PROCESSING PERSONAL DATA OF EU RESIDENTS FROM THE MENA? –GDPR APPLIES TO YOU

Key issues:

- The GDPR becomes effective on 25 May 2018
- The GDPR can apply to MENA companies that process personal data of EU residents
- Companies should identify if GDPR applies to them and ensure compliance to avoid hefty fines.

WHAT IS THE GDPR?

The EU's General Data Protection Regulation ((EU) 2016/679) (GDPR) comes into effect on 25 May 2018. It is a sweeping EU data privacy law with broad extraterritorial effect that can impact companies in the MENA region which process data of individuals resident in the EU. Companies that fail to comply with GDPR can face fines of EUR20 million or up to 4% of global revenue.

How can it affect companies in the MENA?

The GDPR significantly expands the obligations of non-EU companies that process personal data of individuals resident in the EU. "Personal data" is broadly defined under the GDPR and can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address through which a person can be identified.

The GDPR applies to companies in the MENA region that process Personal data of individuals in the EU:

- for a data controller entity in the EU
- for targeting offers of goods or services to individuals resident in the EU (irrespective of whether payment is required), for example websites and apps offering goods or services that are targeted at individuals in the EU or
- for monitoring the behaviour of individuals in the EU, for example cookies and tracking activities on websites and apps.

The GDPR might not apply to companies that do not directly offer their goods or services to individuals in the EU (for example, where individuals resident in the EU purchase goods from a website not targeted at them). Equally, in a change from the earlier position, a non-EU data controller who outsourced its data processing to processer-service providers in the EU might no longer fall within the EU regime.

Companies in the MENA to whom GDPR applies and who fail to comply could be exposed to very high penalties for serious breaches - up to 20 million Euros or 4% of global turnover (whichever is higher). The financial impact apart, there is also the reputational damage of being found in breach of the GDPR.

What are the GDPR's Key Requirements?

- Requires non-EU companies processing the data of individuals in the EU for the above mentioned purposes to appoint a representative in an EU member state as the point of contact for the relevant data protection authority. This will not apply if the data processing is occasional, is not large scale or where the company employs less than 250 employees.
- Sets a short deadline of 72 hours on data controllers for notification of security breaches to the relevant data protection authority. If a non-EU company processes data for such EU based data controllers it needs to bear this timeline in mind.
- Requires that processing be proportionate to the purposes for which the data was collected and deleted when no longer needed.
- Imposes record keeping obligations on data processor companies (regardless of location).
- Requires that all data processing be justified by the data subject's informed consent, compliance with obligations arising under the law and the data controller's legitimate interests outweighing prejudice to the privacy of the data subject.

What can you do to protect your business?

- Determine whether your business (irrespective of location(s)) is a data processor in respect of EU personal data. If yes, you are caught by the GDPR
- Assess if your online activities, for example, result in you processing EU personal data for the purposes of GDPR – for example, your website and/or app directly offers goods/services to individuals within the EU, or where cookies and tracking activities on your website and/or app monitor the behaviour of individuals within the EU. If so, you are caught by the GDPR.
- Ensure you fully understand the new legal obligations under GDPR on processors, and their application to your business.
- Build a compliance structure internally with policies and guidance. Communicate it within the organisation along with appropriate training.
- Engage your IT team now. Review all existing systems to identify any gaps in current capability against the new requirements of the GDPR. This is likely to be a very significant work-stream with any GDPR compliance programme.
- Develop a security breach readiness strategy, to help data controllers meet the 72 hour breach notification requirement.
- Consider the impact of the GDPR on contracts with data controllers to ensure appropriate risk allocation.
- Carry out regular audits for compliance with GDPR rules.

How can we help?

We can help you analyse if you fall within the GDPR's scope and draw upon our global expertise from specialists throughout the EU and other regions to help you comply with the GDPR.

Key Terms:

- **Personal data** – all information relating to an identifiable EU resident, particularly by reference to an identifier such as a name
- Data **controller** – entities who determine the purposes and means of processing of personal data
- **Processing** – any operation performed on personal data such as collection, recording, organization, retrieval, etc
- Data **processor** – service providers who process data on behalf of their controller-customers
- **Consent** – freely given, specific, informed, and unambiguous indication of a data subject's wishes (a higher standard than under the previous EU privacy directive)
- **Transparency** – data subjects must be told about the processing of their information and given other necessary information so that the processing is "fair".

CLIFFORD CHANCE

CONTACTS

James Abbott
Partner, Dubai

T +971 4503 2608
E james.abbott
@cliffordchance.com

Arun Visweswaran
Senior Associate, Dubai

T +971 4503 2748
E arun.visweswaran
@cliffordchance.com

Djamela Magid
Associate, Dubai

T +971 4503 2696
E djamela.magid
@cliffordchance.com

Jonathan Kewley
Partner, London

T +44 207006 3629
E jonathan.kewley
@cliffordchance.com

Richard Jones
Director of Data Privacy, London

T +44 207006 8238
E richard.jones
@cliffordchance.com

André Duminy
Partner, London

T +44 207006 8121
E andre.duminy
@cliffordchance.com