While Turkey was welcoming its new Data Protection Law in April 2016, the EU introduced the General Data Protection Regulation (GDPR) which will replace the outdated EU Data Protection Directive. GDPR is accepted as a new era in data protection as it is expanding its applicability to data controllers residing outside the EU.

Begüm Yavuzdoğan Okumus
Managing associate, Gün + Partners

Bensu Aydın
Associate, Gün + Partners

In this sense, the Regulation has a global effect, since it applies to data controllers or processors outside the EU who offer goods or services to data subjects in the EU or who monitor the behaviours of data subjects who are in the EU.

Extra-territorial effect of GDPR

The Regulation aims to provide a level playing field for everyone in terms of data protection, both for those in and outside the EU. Compared to the Directive, which focused on the “use of equipment”, GDPR has an expansive approach with regards to jurisdiction and applicable law, introducing a possible universal application of EU laws and regulations.

Under GDPR, the representative must be established in one of the Member States where the data subjects reside whose personal data is processed in relation to the goods or services they are being offered or whose behaviour is being monitored. The representative must be mandated by the controller/processor to be addressed in addition to or instead of the controller or the processor, in particular by supervisory authorities and data subjects on all issues related to processing for the purposes of ensuring compliance with GDPR.

This new extraterritorial approach brings some ambiguities with it, which can be summarised into four important issues:

1. Determining how the controller/processor will be held within the scope of GDPR (the Regulation provides guidelines on the interpretation to some extent of points such as the use of a language, a currency generally used in the EU Member States, the possibility of ordering goods and services within that other language or currency.)

2. The enforceability of the sanctions.

3. Understanding who will be regarded as a data subject since “data subjects who are in the EU” is a broad term and it is not clear whether all persons residing or simply present (without residence) in the EU will be regarded as data subjects for the purpose of this provision.

4. What is meant by “establishing a representative” is not clear - is the appointment of a real person by a data processor for this purpose sufficient for this requirement?

Putting these ambiguities aside, non-EU data controllers and processors must understand that they have entered a new realm of data protection.

What should non-EU data controllers and processors do now?

It can be said that GDPR will most probably make non-EU companies that touch EU data uncomfortable, taking into account that there is a whole new Regulation with which they must now comply. Some emerging market companies do not have a data protection-focused state of mind due to the absence of local data protection requirements, whereas they must now adapt themselves to the highest level of data protection rules ever enacted.

However, non-EU data controllers and processors must bear in mind that thorough planning starting from today will serve to meet the eventual compliance requirements. For instance, in Turkey, data controllers are busy adapting their systems to data protection requirements newly-introduced under Turkish Law and, from now on, those who are subject to GDPR must also take into account its requirements.

Although there are some issues regarding GDPR’s application that remain controversial and unsettled for the time being. As a starting point, non-EU controllers and processors must review their current global services (especially those with the EU) and data collection practices in order to determine whether their data processing activities fall within the scope of GDPR and thus would be caught by its extra-territorial reach.

With regards to the data breach obligations, non-EU businesses should have competent and well-tested standards of security, along with back-ups to ensure logs are duly kept for future audits. Further, having a crisis control procedure in place would minimise the regulatory risks as it would add to the reporting duties of data controllers.

Data processors/controllers outside EU must always remember that the sanctions are substantial and, by establishing a representative in the EU, non-EU businesses are more vulnerable to GDPR than ever before. Therefore, these players must accept and internalise the Regulation and the challenges which come with it, rather than avoiding them.

This article was published in **DataIQ**

The online version can be found here