Regulation (EU) 2016/679 (The General Data Protection Regulation):

New Obligations on Financial Institutions

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) (hereinafter referred to as "**the GDPR**") has been in force since 24/05/2016 and **will apply as of 24/05/2018**, as per Article 99(2) thereof.

The GDPR is directly applicable on all Member States, which are vested with limited discretionary powers as to the transposition of specific articles of the GDPR and their aims thereof. The GDPR purports to implement a consistent and high level of protection of the rights and freedoms of natural persons in relation to the processing of their personal data and to remove obstacles to flows of personal data not only within the European Union (hereinafter referred to as "**the Union**"), but to third countries and international organizations as well.

The Department of the Personal Data Protection Commissioner (hereinafter referred to as "**the Commissioner**") issued on its official website an official Announcement dated 31/05/2016 stating that the Regulation will be applied as of 24/05/2018 and that the Commissioner will proceed with the preparation of a relevant Bill and submission before the House of Representatives of the Republic of Cyprus for legislative enactment, so as to ensure the effective implementation of certain provisions of the GDPR.[1] It is thus expected that the relevant Legislation currently in force in the Republic of Cyprus, namely the Processing of Personal Data (Protection of Individuals) Laws 2001 to 2012 (hereinafter referred to as "**the Personal Data Law**"), will be repealed and replaced with a new legislative framework.

According to the aforesaid announcement of the Commissioner dated 31/05/2016, **every legal person that processes personal data shall implement all necessary preparatory measures, so that they comply with the provisions of the GDPR by 24/05/2018**.

The GDPR seems to comprise one of the most rigorous and comprehensive data protection regulatory framework in the world. Even though it is based on rules and principles that are familiar under the Personal Data Law, the GDPR broadens up the rights of data subjects and national data authorities, increases the responsibility of data controllers, raises the burden of compliance and introduces greater sanctions.

[1] To that effect see (in Greek) the relevant Announcement available online at http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/E3D3ED6F553B0035C2257FC40035366B?OpenDocument

L. Papaphilippou & Co LLC has prepared this note to raise awareness of the main changes to the current data protection framework, which may be of particular interest to financial institutions operating in the Republic of Cyprus.

1. Scope of application

The provisions of the **material scope** of the GDPR are essentially the same as the respective provisions of the Personal Data Law. In effect, the GDPR is applicable to the processing of any information relating to an identified or identifiable natural person.

It is further clarified that, in practice, financial institutions are deemed to be **controllers** when processing personal data for their own purposes (i.e. when they determine the purposes and means of processing of personal data), whereas any natural persons/legal entities that process personal data on behalf of financial institutions (for example, on the basis of an outsourcing service agreement) are considered to be **processors**.

The **territorial scope** of the GDPR though is broader than the scope of application of the Personal Data Law, as the legal personality, seat and residence of the data controller and/or processor are no longer decisive factors for its applicability. More analytically, the GDPR applies to:

a) all data controllers and processors which have Union establishments, *regardless of whether the processing takes place in the EU or not*; and
b) all data controllers and processors established *outside* the EU which offer goods or services to EU data subjects (even if for free), or which monitor the behavior of EU subjects (including the profiling of internet users for market research purposes and the use of cookies for a strictly technical purpose). In such cases, the data controllers and processors must designate a representative in the Union.

Accordingly, financial institutions that operate in the Republic of Cyprus fall under the scope of the GDPR's application, regardless of whether they process personal data themselves or through other natural persons/legal entities; where the actual processing takes place; and where they are established and/or their legal form.

The GDPR is also applicable in relation to the natural persons/legal entities that process data on behalf of such financial institutions, regardless of where they are established.

2. Reinforced Consent Requirements

In contrast with the Personal Data Law, the GDPR explicitly provides for particular conditions for consent.

In particular, *where processing is based on consent*, the controller ought to be able to demonstrate that data subjects had indeed consented to processing of their personal data. Consent ought to be given either *in the form of a statement or another clear affirmative act*,

establishing a *freely given, specific, informed and unambiguous* indication of the data subjects' agreement to the processing personal data relating to them. Consequently, silence or any other inactivity or even pre-ticked checkboxes do not constitute valid consent for the purposes of the GDPR.

Data subjects should give additional consent for each additional processing operation and should always have the right to easily withdraw their consent at any stage.

The GDPR further provides that consent will be deemed involuntary if the performance of a contract, including the provision of a service, is dependent on consent despite such consent not being necessary for such performance.

3. Rights of the Data Subject

The GDPR purports to furnish individuals with greater control over the processing of their personal data, by enhancing existing rights and creating new ones. *Inter alia*, the GDPR:

a) strengthens the requirement for **transparency** by providing that the controller should furnish data subjects with certain information in a concise, transparent and easily accessible form, using clear and plain language;
b) enhances the **right to object**, especially in relation to direct marketing activities;
c) restricts **automated individual decision-making**, which ought to be kept within narrow limits;
d) codifies the **right to erasure** ('right to be forgotten'), which bounds the controller to erase data without undue delay upon the data subjects' request provided that specific conditions are met;
e) introduces the new **right to data portability**, which facilitates the transmission of personal data between service provides;
f) reinforces the **right to compensation** in relation to material or non-material damages.

4. General Obligations on Controllers and Processors

Controllers ought to implement appropriate technical and organizational measures to ensure and to be able to demonstrate that they comply with the provisions of the GDPR. In contrast with the Personal Data Law (but in agreement with Union-wide judicial practice), the GDPR explicitly regulates the possibility of joint data control.

Moreover, the GDPR expressly obliges controllers to only use processors that provide sufficient guarantees of their compliance with the GDPR. To that effect, the GDPR stipulates detailed requirements regarding the terms of the **contract** to be entered into with processors.

Moreover, the GDPR introduces direct and specific obligations on data **processors** regarding accountability, confidentiality, data security, data transfers to thirds countries etc.

Accordingly, financial institutions should always ensure that natural persons/legal entities that process personal data on their behalf also comply with the provisions of the GDPR. Otherwise, they may be held liable for any act or omission of these natural persons/legal entities that violate the provisions of the GDPR.

5. Privacy by design and default

The new concepts of "data protection by design and by default" are established by the GDPR.

"**Data protection by design**" obliges controllers to take data protection risks into account and to implement appropriate technical and organizational measures in order to meet the requirements of the GDPR and protect the rights of data subjects (such as data minimization and the new concept of pseudonymisation). These measures should be implemented not only at the time of processing, but at the time of designing a new service and planning the data processing as well.

"**Data protection by default**" refers to the obligation of the controller to implement technical and organizational measures and procedures for ensuring that, by default, only personal data that are necessary for each particular purpose of processing are processed.

6. Records of Processing Activities

The GDPR abolishes the duty imposed by the Personal Data Law to register certain processing activities with supervising authorities (i.e. the Commissioner). Instead, controllers are obliged to maintain an **internal record** of processing activities, whereas processors are obligated to keep a record of all categories of processing activities carried on behalf of controllers.

It is noted that this obligation is applicable only to legal persons employing 250 or more persons, or those engaged in high risk data processing or the processing of special data.

It is further clarified that the GDPR does not provide a definition of '**high risk data processing**'. It instead explains that the likelihood and severity of the risk to the rights and freedoms of the data subject should be determined in light of the *nature, scope, context and purposes of the processing* and that such risk may result from processing activities that may give rise, *inter alia*, to *identity theft or fraud, or loss of confidentiality of personal data protected by professional secrecy, or financial loss or any other significant economic disadvantage*.

It may thus be said that the majority of financial institutions engage in 'high risk data processing'; accordingly, they seem to fall under the scope of this obligation, regardless of the number of their employees.

7. Personal Data Breach Notification

The GDPR creates a compulsory data breach notification mechanism, whereby processors ought to inform controllers of any such breach and controllers ought to notify supervisory authorities (i.e. the Commissioner), without undue delay. If any such breach is likely to result in a high risk to the rights and freedoms of individuals (as explained above), controllers further ought to inform the individuals concerned.

8. Data Protection Impact Assessment

Under the GDPR, controllers ought to undertake a mandatory data protection impact assessment *before* processing personal data, where the processing is likely to result in a high risk to the rights and freedoms of individuals. To this end, a common list of the kind of processing operations that are subject to the aforesaid requirement will be published, in the context of the consistency mechanism that will be applied by all supervisory authorities.

Where the impact assessment indicates high risks in the absence of measures to be taken by the controller to mitigate the risk and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the Commissioner should be consulted prior to the start of processing activities.

9. Data Protection Officer

A new governance obligation imposed on controllers and processors by the GDPR is the requirement to appoint a data protection officer when, *inter alia*, they carry out regular and systematic large scale monitoring of data subjects. It thus seems to follow that most financial institutions ought to comply with this obligation.

It is further noted that a group of undertakings may appoint a single, joint data protection officer, provided that a data protection officer is easily accessible from each establishment.

10. Codes of Conduct and Data Protection Certification Mechanisms

The GDPR encourages associations and other bodies representing categories of controllers or processors to prepare codes of conduct for the purpose of specifying its application (e.g. in relation to data transfer to non-Union states). It also encourages the establishment of data protection certification mechanisms and of data protection seals and marks for demonstrating compliance with it.

11. Personal Data Transfers

In contrast with the Personal Data Law, under the GDPR a data transfer to non-Union states or to international organisations may occur **without a special permission** by the supervisory authority (i.e. the Commissioner), provided that:

a) the European Commission has issued an adequacy decision; or

b) specified adequate safeguards are provided for by the controller or the processor and given that enforceable data subject rights and effective legal remedies are available for data subjects.

Such transfers may also occur **subject to the authorization** of the supervisory authority (i.e. the Commissioner) on condition that adequate safeguards are provided for by the controller or the processor by means of, *inter alia*, contractual clauses.

In absence of an adequacy decision or of appropriate safeguards, such transfers may exceptionally take place only the basis of the conditions specified by the GDPR, such as where the data subjects have given their explicit consent and where the transfer is occasional and necessary in relation to a contract or a legal claim.

It is also noted that authorisations that have already been issued by the Commissioner in relation to such transfers remain valid until amended, replaced or repealed.

12. <u>One Stop Shop</u>

The GDPR introduces the concept of the '**one stop shop**', whereby the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as *lead* supervisory authority for *cross-border processing* carried out by that controller or processor.

Moreover, the GDPR regulates the matters of the **cooperation** of national authorities and the **consistency** of their practice and provides for the establishment of the **European Data Protection Board**. It is thus envisaged that a uniform personal data protection regulatory system will be established across the Union.

13. <u>Administrative Fines</u>

The GDPR entitles data protection authorities (i.e. the Commissioner) to impose much higher administrative fines than those specified by the Data Protection Law. Under the GDPR, the level of the fine will depend on the particular provision breached, whereas specified aggravating and mitigating factors will be taken into account. Infringements of the GDPR will thus result in fines of up to EUR 20,000,000, or, in the case of an undertaking, 4% of the total worldwide annual turnover of the preceding financial year.

For more information or our advice regarding the aforementioned changes and the preparatory measures to be undertaken in order to ensure compliance with the GDPR, please contact Ms. Irene Anthis Christofides, advocate, at <u>ia@papaphilippou.eu</u>.