Minding your own Business: The Extra-territorial Application of the EU's Data Protection Regulation

by Andrew Fawcett - a.fawcett@tamimi.com - Abu Dhabi
Roberto Lusardi - r.lusardi@tamimi.com - Doha

May 2018

As you may well be aware, the European Union (EU) has introduced new legislation on the protection of personal data: the General Data Protection Regulation (GDPR), which came into effect on May 25, 2018. Businesses in Europe have been frantically trying to get their houses in order so that their processing of personal data relating to identifiable natural persons is compliant with the new legal requirements. Because of the expanded territorial scope of the GDPR, businesses based outside the EU – including businesses in the Middle East – will need to comply with the GDPR in some circumstances.

Which non-EU businesses are caught under the GDPR?

The GDPR applies to non-EU entities that are 'controllers' and 'processors' processing personal data of individuals who are in the EU, if the processing activities relate to the:

- Offering of goods or services to data subjects in the EU (irrespective of whether the goods/services are offered for a fee or for free) ("targeting"); or
- Monitoring of the behaviour of data subjects, as long as their behaviour takes place in the EU ("monitoring").

GDPR application by way of targeting

There is no straightforward explanation as to what will be considered as the offering of goods or services to data subjects in the EU. A case-by-case analysis must be made. Generally, for the GDPR to be applicable by way of targeting, it is envisaged that there needs to be an active direction of activities towards individuals within the EU, rather than the mere availability of a website or online advertising to EU individuals.

The targeting of individuals in the EU would likely need to include additional factors such as the:

- having contact details that are in the EU;
- availability of a website in one or more European language;
- possibility of making payment in the Euro currency;
- use of any EU domain name (e.g. ".eu", or ".de" or ".it", etc.); or
- displaying of references to/from EU customers.

GDPR application by way of monitoring

In order for the GDPR to be applicable by way of monitoring, the behaviour and/or movement of individuals within the EU needs to be monitored. Again, this is determined on a case-by-case basis but can be undertaken or deemed to occur by:

- gathering location data;
- allowing EU individuals to join/use a social network; and
- tracking online activities of EU individuals to create profiles (for the purposes of analysing or predicting personal preferences, behaviours and attitudes).

For example, using website ‘cookies’ (such as targeting advertisement cookies) and social media plug-ins may constitute the monitoring of EU individuals.

GDPR indirect application to non-EU businesses

The GDPR provisions will also apply indirectly to non-EU businesses that have agreements under which they carry out data processing activities on behalf of an EU business.

An EU data controller is expressly required by the GDPR to have a contract with a data processor (whether or not the processor is located in the EU) that stipulates certain prescribed matters, including that the processor:

- processes the personal data only on documented instructions from the controller;
- ensures that persons authorised to process the personal data are subject to an obligation of confidentiality;
- does not transfer the data overseas unless in compliance with GDPR requirements for transfers;
- does not engage another processor without prior written authorisation of the controller; and
- allows for and contribute to audits, including inspections conducted by the controller.

Consequently, non-EU businesses will be expected to agree to contracts with EU businesses that contain such terms and conditions concerning any data processing (often known as ‘Data Processing Agreements’).

What obligations do non-EU businesses have in relation to international transfers of data?

The GDPR limits the transfer of personal data to countries that are outside the European Economic Area (EEA) unless particular conditions are met. The restrictions are intended to prevent the level of protection provided by the GDPR from being ‘watered down’ or avoided when personal data is transferred outside the EEA to other countries whose laws do not offer the same level of protection.

Under the GDPR, personal data can only be transferred to country outside of the EEA if:

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

An adequacy decision is a decision made by the European Commission that determines that there is an adequate level of protection in a specific non-EEA country, and that transfer of personal data to such country can be made without the need for any further authorisation or safeguards. A finding of adequacy means the European Commission is satisfied that appropriate standards of data protection will be met when personal data is transferred to that other country.

Even where there is not an applicable adequacy decision, the transfer personal data outside the

EEA may still legally allowed if appropriate safeguards are used to oblige the recipient of personal data who is located outside the EEA to protect that data to a similar standard to the GDPR. Appropriate safeguards are legal mechanisms such as binding corporate rules, standard contractual clauses (model clauses) approved by the European Commission, approved codes of conduct and international agreements.

If neither an adequacy decision nor appropriate safeguards are available, then the only way to legally transfer personal data to recipients in countries outside the EEA is to fall within the scope of a derogation which is set out by the GDPR to allow the transfer of personal data to third countries. A derogation is an exceptional situation such as, for example, reasons relating to the public interest.

Penalties

The GDPR introduces serious penalties for non-compliance. There are two tiers of administrative fines that can be levied:

- Up to €10 million, or 2% annual global turnover (whichever is higher).
- Up to €20 million, or 4% annual global turnover (whichever is higher).

The fines (which are discretionary rather than mandatory) are based on the specific article of the GDPR that has been breached. Infringements of their obligations under the GDPR by 'controllers' and 'processors', including data security breaches, will be subject to the lower level. Infringement of an individual's privacy rights will be subject to the higher level.

In addition to any administrative fines, the supervisory authorities can also impose a range of corrective measures or sanctions. These include imposing a temporary or permanent ban on data processing; ordering the rectification, restriction or erasure of data; and suspending data transfers to third countries.

Separately, the GDPR also gives individuals the right to directly claim compensation from the controller or processor for damages suffered due to an infringement of the GDPR. In certain cases, not-for-profit bodies can bring representative action on behalf of individuals.

A processor will be liable for the damage caused by processing only where it has not complied with obligations of the GDPR that are specifically directed towards processors, or where it has acted outside or contrary to lawful instructions of the controller (e.g. by failing to delete personal data when requested).

Appointment of an EU representative

What may be a surprising consequence of the GDPR to many non-EU businesses is that they may need to appoint an EU representative. For the purposes of compliance with the GDPR, controllers and processors that are not resident in the EU, but that are obliged to comply with the GDPR, must appoint representatives within the EU to act as a point of contact for the EU personal data subjects and regulators on all issues relation to processing. The EU representative must be established in one of the EU member states where the affected data subjects are located.

This obligation will not apply to a public authority or body; or if the 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. However, in order for this latter 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.

What to do?

The GDPR is a complex area of legal compliance, with ramifications for all companies who have activities in the EU, irrespective of whether their operations are actually based within the EU or elsewhere.

By 25 all non-EU businesses should have determined:

- Whether they fall within the scope of the GDPR.
- Whether any operational and/or technical measures will have to be implemented in the business in order to comply with the GDPR.
- Whether their cross-border/intra-group personal data transfers are compliant with the GDPR or whether they might wish to adopt binding corporate rules.
- Whether an EU representative needs to be appointed.

By the time you are reading this, the deadline will have passed and the GDPR will be in effect. This does not mean it is too late to consider and address data protection compliance, including whether the GDPR applies to your business. If there is any likelihood that GDPR affects your business, we suggest that you address the risk as a matter of priority.

Al Tamimi & Company's Technology, Media & Telecommunications team regularly advises on data protection and privacy issues, including the impact of GDPR on regional entities. For further information about these matters, please contact Andrew Fawcett, Senior Counsel (a.fawcett@tamimi.com) or Roberto Lusardi, Senior Associate (r.lusardi@tamimi.com).