Transport and Telecommunication, 2022, volume 23, no. 4, 344–351
Transport and Telecommunication Institute, Lomonosova 1, Riga, LV-1019, Latvia
DOI 10.2478/ttj-2022-0028

RELEVANCE OF REGULATORY AND DATA AVAILABILITY ISSUES TO TRANSPORT AND LOGISTICS PROCESSES, BASED ON THE INSIGHTS OF THE EPICENTER PROJECT

***Darius Bazaras*[1]*, Viktor Skrickij*[1]*, Algirdas Šakalys*[1]*, Raimondas Šakalys*[1]**

[1]*Faculty of Transport Engineering, Vilnius Gediminas Technical University*
Saulėtekio ave. 11, LT-10223, Vilnius, Lithuania
darius.bazaras@vilniustech.lt

The article was prepared using research output received implementing the ePIcenter project funded by the European Union program HORIZON 2020. A brief description of the project is presented. The paper presents theoretical research regarding essential data requirements that may be important for improving logistics processes. After identifying the main data requirements, scientific research is presented. Analysis of valid legal acts to determine the regulatory criteria and aspects of the relevance and availability of data is performed. Essential areas of data exchange, their importance and trends are identified, taking into account business and governmental organisations. Trends and possible development perspectives are presented.

Keywords: Logistics, ePIcenter, BIG DATA, regulation, management, technology

1. Introduction

In recent years, global political, social, and military changes have been taking place in the world, directly impacting the operation and synchronisation of global logistics supply chains. International agreements, competition, cooperation and conflicts form a new reality in which transport and logistics companies must operate. Perhaps the essential aspect of these transformations and changes is related to the generation of data, including BIG DATA, and the need to properly process them to effectively manage the logistics supply chain and transport flow in transport corridors. Launched in 2020, the European Commission's Horizon 2020 program funded project "ePiCenter – Improved physical internet supporting environmentally friendly freight transportation" covers a very wide range of analysed areas from political and legal regulation, BIG DATA availability and management to synchronised management of traffic flows in transport corridors (ePIcenter). During the implementation of the project, its goals were and are affected by significant environmental changes – the COVID-19 pandemic, the war in Ukraine and other geopolitical changes that affect the processes in the logistics supply chain.

When analysing the BIG DATA issue, an analysis of documents, legal and regulatory acts operating in the European Union (EU) and other countries was carried out. All the documents examined emphasise the importance of data and its impact on prosperity, decision-making, and innovation. They state that successful data management directly impacts the economy, competitiveness, and positive change.

2. ePIcenter project in brief

International / Global supply chains are becoming bigger and more complex; therefore, harder to manage. This increasing complexity results in a loss of efficiency. The ePIcenter project aims to create an interoperable living toolset of software tools, services and methodologies that can be rapidly deployed by a wide range of public and transport industry stakeholders to address the many challenges of the multimodal transport system. The project outcome will help us understand the actual impact of One Belt One Road (OBOR) initiative on EU freight flows and interfaces/nodes capacity needs to link EU (TEN-T) and global networks (ePIcenter).

The ePIcenter project unites 36 partners (port authorities, logistic service providers, manufacturers, academic institutions, and technology partners) throughout Europe and beyond to develop and test AI-driven logistic software solutions, new transport technologies and supporting methodologies to increase the efficiency of global supply chains and reduce their environmental impact (ePIcenter).

The first aspect is visibility and collaboration, making the supply chains or logistic processes more transparent through cyber-secure data exchange and sharing. The second aspect is optimisation, using new data and emerging technologies smartly, developing AI algorithms and simulation techniques that can optimise the real life logistics and synchromodal planning processes end users face daily.

The work on these two tasks will take a major step toward the Physical Internet concept and seamless, sustainable global freight flows. By working closely with industry partners and dealing with real-life cases, the project delivers relevant applications that can easily be transferred to end-users. In the simulation environment, the project also prepares for the future and challenges ahead by considering emerging technologies (e.g. hyperloop, automated vehicles) and trade routes (Silk route, Arctic route). Ultimately the project will contribute to a more efficient and sustainable multimodal freight transport system and logistics.

3. Investigation of data importance and requirements for data in the supply chain

The amount of data around us is exponentially growing, and its correct usage gives many benefits. Many logistics providers manage a massive flow of goods and, as a result, create large data sets. The main problem is that data is not used efficiently up today. In some cases, the company uses internal digital systems, but paper documents lead the cargo, and in other companies, data need to be typed manually. Correct usage of data will bring many benefits in different areas of the supply chain. The main values that correct usage of data may bring are (Lekić *et al*., 2021): Optimisation to the core; Tangible goods, tangible customers; in sync with customer business; A network of information; Global coverage, and local presence.

At the current stage, one of the feasible ways of value creation using available data is a creation of a network between supply chain stakeholders. A central role in such an ecosystem goes to a cloud-based data-sharing platform.

Such a platform offers the benefit of a single connection and authentication mechanism that can be used. During platform development, it is important to define general role models. Commonly the main roles related to the actors involved in the data exchange are (ePIcenter): data provider - party sharing the data with others (also known as data supplier); data owner - party identified as the owner of the data (the data provider will also be the data owner in most cases, but this is not necessarily always the case); data user - party using the data shared by the data provider.

Data quality is beneficial when we want to increase the efficiency of the processes. Even trusted (validated) data providers/owners don't necessarily provide data of sufficient quality. The platform should include data quality validation mechanisms and provide feedback to members. The data provider can upload part of the data; another part is collected and transmitted without human intervention, e.g. by running through IoT devices and automatically transmitting data to the platform. Data quality validation can be provided in two-level: technical and business. In the first case, validation provides if all the data was correctly transmitted; in the second case, if there are no human errors, a person does not fill all the necessary information. These validations ensure that data shared by the commodity can be processed by a user, although the data user might also implement particular data quality validation rules. In the AEOLIX project, Data-providing legacy systems are responsible for data quality, and the DTS checks whether the data sets to be exchanged are complete (AEOLIX, 2015). The lifecycle of data should be taken into account as well. There is no possibility of saving all the information for an indefinite period. The retention, processing, possession, disclosing, and deleting of customers' data should be done cost-effectively with a focus on the data that other stakeholders can reuse in the future.

What is still evident from the logistics landscape is that mutually trusted collaboration is still problematic (SELIS Project). Trust is essential for digital services. Logistics actors will not embrace digital services if they do not trust that their data will be protected. Data sovereignty is essential for data security, with other security aspects, such as secure communication between network nodes. Data sovereignty means maintaining authority and control of data within jurisdictional boundaries.Trusted, safe and secure – the commodity and its (integration with) end-users should be trusted, data sharing should be safe and secure, based on minimal central governance.

One of the main aspects that need to be taken into account in developing governance models is security issues. There are three security levels (AEOLIX, 2015): 1) policy level, 2) software level, and 3) hardware level.

In a globalised world, compliance with recognised data management models helps organisations create trust, inspiring business users to trust their master data, developing alliances, and fostering collaboration (New ICT, 2018; AEOLIX, 2015). Compliance with the General Data Protection

Regulation (GDPR) is required. It is a legal framework that sets guidelines for collecting and processing the personal information of individuals. The platform should ensure compliance with laws. The contract between a provider and a customer stipulates what services the service provider will deliver are needed to regulate cooperation. Such a contract could be a service-level agreement (SLA) (AEOLIX, 2015); in NIMBLE, such a document is called User's Registration Agreement. Such agreement should include:

i) Regulation that specifies which data can be shared and how;
ii) Regulation regarding where data can be stored;
iii) Regulation regarding the sharing of data across borders.

Software level may be directly affected by third parties. There are two possible types of attacks: i) passive – an unauthorised interception and data access do not change data quality or integrity (FENIX Project). Such attacks are considered commercially sensitive. ii) active – cyber-attacks can change the quality of data by changing the data, causing its loss, leading to incomplete data sets and preventing data availability (FENIX Project). A user identity management system is critical to increasing data security at the software level. The module that performs user authentification and identification is needed to facilitate the creation and management of users across the platform (AEOLIX, 2015). Data protection functionality is needed to keep unauthorised parties from accessing private data and can also be used for giving different access permissions to different people. Protection must be ensured while data is in transit, and functionality is usually based on IP security (NIMBLE Project). Firewalls and malware protection also ensure data protection.

In projects AEOLIX and FENIX, an audit trail module that provides a track of business operations, including the data's traceability, was proposed. An audit of the organisation's information shared among systems would reveal where data is created. The logger module contains all the different transactions made between the stakeholders but never stores data for sensitive information.

Data encryption is the second element that increases system security. Secure encryption algorithms are used to maintain and guarantee that only authorised applications; user processes consume the data (SELIS Project). The procedure converts data into another format so that only entities with access to the decryption key can transform it into a readable format. Data flows among systems both on the organisation's premises and on external premises (cloud), and data encryption is becoming increasingly imperative (FENIX Project). Data encryption prevents passive attacks, as it is useless without a proper decryption key. By applying so-called asymmetric encryption algorithms with public / secret key solutions, encryption always provides data from a known source. This prevents an active attack where someone pretends to act on behalf of someone else. The HTTPS encrypted version of Hyper-Text Transfer Protocol (HTTP) is commonly used to access the platform. This protocol adds a layer of security. It requires authentication of the accessed website and decreases the possibility of website attacks (AEOLIX, 2015).

A useful tool for increasing the system's resistance to active cyber-attacks is implementing Blockchain technology. Encrypted hashes chained with previous waybills ensure data integrity. In the case of distributing these hashes to many IT systems, like in blockchain technology, active attacks are very difficult. Note that hashes can also be used to validate the correctness of documents, where a hash can be linked to unique other sources. This type of chained hashing provides immutability (data cannot be changed) and irrefutability (there is no denying that data is shared) (AEOLIX, 2015).

An example of distributed Blockchain Platform is a CORE project (Tan *et al*., 2018). Developed Blockchain network by IMB and MAERSK architecture to ensure segregation across carriers. Each stakeholder will host and manage a blockchain node. Nodes include the blockchain platform components and dedicated blockchain-managed document storage for that node. Sensitive information, including documents, is distributed only to those nodes participating in a channel; this means that none of a carrier's customer information will be distributed to other carriers. Documents are stored on a single node only and are accessed at runtime by other nodes on a channel as permissions allow. The platform provides the isolation required by the participants to ensure a verifiable, immutable, consensus-driven and binding service (Tan *et al*., 2018).

At a hardware level, it is essential to consider three aspects (AEOLIX, 2015): hosting location, disaster recovery, and server security. Due to hosting location, it is essential to know where cloud providers are storing the data. A well-chosen location allows for reducing political risks. EU hosting providers must fulfil the GDPR rules; countries outside Europe could promote different data protection policies over time, resulting in a possible loss in data protection (AEOLIX, 2015). Disaster recovery is the next point that needs to be taken into account. Hostings should be located in a maximally safe environment, where ambient conditions would not affect the hosting. To obtain minimum security standards, server owners should apply security measures. These security measures range from firewalls, disaster recovery policies, patching, backup policies, and malware protection (AEOLIX, 2015).

4. A study on the data usage and data access legislation

In addition to the theoretical aspects mentioned in the previous chapters, related to the importance of data for logistics processes, extensive scientific research was carried out within the framework of the project, which included the analysis of valid legal acts and expert research. The studies aimed to clarify the essential problem areas of data management and their availability and focus on possible solutions. In this article, the essential observations obtained from the analysis of legal acts are presented. Essential documents of the EU, which regulate aspects of data formats, technical parameters, security and availability, were analysed. Among other documents, this chapter has analysed the legislation governing data policy in the EU:

- General Data Protection Regulation (GDPR) Regulation (EU) 2016/679; 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) (Text with EEA relevance) (Regulation (EU) 2016/679, 2016).
- Regulation on the free flow of non-personal data (FFD) – Regulation (EU) 2018/1807; Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.) (Document 32018R1807, 2018).
- Cybersecurity Act (CSA) – Regulation (EU) 2019/881; Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) (Regulation (EU) 2019/881, 2019).
- Open Data Directive – Directive (EU) 2019/1024. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public sector information (recast) (Document 32019L1024, 2019).

Other legislation, strategies and documents are mentioned in the citations.

One of the most important documents was adopted on 19-02-2020. The communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions entitled "A European Data Strategy" is hereinafter "the Strategy". The Strategy assesses the current data management situation and legal regulation and anticipates possible future developments and tasks. (COM (2020) 66 final). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS a European strategy for data. (Document 52020DC0066, 2020).

Virtually all documents emphasise the impact of data on well-being, decision-making, and innovation management. In particular, the fact that digital and information technologies and data management directly impact the economy, competitiveness and positive market developments is highlighted. The main focus is that the public sector and business can make better and better decisions using data and then pursue quality and address relevant issues related to the transport and logistics sector. However, when it comes to the use of domains, it is necessary to emphasise that it is not about personal data. The protection of personal data is a separate subject of legal regulation and includes data that can be used to identify an individual and his or her activities.

The legal framework is based on several important factors, such as the growing volume of data, the importance of data to the economy and society, and the EU's place in the global context of data storage and management. Analysing data growth trends, it is emphasised that by 2025, the amount of data generated in the world will increase to 175 zettabytes (Strategy, 2018). Another important aspect is data deployment, which states that by 2025, 80% of data will be generated and stored on consumer devices (cars, home appliances, and other devices. Furthermore, 20% of data will be generated and stored in centralised data centres (Gartner, 2017). This observation must be taken into account in the development of possible data evaluation and operation mechanisms.

The importance of data to the economy and society is primarily understood as an opportunity to individualise processes and consumption, which would save energy, and resources and be able to trace the origin of products based on blockchain technology, which is very important in modern logistics supply chain management. The data and individualised data will likely serve the development of Startups and Small and Medium-sized Enterprises. The strategy mentions and enables the digital twinning approach, where a virtual copy of a physical product, process, or system is created that allows it to be used for modelling, forecasting, or design. The digital twin allows you to save resources, perform a wider range of experiments, and ensure security. On the other hand, it is important to note that information technology infrastructure, such as large data centres, impacts the environment through energy consumption and emissions. To this end, the Green Course and the aspects of Green Logistics are relevant here.

The documents also address the EU's place in the global context of information technology and data management infrastructure. The EU's competitive advantage in the global market is that of the data traffic generated by industry, the public interest and the Internet of things. China and the United States (US) are the EU's main competitors in the field of data management. US data management is entrusted to the private sector when China has a sufficiently rigorous process for controlling and tracking traffic flows and does not provide adequate protection for personal data. The European path in data management is defined as ensuring the flow of data, its widespread use, security, privacy and ethics.

A key milestone mentioned in the Strategy is the goal of creating a favourable political environment by 2030, based not on instruction but on free choice measures to ensure the growth of the data space and its impact on the economy. It can be assumed that the European path is understood as a path of finding the best solution involving stakeholders. However, the essential principles are maintained and declared. Common European rules and efficient enforcement mechanisms should ensure that:

- Data can flow within the EU and across sectors;
- European rules and values, in particular personal data protection, consumer protection legislation and competition law, are fully respected;
- The rules for access to and use of data are fair, practical and clear, and there are clear and trustworthy data governance mechanisms in place; there is an open but assertive approach to international data flows based on European values. (COM (2020) 66 final) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS a European strategy for data. COM/2020/66 final (Document 52020DC0066, 2020).

5. Main challenges in the field of data exchange and data availability

Areas of concern include the fact that not all EU Member States have the same level of IT infrastructure, achievements, activities, and data use culture. There are examples of ongoing projects where the data exchange is practical and easily accessible to the public, such as the Finnish Forest Act, the Health and Social Data Use Act and others. Therefore, it makes sense to analyse good practice examples and develop practical projects. A very broad problem area is data availability. As the EU has set up a mechanism for protecting personal data, this response to the classification of data and the possibilities for their availability. In principle, there can be pure datasets and mixed datasets. In this context, data of public interest are singled out, data that are generated by society and can help to manage emergencies.

Data delivery from public sector to business entities (G2B). Access to public data is governed by Directive 2003/98 / EC (Directive 2003/98)/EC of the European Parliament and of the Council of 17 November 2003 on the reuse of public sector information (Document 32003L0098, 2003) on the reuse of public sector information and Directive (EU) 2019/1024 Open Data Directive (Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public sector information (recast) (Document 32019L1024, 2019). The basis for data exchange and ensuring its availability is based on the premise that if data has been generated with public funds, it should be available to the general public. The range of such data users is extensive and includes both the business sector and civil society, as well as research and study institutions. The legislation is intended to promote and support data exchange processes. It is noticeable that problems remain in this process, and the role of state institutions could be more active here. It is also noticeable that different data sets are generated in different Member States, which may contain, for example, undisclosed information or personal data. In most cases, this is the case in the field of health care. But, in principle, the G2B process is promotable, legally supported and primarily targeted at small and medium-sized enterprises.

Data exchange between private entities and business institutions (B2B). As it should be, this process is left to market regulation and is not strictly regulated by legal instruments. The strategy notes that these exchanges are not enough and could be more active. First of all, there is the issue of trust, unclear economic incentives, fears of losing competitive advantage and so on. Data exchange between business entities is influenced by the legal regulation of personal data protection. However, it is noticeable that partial legal regulation makes sense here, especially if business institutions create the data jointly.

Data delivery held by businesses to public authorities (B2G). In this case, it would seem that a distinction should be made between the two data flows, the first of which is the data that is provided to the business supervisory authorities under the current legal framework – the tax inspectorate, the social security authorities and others. It can be said that this area of activity is sufficiently clearly regulated and has been playing its role for many years. A much more critical second flow of data, which is not well enough developed, is the provision of data from business institutions to public authorities, which would allow for the development of better public policies. Examples of such information from private carriers, transport and logistics companies could help to develop quality mobility plans or strategies. It is noteworthy that this area is still under-regulated, and, likely, possible solutions will still be sought, including in the context of regulation.

Data sharing between public authorities (G2G). These activities should also be encouraged, leading to better policy-making and the provision of public services. Applying the G2G principle could reduce administrative burdens and streamline processes. However, like other processes, the legal regulation of this process is still possible in the future.

All the documents examined emphasise the importance of data and its impact on prosperity, decision-making and innovation and state that successful data management directly impacts the economy, competitiveness and positive change. The situation differs from country to country: the EU has a balanced approach to data management, involving both the governmental, public and private sectors. In the US, most large data centres are concentrated in the private sector, but there is a "Cloud Act" governing data management. China stands out for its strict control and direct state involvement in data management. In the EU, an important provision in the government's provision of data to the other sectors (G2B) is that publicly generated data must be freely available to the general public, except for personal data. All the data management and availability provisions mentioned here, including the personal data aspect, are also relevant in transport and logistics activities, as most data is generated on user devices - mobile phones, cars, and other equipment. Moreover, another problem is that most consumer devices' operating systems are developed in the US, which inspires the need for international agreements on data management. Within the EU, there is also a noticeable problem – different Member States have different infrastructure experiences and generated data, which creates preconditions for the analysis of unification or standardisation processes. On the other hand, the exchange of data between business (B2B) structures is left to the free market and trust regulation. It can be concluded that there is a process to encourage (B2G) in which, in addition to the provision of mandatory data, the business would provide additional data to the government sector to enable it to organise appropriate and measurable public services. The involvement of the transport and logistics sector is also significant here, as the data provided by this business could transform and/or create an efficient public transport system, freight distribution, urban logistics, green logistics and other systems in which the state is somehow involved. At the national and cross-border levels, data standards remain relevant. It should also be noted that the EU is "open" to searches and best practices – in other words, most possible data management solutions would be sought through calls for proposals or other public tasks. Summarising the analysis of the legal regulation of data management in the transport sector, it can be stated that it contains general rules and specific tasks related to solutions that would increase the efficiency, security and competitiveness of this sector.

6. Conclusions

Research reveals that when analysing the importance of data for logistics processes, the focus goes on the description and standardisation of the given technical parameters and the essential parameters – quality, reliability and safety. In scientific works and legal sources, the provision is widely emphasised that the amount of data will grow enormously in the near future, and this will cause new demands related to data formats and standards, accumulators and processing capabilities. Most documents emphasise the importance of data and its impact on the economy, well-being, decision-making and innovation, stating that successful data management directly impacts competitiveness. Despite the obvious need to organise and systematise the mechanisms and procedures of data access and processing, at the moment, quite different approaches and applied solutions in different countries exists. In some countries focus goes on the protection and portability of personal data; in others, the private sector dominates data processing; and in still others, there is strict control of data and information and extensive participation of the public sector. As a positive trend, we can consider the prevailing provision that the data collected at taxpayers' expense must be available to everyone, including business institutions. A new trend is also related to transport and logistics activities: much data is generated in user devices – cell phones, vehicles, and other equipment – so their use must be maximally useful for the user who generates this data. At the same time, there are noticeable trends and the need to exchange relevant data between business structures. Although the issue of maintaining a competitive advantage is very sensitive in this area, new opportunities for business cooperation are being discovered, which require data exchange to support. A vital area of activity for future development is the provision of data by business institutions to authorities. In the classic case, it is limited to providing only formal reports, balance sheets and statistical data. By creating a suitable mechanism that does not burden businesses with additional costs, it would be possible to expand the range of data that would allow public authorities to form efficient public services in the future. These could be: balanced public transport routes, optimised delivery systems and solutions related to Green Logistics. However, the issue of standardisation of information and data remains open – an optimal solution is still being sought that would satisfy all participants in the process and ensure international cooperation and smooth management. As shown by the study described in this article – the basics are already in place – technical data formats and requirements for them are being created and developed, and essential requirements for the nature of data have been formulated, that is – security, reliability, personal data protection and the ability to positively influence transport and logistics processes.

Acknowledgements

This research was funded from the European Union Horizon 2020 Framework Program, under grant agreement no. 861584.

References

1. *ePIcenter. About the project.* (n.d.). Retrieved from ePIcenter: https://epicenterproject.eu/about-the-project
2. *AEOLIX Architecture for EurOpean Logistics Information eXchange.* (MG-6.3-2015). (2020) Retrieved from European Commission: https://ec.europa.eu/inea/en/horizon-2020/projects/h2020-transport/aeolix
3. Document 32003L0098. (2018) Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. (2003, November 17). Retrieved from EUR-Lex. Access to European Union law: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32003L0098)
4. Document 32018R1807. (2018) Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.). (n.d.). Retrieved from EUR-Lex. Access to European Union law: http://data.europa.eu/eli/reg/2018/1807/oj
5. Document 32019L1024. (2019) Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast). (2019, June 20). Retrieved from EUR-Lex. Access to European Union law: http://data.europa.eu/eli/dir/2019/1024/oj
6. Document 52020DC0066. COM (2020) 66 final. Communication from the commission to the European parliament, the council, the european economic and social committee and the committee of the regions a European strategy for data. COM/2020/66 final. (2020, 2 19). Retrieved from EUR-Lex. Access to European Union law: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066
7. *FENIX Project*. (n.d.). (2020) Retrieved from D2.2.2 Common requirements for the federated architecture of platforms: https://fenix-network.eu/wp-content/uploads/2020/07/FENIX-Deliverable-D2.2.2_v2.0_FINAL.pdf
8. Lekić, M.; Rogić, K.; Boldizsár, A.; Zöldy, M.; Török, Á. (2021) Big Data in Logistics. *Periodica Polytechnica Transportation Engineering*, 49(1), 60–65. doi:10.3311/PPtr.14589
9. New ICT Infrastructure & Reference Architecture to Support Operations in Future PI Logistics Networks. (2018) Retrieved from ICONET: https://www.iconetproject.eu/
10. *NIMBLE Project*. (n.d.). Retrieved from https://www.nimble-project.org/
11. 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. (2016, April 27). Retrieved from EUR-Lex. Access to European Union law: https://eur-lex.europa.eu/eli/reg/2016/679/oj

12. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA.* (2019, April 17). Retrieved from EUR-Lex. Access to European Union law: https://eur-lex.europa.eu/eli/reg/2019/881/oj
13. *SELIS Project*. (n.d.). Retrieved from https://selisproject.eu/
14. *Strategy*. (2018) Retrieved from IDC: https://www.idc.com/
15. Tan, Y.-H., Buhmann, N., Kouwenhoven, N. (n.d.). *(IBM) CORE WP23 Global Trade Digitization (GTD) Platform.* Retrieved from http://www.coreproject.eu/media/25745/07_core_yao-hua_tan_tudelft_28.pdf
16. *Gartner, Inc g*. (2017) Retrieved from Gartner: https://www.gartner.com/en