting Gate’, where the AAP is established as a separate component outside of the eFTI Gate, by verifying the security key of the AAP through which the request or follow-up communication was lodged;

(ii) when acting as ‘receiving Gate’, by verifying the security key of the eFTI Gate from which it received the request or follow-up communication;

(iii) when the validation of the security key of the respective eFTI Gate fails, by returning an error message to the ‘requesting Gate’, the AAP or the competent

authority officer responsible for the request or follow-up communication, as appropriate;

(b) process the request for access to eFTI data and, where lodged, follow-up communication, by means of the search mechanism in accordance with Article 8 and, on that basis, forward the request or follow-up communication, as applicable:

(i) to the appropriate eFTI platform or eFTI Gate(s), when acting as 'requesting Gate';

(ii) to the appropriate eFTI platform, when acting as 'receiving Gate';

(c) keep an audit trail of all the requests for access to eFTI data or follow-up communications it has processed, by logging at least the following information:

(i) the unique identification number of the request for access to eFTI data or of the follow-up communication;

(ii) the identifier of the AAP or of the 'requesting eFTI Gate' from which it received that request or follow-up communication;

(iii) the date and time it received that request;

(d) validate the response received to a request it processed, as follows:

(i) when receiving the response directly from the eFTI platform, by checking the security key and certification status of the eFTI platform, on the basis of the registry referred to in paragraph 3(e);

(ii) when receiving the response from a 'receiving eFTI Gate', by checking the security key of that eFTI Gate on the basis of the registry referred to in paragraph 3(f);

(iii) when the validation of the security key of the respective eFTI Gate or eFTI platform fails, by sending a corresponding error message to the 'requesting Gate', the AAP or user application of the competent authority officer responsible for the request, as applicable;

(e) forward the response received to a request it processed through the same route, in reverse sequence, as the forwarded request, as applicable:

(i) to the 'requesting eFTI Gate'; or

(ii) to the user application of the competent authority officer responsible for that request, directly or via the AAP;

(f) when an acknowledgement of receipt of the request is received but no other response is received within 60 seconds of that acknowledgement, transmit a 'no response' message to the 'requesting Gate', AAP or user application of the competent authority officer responsible for the request, as appropriate;

(g) keep an audit trail of all the responses to the requests for access it has forwarded, by logging at least the following information:

(i) the UIL of the eFTI data set it received in response to that request;

(ii) the unique identification number of the eFTI platform or 'receiving eFTI Gate' from which it received the response;

(iii) the date and time it received that response;

(iv) where no response was received, an indication to that end;

(h) archive and keep available for auditing purposes the logs specified in points (c) and (g), for a period of 2 years or, where national provisions on the availability of evidence for the enforcement of the provisions for which access to eFTI data is required provide for a longer period of time, for that period of time.

3. To enable the functionalities referred to in paragraph 2, an eFTI Gate shall:

(a) use a search mechanism, in accordance with Article 8;

(b) establish and maintain a secure connection to the AAPs that mediate the access to the eFTI exchange environment of the competent authority officers of the Member State that established the respective eFTI Gate;

(c) where the AAPs are established as integrated components to the eFTI Gate, establish and maintain a secure connection to the user application or applications, as applicable, of the competent authority officers of the Member State that established the respective eFTI Gate;

(d) where AAPs are established as separate components to the eFTI Gate, establish and maintain an up-to-date registry containing the unique identification numbers and security certificates of those AAPs;

(e) establish and maintain a secure connection to all the other eFTI Gates, as well as an up-to-date registry containing the unique identification numbers and the security certificates of those eFTI Gates;

(f) establish and maintain a secure connection to all the eFTI platforms that received certification in the Member State or Member States that established the respective eFTI Gate, as well as an up-to-date registry containing the unique identification numbers, security keys and certification status of those eFTI platforms;

(g) be able to use commonly defined services or artefacts, such as configuration, error codes, taxonomies or code lists in the eFTI exchange environment, where these services or artefacts are agreed in the framework of the network of operational support referred to in Article 13.

4. Where no conformity assessment body is accredited in a Member State to certify eFTI platforms in accordance with Article 11 of Regulation (EU) 2020/1056, that Member State shall ensure that its eFTI Gate establishes and maintains the secure connection and up-to-date registry, as referred in paragraph 3(f), for eFTI platforms that received certification from conformity assessment bodies accredited in other Member States. That Member State shall do so upon request from the economic operator or eFTI service provider operating that platform and after having requested and received confirmation from the Member State where the eFTI platform received the certification that it received no other confirmation request for that same eFTI platform from another Member State. That shall relieve the eFTI Gate of the Member State where the eFTI platform received the certification from the obligation to establish and maintain a secure connection to that platform.

Article 7

User application

1. The user application shall enable a competent authority officer to interact with the AAP.

2. A user application shall provide at least the following functionalities:

(a) generate the requests for access to eFTI data, based on the information provided by a competent authority officer, once the responsible officer has been duly identified, authenticated and authorised by the AAP;

(b) receive and display for viewing by the competent authority officer responsible for the request the corresponding eFTI data provided by the respective eFTI platform(s) in response to that request or the 'no response' or error messages transmitted by the AAP or the 'receiving eFTI Gate';

(c) enable other processing operations by the competent authority officer responsible for the request of the eFTI data received, in line with the processing rights of that officer;

(d) where applicable national provisions allow, generate follow-up communications, based on the information provided by a competent authority officer.

3. To enable the functionalities referred to in paragraph 2, a user application shall, as a minimum:

(a) provide the competent authority officers with a graphical user interface;

(b) establish and maintain a secure connection to an AAP or an eFTI Gate, as applicable;

(c) for data processing, use as reference the data subsets corresponding to the provisions of the Union and national legal acts, as established by Commission Delegated Regulation [*OP insert reference to eFTI delegated act on eFTI common data set and data subsets*], in relation to which the competent authority officers have competences.

Article 8

Search mechanism

1. The search mechanism shall be a component integrated into an eFTI Gate that shall, as its main functionality, process the information included in the request or follow-up communication, as follows:

(a) from the UIL of the eFTI data, retrieve the identifier of the eFTI platform that stores the eFTI data for which the request for access or the follow-up communication was made and, respectively, the identifier of the eFTI Gate to which that platform is connected;

(b) when the request of information includes one or more of the identifiers set out in Article 11(3), search the registry of identifiers for a matching value and

(i) if a match is found, retrieve the active UIL or set of UILs connected to the respective identifiers, then process the information in the respective UILs in accordance with point (a);

(ii) if no match is found, notify the eFTI Gate accordingly.

2. To enable the functionality referred to in paragraph 1, the search mechanism shall:

(a) operate a registry of identifiers, in accordance with Article 11;

(b) use a service metadata publisher (SMP) registry and a service metadata locator (SML) in accordance with the eDelivery specifications or a registry service with

similar capabilities, to enable the discovery of the eFTI platforms, based on the information contained in the request or follow-up communication.

CHAPTER III

TECHNICAL SPECIFICATIONS

Article 9

Message exchanges

1. Member States shall ensure that the eFTI Gates they establish, as well as the AAPs and user applications of their competent authorities, communicate and are able to receive communication in a standardized message exchange format. Communication between eFTI Gates and between eFTI Gates and eFTI platforms shall be done using the XML format.

2. All communication between the eFTI Gates shall take place as message exchanges through eDelivery Access Points, in compliance with the eDelivery message exchange specifications, and using the static discovery mechanism of eDelivery.

3. Message exchange through eDelivery Access Points, in compliance with the eDelivery message exchange specifications, using the dynamic discovery mechanism of eDelivery, shall also be enabled for the communication between the eFTI Gates and the eFTI platforms.

4. Where a Member State has already set in place equivalent, nationally defined, secure message exchange specifications for digital public services, it may decide to enable that communication between the eFTI platforms and the eFTI Gate established by that Member State may take place also based on such equivalent message exchange specifications. In such cases, Member States shall ensure that those specifications, duly detailed and up to date, are publicly available.

Article 10

Security certificates

1. Member States shall issue security certificates, through a certificate authority, to the eDelivery Access Points integrated in the eFTI Gates they established, and to the eDelivery Access Points or, where applicable, to the equivalent message exchange access point of each eFTI platform that received certification from a conformity assessment body accredited in their respective Member State.

2. Member States shall ensure that the private security keys of the eDelivery Access Point integrated in the eFTI Gate(s) are securely stored and their corresponding digital certificates are delivered in a secure way between the eFTI Gates and between an eFTI Gate and the eFTI platforms connected to that Gate.

3. Member States shall ensure secure mechanisms for receiving, recording, retrieving and validating the public keys or security certificates of the eFTI platforms connected to their eFTI Gate. Where a Member State establishes an SMP registry in

line with the eDelivery SMP specifications, with adequate security mechanisms, an SMP registry may be used for this purpose.

Article 11

Registry of identifiers

1. The registry of identifiers referred to in Article 8(2)(a) shall allow the economic operators to upload, by means of an eFTI platform, the UIL of an eFTI data set together with the identifiers that allow the unique retrieval of that UIL, as listed in paragraph 3. The registry of identifiers shall enable the upload, activation, deactivation, or deletion of the UIL of an eFTI data set and of the respective identifiers.

2. The UIL composition shall allow the retrieval of the eFTI Gate identifier, the eFTI platform identifier, and the unique identifier of the eFTI data set corresponding to the regulatory information made available by the economic operators on the respective eFTI platform, where:

(a) the eFTI Gate identifier shall be constituted by an identifier that allows it to be uniquely discovered in the eFTI environment;

(b) the eFTI platform identifier shall be constituted by an identifier that allows it to be uniquely discovered in the eFTI environment;

(c) the unique identification of the eFTI data set shall be constituted by a unique number in the format of a Universal Unique Identifier (UUID) allocated automatically by the eFTI platform.

3. The identifiers to be supported by the registry shall consist of:

(a) data elements of the eFTI data set corresponding to the regulatory information made available by the economic operators, as described in Section 2 of the Annex to Commission Delegated Regulation [*OP: Insert reference to eFTI delegated act on eFTI common data set and eFTI data subsets*], with the following identification numbers:

(i) eFTI39;

(ii) eFTI188;

(iii) eFTI374;

(iv) eFTI378;

(v) eFTI448;

(vi) eFTI581;

(vii) eFTI578;

(viii) eFTI618;

(ix) eFTI620;

(x) eFTI987;

(xi) eFTI1000.

(b) a data element indicating whether or not dangerous goods are being transported, to be identified with the following characteristics: data element ID ‘eFTI1451’; name ‘Dangerous goods on board indicator’; definition ‘The indication of whether or not dangerous goods are being transported according to ADR/ADN/RID. “Yes” means that dangerous goods are on board the transport unit, “No” means that the goods being transported are not on the ADR/ADN/RID list of dangerous goods or the dangerous goods are exempted from the information requirements as stipulated in 3.5.6, 5.1.5.4.2, 5.4.1, 5.5.2.4.1 or 5.5.3.7 ADR/ADN/RID.’

4. The registry of identifiers shall activate the UIL, to make it available for queries, upon upload, and deactivate it when the identifier referred to in paragraph 3(a)(ii) of this Article is uploaded. To enable checks in accordance with the provisions of Regulation (EC) No 1072/2009, for each UIL for which the identifier indicated in paragraph 3(a)(vi) of this Article has the value ‘3’, corresponding to ‘road transport’, the registry of identifiers shall deactivate the UILs only after the period of time referred to in Article 8(2) of Regulation (EC) No 1072/2009. Upon deactivation, the registry shall delete the UIL and the identifiers connected to it.

CHAPTER IV

MAINTENANCE AND GOVERNANCE

Article 12
Network of technical support

1. Member States shall establish helpdesks at two distinct levels:

(a) a ‘level 1’ helpdesk shall be available to provide technical support to the competent authorities’ officers in case of operational issues;

(b) a ‘level 2’ helpdesk shall be available to support the following:

  (i) the ‘level 1’ helpdesks that support the controlling officers;

  (ii) the ‘level 1’ helpdesks that are established by the owners of the eFTI platforms to provide technical support to the economic operators.

2. The Commission shall establish a ‘level 3’ helpdesk that shall:

(a) provide technical support to ‘level 2’ helpdesks to resolve operational issues which are linked to the functioning of the overall eFTI exchange environment, including the rules, procedures and functional and technical implementation specifications as well as eFTI common data set and subsets set out in the implementing and delegated acts established pursuant to Regulation (EU) 2020/1056;

(b) act as a facilitator for operational issues which concern two or more Member States and where coordination at Union level is required, including the technical interoperability of the eFTI Gates and the communication between the eFTI Gates;

(c) interact with the Commission services that provide dedicated software or specifications of products used by the eFTI exchange environment, such as eDelivery.

3. Helpdesks ‘level 1’ and ‘level 2’ shall also contact one another to resolve issues of common interest at their respective levels.

4. The availability of the helpdesks shall be synchronised across the Union to ensure a minimum period of common availability during workdays between 10:00 hours and 16:00 hours Central European Time (CET/CEST), except national public holidays. During weekends and national public holidays an emergency service shall be available where at least one on-call staff member will be available for urgent issues that severely affect the functioning of the eFTI exchange environment either at national or Union level.

5. All helpdesks shall use dedicated assistance tools that allow the unique identification and follow-up of each request for technical support, including when solving a request requires communication between the helpdesks.

6. Helpdesks shall keep logs of all assistance requests and their history and shall regularly compile reports on their activities.

7. Member States shall communicate to each other and to the Commission the contact details of their respective 'level 2' helpdesks.

8. The start date of availability of the helpdesks shall be the date referred to in Article 5(1) of Regulation (EU) 2020/1056. The adequacy of the minimum period of common availability of the helpdesks shall be assessed within 12 months from that date.

Article 13

Network of operational support

1. A dedicated working group shall be set up as a subgroup of the expert group established pursuant to Commission Decision C(2018) 5921, with a mandate to ensure the eFTI operations take place at the required level of quality.

2. The members of the working group appointed by the Member States shall also act as 'eFTI national contact points'.

3. The members of the working group shall cooperate and meet regularly to, among others:

(a) provide updates on the operational status of the eFTI exchange environment;

(b) assist the Commission services in their efforts to resolve technical and operations issues reported by the Member States or the 'level 3' helpdesk that require coordination and operational guidance at Union level;

(c) assist the Commission with drafting technical guidance documents to support the implementation of this Regulation.

CHAPTER V

FINAL PROVISIONS

Article 14

Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from the date of entry into force of this Regulation.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 5.7.2024

For the Commission
The President
Ursula VON DER LEYEN