SLAUGHTER AND MAY

The long arm of the law: EU privacy regulators enforcing extra-territorial reach

November 2018

The UK Information Commissioner's Office has recently issued GDPR enforcement notices against a company based in Canada. This demonstrates the willingness of the EU data protection regulators to exercise their extra-territorial powers under the GDPR, including potentially against organisations in Asia.

Background

The EU's General Data Protection Regulation (**GDPR**) took effect on 25 May 2018 and represents a significant expansion of the EU data protection regime, because in certain circumstances it applies to organisations outside the EU. We discussed the extra-territorial scope of the GDPR in a previous Briefing, which can be accessed here. In addition to the new provisions regarding extra-territoriality, the GDPR introduces enhanced powers of investigation for the EU privacy regulators as well as significantly enhanced penalties, including fines of up to EUR 20 million or 4% of worldwide turnover, whichever is higher.

The first enforcement notices under the GDPR were recently issued by the UK Information Commissioner's Office (**UK ICO**) to a Canadian company located outside the EU. In addition, claims have been filed in the UK against companies outside the EU for alleged breaches of data privacy rules. This Briefing considers the steps taken by the UK ICO and how, in light of the increasing number of high profile data incidents, Asia-based organisations need to be aware of the steps they should take in order to mitigate the risks of such incidents occurring and, if they do, how to avoid enforcement action by the EU privacy regulators or related litigation.

The UK ICO's enforcement notice

On 6 July 2018 and 24 October 2018, the UK ICO issued enforcement notices against AggregateIQ Services Ltd (**AggregateIQ**), a Canadian company located outside the EU. The notices were issued under the UK's new Data Protection Act 2018 (**UK DPA**) and enforce the provisions of the GDPR, through the UK DPA. They concern AggregateIQ's processing of personal data obtained during the UK's referendum on its membership of the EU, held in 2016. The UK ICO noted that such data was used to target individuals with political advertising messages on social media and that such data was still held by AggregateIQ after the GDPR took effect on 25 May 2018. As such, Article 3(2)(b) of the GDPR applied to AggregateIQ because it was monitoring the behaviour of data subjects in the EU (i.e. based in the UK).

The notices cited Articles 5(1)(a)–(c) of the GDPR regarding the principles of: (a) lawfulness, fairness and transparency; (b) purpose limitation; and (c) data minimalisation. They also referred to Article 6 (which states that processing of personal data will only be lawful if one of the six grounds of processing applies) and Article 14 (which specifies the information that a controller must provide to data subjects about the processing of their data where the controller has not obtained that data from those data subjects).

The UK ICO was satisfied that there had been a breach of the Articles cited on the basis that AggregateIQ had "*processed personal data in a way that the data subjects were not aware of, for purposes which they would not have expected, and without a lawful basis for that processing". Furthermore, the processing was incompatible with the purposes for which the data was originally collected*". It was also satisfied that such breaches were likely to cause any person damage or distress.

The notices therefore required AggregateIQ to carry out certain remedial measures and referred to the potential penalties for non-compliance. AggregateIQ had appealed the July notice, which resulted in the UK ICO issuing the October notice, the effect of which was to vary and replace the July notice (by being narrower in scope). AggregateIQ has not appealed the October notice and has said it will comply with its requirements (which are essentially to erase certain personal data relating to data subjects in the UK). Failure to do so will mean the UK ICO can issue a fine of up to EUR 20 million or 4% of worldwide turnover, whichever is higher.

Relevance to Asia

It is clear that many organisations based in Asia have exposure to the GDPR. That may be, for example, because they process personal data in the context of one of their EU-based establishments (e.g. a subsidiary or other group company). However, some organisations may either: (i) offer goods or services to people in the EU; or (ii) monitor the behaviour individuals in the EU. Both these factors are relevant to the extra-territorial application of the GDPR.

The UK ICO's enforcement notices against AggregateIQ, which came within the first few months after the GDPR took effect, are relevant to such organisations because they show that the EU privacy regulators are prepared to enforce the extra-territorial provisions of the GDPR.

The action against Aggregate IQ related to breaches of the GDPR which resulted in data subjects' personal data being processed in a way that they were not aware of, for purposes which they would not have expected and without a lawful basis for that processing. The identification of relevant data processing activities carried out by organisations and the lawful basis on which such activities are carried out has been one of the major challenges for all organisations subject to the GDPR, particularly those based outside the EU. Similarly challenging is the need to document that analysis in a way that provides the required level of information to the data subjects – this is particularly so when considered alongside requirements of local data privacy law.

Even if the relevant processing activities have been properly identified and the relevant information has been communicated to data subjects, potential harm can still be caused to those data subjects through, for example, data breaches. In order to avoid such incidents, the GDPR introduces requirements for organisations to adopt appropriate technical and organisational measures to ensure appropriate levels of security of personal data.

Nevertheless, data breaches do occur. When they do, the GDPR imposes strict requirements on data controllers to notify both EU privacy regulators and affected data subjects when the breach is sufficiently serious. Such notifications must be made without delay and, where feasible, within 72 hours after having become aware of the breach having occurred.

At the same time organisations may have to consider notifications to – and investigations by – other regulators, including their domestic privacy regulator and, for example, for listed companies any announcement obligations.

The GDPR retains private action rights for affected data subjects who are entitled to recover damages in certain circumstances. As a result, in the UK there are now law firms which specialise in attempting to organise and bring group litigation proceedings against organisations that may have breached their GDPR obligations. Such claims have had mixed results in recent

decisions, but the ability to claim is clear in principle and if such proceedings are brought, the fact that there are likely to be very large claimant/plaintiff groups (not least to make the claim financially viable for the firms organising them) means that even low damages awards for individuals may in aggregate incur significant expense for the defendant organisation.

What should organisations in Asia do?

In order to avoid enforcement action along the lines of that taken against AggregateIQ and associated litigation risks, Asia-based organisations that are exposed to the GDPR need to ensure that they have carried out an appropriate '**data mapping**' exercise in order to identify not only relevant data processing activities, but also a lawful basis for each processing activity. Such exercises must be properly documented and the relevant information communicated to the data subjects, for example through an appropriate **privacy notice**.

Related to the data mapping exercise, each affected organisation must assess the level of risk of its processing activities and **implement appropriate technical and organisational measures** to ensure a level of security appropriate to that risk. This will require a number of external/customer facing measures as well as addressing internal operational/procedural matters.

Even then, in the unfortunate event that a data breach does occur, organisations must act quickly and decisively. As part of the suite of measures taken to comply with the GDPR, organisations should ensure they have an adequate **data breach policy** and that adequate **training on how to react to a breach** has been given to relevant staff. Organisations are required to carry out a risk assessment in relation to the breach (including for example an assessment of the risks to the rights and freedoms of individuals), the outcome of which will determine whether it is necessary to notify the breach to regulators and the affected data subjects (including steps taken to address the breach). The risk of harm to data subjects once a breach has occurred can increase, so ensuring a swift and effective response will allow affected organisations to mitigate the effect of the breach, retain greater control of the public and regulatory communications and reduce the risk of any potential future enforcement action or litigation. Even absent such enforcement action or litigation, breaches can result in reputational harm to organisations, which an appropriate reaction and communications and plan can help mitigate.

We have previously written about the importance of taking sufficient steps to ensure GDPR compliance. That article is available here.

To the extent you have any questions regarding the above, please contact either Mark Hughes or Kevin Warburton in Hong Kong, or Rebecca Cousin or Richard Jeens in London. Relevant contact details are below.

Mark Hughes
T +852 2901 7204
E mark.hughes@slaughterandmay.com

Kevin Warburton
T +852 2901 7331
E kevin.warburton@slaughterandmay.com

Rebecca Cousin
T +44 (0)20 7090 3049
E rebecca.cousin@slaughterandmay.com

Richard Jeens
T +44 (0)20 7090 5281
E richard.jeens@slaughterandmay.com