The General Data Protection Regulation: Achieving Compliance for EU and non-EU Companies

Ozan Karaduman*

The European Union (EU) has introduced new legislation on the protection of personal data: the General Data Protection Regulation (GDPR). The GDPR was adopted on 27 April 2016 and it will come into force on 25 May 2018 after a two-year transition period.

Businesses in the EU are readjusting their processing activities in order to ensure compliance with the GDPR. However, it is not only EU businesses that should be working towards compliance, but also some non-EU businesses because of the expanded territorial scope of the GDPR.

Expanded territorial scope of the GDPR

Article 3 of the GDPR sets forth that data controllers and data processors that are not established in the EU will be subject to the GDPR if processing is related to: (1) the offering of goods or services to data subjects in the EU (even if no payment is required for such goods or services); or (2) monitoring the behaviour of the data subjects provided that such behaviour takes place in the EU.

There is no straightforward explanation as to what would count as offering goods or services as regards Article 3 of the GDPR. According to Recital 23, a case-by-case analysis must be made in order to determine whether an activity can be regarded as 'offering of goods or services' in terms of Article 3. The important point is to understand whether or not the data controller or the processor contemplates or intends to offer goods or services in the EU. This is not an issue easy to determine. A combination of facts should show that the relevant controller or processor contemplates to offer goods or services to individuals in the EU. A good example is electronic commerce: websites

* Ozan Karaduman is Managing Associate, Gün + Partners and IAPP KnowledgeNet Istanbul Co-Chair.

operated by data controllers in non-EU countries are accessible by individuals in the EU. However, the accessibility of such websites in and of itself does not mean that the relevant controller contemplates offering services to individuals in the EU. Other features of the website (eg, the languages used, the possibility of sending goods to the EU and whether or not the website accepts users from abroad) must be taken into consideration in order to come to a conclusion that the relevant website owner/operator falls under the scope of the GDPR. For example, if a Turkish electronic commerce company targets Turkish-speaking data subjects residing in the EU (eg, Germany) and its website is only written in the Turkish language, then that company will fall under the scope of the GDPR even if the Turkish language is not one of the official languages of any of the Member States of the EU.

Another important point regarding territorial scope is that if a data controller or data processor is established in the EU, it will directly fall under the scope of the GDPR even if the processing activity does not take place in the EU. This is important for companies that have subsidiaries in the EU. If those subsidiaries can be regarded as a data controller or data processor, then they will be subject to the GDPR, even if their data processing activity takes place outside the EU. For example, if a group of companies has an affiliate in the EU but that affiliate keeps personal data in group servers that are located outside the EU, it will still have to comply with the GDPR rules.

This shows how important it is for data controllers or data processors to make a self-evaluation of whether or not they fall under the scope of the GDPR. The biggest mistake a company that is not specifically within the EU could make would be to think itself outside the application scope of the GDPR.

What are the important rules that a company falling under the scope of the GDPR must comply with? The following sections briefly respond to this question.

Appointment of a representative

A data controller or data processor must appoint a representative in the EU if the processing is related to: (1) the offering of goods or services to data subjects in the EU (even if no payment is required for such goods or services); or (2) monitoring the behaviour of data subjects provided that such behaviour takes place in the EU.

This obligation will not apply if processing is occasional, or does not include, on a large scale, processing of special categories of data or processing of personal data related to criminal convictions and offences referred to in Article 10 of the GDPR. However, in order for this exception to apply, processing must also be unlikely to result in a risk to the rights and freedoms

of natural persons, taking into account the nature, context, scope and purposes of the processing; or if the data controller or processor is a public authority or body. In light of this, even if a company that offers goods or services to data subjects residing in the EU seems to fall under the exception set out above (eg, if the data controller or processor processes personal data on an occasional basis), that company must also evaluate whether or not the processing of the personal data bears a risk to the rights and freedoms of the natural persons residing in the EU. After reviewing these factors, only if there is no risk to the rights and freedoms of the natural persons residing in the EU, will the relevant company be exempt from the obligation to appoint a representative.

The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are located. Let's take our example of the electronic commerce company offering services to Turkish-speaking residents in the EU. If that company's processing of personal data is not occasional and does not include processing of special categories data on a large scale, then that company must appoint a representative in one of the Member States where its targeted customers live (eg, Germany or Belgium).

Appointment of a data protection officer

One of the most discussed provisions under the GDPR is related to the appointment of a data protection officer (DPO). According to the International Association of Privacy Professionals, more than 75,000 DPOs will be required to meet the GDPR requirements. This is a serious number, which will definitely constitute a considerable cost for companies in relation to compliance with the GDPR.

According to the GDPR, the data controller and processor must designate a DPO in any case where:

1. processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
2. the core activities of the controller or processor consist of processing operations, which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
3. the core activities of the controller or the processor consist of the large-scale processing of special categories of data and personal data relating to criminal convictions and offences.

If our electronic commerce company (mentioned in the examples in the above paragraphs) has a large client base in the EU and if it monitors the shopping tendencies of its clients, it will need to appoint a DPO.

A DPO can be an employee of the company, but it must maintain a level of impartiality and objectivity regarding matters of personal data: it cannot receive any instructions from the data controller or processor when performing its tasks as a DPO.

Lawful processing of personal data

According to Article 6 of the GDPR, the processing of personal data will be regarded as lawful if:

1. the processing is made in accordance with unambiguous and informed consent freely given by the data subject;
2. processing is necessary for performance or entry into a contract;
3. processing is necessary for compliance with a legal obligation;
4. processing is necessary for protecting the vital interests of the data subject or another person;
5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child.

If processing is based on legitimate interests as mentioned under (6) above, the data controller should be especially cautious; it must make a balance check between its legitimate interests and the fundamental rights and freedoms of the data subjects. If the legitimate interests come out to be heavier in scale, than the fundamental rights and freedoms of the relevant data subjects then the personal data can be processed; if not, the data controller must refrain from processing the personal data.

There are stricter measures applied to processing sensitive personal data. Article 9 of the GDPR accepts as a principle that sensitive personal data should not be processed but also provides certain exceptional situations in which such personal data can be processed. It is important that these situations are set out as exceptions to the general principle. It means that these exceptional situations should be interpreted strictly when determining whether or not a processing activity falls under the scope of those exceptions.

Data protection by design and by default

Data protection by design and data protection by default are concepts that have long been considered as good practices in the privacy sphere. The GDPR accepts these concepts and requires controllers to adhere to these concepts with its Article 25.

According to Article 25 of the GDPR, the data controller is required to implement the appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into processing in order to meet the requirements of the GDPR, protect the rights of data subjects and keep the data secure. Data controllers should also implement the appropriate technical and organisational measures for ensuring that, by default, only personal data that are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible, without the individual's intervention, to an indefinite number of natural persons.

These are important and high-level standards; these principles require data controllers to review their processing structures as a whole and readjust them in a way that – by default – the personal data is collected and processed only to the extent required for the purpose of processing and is accessed by third parties only to that extent too.

Accountability

The GDPR also sets out high accountability standards. This is very important, especially for data controllers and processors that are not used to complying with complex privacy rules. In a nutshell, accountability standards under the GDPR require data controllers and processors to be able to demonstrate their compliance with the GDPR. It may seem a straightforward obligation but it is not.

Data controllers will need to issue comprehensive policies in relation to their processing activities, where they set out all the details regarding processing, such as the legal basis of the processing, the safeguards in place for international transfers, data retention, access to personal data by data subjects, and so on.

Data controllers will need to conduct data protection impact assessments for activities that involve high risk for the rights and freedoms of the data subjects. The risks determined and the measures taken will need to be documented as well.

Informing the data subjects

Data controllers need to inform the data subjects of the details regarding their processing activities, such as how the data is processed, the purpose of processing, the rights of the data subjects, and so on. In this respect, data controllers need to prepare a policy addressed to data subjects, which gives proper but not complicated information regarding processing activities and the rights of the data subjects such as access to data, right to request deletion, and so on.

Cross-border data transfers

Cross-border data transfers, more specifically data transfers outside the European Economic Area (EEA), are regulated under the GDPR. The GDPR does not want personal data to be transferred to third countries unless certain specific conditions are met. The reason behind this restriction is to avoid the undermining of the level of protection provided by the GDPR when personal data is transferred to third countries.

Under the GDPR, personal data cannot be transferred to a third country if:

1. there is an adequacy decision made by the European Commission regarding that country;
2. there are appropriate safeguards; or
3. there are derogations related to such transfer.

Adequacy decisions are decisions made by the European Commission, which state that there is an adequate level of protection in a certain country, territory, sector or organisation and that transfer of personal data to such country, territory, sector or organisation can be made without any further authorisation.

In the absence of adequacy decisions, appropriate safeguards can be used to transfer personal data legally outside the EEA. Appropriate safeguards are legal tools that ensure that the recipients of personal data that are located outside the EEA protect the personal data that they receive to a similar standard to the EU. Appropriate safeguards consist of binding corporate rules, standard contractual clauses (model clauses), approved codes of conduct or certification mechanisms, ad hoc contractual clauses and international agreements. Appropriate safeguards need to be approved by the supervisory authority. Binding corporate rules and model clauses are particularly important. Binding corporate rules are a set of rules accepted by a group of companies regarding the protection of personal data in the GDPR standards. If these rules are approved by the supervisory authority, personal data can be transferred within a group of companies. Model clauses

are clauses that are adopted by the European Commission or accepted by a national supervisory authority then approved by the European Commission. They are non-negotiable contractual clauses regarding the protection of personal data and once a controller or processor outside the EEA signs the model clause, it is considered safe to transfer the personal data to such controller or processor.

When there is neither an adequacy decision nor the appropriate safeguards in place, the only way to transfer personal data to the countries outside the EEA is to fall under the scope of a derogation. Derogations are exceptional situations set out by the GDPR to allow the transfer of personal data to third countries. As these are exceptional situations, their scope must be interpreted narrowly.

Penalties

The GDPR introduces serious penalties for non-compliance. In certain cases administrative penalties can go up to two per cent of annual global turnover or €10m (whichever is greater) and in some other cases these penalties can go up to four per cent of global annual turnover or €20m (whichever is greater). These administrative penalties are in addition to the corrective measures that can be imposed by the supervisory authorities.

What to do now?

The GDPR comes into force on 25 May 2018; it applies not only to data controllers and processors established in the EU but also to controllers and processors outside the EU (subject to the conditions mentioned above). What should a data controller or processor outside the EU do in order to prepare for the GDPR?

The first thing to do is to determine if the data controller or the processor falls under the territorial scope of the GDPR. If it does, the amount of work to be carried out for compliance would change based on how similar data protection legislation in the data controller or processor's jurisdiction is to the GDPR, and how compliant the data controller or processor is with that legislation.

If the data protection legislation in the jurisdiction of a data controller is not similar to the GDPR, or if a data controller is not compliant with its own data protection legislation, that controller will need to undertake a serious compliance project. The first step in that project would be to prepare an inventory of the personal data it holds and map it, so that the controller can

see at which points it gathers personal data, what it does with that data and what kind of personal data it processes.

After these issues have been determined, the data controller must review whether it processes personal data in accordance with the GDPR. The points at which personal data is not processed in accordance with the GDPR must be readjusted to ensure compliance: necessary steps must be taken to ensure the security of the personal data. If a representative is required, the data controller or processor must find and appoint a representative. Likewise, if a DPO is required, the data controller must find and appoint a DPO.

Data controllers and processors should review their systems to determine at which points what types of personal data are transferred from the EEA outside the EEA. If there is no adequacy decision for the country of destination, the controller or processor must determine if it can benefit from appropriate safeguards. If it feels it cannot benefit from appropriate safeguards, the controller or processor must determine whether it falls under the scope of one of the derogations.

This compliance project would be complicated in nature: it requires knowledge of the GDPR and experience regarding personal data protection. Data controllers and processors should consult with experts in this field in order to handle this complicated compliance project properly.