FOSTERING TRUST AND SECURITY FOR RESILIENT DIGITAL SUPPLY CHAINS

A CHARTER FOR PROTECTION AND GOVERNANCE OF DATA IN INTERNATIONAL TRADE

GLOBAL SHIPPERS FORUM

International Federation of Freight Forwarders Associations

The global voice of freight logistics

INTRODUCTION

The conduct of international trade and transport involves numerous actors, including shippers, freight forwarders and logistics providers, vessel operating common carriers, ports, and other parties ("supply chain stakeholders"). Throughout the course of the transport journey, supply chain stakeholders are required to provide various documents and information as part of legal and regulatory procedures, as well as to communicate requirements from service providers. The provision of such information often includes disclosure of personally identifiable information and/or potentially commercially sensitive data.

Currently, the exchange of such information takes place predominantly through paper-based processes. Initiatives are currently in progress to digitalize these processes, in the interests of achieving greater efficiency, security, and trade facilitation. This raises a number of new issues as regards the collection, storage and use of information exchanged by digital means. As compared to the exchange of paper documents, information supplied through a digital trade or transport application or platform can be stored, analyzed or processed so as to observe trends and other patterns in the shipments to the potential commercial benefit of other parties.

It is crucial that there is a framework in place that fosters trust between supply chain stakeholders when sharing data by digital means. This Charter sets out minimum rights and responsibilities that should be incorporated in User Agreements between providers of digital applications, platforms and supply chain stakeholders. It is intended to establish principles and practices to protect the interests of supply chain stakeholders in the storage and use of their data and should be considered advisory in nature. Any incorporation of these principles into contractual agreements should be subject to legal advice. This document will be subject to periodic review to ensure it remains aligned with future developments.

1. Ownership of data supplied by a supply chain stakeholder

In transacting trade and transport contracts in digital form, supply chain stakeholders need to present and handle the data of other entities, such as shippers, forwarders, carriers and other commercial parties that identifies some or all of the following features of a shipment:

- The names and contact details of parties to the shipment
- The origin and destination of the shipment
- The nature of the goods being shipped
- The weights and volumes of the goods involved
- The value of the goods
- Other distinguishing features of the goods
- Insurance-related details

Principles

a. This data is owned by the different supply chain stakeholders at different stages of the shipment as identified in the transport contract.

b. The inclusion of these data in a digital trade or transport document, does not in itself confer rights of ownership, use, or transfer on any other party, even in an anonymized form.

c. User agreements for the use of digital transport and trading applications and on-line platforms should explicitly acknowledge that ownership of data supplied by the stakeholder rests with the stakeholder unless separately agreed.

d. Rights to access, use or transfer data supplied by the stakeholder should be agreed between the parties in the User Agreement or by a separate agreement.

2. Permission to store, transfer or analyze data supplied by a supply chain stakeholder

For legal and commercial reasons, data supplied by supply chain stakeholders may need to be stored in digital form within a digital application or an on-line system. The accumulation of data over time will constitute a potential source of insight and intelligence on the trading behaviour and patterns of the stakeholders, individually and collectively.

Principles

a. Consistent with the rights of ownership, the use, transfer or analysis of these data should not be undertaken by a provider of a digital application or platform and its affiliates without the express consent of the concerned stakeholder, either in the User Agreement or by separate agreement.

b. There should be no presumed right of access or use of the data by application or platform providers and their affiliates, nor should forfeiture of these rights be made a condition of the use of the application or platform

c. Permission to store data should be limited to a specified period and for specific purposes explicitly stated. Following such period, permission is renewed by agreement between the parties, or the data are deleted.

3. Duty of care to protect data supplied by a supply chain stakeholder

There should be an expectation that the provider of the digital application or platform and their affiliates have a duty of care towards the protection and integrity of data provided by stakeholders and that reasonable precautions are taken to prevent the loss, unauthorized access or corruption of the data whilst in the custody of the application or platform provider.

Principles

a. Digital application and platform providers should employ industry-standard data security and encryption techniques and practices to protect shippers' data against loss or unauthorized access.

b. Data security and protection practices approved to or compatible with ISO Standard 270001 should be expected

c. A Data Protection Officer should be designated by the application or platform provider at a sufficiently senior level so as to take responsibility for the protection and security of data stored within the system.

d. Stakeholders should be able to request a statement of the extent of data stored by application or platform.

e. There should be a point of contact at such platforms/companies to address stakeholder data protection concerns and provide necessary clarifications.

f. All parties who store, transfer, analyse data from supply chain stakeholders should contract to observe or incorporate by reference applicable legislation and regulations in their terms and conditions.

g. All parties who have access to the relevant data should contract to observe Confidentiality Obligations for handling the data, which should be provided on request.

h. All parties who store, transfer, analyse data from supply chain stakeholders should hold approved Cybersecurity Insurance with a reputable firm for an agreed amount and provide certificates of validity of such insurance on request.

4. Obligation to report data loss or unauthorized access to relevant supply chain stakeholders

Should a loss or unauthorized access to stakeholders' data occur, the provider of the digital application or platform should be under a contractual obligation to notify the owner(s) of data that a loss or breach of security has occurred, as soon as is practicable and take necessary measures to limit the compromise of data. This is in addition to any notification of statutory agencies that may be required under applicable national laws.

Principles

a. Notification of the circumstances of data loss or a security breach should be sufficient to enable stakeholders to identify the data affected and the likely means of access so that they may in turn notify parties identifiable from, or affected by, the lost data.

b. Rights to compensation for costs or consequential losses arising from a data loss or breach should be agreed and set out in the User Agreement.

c. Companies processing sensitive and large volumes of data have an obligation to report such events to the relevant government agency and insurer as soon as possible. Stakeholders may request inclusion of an indemnity for costs and consequential losses arising from a breach.

5. Obligations for "Big Transport"

The largest companies in supply chains who manage and process data should ensure fair and open digital markets in keeping with obligations applicable to 'gatekeepers' of the industry.

Principles

a. Ensure interoperability between third parties' data models and the gatekeeper's own services and systems.

b. Allow business users to promote their offers and conclude contracts with their customers outside the gatekeeper's platform.

c. Provide business users with access to the data generated by their activities on the gatekeeper's platform.

d. Use of the data of business users should be prohibited in situations where gatekeepers compete with them on their own platform.

Tracking end users outside of the gatekeeper's core platform service for the purpose of targeted advertising should be prohibited, in the absence of effective consent.

DISCLAIMER

This document is NOT to be construed as providing any legal advice. FIATA and GSF recommend that readers seek independent legal advice if they have any questions on dealing with their specific circumstances.

This Data Protection and Governance Charter provides general considerations that are of relevance in global trade in the digital age as a basis for risk management and does not include technical advice. It is recommended that readers adjust and implement the recommended measures in accordance with the applicable laws and regulations in their jurisdiction, its corporate structure, business model and risk control requirements in the country or geographic areas where it is operating. FIATA and GSF accept no responsibility for the consequences of the use of the information contained in this document which may be periodically updated.

For further information, please contact: FIATA **legal@fiata.org**; or GSF: **secretariat@globalshippersforum.com**

Photos: khunkorn from Canva (front cover); MNBB Studio from Shutterstock (back cover)

GLOBAL SHIPPERS FORUM

International Federation of Freight Forwarders Associations

The global voice of freight logistics

Rue Kléberg 6 | 1201 Geneva | Switzerland
Tel.: +41 22 715 45 45 | info@fiata.org | www.fiata.org

Design: Services Concept Sàrl, Geneva
Layout: Svitlana Ivanova