Companies outside the EU may have data protection compliance obligations under the GDPR

Much focus has centred on the impact of the GDPR on data transfers involving processors and controllers in the EU. The increased territorial scope of the GDPR means that even businesses based outside the EU will need to ensure they take steps to comply with the GDPR, including in some cases appointing a EU representative.

The following are the key considerations arising under the GDPR for non-EU businesses:

**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), or
- the monitoring of the behaviour of the data subjects, as long as their behaviour takes place in the EU.

**What fines apply under the GDPR?**

The GDPR adopts a tiered approach to fines, however Data Protection Authorities can impose fines for certain infringements of up to the higher of 4% of annual global turnover or EUR 20 million.

**What does the obligation to appoint an EU representative entail and who does it apply to?**

Non-EU resident controllers and processors 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 relating to processing, for the purposes of compliance with the GDPR. Certain types of processing are exempt including where processing carried out by a public authority or body.

The EU representative must be established in one of the EU member states where the affected data subjects are located.

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

The GDPR expands the list of appropriate safeguards which allow a controller or processor to implement international transfers of data (for example, the GDPR recognises binding corporate rules and sets out conditions related to international transfers of data).
In light of the increased penalties and the reputational damage attaching to non-compliance in the area of data protection, a multinational company may wish to audit its existing intra-group data transfer arrangements or consider developing binding corporate rules to align more closely with the GDPR.

**What are key dates and steps that non-EU businesses should take into account in light of the GDPR?**

The GDPR has come into force and is applicable from 25 May 2018. By this date all non-EU businesses will have to determine:

- 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 require are compliant with the GDPR or whether they might wish to adopt binding corporate rules;
- Whether there are any local data protection rules that the business will need to take into account; and
- Whether an EU representative needs to be appointed and necessary notifications made.

**Conclusion**

The GDPR is a complex area of legal compliance which has ramifications for all companies with activity in the EU, regardless of whether their headquarters or the majority of their operations are based within the EU or elsewhere.

The GDPR is wider in scope than its predecessor and data controllers and processors, including non-EU businesses caught by the GDPR, must have undertaken self-assessments, audits, compliance paper trails and the like to ensure compliance by 25 May 2018.