your Legal Lab

Preparing for the General Data Protection Regulation:

A roadmap to the key changes introduced by the new European Data Protection Regime

If you have questions or would like additional information on the material covered in this article, please contact:

Katerina Christodoulou, Partner
+302103388831
katerina.christodoulou@yourlegalpartners.gr

Alexandra Varla, Associate
+302103388831
alexandra.varla@yourlegalpartners.gr

www.ylp.gr

On the 27th of April 2016, after four years of drafting and negotiations, the European Council and Parliament finally adopted the long awaited General Data Protection Regulation (hereinafter the **"GDPR"** or **"the Regulation"**). Although the Regulation will be directly applicable in all EU Member-States as of the 25th of May 2018, companies and organizations must take advantage of the two-year window to conduct risk assessments, review existing practices and start preparing for the GDPR's implementation, while evaluating possible compliance gaps.

The Regulation's principal aim is to combat fragmentation in terms of compliance requirements and to unify data protection law within the European Union, while increasing the data subject's rights and introducing stricter obligations for companies acting as both data controllers and processors. At the core of the new regime one can also discern the digital economy and the effort of bridging the gap between the existing, outdated and practically unenforceable Data Protection Directive and the new regulatory framework, which has incorporated to its provisions more technologically sophisticated concepts, such as "pseudonymisation", "profiling" and "biometric data".

Compliance with the new principles and pillars of privacy and data protection includes increased transparency obligations, the implementation of a privacy impact assessment and the appointment of a Data Protection Officer, while heavy sanctions will be incurred if a company fails to meet the said privacy standards. The key changes introduced by the Regulation include the following:

Broader territorial scope

Currently, the EU data protection regime is applicable to non-EU data controllers on the condition that they make use of equipment established in the European Union territory and only when the processing takes place within the EU. Contrary to the existing regime, the GDPR catches data controllers and processors outside the EU, whose processing activities relate to the offering of goods or services (even if for free) to, or monitoring the behavior (within the EU) of, EU data subjects. . Such extraterritoriality, as

described above, constitutes one of the most important aspects of the new regime: in practice, a company outside the EU which is targeting consumers in the EU will be subject to the GDPR.

Wider definition of personal data

The Regulation has adopted a wider definition for the notion of "personal data", which now expressly includes location data and online identifiers. Consequently, and to the disappointment of many businesses acting as data controllers, IP addresses will most likely be considered personal data, particularly when combined with unique identifiers and, as a result, their collection and processing falls under the scope of the new data protection regime. The aforementioned amendment is quite ground-breaking, especially for organizations whose core business is to monitor, through the collection and processing of IP addresses, the users' browsing activities and to use such data for advertising and marketing purposes, as they will now need to obtain, in the majority of cases, the data subject's explicit, prior written consent. Pseudonymisation (i.e. the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information) is considered a security measure to mitigate the risk of singling out an individual, however it is subject to the additional information (which, combined, may lead to the identification of the subject) being kept separately and secured by technical and organizational measures.

Consent

With the objective of implementing a more dynamic, consent-based model in the processing of personal data, the Regulation has refined the notion of "consent", stipulating that it must be freely given, specific, informed, unambiguous, indicated by a statement or clear affirmative action. Implied consent will no longer be sufficient for the lawful processing of personal data, as the underlying purpose is for the data subject to clearly demonstrate that he/she has detailed knowledge of the specific data to be collected, the explicit purposes of the processing and wishes to agree to such processing. To that extent, the new regime provides the guidelines for obtaining consent, in compliance with the Regulation, by stipulating that the request for consent must be presented in an intelligible and easily accessible form, using clear and plain language.

In the context of a digital environment, where consent is usually obtained by the ticking of a box, data controllers must ensure that, prior to the user stating his/her consent, he/she must have been provided with all relevant information, as per the aforementioned guidelines, while it is of utmost importance that the user is allowed to keep browsing the website ("freely given"), irrespective of whether he/she has granted consent to the personal data processing.

Within its avant garde provisions, the new regime further acknowledges the need to provide enhanced protection to specific categories of data subjects and imposes stricter conditions to the child's consent, in relation to information society services. In particular, the Regulation designates that, in cases where the child is below the age of 16 years, the processing shall be lawful only to the extent that such consent is given or authorised by the holder of parental responsibility over the

child. The Member-States are allowed to lower the age up to which consent must be provided pursuant to the aforementioned process, however such lower age must not be below 13 years.

Role of data processors

Another notable change introduced by the GDPR is that data processors have direct obligations for the first time. . The Regulation has shifted, to a more rigorous legal framework, which imposes on the data processors (i.e. organizations that process personal data on behalf of data controllers) a wide range of duties including, inter alia, the implementation of security standards, the appointment of a Data Protection Officer, the conduct of regular impact assessments and the maintenance of documentation. For the purposes of providing sufficient guarantees that the processing shall meet the Regulation's requirements, the data processors must enter into a binding agreement with the data controllers, which sets the processing's subject-matter, duration, nature and purpose, the type of the data collected and categories of the data subjects.

Reinforcement of data subjects' rights

In conformity with one of the core objectives underpinning the GDPR, i.e. enabling data subjects to take control of their own data, the Regulation has granted the data subjects a new set of rights, which re-balance the interests in favour of the individuals. The most notable is the right to erasure ("right to be forgotten"), which will enable the data subjects to request the controllers to delete their data, if there are no legitimate grounds for their retention. The innovation, compared to the existing regime, is that the current data protection law provides the data subjects with the right to seek a court order to cease the data processing, when the latter causes damage, whereas the Regulation enables individuals to bypass court intervention and settle the issue directly with the data controller. For the lawful exercise of the right to erasure, the GDPR has introduced specific requirements to be met including, but not limited to, the data being no longer necessary for the purpose for which they were collected, or the data subject withdrawing its consent, or the data being unlawfully processed.

To complement the right to be forgotten, the Regulation has also "armed" the data subject with the right to object to the processing of its data, the right to data portability (i.e. the right to transmit his/her personal data to another controller) and the automated individual decision-making, including profiling. Of the aforementioned rights, the latter (automated individual decision-making) is expected to have considerable implications to businesses that monitor consumer behavior online and further use such data for marketing purposes. More specifically, according to the Regulation, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling – i.e. the construction of a user profile, based on the browsing activities and preferences, as such are illustrated by the monitoring of the said user's online behavior. In practical terms, this means that a consumer may at any time, subject to the fulfilment of certain conditions, object to profiling and, as a result, the business will no longer be allowed to send him/her any targeted advertisements, which are tailored on the basis of

the individual's personal taste, preferences and habits.

Heavy sanctions

Finally, to ensure compliance with the legal framework for data protection and the implementation of the new provisions, the Regulation has introduced an enforcement regime of heavy financial sanctions to be imposed to violators, up to 4% of the annual worldwide turnover of the business, or 20.000.000 Euro – whichever is higher.

What next?

Although the GDPR will not apply until 25 May 2018, companies are advised to act now and utilise the two-year grace period to bring their business into full compliance with the GDPR. On that direction, Your Legal Partners are designing specific ***GDPR Seminars*** for our clients, analyzing risk, putting in place clear policies and advice on actions that need to be taken.

.