Countdown to the New Data Protection Law – The impact of General Data Protection Regulation (GDPR) for Companies

By Ms. Xenia Kasapis, LL.B, LL.M, MCIArb

Leading lawyer of the Data Protection and Privacy Department, E & G Economides LLC

With its newly adopted General Data Protection Regulation (GDPR), the European Union is embarking into a new era of data handling framework. The new Regulation, which is designed to strengthen and unify data protection, replaces the Data Protection Directive 95/46/EC. The GDPR was adopted on 6 April 2016, and will be directly applicable across all Member States of the EU on 25 May 2018 and it will affect the way organizations treat, manage and maintain users data; as regards to both clients and employees.

The provisions of the GDPR do not apply for purely personal activities, as they only apply on physical persons and not legal entities Personal data is defined as any information relating to an identified or identifiable individual. Examples of personal data are names, photos, email addresses, bank details, IP addresses and more.

The new EU Data Protection Framework - Key changes

The GDPR introduces a number of novel elements strengthening the protection of individual rights:

Data governance and accountability

The concept of accountability is at the heart of the GDPR rules. Companies will need to be able to demonstrate that they have analysed the GDPR's requirements in relation to their processing of personal data and that they have implemented a system or program that should eventually enable them to be compliant. . Accountability measures are Privacy Impact Assessments, policy reviews audits, activity records and (potentially) appointing a Data Protection Officer (DPO).

Directors have a fiduciary duty to ensure that their organisations comply with the law and that personal data is managed in an appropriate manner.

Penalties

Under GDPR the maximum fines for non-compliance are the higher of €20m and 4% of the organizations' worldwide turnover. This is the maximum fine that can be imposed for serious infringements; i.e not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. Additionally, a company can be fined 2% on the global turnover of €10m for "less serious" breaches such as not having their records in order, or not notifying the supervising authority and Data Subject about a breach nor conducting impact assessment etc.

Appointment of Data Protection Officer

Many companies might be required to appoint a Data Protection Officer (DPO). A DPO is required in: (a) public authorities, (b) organizations that require systematic and regular monitoring of data subjects on a large scale or (c) organizations that engage in large scale processing of special categories of personal data. The Data Protection Officer assumes the tasks of advising, monitoring internal compliance and cooperating with the supervisory authority and is bound by secrecy and confidentiality.

Territorial Scope

One of the most crucial changes of the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR. The GDPR applies to all EU and non-EU companies and organizations that either offer goods or services to EU clients or monitor the behavior of individuals within the EU. Consequently, a business based outside of the EU may be required to appoint a representative based in the EU who is accountable for data protection.

Data Controllers and Data Processors

Some tasks, such as payroll, generally deal with data collected by third parties. A "Data Subject" is a physical person whose personal data is processed by a controller or processor. The data controller

determines the purposes, conditions and means of the processing of personal data while the data processor elaborates further said personal data on behalf of the controller and according to its instructions. GDPR requires a contract to be in place, in order to ensure that liabilities and responsibilities between the controller and processor are stipulated. Processors will also need to comply with GDPR and ensure that data subject's rights are protected.

Privacy by Design

Organisations shall implement all appropriate technical and organisational measures in an efficient way, in order to comply with the Regulation and to protect the rights of data subjects. More specifically, adopting appropriate staff policies as is the use of pseudonymisation (to ensure compliance with data minimisation obligations).

Consent

The new Regulation strengthens the level of consent that is required to justify the processing of personal data. Companies, when requesting consent from its clients for using their personal data, need to do so through a statement or a clear affirmative action. Consent is also required for the processing of personal data of children under the age of 16. It must be clear and distinguishable from other matters and provided in an comprehensible and easily accessible form, using clear and plain language.

Breach Notification

GDPR includes a personal data notification rule. That is when a data breach occurs, organisations shall notify the supervisory authority (SA) within 72 hours. Additionally, if this incident is likely to result in a high privacy risk for the rights and freedoms of individuals, such individuals need also to be informed of the breach.

Data Portability

GDPR also introduces data portability. Individuals have the right to receive the personal data concerning them and have the right to transmit that data to another controller in a structured, commonly used and machine-readable format.

The Right to be forgotten

The right to be forgotten, allows an individual to request that any online content to be deleted. The conditions for erasure are defined in Article 17 of GDPR.

Key Steps to comply with this Regulation:

1. Awareness to the top management of the requirements of the GDPR and the impact that this might have in the company.
2. Identification and documentation of the legal basis of the processing.
3. Creation of a document of all personal data that the business holds; its origin and with whomthey have been shared with.
4. Update and review privacy notices and procedures to ensure they cover all the rights to individuals.
5. Review the GDPR's provisions on consent.
6. Establishment of a Data Breach process and response.
7. Creation and implementation of a Data Protection Impact Assessment (DPIA) process in relation to already collected information.
8. Consider if there is a need to appoint a DPO.
9. Security measures, reviews and updates in light of the increased GDPR security obligations.
10. If the business operates in more than one EU member state, a determination of the lead data protection supervisory authority shall take place.

Concluding Remarks

Even though the new data protection framework has been built on the existing data protection legislation, it will have a wide-ranging impact and will require significant operational adjustments in many aspects. For this reason, the Regulation allows for a transition period of 2 years until 25 May 2018 in order to give Member States and stakeholder's time to be prepared for the newly imposed regulation. The reform, however, can only be considered as successful if all those involved embrace their

obligations and their rights.

In her current position, Xenia is the leading lawyer of the Data Protection and Privacy Department of E & G Economides LLC. She has a broad commercial practice with particular focus in technology, employment, data protection law, intellectual property, company and e-commerce law. Xenia advises on privacy related issues across all industries in the likes of communication companies, shipping and health care organizations. Xenia is also assisting companies with establishing and maintaining data privacy and security compliance matters and is drafting and reviewing commercial transaction documents.

Cyprus Funds as a Solution for Maritime Finance Drainage

By Mr. George Karatzias, FCCA

Member of CIFA and Senior Manager in Alter Domus (Cyprus) Limited

By Mr. Andreas Panayiotou, ACA

Manager in Alter Domus (Cyprus) Limited

For the first time since the global financial crisis of 2008 and 2009, the global ship industry seems to be recovering its upward pace. There is one critical factor however, either being totally unavailable or very hard to obtain for shipping companies which would drive recovery, which is financing.

When the markets came crashing down, subsequently affecting demand around the world, many prominent banks found themselves with significant exposures in now devalued loans offered in the shipping industry. Mostly affected by the downturn were the European banks which as at the end of 2017 were estimated to have US$150 billion of loans at risk devalued. This resulted in banks previously playing a big role in shipping finance to either abandon the industry whatsoever or be left battling to recover the inherited situation of devalued and non-performing loans given to the industry.

Following the financial crisis and the bitter experience of the banks in the past, the more stringent stress tests are further hindering the barriers imposed to banks, resulting to them being driven away despite the signs of an inclining industry.

With GDP estimations for 2018 to be laying at an increased 4%, a push to the need of cargo

Global Shipfinance Portfolio Development

Source: Petrofin Bank Research

transportation is expected, which is currently estimated by Clarksons to be at an increasing rate of 3% to 3,5% per annum (sourced by Seven Capital). As 90% of international trade is performed through shipping and the fact that the volume of trade is directly affected by the increase on GDP, it is expected that a need for financing the industry growth and the search of alternate sources of finance is inevitable and is in fact already observed. One of these sources can very effectively be Alternative Investment Funds which have already attracted players of the shipping industry to turn to.