The impact of new EU data protection rules on Qatar businesses

Background/Introduction

Qatar recently introduced legislation in respect of privacy and data protection (Law No. 13 of 2016, the "Data Protection Law"), which is based on, and tries to capture certain aspects of, European-style data protection and privacy. Due to the absence of the relevant regulations relating to the Data Protection Law, it is difficult to properly understand how the law and its procedures will be applied in practice. On the other hand, the new General Data Protection Regulation ("GDPR") is due to come into force across the European Union ("EU") on 25 May 2018. Consequently, in addition to understanding and complying with the provisions of the Data Protection Law, certain Qatari entities may also be subject to, or may need to comply with, the GDPR due to its intended extra-territorial reach.

GDPR Scope

The previous data protection regulation for the EU (the Data Protection Directive) was also intended to have a broad scope. Its provisions, however, covered only data processing activities carried out within the EU unless there was deemed to be an "inextricable link" between such activities carried out by an entity outside the EU and an entity located within the EU. This prevented EU organisations and competition authorities from regulating data processing activities in respect of EU individuals where such processing activities were performed by data controllers outside of the EU.

The need for extended territorial scope is due to (i) increase in global access to, and use of, the internet, (ii) online/electronic commerce, (iii) establishment of global corporate networks and (iv) growth of cloud services.

Due to the above, territorial borders have become blurred and caused concerns relating to protection of privacy when processing personal data in connection with online services (specifically cross-border ones). The GDPR thus extends its territorial scope to data controllers and processors outside the EU in certain instances. There are exemptions available in circumstances where (i) personal data from EU individuals is only occasionally processed, (ii) processing is not on a large scale and (iii) the nature and purpose of the processing is unlikely to result in a risk to the privacy rights of the relevant individuals.

As a consequence, certain non-EU organisations now fall within the scope of the GDPR in relation to either: i) targeting, or ii) monitoring, individuals in Europe and would be determined on a case-by-case basis.

GDPR application by way of Targeting

For 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 mere availability of a website or online advertising to EU individuals. The targeting of individuals in EU would need to include additional factors such as:

1. contact details in the EU,
2. option of accessing the website in one or more of the various European languages,
3. allowing for payment in the Euro currency,
4. use of any EU domain name (such as ".eu" or ".de" for Germany or ".it" for Italy), and

5. references to/from EU customers.

Interestingly, the GDPR will apply whether the offered goods or services are paid for or free.

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

GDPR indirect application to Foreign Entities:

The GDPR provisions would also apply indirectly to a foreign entity that has an agreement with an EU entity (eg. for agency or marketing services) involving data processing activities. In such an event, the agreement between such entities would need to provide for compliance with the GDPR and the foreign entity would be required, as data processor, to comply with all applicable GDPR measures.

GDPR Obligations:

A foreign entity which falls within the scope of the GDPR, acting as data processor or controller (as applicable), would be required to comply with some or all of the following obligations:

- general data protection principles relating to, inter alia, purpose, transparency, erasure, lawfulness, fairness and accountability in respect of personal data processed;
- appointment of a data protection representative based within the EU, subject to certain exemptions;
- appointment of a Data Protection Officer (mainly applicable to public authorities, organisations engaged in large scale monitoring, and organisations engaged in large scale processing of personal data);
- maintenance of records and related documentation requirements;
- conduct of a data protection impact assessment ("DPIA") before undertaking certain processing activities with high privacy risk;
- implementation of various data protection measures, e.g. pseudonymisation of data;
- implementation of necessary organisational and technical measures to ensure appropriate level of security; and
- notification of any security breaches to the relevant data protection authorities and, in certain cases, the relevant individual.

Sanction for Non-Compliance

Breach of the GDPR can result in the imposition of different categorised fines, with the maximum level of fine being an amount equal to Euro 20,000,000 or 4% of the defaulting organisation's total, global annual turnover (whichever is the highest).

Commentary vis-à-vis Qatar and Enforcement

With the extended scope of GDPR, non-EU entities dealing with EU data may be concerned as they may have to take into consideration, and comply with, extensive EU data protection requirements.

The GDPR may also extend to Qatar-based entities (without any EU presence or establishment) actively targeting and/or conducting EU business, based on (substantial) targeting and monitoring provisions referred to above. However, this is yet to be tested. Generally, not every web-based Qatari business that is accessible from within the EU would fall under the GDPR.

It is unlikely that any EU-based organisation or competition authority would look to implement and enforce the GDPR provisions against such Qatari entities because enforcement of any applicable sanction/fine would need to be undertaken via the application of international law and any existing or potential cooperation agreement or treaty and would ultimately require the assistance of local Qatari authorities.

Notwithstanding the above, it is advisable for any Qatari entities that are conducting business and/or monitoring individuals within the EU as part of their global services that are unsure as to whether or not they need to comply with the GDPR (or that simply wish to pursue “best practice”) to do the following:

1. review their relevant data processing activities;
2. inventory all data;
3. carry out an impact assessment to determine any risk of infringing the GDPR; and
4. establish/update any privacy policies and/or data handling procedures in line with GDPR.

Entities should also note that under the GDPR a much wider definition is given to personal data and includes online identifiers such as IP addresses and cookie identifiers vis-à-vis the Data Protection Law.

In respect of Qatari entities that have operations or establishments in the EU (through any legal form including a branch, a subsidiary, or a joint venture), the data processing activities of such establishment will be subject to the GDPR irrespective of whether the processing takes place in the EU or not. In order to ensure that they will be compliant with the new GDPR provisions, such Qatari entities should immediately undertake appropriate measures and implement plans to meet the eventual compliance requirements, including, without limitation:

1. adapting their systems for purposes of data protection requirements;
2. reviewing global services arrangements (particularly with the EU) and data collection practices; and
3. reviewing and testing their security standards and/or reviewing back-ups for record-keeping purposes and future audits.