I was asked to deliver a short speech on the changes that will take effect with the GDPR.

So, what changes does the GDPR bring? Back in 2010, when the European Commission launched a public consultation for the preparation of the initial proposal, a lot of private sector stakeholders had been asking for 3 things. A uniform set of rules, not having 28 Data Protection Authorities (DPAs) breathing down on their necks and a leveled playing field on both sides of the Atlantic. The later was a pressing demand from US based companies. At that time, DPAs cautioned stakeholders to be careful for what they wished. Eventually, they got exactly what they had asked for.

First of all, the GDPR applies one uniform set of rules instead of having 28 fragmented national legislations. It is true, that the GDPR allows Member States to implement some Articles with a degree of flexibility. Yet, Member States, in no case, can deviate from or go beyond the letter or the spirit of the GDPR.

Second, it was the issue of supervision. If a bank operates in 20 of the 28 MS, today, 20 DPAs are tasked to supervise the bank's compliance with the 20 respective national legislations. The GDPR introduces the Principles of Accountability and Transparency, which obliges the bank to demonstrate its compliance with the GDPR. In practice, this means that, as of the 25th of May, instead of having 20 Commissioners running after the bank to check its compliance, this bank will have to run after them, to demonstrate its compliance.

Thirdly, there was the issue of the leveled playing field. The GDPR provides for stringent administrative fines, which reflect its global nature. For decades, data protection did not receive the attention it deserved. Alas, it

was these stringent fines that alarmed most stakeholders and brought the GDPR in the center of international attention.

I am often asked about inspections. Both the current legislation and the GDPR empower me to carry out inspections, on my own accord or pursuant a complaint. What changes with the GDPR, is the subject of the inspection. Since a bank will be obliged to demonstrate its compliance with the GDPR, some of these inspections will be carried out with purpose to examine if this bank truly processes personal data the way it claims it does.

I should note that the GDPR does not aim to re-invent the wheel. A number of rights and obligations provided for by the existing legislation are also provided for by the GDPR. The GDPR simply strengthens some of the existing rights and regulates more firmly some of the existing obligations. For example, the right to erasure is elevated to the right to be forgotten. Banks do not need to be alarmed by this right. You will not be asked to forget all the loans you have granted to your customers. This right can be exercised only in specific circumstances.

I should add that the GDPR introduces new rights and obligations, such as the novel right of data portability and the novel obligations for the restriction of processing, pseudonymisation and data protection by default and by design. In practice, a bank should have mechanisms in place for the exercise of such rights and for fulfilling these obligations. As I have said, we are not re-inventing the wheel. Companies with a cultivated culture of corporate responsibility should not have a problem in demonstrating that they have such mechanisms in place.

A number of stakeholders are concerned that the GDPR obligations, which relate to data breach notifications and to communicating a data breach to affected customers may have adverse effects on them. To this, I reply that, in the recent years we had some serious breaches, by apple, yahoo and others. Experience has shown us that informing the affected customers in a responsible manner, does not affect their loyalty. It should also be added that these companies did not have a statutory obligation to inform their customers of the mentioned data breaches, but did so in the frame of their corporal responsibility.

Particular attention should also be given to transfers to third countries. In relation to the existing regime, the GDPR offers many more tools, which can be used as legal basis for such transfers. Transfers can be carried out on the basis of an adequacy decision, on the basis of appropriate safeguards such as standard contractual clauses, either adopted by the European Commission or adopted by a DPA and approved by the Commission, or on the basis Binding Corporate Rules, or on the basis of derogations for specific situations. Each bank can choose a tool from this tool box, which satisfies its particular needs.

When a bank intends to transfer data to an organization in a third country, outmost account should also be given to the legal obligations that this organization is subject to. For example, if a bank intends to transfer data to an affiliated bank in the Russian Federation, it should examine, inter alia, if this bank has a statutory obligation, by virtue of Russian Law, to disclose data, to some Russian regulatory authorities. This is of particular importance, not only for determining the lawfulness of the transfer, but also for appropriately informing its customers for this disclosure.

Adherence to a code of conduct is voluntary. Yet, approved codes of conduct can be used as an appropriate safeguard for transfers to a third country. Members of the Association of Cyprus Banks should explore the possibility for the adoption of such a code by the Association. A code of conduct should include, inter alia, a mechanism for monitoring its parties' adherence and binding commitments for respecting data subjects' rights.

So, what should a bank do, in order to be compliant with the GDPR? In my view, carrying out the exercise of Article 30 is a good starting point. Article 30 obliges banks to keep a record of all its processing activities. Most business schools' text books emphasize on the importance of knowing one's own customers but often give lesser emphasis or undermine the importance of knowing one's own business. Carrying out the exercise of Article 30 will help banks to better understand what data they process, why and how these data are processed and, in effect, to better understand their own business models.

My Office has recently published on its website a sample Index table for carrying out the exercise of Article 30 and a Guide for assisting companies

to fill in this table. I strongly recommend that you consult both. As a second step for road mapping a bank's compliance with the GDPR, I suggest that the bank follows the Guidelines adopted by the Article 29 Working Party, the collective body of the national DPAs. These Guidelines will help the bank to understand how certain provisions of the GDPR apply, specifically to the banking sector.

I hope that this brief introduction has given you an insight to what lays ahead with the GDPR.

Irene Loizidou Nicolaidou
Commissioner for Personal Data Protection

11/05/2018