This issue of the Geostrategic Maritime Review gives the reader some background and depth on the history of the Baltic Sea region. The studied topics are the geostrategic situation, the geopolitical and geoeconomic stakes of logistic hubs in the Baltic states, and finally, the digitalization and modernization of European transportation and the roles that the US, Russia and the EU play together to ensure national, economic and energy security in Eurasia.

Other issues are available online :

QUEST OF THE ARCTIC
The geostrategic Maritime Review 7
décembre 2016

MIGRATION OVER SEAS
The geostrategic Maritime Review 6
juillet 2016

TABLE OF CONTENTS

The Digitalisation of the Maritime industry:

Perspectives and key legal challenges for improved efficiency

Today connected containers, tomorrow crewless ships: Maritime transport will not be able to escape the wave of the Internet of Things (IoT) and the unstoppable digitalisation megatrend.

In January, a Danish shipowner, Maersk, made public its decision to equip its fleet of over 260,000 refrigerated containers with machine-to-machine (M2M) technology that gives global real-time visibility into equipment location and status, and enables the carrier to remotely control temperature, humidity and other climate settings for perishable cargoes. Cisco, an American company, offers various connected port solutions, which notably include intelligent traffic management, for fast, efficient cargo tracking and routing, but also intelligent video surveillance and perimeter controls, for safer ports.

These are just two examples which represent the seeds of future innovations. Indeed, the use of technologies and real-time data are expected to increase, in a not-so-distant future, and to boost operational effectiveness, safety and security while preserving the environment. Among other big shifts that will change the mobility sector, Rolls-Royce announced in February 2017 that it planned to release its first fleet of autonomous ships by 2020, in a move that could cut sea transport costs by as much as 20%.[1]

This embodies a very positive evolution for the Maritime transport of both goods (cargo) and passengers. Indeed, **Maritime transport is essential to the world's economy**, as over 90% of the world's trade is still carried by sea and it is by far the most cost-effective way to carry bulk goods and raw materials around the world. Maritime transport is thus *the "backbone of global trade and the global economy"*, said the UN chief in a message on World Day, September 29, 2016. *"Yet the vast majority of people are unaware of the key role played by the shipping industry, which is largely hidden from view,"* Mr. Ban-Ki moon said, adding that *"this is a story that needs to be told."*[2]

For many years, or more likely decades, the maritime sector remained very traditional where old habits were difficult to overrule (for instance, paper format documentation remained the most used format even recently). Digitalization had then to confront traditional mentalities. However, probably due to the economic struggle faced by the sector, many more of its actors have been convinced of the necessity to modernize processes, and adopt innovative strategies.

Technology has then managed to pervade the Maritime transportation industry over the past years, paving the way to digital "intelligence". Innovation includes solutions to disrupt the current model of intermediation by a direct online connection of loaders and carriers, software products to manage "complexity", or real-time tracker of containers. There is so much potential that a "port hackathon" was organized, for the first time in France, in Le Havre in November 2016 (the 5th world port hackathon was organized in Rotterdam, Netherlands, in September 2016). The aim was to stimulate creativity in order to create new services and businesses around the theme of "Smart port".

This ambition is readily understandable and can only be backed up. Digitalization offers various and obvious **benefits to the Maritime industry**, such as increased efficiency, resilience and supply chain visibility, reduction in the administrative burden and cost cutting, transportation management optimization, more options of transportation means, greener solutions and new economic

---

[1] Rolls-Royce is working with bodies in Northern Europe, including the Norwegian Forum for Autonomous Ships – established by Norway's Maritime Administration – and DIMECC, funded in part by the Finnish government innovation investment arm Tekes. It is also embarking on major research projects in Britain and Singapore.

[2] UN News center, *On World Day, UN spotlights role of maritime transport as backbone of global economy* , September 29, 2016.

opportunities. This way, the biggest beneficiaries of the new technology would be the shipping companies, which could reduce long-term costs and ecology damage because of improved fuel economies. More globally, digitalization is also of utmost importance on **the international scene** which faces an unstable geopolitical context.

For instance, it should be noted that Europe in general, and the Baltic Sea region in particular, has a part to play at a time when China is seeking to rebuild the Silk Road between Europe and Asia (the 'One Road, One Belt' or 'OBOR' initiative). On this specific subject, Europe, through the Baltic region, should focus on new markets created in innovative areas, rather than solely relying on traditional cooperation. As underlined by Alice Rezkova, chairman of the Asia Innovation Forum, on this specific subject, *"the digital economy offers a vast space for cooperation – provided both sides contribute equally to the relationship".*[3]

Besides, China represents a huge economic opportunity for the cruise industry as the Chinese market could take first place on a global scale in 2030, thus supplanting the United-States. On this point, the most technologically advanced cruise ship, the 'Quantum of the Seas' (built by STX France for Royal Caribbean), has been repositioned to Shanghai, increasing the company's capacity in the region by 66 percent.[4]

The **European Union** must therefore fully grasp this potential and establish the policies and conditions for its deployment. Innovative technologies are especially crucial for **the Baltic Sea region**. Indeed, the region is one of the first to enforce the International Maritime Office (IMO)'s SECA-restrictions (Sulphur Emission Control Areas)[5], which allows for the development of potential innovative and forward-looking maritime technology solutions. In this regard, the Baltic Sea region could be a forerunner for other regions of the world to follow in the field of Liquefied natural gas (LNG).

Already, EU institutions seem to be aware of the major challenge represented by intelligent transportation, since it is a watermark in its strategy for a digital single market.[6] In its communication dated May 6, 2015, the Commission even stressed the opportunities offered by the digital conversion for transport industries, making reference to the example of Intelligent Transport Systems (ITS). To feed its reflection and to make progress on this subject, the Commission has set up **the Digital Transport and Logistics Forum (DTLF)** in 2015, bringing together Member States and all transport and logistics stakeholders.

To date, the subject is more advanced for the road transport sector, as illustrated by the adoption of a directive in 2010[7]; and more recently with the Commission's strategy for cooperative intelligent transport (STI-C) for the road sector[8], which should lead to the adoption of an appropriate legal framework by 2018. Nonetheless, Maritime transport is also at the center of the EU Commission's attention as shown by its 2017 work programme, where the use of innovative communication technologies (ICT) is imagined for future logistics operations as well as for energy efficiency and emission control in waterborne transport.[9]

---

[3] *The EU's response to the OBOR should be the Digital Silk Road*, Friends of Europe, October 4, 2016.

[4] Royal Caribbean Press release, April 16, 2014.

[5] IMO Sets 2020 Date for 0.5% Global Sulphur Cap, World Maritime News, October 28, 2016.

[6] Communication from the EU Commission, *a Digital Single Market Strategy for Europe*, May 6, 2015.

[7] Directive 2010/40/EU of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport.

[8] Communication from the EU Commission, *a European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility*, November 30, 2016.

[9] European Commission, Horizon 2020 Work Programme 2016 - 2017, *11. Smart, green and integrated transport.*

As smart transportation cannot exist without a high level of connectivity, the EU Commission's plan to boost EU efforts for the deployment of 5G infrastructures and services across the Digital Single Market by 2020 will also play an essential part to achieve smart EU transportation industries.[10]

These first steps, if yet limited, define a course of digitalization action for the Maritime industry and chart the way forward. **The movement is currently underway even if some challenges remain.**

In this global framework, the present study will firstly focus on EU stakes and how digitalization of Maritime transport is currently under EU institutional scrutiny. It will also consider more closely two major issues for any operator willing to develop in this area: cybersecurity and personal data protection. Indeed, these topics are particularly crucial as data and information systems lead transport digitalization and need to be secured in order to fulfill all the potential in this area.

- ***EU Maritime transport policies and digitalization***

Many European legal texts apply to Maritime transport and are often issued as" legislative packages" by the European Union legislative bodies. The first Maritime legislative package[11] was adopted on December 22, 1986 and essentially aimed at enforcing the principle of freedom to provide services as well as rules on competition in the Maritime transport area. A second legislative package was adopted in 1992[12]and addressed the liberalization of national coastal navigation. Other provisions have subsequently been passed to regulate a series of issues such as working conditions, the protection of the marine environment and safety in Maritime transport.

Within this context, some major steps have paved the way towards Maritime transport digitalization at the EU Level, from the e-Maritime initiative to the efforts initiated by the Slovakian, Dutch and then Maltese Presidencies, to boost the use of NTIC and to meet the challenges still faced by both the private and public sectors.

- *Act 1: the EU e-Maritime Initiative and subsequent actions*

Following the general trend, the EU has gradually incorporated information technology into Maritime transportation. While "e-Maritime" technologies may be numerous, there are common objectives to their use: facilitating communications, simplifying procedures, and enabling safer, quicker and more efficient operations of Maritime transportation.

In particular, the use of technology has enabled the harmonization of practices and the sharing of data in a dematerialized form. This is a major turning point for Maritime transportation considering the administrative burdens to face. On this point, maritime transportation is still a very traditionally run industry. Take the bill of ladings: a paper form is still used for the most part (according to models of documents which have not changed for years). Technological advancements also contribute to the

[10] Communication from the EU Commission, *5G for Europe: An Action Plan*, September 14, 2016.

[11] Council Regulation (EEC) No 4055/86 of 22 December 1986 applying the principle of freedom to provide services to maritime transport between Member States and between Member States and third countries ; Council Regulation (EEC) No 4057/86 of 22 December 1986 on unfair pricing practices in maritime transport; Council Regulation (EEC) No 4058/86 of 22 December 1986 concerning coordinated action to safeguard free access to cargoes in ocean trades; Council Regulation (EEC) No 4056/86 of 22 December 1986 laying down detailed rules for the application of Articles 85 and 86 of the Treaty to maritime transport.

[12] 1992 package: Council Regulation (EEC) No 3577/92 of 7 December 1992 applying the principle of freedom to provide services to maritime transport within Member States (maritime cabotage); Council Regulation (EEC) No 479/92 of 25 February 1992 on the application of Article 85 (3) of the Treaty to certain categories of agreements, decisions and concerted practices between liner shipping companies (consortia).

preservation of the environment, sustainable development and ensuring EU member states' climate commitments[13]. This subject has thus been put on the top of the European Union agenda.

In 2006, the Commission announced the adoption of future **measures in favor of "e-Maritime" services** to improve Maritime transportation quality and efficiency.[14] Following this declaration in 2009, the Commission laid the groundwork for the EU Maritime transport policy until 2018.[15] Among priorities for action, the Commission advocated for the creation of a framework for "e-Maritime" services. In addition, the Commission unveiled a plan to promote a single market for shortsea shipping and the adoption of advanced technologies.[16]

A first step towards this end has been taken with the **Directive 2010/65 of October 20, 2010 on reporting formalities for ships arriving in and/or departing from ports of EU Member States.**[17] It encouraged dematerialized procedures and as of January 1st, 2015, imposed the establishment of "one-stop-shops" in EU Member States ports. This welcome change has opened up the possibility to provide data for value-added services.

In 2009, the EU vessel traffic monitoring and information system, "**SafeSeaNet**"[18], became operational. It enables Member States to interconnect and communicate information to each other on a continuous basis through a dedicated interface system/platform. This tool has improved the safety and efficiency of maritime traffic, the management of incidents, accidents or potentially hazardous situations at sea, as well as the prevention and detection of pollution by ships.

The objective of a ***"Maritime transport without borders"*** was included in the 2011 white paper on transport[19], which aimed at creating a "**blue belt**" through the EU, i.e. a zone within which Maritime traffic would be free (in the sense of a real EU internal and single market). This program's potentialities are far reaching. Among other things, the European Commission advocated for the full interoperability of ICT systems in the water transport sector, as well as the use of the SafeSeaNet as the basic system for all Maritime information tools. Finally, the Commission renewed its support for research and innovation for the development of smart systems.

In 2013, the EU Commission further proposed a **Blue Belt package** with two main measures aimed at reducing the unnecessary administrative burden for the Maritime industry. The first part of the package consists in a further simplification of application procedures for the 'regular shipping service', a customs facilitation scheme for vessels carrying mainly EU goods and sailing to the same EU Member States ports on a regular basis. The second part deals with the implementation of a new tool, called the "eManifest", consisting of a harmonized electronic cargo manifest, to facilitate customs proceedings for mixed cargo (*i.e.*, both EU and non-EU goods that transit regularly via non-EU ports, *e.g.*, in the Baltic, Mediterranean or Black sea).

---

[13] For example, the 2030 climate and energy framework which sets three key targets for the year 2030:
•At least 40% cuts in greenhouse gas emissions (from 1990 levels) ;
•At least 27% share for renewable energy ;
•At least 27% improvement in energy efficiency.

[14] Communication from the EU Commission, *Keep Europe moving – sustainable mobility for our continent*, June 22, 2006.

[15] Communication from the EU Commission, *Strategic goals and recommendations for the EU's Maritime transport policy until 2018*, January 21, 2009.

[16] Communication from the EU Commission, *Towards a European Maritime transport space without barriers*, January 21, 2009.

[17] Repealing the Directive 2002/6/CE. The Directive applies to ships of 300 gross tonnage and upwards, unless stated otherwise.

[18] Directive 2002/59/EC of June 27, 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC, modified by directive 2014/100/UE of October 28, 2014.

[19] Roadmap to a single European transport area: Towards a competitive and resource-efficient transport system, March 28, 2011.

Along with this administrative simplification, the European Commission has taken different measures to boost **investment and competitiveness**, such as the new TEN-T guidelines and the Connecting Europe Facility instrument (CEF). The Connecting Europe Facility regulation sets forth/establishes the rules for awarding EU financial support, priority projects and the maximum limits of EU co-financing per type of project. It also includes a pre-identified list of projects where most CEF investments will be placed.

- *Act 2: Digitalization of Maritime transport, a priority of the recent Presidencies*

The Maltese Presidency of the Council of the European Union, which took office in January 2017, announced its strong intention to continue the work of the Slovakian and Dutch Presidencies in the Transport, Telecommunications and Energy Council, while focusing on several issues in the field of Maritime transport, including digital Maritime systems. Above all, the Maltese Presidency was entrusted with the task of adopting a political declaration on the revision of the EU Maritime Transport Strategy.

This declaration was adopted by the ministers of the Member States in Valletta on March 29, 2017, and sets the priorities for the industry by 2020. Among the six priorities that have been mapped, digitalization is a key feature with the aim to increase the attractiveness of the EU Maritime industry. More precisely, the declaration highlights the need for a 21st century Maritime shipping system and logistics chain, and calls for better connectivity and reliable shipping connections. Indeed, digitalization was considered to be crucial by the majority of respondents to the corresponding public consultation[20] that has been launched on a mid-term review of the EU Maritime Transport Strategy. These inputs will feed **the future EU Maritime Transport Strategy** as well as the ongoing Maritime legislation fitness check.[21]

Innovation also plays an important role to implement the **"Sustainable Blue Growth Agenda for the Baltic Sea Region"**, adopted by the EU Commission on May 16, 2014. This Agenda highlights the extraordinary potential for developing the Maritime economy in the Baltic Sea Region (BSR). More precisely, the BSR is considered as a hotbed for innovation and competitiveness. Sustainability is an integral part of the plan as it can act as a driver for innovation and more jobs, like in the area of clean shipping. On this subject, maritime technologies and Big Data have been identified as high-potential and emerging areas for the BSR. On April 20, 2017, the EU Maritime Ministers signed a Declaration on Blue Growth, reaffirming their political commitment to further grow the EU's sustainable blue economy.

One may see from the foregoing that the next wave of innovation is now definitely on its way for Maritime transport. This being said, in order to become a reality and to be fully efficient, some challenges still need to be met by the Maritime industry and regulatory bodies.

- ***Mind the gap: Remaining challenges for smart Maritime transport***

Many challenges remain for the EU Maritime industry. Indeed, some important issues still exist, mainly with respect to standards interoperability, interconnection of systems, access to data, cooperation or the admission of electronic transport documents.

---

[20] Public consultation on a Mid Term Review of the EU Maritime Transport Strategy (consultation period: 28/01/2015 – 22/04/2015).

[21] The DG Move is currently working on a maritime legislation fitness check covering legislation on flag state responsibilities, accident investigation, port state control, the vessel traffic monitoring and information system and, the reporting formalities for ships arriving in and/or departing from ports of Member States.
The outcome of the fitness check should allow to assess whether overall the selected elements of the existing regulatory framework serve well the objectives of the policy area – is fit for purpose – or whether there are possible adjustments which can increase the cumulative impact of these measures and/or minimise regulatory burdens.

To take it as an example, access to raw data is a key issue which is more globally under the scrutiny of the European Commission.[22] As far as Maritime transportation is concerned, part of the problem lies in the fact that ports and Member States all use different information systems. A harmonized interoperability between supply chain partners would allow easy information sharing and trust in the complexity of multi-modal transport. Solutions should link all public and private stakeholders.

On all these different subjects, essential R&D programs supported by the European Commission are on their way, such as Waterborne[23] or the 'vessels for the future' initiative.[24] They highlight both the industry perspectives for the medium to long-term and the obstacles that have yet to be overcome.

Lastly, the Maritime transport industry faces two other challenges that are already addressed by two new EU regulation tools but which actors still need to get prepared for in order for these challenges to be achieved: **cyber-security and personal data protection**.

- ***Two enhanced imperatives for 2018: cyber security and data protection***

The example of the above mentioned first smart ship, the 'Quantum of the Seas', gives an overview of possible benefits for the cruise industry gained by using new technologies and how it can attract passengers. Nonetheless, anyone familiar with technologies and their flaws can also discern some potential associated risks.

Among technologies that make the difference onboard, the Quantum offers the following services to its passengers and employees: the Royal iQ app that allows them to track every aspect of their trip once onboard; a fast curb-to-cabin check-in; RFID WOWbands[25]which act as an onboard ID; the crew's use of tablets loaded with custom apps that archive details about passengers and their travel likes and dislikes as well as special requests; or yet the Quantum's new satellite Internet that delivers wireless Internet speeds that match fast broadband connections on land. All these technologies could be an industry game changer, provided they do not open the door to data vulnerabilities or data protection breaches.

This is why organizations wishing to develop activities in the transportation industry should particularly raise awareness, at least and concern at most, on two crucial issues: the protection of their information systems and of personal data (in particular those relating to passengers[26]).

On these two critical points, the EU has recently adopted new tools to improve member states' regulation and ensure a common and stronger approach. Such new regulations are aimed at increasing the level of security for information systems and databases throughout EU Member States. This necessarily has important impacts as far as intelligent transport systems are concerned, which must therefore be carefully designed and implemented. Indeed, these new regulations must take into account state of the art technologies and provide an adapted framework to secure the use of data by

---

[22] Communication from the EU Commission, *Building a European data economy*, January 10, 2017 (and the associated public consultation which ran from 10.01.2017 to 26.04.2017).

[23] Waterborne is an initiative that came forth from the Maritime Industries Forum (MIF) and its R&D committee in 2005. The stakeholders include EU associations covering deep and short sea shipping, inland waterways, yards, equipment manufacturers, marine leisure industry, research and university institutions, classification societies etc. The so-called stakeholder Support Group is matched by a Mirror Group of government appointed delegates.

[24] Vessels for the Future comprises a leading group of Maritime stakeholders with a common interest in the development of advanced waterborne technologies, who want to ensure that the Maritime industry has a strong and vibrant future and remains competitive in the global market.

[25] WOWbands are RFID bracelets that allow passengers tap it and quickly navigate the ship, make on-board purchases, access staterooms and access the Royal iQ app. It is an optional replacement for the SeaPass card.

[26] On this point, it can be noted that the French law on the "blue economy" (or "Leroy") enacted on June 20, 2016 has extended to Maritime carriers the obligation to communicate passenger data to competent authorities.

both private and public organizations. They also aim at guaranteeing an appropriate level of security to tackle new threats in the cyberspace.

- *Cyber security and the NIS Directive*

When it comes to cyber security, one should notice that threats are numerous and varied in nature. They range from vessels (*e.g.*, attack on navigation systems to bring the vessel into hazard zones …), to ports (*e.g.*, attack on systems such as video surveillance or door opening controls…), through passengers and freight (*e.g.*, attacking management systems in order to steal data relating to passengers or to the freight in order to drive physical attack or theft…).

In 2014, TrendMicro[27] teams demonstrated that malicious Automatic Identification System (AIS) messages could attack Vessel Traffic Services (VTS) servers by exploiting "common" security vulnerabilities (SQL injection, buffer overflow).[28] Examples of real attacks are numerous. For instance, in 2011, an Iranian company, IRISL, was the victim of an attack that erased all the data regarding the cargo it was managing.[29] Another well-known example is when the Port of Antwerp was infiltrated/ hacked by cyber criminals between 2011 and 2013. The hackers installed physical devices, such as key loggers, and sent malware attached to emails, to infiltrate the computerized cargo tracking system of different companies within the port. In this way, they could identify the shipping containers in which the drugs were hidden. Once these containers had been localized, they dispatched their own drivers to retrieve their containers and their merchandise and covered their tracks afterwards. Moreover, it should be noted that public reporting on this issue is inversely related to actual amount of malicious activity occurring in the industry.

More globally, it appears that there is still too much vulnerability, while the risks are real and growing, as soon as information systems and data are placed at the heart of Maritime transport developments. Significant and dedicated efforts are therefore needed to improve the situation and maritime companies should have specific cybersecurity technologies, processes and practices in place.

The issues of **cybersecurity** and sea-tech have been the subject of numerous developments, notably by the European Network and Information Security Agency (ENISA).[30] For a more recent overview, the report published in April 2017 by the Netherlands Maritime Technology Trade Association is quite instructive: *"Safety of data, the risks of cyber security in the maritime sector"*. The author makes several recommendations to maritime companies on how to protect networks, computers, programs and data from being accessed without an authorization, or attacked or damaged. The report underlines the importance of preventive measures and of staying agile as well as resilient, considering that *"being a hundred percent secure is unfeasible and undesirable, because it limits flexibility and innovation."*

The European Union has tried to take some measures to strengthen Maritime safety and security and to complement existing international instruments (by the SOLAS Convention[31], the ISPS Code, the STCW Convention…). Nonetheless, it is mainly through the adoption of the Directive on security of network and information systems of July 6, 2016 (the **NIS Directive**)[32] that cybersecurity will be further guaranteed.

---

[27] TrendMicro is a global security software company based in Tokyo.

[28] Lars Jensen, Challenges in Maritime Cyber-Resilience, April 2015, TIM Review.

[29] Ibid.

[30] ENISA, Analysis of cybersecurity aspects in the Maritime sector, November 2011.

[31] The International Convention for the Safety of Life at Sea (1974); the International Ship and Port Facility Security Code (2002); The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (1978).

[32] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

The NIS Directive is the main piece of legislation of the "2013 EU Cybersecurity Strategy".[33] Under the NIS Directive, Maritime transport operators are classified as providing essential services, implying new obligations in terms of security.[34] Indeed, the Directive aims at ensuring a high common level of network and information security ("NIS") across the EU and in particular, requires from operators of critical infrastructures (such as in the transport area but also among others, energy or banking), and so-called digital services providers (*i.e.*, marketplaces, cloud computing services, search engines…) that they adopt appropriate steps to manage security risks and report serious incidents to the national competent authorities.

The security measures that will need to be implemented should be adapted to the individual risks faced and implemented in a manner that will both prevent and minimize the impact of incidents on the IT systems or facilities used to provide the services.

As to the threshold to determine whether or not an event will need to be notified, the Directive provides for certain parameters to be taken into consideration: (i) the number of users affected, (ii) the duration of the incident and (iii) its geographic spread. These parameters are likely to be clarified by EU-level common guidelines and formalized when the Directive is implemented into national legislations. The procedural framework to support notification will need to be established by EU Member States.

The NIS Directive will consequently extend the application of appropriate cybersecurity rules to Maritime transport and should lead to more harmonized approaches, which are essential in improving cybersecurity worldwide. The Directive also provides for measures in support of a stronger cooperation between EU Member states.

- *Personal data: implementing the GDPR*

Previous observations also call for special caution concerning the security of **personal data** which can be held and processed by operators. Spontaneously, one may think about personal data of crew members and/or passengers in the cruise, ferry and yachts markets. However, this more globally concerns the entire transportation industry where all types of personal data are at stake, including HR, clients, prospects, suppliers, partners, public authorities being in relation with the operator, etc.

Since the issuance of Directive no. 95/46 of October 24, 1995, EU law has availed itself to rules and guidelines for the protection of personal data, on the basis of which EU Member States have been in a position to design or reinforce their related national regulations (such as the French Act no. 78-17 of January 6, 1978, as modified, which had inspired the 1995 Directive adoption and principles). However, some inconsistencies have emerged among EU Member States data privacy legal regimes which have acted as a brake on smooth trade flows within the EU, as well as unified EU sovereignty towards big data players such as GAFAs or their Asian equivalents. Also, the number of data security breaches has dramatically increased these past years and stronger security standards and rules are needed (hopefully) with a wide geographical scope, in order to bring more trust in all economic sectors.

In view of achieving all these objectives, EU Member States adopted the new EU General Data Protection Regulation no.2016/679 of April 27, 2016 for the protection, processing and circulation of Personal Data (known as the "**GDPR**").

The GDPR is much more extensive in its technical, organizational, legal and geographical scope than the above-mentioned 1995 European Directive.

First, the GDPR extends the rights of individuals by reinforcing existing rights or creating new ones such as the right to a large transparency on data processing, the right to data oblivion, data portability or to reinforced indemnification mechanisms. In parallel, it imposes a series of new obligations on

[33] Communication from the EU Commission, *An Open, Safe and Secure Cyberspace*, February 7, 2013.

[34] Maritime transports are already treated as 'OIV' in France, since the military programming Act adopted in 2013.

organizations that are far-reaching and now required to develop clear policies and procedures to protect personal data, and adopt appropriate legal, technical and organizational measures: **privacy by design and privacy by default** (*i.e.*, the need to protect data privacy and comply with related rules as from the very beginning of devices or projects design, and as a minimum requirement); specific **standard clauses** to be inserted in contracts with data processors; under certain conditions, holding and maintenance of a **personal data registry;** appointment of a **Data Protection Officer (**acting as the internal coordinator and controller, and external contact of data protection authorities and subjects for the data processing activities of a given data controller or data processor); conduct of prior **privacy impact assessments (PIA)** before conducting a data processing entailing a given level of risk for personal data … etc. More generally, the approach is now based on the **accountability** of and **self-assessment** by organizations themselves, while the main bulk of declaration filings will no longer be necessary (except for certain cases of sensitive data processing on the basis of what EU Member states will decide at a national level).

The GDPR will come into effect on May 25, 2018 and will then automatically apply to all EU Member States in a harmonized way (with some derogatory powers left to Member States for certain categories of data, more particularly health, biometric or genetic data).

This means that only a few months are left to prepare and to involve all economic operators to consider the impacts of the GDPR for their businesses and what steps they should be taking now in preparation for its legal, technical and operational implementation.

Indeed, penalties for non-compliance with EU data privacy rules have been much increased with the GDPR as infringers now face a **variety of possible sanctions including fines of up to 10 million EUR or 2% of the operator's annual global turnover** (the higher amount being chosen), **or 20 million EUR or 4%,** for certain categories of obligations being breached (for example the unlawful processing of sensitive data or an unlawful transfer of personal data outside the EU shall fall within the second and higher category of sanctions).

From a geographical scope, the GDPR is not European specific since it will affect every organization that processes the personal data of EU residents, either by being headquartered in the EU or in a country outside the EU but from where the operator shall be offering goods or services (even with no price) to EU residents or monitoring them (another case of application being that a given EU Member State's law applies due to the enforcement of international public law rules). Consequently, non-EU organizations that do business in the EU with EU data subjects' personal data (providing products or services to EU customers or processing their data) will have to face the long arm of the law and may need to appoint representatives in the EU.

When focusing on the more specific topic of international transfers of personal data (*i.e.* outside the European Union), a particular caution should be paid by organizations and appropriate measures taken. In this respect, the position under the GDPR is similar to the existing 1995 regime, *i.e.*, data export outside the EU and a dozen of countries, such as Canada, Argentina, Israel, Switzerland or New Zealand…(whose legislations are considered as offering an adequate level of personal data protection), shall be accompanied by specific guarantees including the use of standard contractual clauses or "Binding Corporate Rules" or "BCRs" (for intra-group transfers) based on models or guidelines established by the European Commission. However, under the GDPR, it will no longer be necessary to file a prior declaration with the data protection authority or to obtain its prior authorization if the requirements of the GDPR are otherwise satisfied (which can still be guaranteed through BCRs or standard contractual clauses approved by the European Commission or the national data protection authority itself). Codes of conduct or dedicated standards will also be available to valid ground transfers of personal data outside the EU.

On the basis of both the current regime and the GDPR, on top of a dozen already recognized "good friends" mentioned above, the European Commission has the power to approve particular countries as providing adequate levels of data protection, allowing international transfers without any further requirement (but by having data importers adhere to a given list of principles agreed upon between EU

authorities and the hosting country as part of the approval process). The previous adequacy decision adopted in agreement with the United-States (the "Safe Harbor") was invalidated in 2015 because it was considered by the European Court of Justice to not be adequately protecting consumers with respect to their rights to privacy.[35] Following this decision, the **"Privacy shield"** has been adopted to replace it as of August 2016.[36] Nonetheless, this new framework has been criticized[37] and is itself currently challenged in courts.[38] More recently, the European Parliament also adopted a resolution questioning its adequacy.[39] In any event, it is clear from the GDPR provisions that adequacy decisions may not necessarily last indefinitely.[40]

Recently, Isabelle Falque-Pierrotin, chairman of both the French Data Protection Authority (the "CNIL", *Commission Nationale Informatique et Libertés*) and of the WP29[41] at a European level, stressed the need for companies to get ready for the GDPR and to anticipate its changes as soon as possible. Indeed, the new measures to be implemented, which impact a lot of positions in organizations, shall trigger a series of material changes and investments in a majority of companies that will need to update, and train people on privacy policies and culture. Therefore, all businesses should use reasonable efforts to adapt themselves and to implement goods practices, as underlined by the CNIL.[42] The CNIL has recommended to follow a six-step process in order to get prepared : (1) appointing a project leader, (i) mapping data, data flows and processing, (3) prioritizing actions according to risks, (4) managing risks, (5) organizing internal processes and (6) documenting compliance.[43]

In December 2016, the WP29 published a first series of guidelines to help data controllers better understand how to properly implement the GDPR (about data portability, data protection officers, identifying a data controller's or data processor's lead supervisory authority, how to conduct data privacy assessments). Forthcoming guidelines are announced (about consent, profiling, transparency, data breach notifications and data transfers).

Of course, companies needing or wishing to use personal data to conduct their activities in the smart and connected EU Maritime transport area will not escape this new regulatory framework and will have to rethink their organization and culture and set up dedicated teams to implement the new principles in a rigorous but possibly valuable way on a long-term basis.

To that end, it is highly recommended that each company commits to implementing the GDPR, sets up a project team made of a variety of cross practices profiles, including IT and data engineers, data consultants, IT solutions providers and lawyers, working in coordination with all of the organization's departments involved in data processing activities (finance, HR, sales, aftersales, etc.). Such teams may of course be led by, and evolve around, the new Data Protection Officer if one is appointed by the organization.

---

35 ECJ, case C-362/14, Maximillian Schrems v Data Protection Commissioner, October 6, 2015.

36 European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows, Brussels, 12 July 2016.

37 Many privacy advocacy groups remain unconvinced, echoing concerns raised by the Article 29 Working Party.

38 The challenge came from the Irish advocacy group Digital Rights Ireland.

39 Resolution on the adequacy of the protection afforded by the EU-US Privacy Shield (2016/3018(RSP)), April 6, 2017.

40 The text provides for a mechanism of periodic review and a monitoring of developments in third countries and international organizations that could affect the functioning of adequacy decisions taken by the European Commission.

41 Article 29 Data Protection Working Party, made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission.

42 CNIL's activity report for 2016.

43 https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes.

ABOUT THE AUTHORS

Béatrice Fleuris, Partner, De Gaulle Fleurance & Associés

Béatrice Fleuris recently joined De Gaulle Fleurance & Associés as Partner to develop activities in the transportation and aviation sector.

Her renowned expertise in domestic and international issues led her to advise transport players (manufacturers and suppliers, airport managers, logistics and transport operators) and actors from others sectors facing issues related to transport (industrial groups and companies dealing with products logistics, leaders transportation…), as well as insurers, reinsurers and financial institutions.

She advises large corporations and companies in their pre-litigation and litigation procedures related to complex cases of commercial litigation, product liability, and claims regarding transported people and goods. She also acts as a counsel in regulatory, commercial and finance issues – notably in the acquisition, sale and financing contracts of aircrafts.
Béatrice Fleuris is a member of the of the European Air Law Association, the Société Française de Droit Aérien et Spatial and the International Aviation Women's Association.

Member of the Paris Bar since 2003, she holds a LLM in Commercial Law from the University College of Dublin (2001), a Postgraduate degree (DESS) in International Business Law from the University of Toulouse 1 (1999) and a undergraduate degree (Maitrise) in International Business Law from the University of Paris I Panthéon Sorbonne (1998)
Ranked lawyer in the Legal 500 2016 (Aviation) and Chambers Europe 2016 (Transportation: Aviation).

Cécile Théard-Jallu, Partner, De Gaulle Fleurance & Associés

Cécile Théard-Jallu has developed in-depth expertise as an attorney in private practice representing multinational corporations, including major US and European firms and organizations in the R&D and innovation sector (public or private research institutions, academics, pharmaceutical laboratories, biotechnology companies, medical equipment manufacturers, service providers, software or connected health platforms publishers, investors, competitiveness clusters, tech transfer agencies and other intermediaries in the field of innovation…) . She intervenes in a variety of industries such as health and life sciences, transportation or renewable energies, but also in the field of IT and services.

Cecile focuses primarily on complex transactions including R&D and consortiums, technology transfers, licensing deals and other technological change related projects. She assists clients with their responses to calls for projects in the R&D and innovation sector in the context of public funding, for instance, with respect to the future investments program (Programme des Investissements d'Avenir) conducted by the French Government.

She also advises them on the structuring of their contractual flows as well as the design, drafting, negotiation and enforcement of their industrial, commercial or IT contracts. She assists clients on the building and implementation of their digital strategy, including on data privacy issues.

For over one year, she worked in Washington DC as a seconded attorney in private practice at the law firm Covington & Burling LLP, and was also seconded to a global player in the medical equipment sector.

She is a member of the Healthcare / Life Sciences and Technology Law Sections of the International Bar Association (IBA) and is ranked in the international Best Lawyers guide, in the "Biotechnology" and "Information Technology" practice. She holds a Master Degree in Business law from the University of Paris X Nanterre (1994) and Post Graduate Degree in Business law as well as a DJCE in contracts, competition and consumer law from the Universities of Cergy-Pontoise and Montpellier (1995). Member of the Paris Bar since 1997.

This article was drafted with the contribution of Nina Gosse, lawyer at De Gaulle Fleurance & Associés.