EU General Data Protection Regulation (GDPR). What is the way forward?

By Dr Marina Himoni

After four years of debate, the General Data Protection Regulation (hereinafter the "**GDPR**") was finally approved by the EU Parliament on the 14th of April 2016 while its enforcement date is 25th of May 2018, date on which it will be directly applicable in all Members States. On the date of its enforcement, organizations which fail to comply with the provisions of the GDPR run the risk of facing heavy fines. The GDPR replaces the old Data Protection Directive 95/46/EC and it was adopted in an attempt to harmonize data privacy laws across all Member States of the European Union.

Steps for Organizations to follow

In an effort to meet the requirements of the GDPR and ensure compliance with the same, there are steps and/or changes that all organizations will have to consider for this purpose. All organizations must assess the data already held, particularly the kind of data that is being held, the place where data is stored and of course how data is protected, particularly whether there is in place any Software or technology to protect those. A review of the current-data related policies and procedures has to be undertaken by organizations and this includes encryption, remote access, mobile devices, sensitive information, HR exit procedures, third parties and data breach notifications. In reviewing the above, an organization may decide, if deemed necessary, to request a third-party data security company to carry out an objective assessment of them too.

All organizations must evaluate their existing systems, policies and procedures in order to determine whether those are adequate to protect the data stored or whether there are any risks of data breaches. As regards individuals' rights, organizations must consider whether there are systems in place to transfer personal data to other companies and to delete personal data if requested. More importantly organizations must ensure whether the requests for permission to use customers' data is clear on its very purpose and the period of time that the data will be used.

Amongst the issues that organizations shall consider is the appointment a Data Protection Officer or an internal lead contact person who will be responsible for data protection initiatives as well as for communicating and coordinating with the Data Protection Authority if required. The Data Protection Officer or the lead contact will also be the person responsible for communicating with senior management and discuss with them data protection strategies to be approved. Nonetheless, the appointment of a Protection Officer should not be considered as compliance with the Regulation on its own but it constitutes a step amongst others that need to be taken.

Staff training is also key in this respect to ensure staff's awareness of the high importance of data protection and of course of any new/amended processes which are required in order to comply with the GDPR. It is of utmost importance, particularly within larger organizations, to ensure that internal teams communicate between themselves in order to maintain data protection and this includes but is not limited to teams such as IT, Security, Legal and Compliance Department. The GDPR does not simply concern the IT Department of an organization but a data protection governance matter which concerns all actors in an organization and which calls for the awareness of all staff.

Key Points of the GDPR

The provisions of the GDPR will not only be applicable to organizations that process sensitive personal data but on the contrary it will be applicable to all organizations that process personal data of both general and sensitive nature.

The most noteworthy change brought to the regulatory landscape of data privacy is the extension of the ambit of the Regulation itself as it will be applicable to all companies that process personal data of data subjects residing in the European Union irrespective of the company's location. Prior to the adoption of the GDPR, the Directive which was in force was ambiguous on the particular issue as it referred to data process "in context of establishment'" giving rise to ambivalences as to its true meaning. With the adoption of the GDPR the picture is now clear as it will be applicable to the processing of personal data by controllers and processors in the EU regardless of whether the processing takes places within or outside the Union.

More importantly, the GDPR imposes fines which will be applicable to organizations who are in breach of the provisions of the same. Organizations may be fined up to 4% of annual global turnover or €20 Million, whichever is greater. This constitutes the maximum fine that may be imposed for the most serious infringements and breaches of the GDPR. There is however a tiered approach with regards to fines which escalates depending on the seriousness of the infringement. Less serious offences may on the other hand attract a lower fine of 2%. Those rules and applicable penalties thereof can be imposed both to controllers and processors and automatically this means that "clouds" which are widespread nowadays will not be exempted from the ambit of the GDPR.

With regards to consent the relevant conditions have been strengthened in an attempt to give greater protection to data subjects. Organizations will no longer be able to use long and illegible terms and conditions which render it impossible for data subjects to read and comprehend due to the legalese involved. Request for consent must be given in an intelligible and easily accessible form while the very purpose of data processing must be attached to that consent so as to ensure the data subject will be in a position to know the reason behind the data processing. Consent needs accordingly to be clear and

distinguishable from other matters. This also entails the use of clear and plain language, so as to ensure that data subjects are aware of the terms of their consent while it must also be available and easy for data subjects to withdraw their consent if they wish so.

The rights of Data Subjects

The rights that the GDPR brings forward for data subjects are indeed numerous. At the same time those rights are particularly important for the protection and full awareness of the data subjects.
With the entry into force of the GDPR, on 25/05/2018, breach notification will become mandatory in all Member States of the Union where a data breach is likely to result in a risk for the rights and freedoms of individual subjects. Notification has to take place within 72 hours from the moment the breach was made known and data processors will be required to notify their customers, the controllers, without undue delay after they first become aware of the data breach. Breach notification generally requires timely and immediate action to be taken by the actors involved.

In addition, the GDPR provides data subjects with the right to obtain a confirmation from the data controller as to whether their personal data is being processed or not, where and for what purposes. Furthermore, the controller will be under an obligation to provide data subjects a copy of their personal data, free of charge, and in an electronic format. This is one of the important changes brought which aspires at ensuring greater data transparency and empowering data subjects.

Data subjects will enjoy the right to ask from a data controller to erase their personal data and cease the further dissemination of the same, and if possible to stop third parties from processing their data too. There are conditions however that need to be met as contained in Article 17 of the GDPR. The conditions include for example situations where the data is no longer relevant for the original purpose that they have been obtained or the data subject has withdrawn their consent. When such a request arises, controllers have to weigh the subjects' rights against public interest considerations for having the data available. Nonetheless, the above right is subject to an exception which is personal data are required for processing owing to other legislation which cannot be erased.

A new term and right brought forward by the GDPR is the right of a data subject to receive the personal data that concern them which they have previously provided in a commonly use and machine readable format and have the right to transmit that data to another controller.

Conclusion

The driving force behind the adoption of the GDPR has been to protect and empower all European Union citizens' privacy on the one hand and on the other hand to bring a change to the way organizations across the Union approach data privacy. Nonetheless what emerges from the above is that the changes and new processes that organizations need to implement to ensure their compliance with the Regulation before the date of its enforcement are numerous and far reaching. At the same time

due to the very fact that the GDPR envisages a whole new culture, there are doubts as to whether compliance can realistically be achieved until the 25th of May, date on which the GDPR comes into force. On the contrary this is rather a process that will take time in order for universal change to be achieved.

For further information on this topic please contact Dr. Marina Himoni at P. N. KOURTELLOS & ASSOCIATES LLC, by telephone: +357 25 745575 or by fax: +357 25 755525 or by e-mail: mh@kourtelaw.com