

EFTI SERVICE PROVIDERS UNDER REGULATION (EU) 2020/1056

A HIGH-LEVEL INTRODUCTION



Lia Potec, Team Leader eFTI

European Commission, Directorate-General for
Transport and Mobility

Key Definitions (Article 3, eFTI Regulation)

- **‘eFTI platform’** means a solution based on information and communication technology (ICT), such as an operating system, an operating environment, or a database, intended to be used for the processing of [electronic freight transport information] eFTI;
- **‘eFTI service’** means a service consisting of eFTI processing by means of an eFTI platform, alone or in combination with other ICT solutions, **including** other eFTI platforms;
- **‘eFTI service provider’** means a natural or legal person which provides an eFTI service to the economic operators concerned on the basis of a contract;
- **‘economic operator concerned’** means a transport or logistics operator, or any other natural or legal person, who is responsible for making regulatory information available to competent authorities in accordance with the relevant regulatory information requirements;

Note: Some eFTI platforms may be operated internally by companies for their own use, without involvement of service providers, but all eFTI service providers must operate a certified platform to be eligible for certification

Why regulate eFTI service providers?

- **Different risk profiles between platforms and service providers**

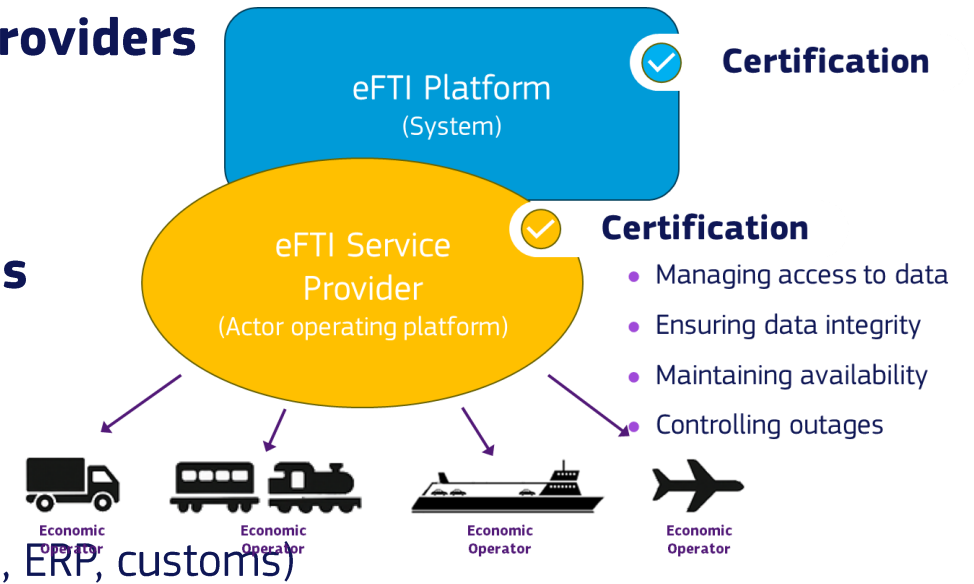
- Platforms = technical tools
- Service providers = actors with operational responsibility

- **Service providers have various roles and responsibilities**

- Manage access rights and enforce user authorisations
- Transmit eFTI data to competent authorities
- Store or archive data for inspection
- Integrate the eFTI platform with other digital systems (e.g. TMS, ERP, customs)

- **Service providers serve as trust & compliance interface**

- Critical to fulfilling obligations in digital-only compliance channels



What would be the risks without clear legal requirements for service providers?

- **Service disruptions = Compliance failures**
 - Lack of continuity planning may cause non-compliance during outages
- **Unclear responsibility**
 - Difficult to determine accountability for errors or breaches
- **Inconsistent quality across the EU**
 - Risk of patchwork practices undermining legal certainty
- **Loss of trust in digital channels**
 - Weak service provider controls can reduce confidence in paperless processes

- **Article 10 – Requirements for service providers**
 - Availability, integrity, and confidentiality of data
 - Logging, traceability, and secure communication
 - Access control and business continuity
- **Article 10(2): Detailed specifications** to be adopted via implementing act
 - Ensure quality and accountability
 - Standardised obligations across Member States
 - Support the certification framework:
 - Define measurable conditions for approval
 - Enable monitoring and trust
- **Article 13 – Certification rules**
 - Commission to adopt procedures for certification of compliance

Broader EU digital law context

- **NIS2 Directive:**
 - Cybersecurity and continuity obligations
- **GDPR:**
 - Role-based access and data processor accountability
- **Data Governance Act:**
 - Trust and transparency in data sharing
- **Digital Services Act:**
 - Due diligence and access control

Shared principle: Trust must extend to digital service providers, not just platforms

- **Specifications for service providers (implementing act)**
 - Commission to adopt detailed operational requirements
- **Certification rules (delegated act)**
 - Commission to define common procedures for assessing compliance
- **Stakeholder input**
 - Essential for balanced, effective implementation
- **Supporting guidance, templates and documentation**
 - Input from DTLF expert group, EU funded projects

Thank you!

Lia Potec, Team Leader eFTI
European Commission, DG MOVE